KOMISJONI RAKENDUSOTSUS (EL) 2023/1795,

10. juuli 2023,

mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete kaitse taseme piisavust ELi-USA andmekaitseraamistiku alusel

(teatavaks tehtud numbri C(2023) 4745 all)

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (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), ([1]) eelkõige selle artikli 45 lõiget 3,

ning arvestades järgmist:

1. SISSEJUHATUS

(1) Määruses (EL) 2016/679 ([2]) on kehtestatud eeskirjad isikuandmete edastamiseks liidus asuvatelt vastutavatelt või volitatud töötlejatelt kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele ulatuses, milles selline edastamine kuulub määruse kohaldamisalasse. Andmete rahvusvahelise edastamise eeskirjad on sätestatud selle määruse V peatükis. Kuigi isikuandmete liikumine Euroopa Liidust väljaspool asuvatesse riikidesse ja neist riikidest Euroopa Liitu on piiriülese kaubanduse ja rahvusvahelise koostöö laiendamiseks hädavajalik, ei tohi andmete edastamisega kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele kahjustada isikuandmete kaitse taset liidus ([3]).

(2) Määruse (EL) 2016/679 artikli 45 lõike 3 alusel võib komisjon võtta rakendusaktiga vastu otsuse, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit tagab isikuandmete kaitse piisava taseme. Kui see tingimus on täidetud, võib edastada isikuandmeid sellesse kolmandasse riiki ilma täiendava loata, nagu on sätestatud määruse (EL) 2016/679 artikli 45 lõikes 1 ja põhjenduses 103.

(3) Nagu on täpsustatud määruse (EL) 2016/679 artikli 45 lõikes 2, tuleb kaitse piisavuse otsuse vastuvõtmisel tugineda kolmanda riigi õiguskorra põhjalikule analüüsile, mis hõlmab nii andmete importijate suhtes kohaldatavaid eeskirju kui ka isikuandmetele juurdepääsul avaliku sektori asutustele kehtestatud piiranguid ja seotud tagatisi. Komisjon peab hindamisel kindlaks määrama, kas kõnealune kolmas riik tagab kaitsetaseme, mis „sisuliselt vastab“ liidus tagatud kaitsetasemele (direktiivi (EL) 2016/679 põhjendus 104). Seda, kas see nii on, tuleb hinnata liidu õigusaktide, eelkõige määruse (EL) 2016/679 ja Euroopa Liidu Kohtu (edaspidi „Euroopa Kohus“) praktika alusel ([4]).

([1]) ELT L 119, 4.5.2016, lk 1.
([2]) Lihtsuse huvides on VIII lisas esitatud loetelu käesolevas otsuses kasutatud lühenditest.
([3]) Vt määruse (EL) 2016/679 põhjendus 101.
([4]) Vt viimati kohtuasi C-311/18, Facebook Ireland ja Schrems (edaspidi „Schrems II“), ECLI:EU:C:2020:559.

(4) Nagu Euroopa Kohus selgitas oma 6. oktoobri 2015. aasta otsuses kohtuasjas C-362/14 Maximillian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems"), ([5]) ei ole nõutav identne kaitsetase. Eelkõige võivad vahendid, mida asjaomane kolmas riik isikuandmete kaitsmiseks kasutab, erineda nendest, mida Euroopa Liidus rakendatakse, kuivõrd need osutuvad praktikas kaitse piisava taseme tagamisel tulemuslikuks ([6]). Kaitse piisavuse nõue ei eelda seega, et liidu õigusnorme tuleb punkt-punktilt kopeerida. Küsimus on pigem selles, kas välisriigi süsteem tervikuna tagab privaatsusõiguste sisu, nende tõhusa rakendamise, järelevalve ja täitmise tagamise kaudu nõutava isikuandmete kaitse taseme ([7]). Kõnealuse kohtuotsuse kohaselt peaks komisjon selle nõude kohaldamisel lisaks eelkõige hindama, kas kõnealuse kolmanda riigi õigusraamistik näeb ette eeskirjad, mille eesmärk on piirata sekkumisi nende isikute põhiõigustesse, kelle andmeid liidust edastatakse, kusjuures neid sekkumisi on selle riigi asutustel lubatud toime panna, kui nad taotlevad õiguspäraseid eesmärke, nagu riiklik julgeolek, ja mis tagavad sedalaadi sekkumiste vastu tõhusa õigusliku kaitse ([8]). Selle kohta annab juhiseid ka Euroopa Andmekaitsenõukogu piisavuse viitedokument, mille eesmärk on seda nõuet veelgi selgitada ([9]).

(5) Eraelu puutumatuse ja andmekaitse suhtes kohaldatavat standardit seoses põhiõigustesse sekkumisega selgitas Euroopa Kohus oma 16. juuli 2020. aasta otsuses kohtuasjas C-311/18, Data Protection Commissioner *vs.* Facebook Ireland Limited ja Maximillian Schrems (Schrems II), millega tunnistati kehtetuks komisjoni rakendusotsus (EL) 2016/1250 ([10]) varasema Atlandi-ülese andmevoo raamistiku ehk ELi-USA andmekaitseraamistiku Privacy Shield kohta. Euroopa Kohus leidis, et isikuandmete kaitse piirangud, mis tulenevad USA riigisisesest õigusnormidest, mis reguleerivad USA avaliku võimu asutuste õigust pääseda riikliku julgeoleku eesmärgil juurde liidust USAsse edastatavatele isikuandmetele, ei olnud piiritletud viisil, mis vastaks nõuetele, mis on oma andmekaitseõigusesse sekkumise vajalikkuse ja proportsionaalsuse mõttes sisuliselt samaväärsed liidu õigusega ([11]). Euroopa Kohus leidis ka, et andmesubjektidele, kelle andmeid edastatakse Ameerika Ühendriikidesse, ei ole kättesaadav õiguskaitsevahend sellises organis, kes pakub harta artiklis 47, mis käsitleb õigust tõhusale õiguskaitsevahendile, ette nähtutega sisuliselt samaväärseid kaitsemeetmeid ([12]).

(6) Pärast Schrems II kohtuotsust alustas komisjon läbirääkimisi USA valitsusega, et võtta vastu võimalik uus kaitse piisavuse otsus, mis vastaks määruse (EL) 2016/679 artikli 45 lõike 2 nõuetele, nagu Euroopa Kohus neid tõlgendas. Nende arutelude tulemusena võtsid Ameerika Ühendriigid 7. oktoobril 2022 vastu täidesaatva korralduse 14086 „Enhancing Safeguards for US Signals Intelligence Activities" („USA signaaliluuretegevuse kaitsemeetmete tõhustamine", edaspidi „korraldus EO 14086"), mida täiendab USA justiitsministri määrus andmekaitseasju läbivaatava kohtu kohta (edaspidi „justiitsministri määrus") ([13]). Lisaks on ajakohastatud raamistikku, mida kohaldatakse nende kaubandusüksuste suhtes, kes töötlevad käesoleva otsuse alusel liidust edastatud andmeid, ehk ELi-USA andmekaitseraamistikku.

(7) Komisjon on USA õigust ja tava, sealhulgas korraldust EO 14086 ja justiitsministri määrust, põhjalikult uurinud. Põhjendustes 9–200 esitatud järelduste põhjal leiab komisjon, et Ameerika Ühendriigid tagavad piisava kaitsetaseme isikuandmetele, mis on ELi-USA andmekaitseraamistiku alusel edastatud liidus asuvalt vastutavalt töötlejalt või volitatud töötlejalt ([14]) põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides.

([5]) Kohtuasi C-362/14, Maximillian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems"), ECLI:EU:C:2015:650, punkt 73.

([6]) Schrems, punkt 74.

([7]) Vt komisjoni teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas", COM(2017) 7, 10.1.2017, punkt 3.1, lk 6–7.

([8]) Schrems, punktid 88 ja 89.

([9]) Euroopa Andmekaitsenõukogu, piisavuse viitedokument, WP 254 rev 01, kättesaadav järgmise lingi kaudu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) Komisjoni 12. juuli 2016. aasta rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 207, 1.8.2016, lk 1).

([11]) Schrems II, punkt 185.

([12]) Schrems II, punkt 197.

([13]) USA föderaalsete õigusnormide kogumi (edaspidi „CFR") 28. jaotise 302. osa.

([14]) Käesolev otsus on EMPs kohaldatav. Euroopa Majanduspiirkonna lepingus (edaspidi „EMP leping") on ette nähtud Euroopa Liidu siseturu laiendamine kolmele EMP liikmesriigile Islandile, Liechtensteinile ja Norrale. EMP ühiskomitee võttis ühiskomitee otsuse (millega inkorporeeritakse määrus (EL) 2016/679 EMP lepingu XI lisasse) vastu 6. juulil 2018 ja see jõustus 20. juulil 2018. Määrus on seega selle lepinguga hõlmatud. Otsuses sisalduvad viited ELile ja ELi liikmesriikidele hõlmavad niisiis ka EMP riike.

(8) Käesoleva otsuse kohaselt võib edastada isikuandmeid liidus asuvatelt vastutavatelt või volitatud töötlejatelt ([15]) Ameerika Ühendriikides asuvatele põhimõtete järgimist kinnitanud organisatsioonidele ilma, et oleks vaja taotleda lisaluba. Otsus ei mõjuta selliste organisatsioonide suhtes määruse (EL) 2016/679 otsest kohaldamist, kui täidetud on selle territoriaalse kohaldamisala tingimused, mis on sätestatud määruse artiklis 3.

2. **ELi-USA ANDMEKAITSERAAMISTIK**

2.1. **Isikuline ja esemeline kohaldamisala**

2.1.1. ***Põhimõtete järgimist kinnitanud organisatsioonid***

(9) ELi-USA andmekaitseraamistik põhineb kinnituste süsteemil, mille kohaselt USA organisatsioonid kohustuvad järgima teatavaid eraelu puutumatuse põhimõtteid ehk ELi-USA andmekaitseraamistiku põhimõtteid, sealhulgas täiendavaid põhimõtteid (edaspidi üheskoos „põhimõtted“), mille on välja andnud Ameerika Ühendriikide kaubandusministeerium ja mis on esitatud käesoleva otsuse I lisas ([16]). Selleks et saada õigus ELi-USA andmekaitseraamistiku kohasele kinnitamisele, peab organisatsioon tunnustama föderaalse kaubanduskomisjoni või USA transpordiministeeriumi volitusi uurimise läbiviimiseks ja täitmise tagamiseks ([17]). Põhimõtted rakenduvad kohe pärast kinnitamist. Nagu põhjendustes 48–52 üksikasjalikumalt selgitatud, peavad ELi-USA andmekaitseraamistikus osalevad organisatsioonid põhimõtete järgimist igal aastal uuesti kinnitama ([18]).

2.1.2. ***Isikuandmete ja vastutava töötleja ning esindaja mõiste määratlus***

(10) ELi-USA andmekaitseraamistiku alusel pakutav kaitse kehtib kõigile isikuandmetele, mis edastatakse liidust USAs asuvatele organisatsioonidele, kes on esitanud kaubandusministeeriumile kinnituse põhimõtete järgimise kohta, välja arvatud ajakirjandusliku materjali trükis või eetris avaldamiseks või muul moel avalikuks edastamiseks kogutud andmed ning massiteabevahendite arhiivide levitatavas varem avaldatud materjalis sisalduv teave ([19]). Seetõttu ei saa sellist teavet ELi-USA andmekaitseraamistiku alusel edastada.

(11) Põhimõtetes on isikuandmed määratletud samamoodi nagu määruses (EL) 2016/679, st kui „tuvastatud või tuvastatava füüsilise isiku kohta käivad isikuandmete kaitse üldmääruse kohaldamisalasse kuuluvad andmed, mida Ameerika Ühendriikides asuv organisatsioon EList saab ja mis tahes vormis salvestab“ ([20]). Seega hõlmavad need ka pseudonüümitud (või võtme ja koodiga varustatud) uurimisandmeid (sealhulgas juhul, kui võtit ei jagata vastuvõtva USA organisatsiooniga) ([21]). Samamoodi on töötlemise mõiste määratletud kui „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“ ([22]).

(12) ELi-USA andmekaitseraamistikku kohaldatakse USAs asuvate organisatsioonide suhtes, kes loetakse vastutavaks töötlejaks (st isik või organisatsioon, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid) ([23]) või volitatud töötlejaks (st vastutava töötleja nimel tegutsevad esindajad) ([24]). USA volitatud töötlejad peavad olema sõlminud lepingu, mille kohaselt nad tegutsevad ainult juhiste kohaselt, mille nad on saanud

([15]) Käesolev otsus ei mõjuta määruse (EL) 2016/679 nõudeid, mida kohaldatakse liidus andmeid edastavate üksuste (vastutavate töötlejate ja volitatud töötlejate) suhtes, näiteks seoses eesmärgi piiramise, võimalikult väheste andmete kogumise, läbipaistvuse ja andmeturbega (vt ka määruse (EL) 2016/679 artikkel 44).

([16]) Vt selle kohta kohtuotsus Schrems, punkt 81, kus Euroopa Kohus kinnitas, et ise kinnituse andmise süsteem võib tagada kaitse piisava taseme.

([17]) I lisa I jao punkt 2. Föderaalsel kaubanduskomisjonil on äritegevuse valdkonna üle laialdane pädevus, kuigi teatavate eranditega, nt seoses pankade, lennuettevõtjate, kindlustusäri ja telekommunikatsiooniteenuste pakkujate ühiste vedajate tegevusega (kuigi USA üheksanda ringkonna apellatsioonikohtu 26. veebruari 2018. aasta otsuses kohtuasjas FTC *vs.* AT&T kinnitati, et selliste üksuste mitteühiste vedajate tegevus kuulub föderaalse kaubanduskomisjoni pädevusse). Vt ka IV lisa joonealune märkus 2. Transpordiministeeriumi pädevuses on tagada, et lennuettevõtjad ja piletimüüjad (lennutranspordi puhul) täidaksid nõudeid, vt V lisa A jagu.

([18]) I lisa III jao punkt 6.

([19]) I lisa III jao punkt 2.

([20]) I lisa I jao punkti 8 alapunkt a.

([21]) I lisa III jao punkti 14 alapunkt g.

([22]) I lisa I jao punkti 8 alapunkt b.

([23]) I lisa I jao punkti 8 alapunkt c.

([24]) Vt nt I lisa II jao punkti 2 alapunkt b ja III jao punkti 3 alapunkt b ja punkti 7 alapunkt d, milles selgitatakse, et piletimüüjad tegutsevad vastutava töötleja nimel viimati nimetatu juhiste kohaselt ja täites täpseid lepingulisi kohustusi.

ELi vastutavalt töötlejalt, keda nad abistavad põhimõtete kohaseid õigusi kasutavate isikute taotlustele vastamisel ([25]). Alamtöötlemise korral peab volitatud töötleja sõlmima lisaks alamtöötlejaga lepingu, millega tagatakse põhimõtetes kehtestatuga samal tasemel kaitse, ja astuma samme selle nõuetekohase rakendamise tagamiseks ([26]).

2.2. **ELi-USA andmekaitseraamistiku põhimõtted**

2.2.1. ***Eesmärgi piiramise ja valikuvõimaluse põhimõte***

(13) Isikuandmeid töödeldakse õiguspäraselt ja õiglaselt. Isikuandmeid tuleks koguda konkreetsel eesmärgil ja kasutada seejärel üksnes määral, mis on kooskõlas töötlemise eesmärgiga.

(14) ELi-USA andmekaitseraamistikus tagatakse see erinevate põhimõtete abil. Esiteks ei tohi organisatsioon *andmete terviklikkuse ja eesmärgi piiramise põhimõtte* kohaselt, sarnaselt määruse (EL) 2016/679 artikli 5 lõike 1 punktiga b, töödelda isikuandmeid viisil, mis ei vasta eesmärgile, milleks need algselt koguti või milleks andmesubjekt seejärel loa andis ([27]).

(15) Teiseks peab organisatsioon enne isikuandmete kasutamist uuel (muudetud) eesmärgil, mis on oluliselt erinev, kuid vastab siiski algsele eesmärgile, või nende avaldamiseks kolmandale isikule, andma andmesubjektidele kooskõlas *valikuvõimaluse põhimõttega* ([28]) võimaluse esitada vastuväide (*opt-out*) selge, arusaadava ja kergesti kättesaadava mehhanismi kaudu. Oluline on, et see põhimõte ei asenda eesmärgiga vastuolus oleva andmete töötlemise sõnaselget keeldu ([29]).

([25]) I lisa III jao punkti 10 alapunkt a. Vt ka juhend, mille kaubandusministeerium koostas andmekaitseraamistiku Privacy Shield raames, konsulteerides Euroopa Andmekaitsenõukoguga ja milles selgitatakse raamistiku alusel liidust isikuandmeid saavate USA volitatud töötlejate kohustusi. Kuna need reeglid ei ole muutunud, on kõnealused juhised / korduma kippuvad küsimused ka ELi-USA andmekaitseraamistiku suhtes jätkuvalt asjakohased (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) I lisa II jao punkti 3 alapunkt b.

([27]) I lisa II jao punkti 5 alapunkt a. Nõuetele vastavad töötlemiseesmärgid võivad olla näiteks auditeerimine, pettuse ennetamine või muud eesmärgid, mis vastavad mõistliku inimese ootustele andmete kogumise kontekstis (vt I lisa joonealune märkus 6).

([28]) I lisa II jao punkti 2 alapunkt a. Põhimõte ei kehti, kui organisatsioon edastab isikuandmeid tema nimel ja juhiste alusel tegutsevale volitatud töötlejale (I lisa II jao punkti 2 alapunkt b). Sellegipoolest peab organisatsioonil sellisel juhul olema sõlmitud leping ja ta peab tagama, et järgitakse *kolmandale isikule andmete edasisaatmise eest vastutuse* põhimõtet, mida on üksikasjalikumalt kirjeldatud põhjenduses 43. Lisaks võidakse isikuandmete töötlemisel *valikuvõimaluse põhimõtet* (nagu ka *teate põhimõtet*) piirata hoolsuskohustuse (võimaliku ühinemise või ülevõtmise osana) või auditite raames sellises ulatuses ja ajavahemikul, mis on vajalik seadusest või avalikust huvist tulenevate nõuete täitmiseks, või sellises ulatuses ja seni, kuni nende põhimõtete kohaldamine kahjustaks organisatsiooni õigustatud huve hoolsuskohustusega seotud uurimiste või auditite konkreetses kontekstis (I lisa III jao punkt 4). Erandi *valikuvõimaluse* põhimõttest (nagu ka *teate* põhimõttest ja *kolmandale isikule andmete edasisaatmise eest vastutuse* põhimõttest) näeb ette ka täiendav põhimõte 15 (I lisa III jao punkti 15 alapunktid a ja b) selliste avalikult kättesaadavatest allikatest pärinevate isikuandmete puhul (välja arvatud juhul, kui ELi andmete eksportija märgib, et teabe suhtes kehtivad piirangud, mis nõuavad nende põhimõtete kohaldamist) või isikuandmete puhul, mis on kogutud avalikest registritest (kui neid ei kombineerita mitteavalike registrite andmetega ja kõiki kasutustingimusi on järgitud). Erandi valikuvõimaluse põhimõttest (samuti *teate põhimõttest* ja *kolmandale isikule andmete edasisaatmise eest vastutuse põhimõttest*) näeb ette ka täiendav põhimõte 14 (I lisa III jao punkti 14 alapunkt f), kui farmaatsia- või meditsiiniseadmeid tootev ettevõtja töötleb isikuandmeid toote ohutuse ja tõhususe jälgimise toimingute jaoks, ulatuses, milles põhimõtete järgmine segaks regulatiivsete nõuete järgimist.

([29]) See kehtib igasugusele ELi-USA andmekaitseraamistiku alusel andmete edastamisele, sealhulgas juhul, kui edastatakse töösuhte raames kogutud andmeid. Ehkki põhimõtete järgimist kinnitanud USA organisatsioonil on seega põhimõtteliselt lubatud kasutada personaliandmeid muudel, töösuhtega mitteseotud eesmärkidel (näiteks teatavates reklaamteadetes), peab ta järgima eesmärgiga vastuolus oleva töötlemise keeldu; lisaks on kasutamine lubatud ainult kooskõlas *teate* ja *valikuvõimaluse* põhimõttega. Erandina võib organisatsioon kasutada isikuandmeid täiendaval kokkusobival eesmärgil ilma *teadet* esitamata ja *valikuvõimalust* pakkumata, kuid ainult sellises ulatuses ja ajavahemikuks, mis on vajalik organisatsiooni teovõime kahjustamise vältimiseks edutamiste, ametisse nimetamiste või muude sarnaste töösuhteid puudutavate otsuste langetamiseks (vt I lisa III jao punkti 9 alapunkti b alapunkt iv). 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 ja seega on tema valik ka tegelikult vaba. Vt I lisa III jao punkti 9 alapunkti b alapunkt i.

2.2.2. ***Isikuandmete eriliikide töötlemine***

(16) „Eriliiki“ andmete töötlemisel tuleks kohaldada erikaitsemeetmeid.

(17) *Valikuvõimaluse põhimõtte* kohaselt kohaldatakse erikaitsemeetmeid juhul, kui töödeldakse „tundlikku teavet“, st isikuandmeid, mis kirjeldavad meditsiinilist või tervislikku seisundit, rassilist või etnilist päritolu, poliitilisi seisukohti, usulisi või filosoofilisi veendumusi, ametiühingusse kuulumist, isiku seksuaalelu puudutavat teavet, või mis tahes muud teavet, mis on saadud kolmandalt isikult ja mille see isik on määratlenud ning mida ta käsitab tundliku teabena ([30]). See tähendab, et põhimõtete järgimist kinnitanud organisatsioonid käsitavad ELi-USA andmekaitseraamistiku raames tundlikuna kõiki andmeid, mida peetakse tundlikuks liidu andmekaitseõiguse kohaselt (sealhulgas andmed seksuaalse sättumuse kohta, geneetilised andmed ja biomeetrilised andmed).

(18) Üldreegli kohaselt peavad organisatsioonid saama üksikisikutelt sõnaselge jaatava nõusoleku (st nõustuv valik (*opt-in*)), et kasutada tundlikku teavet muudel eesmärkidel kui need, milleks andmed algselt koguti või milleks üksikisik algselt loa andis (nõustuva valikuga), või avalikustada need kolmandatele isikutele ([31]).

(19) Sellise nõusoleku saamine ei ole nõutav piiratud asjaolude korral, mis on sarnased liidu andmekaitseõiguses sätestatud võrreldavate eranditega, nt kui tundlike andmete töötlemine on isiku elulistes huvides, on vajalik õigusnõuete koostamiseks või on vajalik arstiabi andmiseks või diagnoosi määramiseks ([32]).

2.2.3. ***Andmete õigsus, võimalikult väheste andmete kogumine ja andmeturve***

(20) Andmed peavad olema õiged ja vajaduse korral ka ajakohastatud. Samuti peavad need olema piisavad, asjakohased ja mitte ülemäärased arvestades eesmärki, mille tarvis neid töödeldakse, ning andmeid ei tohiks põhimõtteliselt säilitada kauem kui see on vajalik isikuandmete töötlemise eesmärgi täitmiseks.

(21) Vastavalt *andmete terviklikkuse ja eesmärgi piiramise põhimõttele* ([33]) tohib koguda üksnes töötlemise eesmärgile vastavaid isikuandmeid. Lisaks peavad organisatsioonid võtma töötlemise eesmärkidel vajalikus ulatuses mõistlikke meetmeid, tagamaks et isikuandmed on plaanitud kasutuseks usaldusväärsed, täpsed, täielikud ja ajakohased.

(22) Lisaks võib isikuandmeid säilitada kujul, mis võimaldab isikut tuvastada või muuta isiku tuvastatavaks (ja seega isikuandmete kujul) ([34]) ainult seni, kuni see vastab eesmärgile või eesmärkidele, milleks andmed algselt koguti või milleks andmesubjekt seejärel *valikuvõimaluse põhimõtte* kohaselt loa andis. See kohustus ei takista organisatsioonidel jätkata isikuandmete töötlemist pikema aja vältel, ent ainult nii kaua ja sellises ulatuses, kui see on mõistlikult vajalik järgmistel konkreetsetel liidu andmekaitseõiguses sätestatud võrreldavate eranditega sarnastel eesmärkidel: arhiveerimine avaliku huvi eesmärgil, ajakirjandus, kirjandus ja kunst, teadus- ja ajaloouuringud ning statistiline analüüs ([35]). Kui isikuandmeid säilitatakse ühel neist eesmärkidest, kohaldatakse töötlemisel põhimõtetega kehtestatud kaitsemeetmeid ([36]).

(23) Isikuandmeid tuleks ka töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest. Selleks peaksid vastutavad töötlejad ja volitatud töötlejad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse tehnika taset ja seonduvaid kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti töötlemisest üksikisikute õigustele tekkivaid riske.

([30]) I lisa II jao punkti 2 alapunkt c.
([31]) I lisa II jao punkti 2 alapunkt c.
([32]) I lisa III jao punkt 1.
([33]) I lisa II jao punkt 5.
([34]) Vt I lisa joonealune märkus 7, milles selgitatakse, et isikut peetakse tuvastatavaks seni, kuni organisatsioon või kolmas isik saab selle isiku mõistliku vaevaga tuvastada, võttes arvesse tuvastamisvahendeid, mida tõenäoliselt kasutatakse (arvestades muu hulgas isiku tuvastamise rahalist ja ajakulu ning töötlemise ajal olemasolevat tehnoloogiat).
([35]) I lisa II jao punkti 5 alapunkt b.
([36]) *Samas*.

(24) ELi-USA andmekaitseraamistikus tagatakse see *turvalisuse põhimõttega*, mille kohaselt tuleb sarnaselt määruse (EL) 2016/679 artikliga 32 võtta mõistlikke ja asjakohaseid turvameetmeid, võttes arvesse töötlemisega kaasnevaid riske ja andmete laadi ([37]).

2.2.4. ***Läbipaistvus***

(25) Andmesubjekte tuleks teavitada nende isikuandmete töötlemise põhitunnustest.

(26) See on tagatud *teate põhimõttega*, ([38]) millega sarnaselt määruse (EL) 2016/679 läbipaistvusnõuetega kohustatakse organisatsioone teavitama andmesubjekte muu hulgas järgmisest: i) organisatsiooni osalemine ELi-USA andmekaitseraamistikus, ii) kogutavate andmete liik, iii) töötlemise eesmärk, iv) millist liiki kolmandatele isikutele ja mis eesmärkidel võidakse isikuandmeid avalikustada, v) nende isikute õigused, vi) kuidas organisatsiooniga ühendust võtta ning vii) kättesaadavad õiguskaitsevahendid.

(27) 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 kasutab neid andmeid oluliselt erineval (kuigi kokkusobival) eesmärgil kui see, milleks need algselt koguti, või avaldab need kolmandale isikule ([39]).

(28) Lisaks peavad organisatsioonid tegema avalikuks oma põhimõtteid kajastavad privaatsustingimused (või kui tegemist on personaliandmetega, siis tegema need asjaomastele isikutele hõlpsasti kättesaadavaks) ja esitama lingid kaubandusministeeriumi veebisaidile (täpsemate üksikasjadega põhimõtete järgimise kinnitamise, andmesubjektide õiguste ja kättesaadavate kaebuste menetlemise mehhanismide kohta), andmekaitseraamistikuga ühinenute nimekirja juurde ning asjakohase alternatiivse vaidluste lahendamise pakkuja veebisaidile ([40]).

2.2.5. ***Üksikisiku õigused***

(29) Andmesubjektidel peaksid olema teatavad õigused, mida saab vastutava töötleja või volitatud töötleja suhtes täitmisele pöörata, eelkõige õigus andmetele juurde pääseda, õigus esitada töötlemise kohta vastuväiteid ning õigus lasta andmeid parandada ja kustutada.

(30) Üksikisikutele annab sellised õigused ELi-USA andmekaitseraamistiku *juurdepääsu põhimõte* ([41]). Eelkõige on andmesubjektidel õigus ilma põhjendusi esitamata saada organisatsioonilt kinnitus selle kohta, kas organisatsioon töötleb nendega seotud isikuandmeid; saada teavet nende andmete kohta ning saada teavet isikuandmete töötlemise eesmärkide kohta, töödeldavate isikuandmete liikide ja vastuvõtjate (kategooriate) kohta, kellele isikuandmed avalikustatakse ([42]). Organisatsioonid peavad juurdepääsutaotlustele vastama mõistliku aja jooksul ([43]).

([37]) I lisa II jao punkti 4 alapunkt a. Lisaks on ELi-USA andmekaitseraamistikus sätestatud personaliandmete kohta nõue, et tööandjad arvestaksid töötajate eraelu puutumatuse eelistusi, piirates juurdepääsu isikuandmetele, tehes teatavad andmed anonüümseks või määrates neile koodid või pseudonüümid (I lisa III jao punkti 9 alapunkti b alapunkt iii).

([38]) I lisa II jao punkt 1.

([39]) I lisa II jao punkti 1 alapunkt b. Täiendavas põhimõttes 14 (I lisa III jao punkti 14 alapunktid b ja c) on kehtestatud erisätted isikuandmete töötlemise kohta terviseuuringute ja kliiniliste uuringute kontekstis. Eelkõige võimaldab see põhimõte organisatsioonidel töödelda kliiniliste uuringute andmeid isegi pärast seda, kui isik on uuringust loobunud, kui see oli ajal, mil isik nõustus osalema, teates selgelt märgitud. Samamoodi, kui ELi-USA andmekaitseraamistikus osalev organisatsioon saab isikuandmeid terviseuuringute jaoks, võib ta neid uue uuringu jaoks kasutada üksnes kooskõlas *teate* ja *valikuvõimaluse* põhimõttega. Sel juhul peaks üksikisikule saadetud teade põhimõtteliselt andma teavet andmete mis tahes tulevase konkreetse kasutamise kohta (nt seotud uuringud). Kui andmete kogu tulevast kasutust ei ole võimalik algusest peale teatesse lisada (sest uus teaduskasutus võib tuleneda uutest arusaamadest või meditsiini/uuringute arengust), tuleb lisada selgitus, et isikuandmeid võidakse tulevikus kasutada ettenägematutes meditsiini- ja farmaatsiauuringutes. Kui selline edasine kasutamine ei ole kooskõlas uuringute üldiste eesmärkidega, milleks andmeid koguti (st kui uued eesmärgid on oluliselt erinevad, kuid siiski algse eesmärgiga kokkusobivad, vt põhjendused 14–15), on vaja saada uus nõusolek (st nõustuv valik (*opt-in*)). Vt lisaks joonealuses märkuses 28 kirjeldatud *teate* põhimõtte spetsiifilised piirangud/erandid.

([40]) I lisa III jao punkti 6 alapunkt d.

([41]) Vt ka juurdepääsu käsitlev täiendav põhimõte (I lisa III jao punkt 8).

([42]) I lisa III jao punkti 8 alapunkti a alapunktid i–ii.

([43]) I lisa III jao punkti 8 alapunkt i.

Organisatsioon võib kehtestada mõistlikud piirangud sellele, mitu korda teatava aja jooksul konkreetse isiku juurdepääsutaotlus rahuldatakse, ja võib nõuda tasu, mis ei ole ülemäära suur, nt kui taotlustega on selgelt liiale mindud, eelkõige korduvuse tõttu ([44]).

(31) Õigust isikuandmetele juurde pääseda tohib piirata vaid erandlikel juhtudel, mis on sarnased liidu andmekaitseõigusega ette nähtud asjaoludega, eelkõige juhul, kui sellega rikutakse teiste isikute seaduslikke õigusi; kui juurdepääsu võimaldamise tülikus või kulud on asjaomasel juhul ebaproportsionaalsed ohuga üksikisiku eraelu puutumatusele (kuigi kulud ja tülikus ei ole otsustavad tegurid, mis määravad kindlaks, kas juurdepääsu andmine on mõistlik); ulatuses, milles avalikustamine võib häirida olulise vastukaaluga avalike huvide kaitset, näiteks riiklik julgeolek, avalik julgeolek või kaitsekaalutlused; teave sisaldab äriliselt konfidentsiaalset teavet või teavet töödeldakse üksnes uurimis- või statistilistel eesmärkidel ([45]). Juurdepääsuõiguse keelamine või piiramine peab olema vajalik ja nõuetekohaselt põhjendatud ning organisatsioonil on kohustus tõendada, et need tingimused on täidetud ([46]). Selle hindamisel peab organisatsioon eelkõige arvestama üksikisiku huve ([47]). Kui teavet on võimalik eraldada muudest andmetest, mille suhtes kohaldatakse piirangut, peab organisatsioon kaitstud andmed eraldama ja muud andmed kättesaadavaks tegema ([48]).

(32) Lisaks on andmesubjektil õigus nõuda ebatäpsete andmete parandamist või muutmist ning selliste andmete kustutamist, mida on töödeldud põhimõtteid rikkudes ([49]). Lisaks, nagu on selgitatud põhjenduses 15, on üksikisikutel õigus vaidlustada/keelata oma andmete töötlemine, kui töötlemise eesmärgid on (kuigi kokkusobivad) oluliselt erinevad nendest, milleks andmed koguti, ja oma andmete avaldamine kolmandatele isikutele. Kui isikuandmeid kasutatakse otseturunduse eesmärgil, on üksikisikutel üldine õigus töötlemisest igal ajal loobuda ([50]).

(33) Põhimõtetes ei ole eraldi käsitletud andmesubjekti mõjutavaid otsuseid, mis põhinevad üksnes isikuandmete automatiseeritud töötlemisel. Igal juhul teeb liidus kogutud isikuandmete puhul kõik automatiseeritud töötlemisel põhinevad otsused tavaliselt liidu vastutav töötleja (kellel on otsene suhe asjaomase andmesubjektiga) ja nende suhtes kohaldatakse seega otse määrust (EL) 2016/679 ([51]). See kehtib ka edastamisolukordades, kus andmeid töötleb välisriigi (nt USA) ettevõtja, kes tegutseb liidu vastutava töötleja esindajana (volitatud töötlejana) (või liidu volitatud töötleja nimel tegutseva alamtöötlejana, kes on saanud andmed need kogunud liidu vastutavalt töötlejalt) ja teeb selle põhjal otsuse.

(34) Seda kinnitas uuring, mille komisjon tellis 2018. aastal andmekaitseraamistiku Privacy Shield toimimise teise igaaastase läbivaatamise ([52]) raames ja milles jõuti järeldusele, et sel ajal ei olnud tõendeid, mis viitaksid sellele, et tavaliselt tegid andmekaitseraamistikus Privacy Shield osalevad organisatsioonid Privacy Shieldi raames edastatud isikuandmete alusel automatiseeritud otsuseid.

([44]) I lisa III jao punkti 8 alapunkti f alapunktid i–ii ja alapunkt g.
([45]) I lisa III jao punkt 4; punkti 8 alapunktid b, c, e; punkti 14 alapunktid e ja f ning punkti 15 alapunkt d.
([46]) I lisa III jao punkti 8 alapunkti e alapunkt ii. Organisatsioon peab teavitama üksikisikut keeldumise/piirangu põhjustest ja esitama andmed selle kohta, kellele või kuhu saata täiendavad päringud, III jao punkti 8 alapunkti a alapunkt iii.
([47]) I lisa III jao punkti 8 alapunkti a alapunktid ii–iii.
([48]) I lisa III jao punkti 8 alapunkti a alapunkt i.
([49]) I lisa II jao punkt 6 ja III jao punkti 8 alapunkti a alapunkt i.
([50]) I lisa III jao punkti 8 alapunkt 12.
([51]) Seevastu erandjuhul, kus USA organisatsioonil on otsene suhe liidu andmesubjektiga, tuleneb see tavaliselt sellest, et ta on ise pöördunud liidus asuva üksikisiku poole, pakkudes talle kaupu ja teenuseid või jälgides tema käitumist. Selle stsenaariumi puhul kuulub USA organisatsioon ise määruse (EL) 2016/679 (artikli 3 lõike 2) kohaldamisalasse ja peab seega järgima otse ELi andmekaitseõigust.
([52]) SWD(2018) 497 final, punkt 4.1.5. Uuring keskendus i) sellele, kui palju võtavad andmekaitseraamistikus Privacy Shield osalevad USA organisatsioonid vastu üksikisikuid mõjutavaid otsuseid, mis põhinevad ELi ettevõtjatelt Privacy Shieldi raames edastatud isikuandmete automatiseeritud töötlemisel, ning ii) USA föderaalseadusega üksikisikutele selliste olukordade puhuks ette nähtud kaitsemeetmetele ja nende kaitsemeetmete kohaldamise tingimustele.

(35) Igal juhul neis valdkondades, kus ettevõtjad kõige suurema tõenäosusega tuginevad isikuandmete automatiseeritud töötlemisele, et teha üksikisikuid mõjutavaid otsuseid (näiteks laenu andmine, hüpoteeklaenud, tööhõive, eluase ja kindlustus), on USA õigusaktidega ette nähtud konkreetsed kaitsemeetmed negatiivsete otsuste vastu ([53]). 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. Tarbijakrediidi valdkonnas sisaldavad õiglase krediidiinfo seadus (Fair Credit Reporting Act (FCRA)) ja võrdsete krediidivõimaluste seadus (Equal Credit Opportunity Act (ECOA)) kaitsemeetmeid, mis annavad tarbijatele teatavas vormis õiguse selgitustele ja õiguse otsus vaidlustada. Need seadused on asjakohased paljudes valdkondades, sealhulgas krediidi, tööhõive, eluaseme ja kindlustuse valdkonnas. Lisaks pakuvad teatavad diskrimineerimisvastased seadused, nagu tsiviilõiguste seaduse (Civil Rights Act) VII jaotis ja õiglase eluaseme seadus (Fair Housing Act), üksikisikutele kaitset seoses automatiseeritud otsuste tegemisel kasutatavate mudelitega, mis võivad põhjustada diskrimineerimist teatavate tunnuste alusel, ja annavad üksikisikutele õiguse sellised otsused, sealhulgas automatiseeritud otsused, vaidlustada. Mis puudutab terviseteavet, siis ravikindlustuse teisaldatavuse seaduse ja vastutuse seaduse (Health Insurance Portability and Accountability Act (HIPAA)) eraelu puutumatuse eeskiri loob seoses isiklikule terviseteabele juurdepääsuga teatavad õigused, mis on sarnased määruse (EL) 2016/679 kohaste õigustega. Lisaks nõutakse USA ametiasutuste juhistes meditsiiniteenuste osutajatelt teavet, mis võimaldab neil teavitada üksikisikuid meditsiinisektoris kasutatavatest automatiseeritud otsustuste tegemise süsteemidest ([54]).

(36) Seetõttu pakuvad need normid liidu andmekaitseõigusega sarnast kaitset ebatõenäolises olukorras, kus ELi-USA andmekaitseraamistikus osalev organisatsioon ise teeb automatiseeritud otsuseid.

2.2.6. ***Andmete edasisaatmise piirangud***

(37) Liidust Ameerika Ühendriikide organisatsioonidele edastatavate isikuandmete kaitse taset ei tohi kahjustada selliste andmete edasisaatmine Ameerika Ühendriikides või muus kolmandas riigis asuvale vastuvõtjale.

(38) *Kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtte* ([55]) kohaselt kehtib erieeskiri nn edasisaatmise suhtes, st juhul, kui ELi-USA andmekaitseraamistikus osalev organisatsioon saadab isikuandmed edasi kolmandast isikust vastutavale või volitatud töötlejale, olenemata sellest, kas nimetatud töötleja asub Ameerika Ühendriikides või kolmandas riigis väljaspool Ameerika Ühendriike (ja Euroopa Liitu). Edasisaatmine võib toimuda ainult i) piiratud ja kindlaksmääratud eesmärkidel, ii) ELi-USA andmekaitseraamistikus osaleva organisatsiooni ja kolmanda isiku vahelise lepingu alusel ([56]) (või võrreldava kontsernisisese kokkuleppe alusel ([57])) ja iii) ainult juhul, kui selle lepinguga nõutakse, et kolmas isik pakuks põhimõtetega tagatud kaitsetasemega võrdset kaitset.

(39) See kohustus tagada põhimõtetega tagatuga sama kaitsetase, tõlgendatuna koos *andmete terviklikkuse ja eesmärgi piiramise põhimõttega*, tähendab eelkõige seda, et kolmas isik võib talle edasi saadetud isikuandmeid töödelda ainult eesmärkidel, mis ei ole vastuolus eesmärkidega, milleks neid algselt koguti või milleks isik seejärel loa andis (kooskõlas *valikuvõimaluse põhimõttega*).

([53]) Vt näiteks Equal Credit Opportunity Act (USA seadustiku (U.S. Code) 15. jaotise § 1691 jj), Fair Credit Reporting Act (USA seadustiku 15. jaotise § 1681 jj) või Fair Housing Act (USA seadustiku 42. jaotise § 3601 jj). Lisaks on Ameerika Ühendriigid nõustunud järgima Majanduskoostöö ja Arengu Organisatsiooni tehisintellekti käsitlevaid põhimõtteid, mille hulgas on ka läbipaistvuse, selgitusvõime, turvalisuse ja vastutuse põhimõte.

([54]) Vt nt suunis selle kohta, millisele isiklikule terviseteabele on isikutel HIPAA kohaselt õigus saada juurdepääs oma tervishoiuteenuse osutajatelt ja tervisekaitse kavade pakkujatelt, mis on kättesaadav aadressil 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Vt I lisa II jao punkt 3 ja täiendav põhimõte „Kohustuslikud lepingud andmete edasisaatmiseks kolmandale isikule“ (I lisa III jao punkt 10).

([56]) Erandina sellest üldpõhimõttest võib organisatsioon ilma vastuvõtjaga lepingut sõlmimata edasi saata väikese arvu töötajate isikuandmeid juhuslikeks töösuhtega seotud tegevusvajadusteks, nt lennupiletite broneerimiseks, hotellitoa või kindlustuse tellimiseks. Siiski peab organisatsioon ka sellisel juhul *teate* ja *valikuvõimaluse* põhimõtet järgima (vt I lisa III jao punkti 9 alapunkt e).

([57]) Vt täiendav põhimõte „Kohustuslikud lepingud andmete edasisaatmiseks kolmandale isikule“ (I lisa III jao punkti 10 alapunkt b). Ehkki see põhimõte võimaldab andmeid edastada ka mittelepinguliste vahendite alusel (näiteks kontsernisisene vastavuse ja kontrolli programm), on tekstis selgelt sätestatud, et need vahendid peavad „tagama jätkuvalt põhimõtetele vastava 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.

(40) *Kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtet* tuleks tõlgendada ka koostoimes *teate põhimõtte* ja kolmandast isikust vastutavale töötlejale edasisaatmise korral *valikuvõimaluse põhimõttega*, mille kohaselt tuleb andmesubjektidele teada anda (muu hulgas) andmete kolmandast isikust vastuvõtja ([58]) liik/isik, andmete edasisaatmise eesmärk ja pakutud valik; teavitada tuleb ka võimalusest edasisaatmisest keelduda (*opt out*) või tundlike andmete korral sellest, et edasisaatmiseks on vaja nende „kinnitavat sõnaselget nõusolekut“ (*opt in*).

(41) Kohustus tagada samal tasemel kaitse nagu põhimõtetes nõutud, kehtib kõigile kolmandatele isikutele, kes on andmete töötlemisega seotud, olenemata 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.

(42) Igal juhul tuleb kolmanda isikuga sõlmitud lepingus sätestada, et nimetatud kolmas isik teavitab ELi-USA andmekaitseraamistikus osalevat organisatsiooni, kui ta leiab, et ei suuda seda kohustust enam täita. Kui selline järeldus tehakse, peab kolmas isik andmete töötlemise lõpetama või tuleb olukorra parandamiseks astuda muid mõistlikke ja asjakohaseid samme ([59]).

(43) Andmete edasisaatmisel kolmandast isikust esindajale (st volitatud töötlejale) kehtivad lisakaitsemeetmed. Sellisel juhul peab USA organisatsioon tagama, et esindaja tegutseb üksnes tema antud juhiste kohaselt ning astuma mõistlikke ja asjakohaseid samme, et i) tagada, et nimetatud esindaja töötleb edastatud isikuandmeid ka tegelikkuses kooskõlas organisatsioonile põhimõtetest tulenevate kohustustega ja ii) vastava teate saamisel loata töötlemine peatada ja heastada ([60]). Kaubandusministeerium võib nõuda, et organisatsioon esitaks lepingu eraelu puutumatuse sätete kokkuvõtte või tüüpkoopia ([61]). Kui (alam)töötlemise ahelas tekivad vastavusprobleemid, on põhimõtteliselt vastutav isikuandmete vastutava töötlejana tegutsev organisatsioon, nagu on sätestatud *kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõttes*, välja arvatud juhul, kui ta tõendab, et ta ei vastuta kahju põhjustanud sündmuse eest ([62]).

2.2.7. ***Vastutus***

(44) Vastutuse põhimõtte kohaselt peavad andmeid töötlevad üksused kehtestama asjakohased tehnilised ja korralduslikud meetmed, et täita tõhusalt oma andmekaitsekohustusi ja suuta sellist vastavust tõendada, eelkõige pädevale järelevalveasutusele.

(45) Kui organisatsioon otsustab ELi-USA andmekaitseraamistiku põhimõtete järgimist vabatahtlikult kinnitada, ([63]) muutub põhimõtete tegelik järgimine tema jaoks kohustuslikuks ja täitmisele pööratavaks. *Kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte* ([64]) kohaselt peavad ELi-USA andmekaitseraamistikus osalevad organisatsioonid pakkuma tõhusaid mehhanisme põhimõtete järgimise tagamiseks. Samuti peavad organisatsioonid võtma meetmeid, et kontrollida ([65]) oma privaatsustingimuste vastavust põhimõtetele ja seda, et neid ka tegelikult järgitakse. Kontrollimiseks võib kasutada enesehindamise süsteemi, mis peab hõlmama sisemenetlusi, millega tagatakse, et töötajad saavad organisatsiooni privaatsustingimuste kohaldamise alast koolitust ja et nõuete täitmist kontrollitakse korrapäraselt objektiivsel viisil, või välist vastavuskontrolli, mis võib muu hulgas hõlmata auditeerimist, pistelist kontrolli või tehnoloogiliste vahendite kasutamist.

([58]) Isikutel ei ole keeldumisõigust, kui isikuandmed edastatakse kolmandale isikule, kes täidab esindajana ülesandeid USA organisatsiooni nimel ja selle juhiseid järgides. Ent selleks peab esindajaga olema sõlmitud leping ja põhimõtetega antud kaitse tagamise eest vastutab USA organisatsioon, kasutades oma juhiste andmise õigust.

([59]) Olukord on erinev olenevalt 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 ELi-USA andmekaitseraamistikus osalev organisatsioon, kes vastutab tema juhiste kohaselt tegutseva esindaja tehtud andmetöötluse eest. Vt I lisa II jao punkt 3.

([60]) I lisa II jao punkti 3 alapunkt b.

([61]) *Samas*.

([62]) I lisa II jao punkti 7 alapunkt d.

([63]) Vt ka täiendav põhimõte „Põhimõtete järgimise kinnitamine“ (I lisa III jao punkt 6).

([64]) Vt ka täiendav põhimõte „Vaidluste lahendamine ja täitmise tagamine“ (I lisa III jao punkt 11).

([65]) Vt ka täiendav põhimõte „Kontrollimine“ (I lisa III jao punkt 7).

(46) Lisaks peavad organisatsioonid hoidma alles dokumendid ELi-USA andmekaitseraamistiku kohaste tavade rakendamise kohta ja tegema need mittevastavuse uurimise või sellekohase kaebuse korral nõudmisel kättesaadavaks sõltumatule vaidluste lahendamise organile või pädevale täitevasutusele ([66]).

2.3. **Haldus, järelevalve ja täitmise tagamine**

(47) ELi-USA andmekaitseraamistikku haldab ja jälgib kaubandusministeerium. Raamistikus on ette nähtud järelevalve- ja nõuete täitmise tagamise mehhanismid, et kontrollida ja tagada, et ELi-USA andmekaitseraamistikus osalevad organisatsioonid järgivad põhimõtteid ning et iga järgimata jätmise korral võetakse meetmed. Nimetatud mehhanismid on sätestatud põhimõtetes (I lisa) ja kohustustes, mille on võtnud kaubandusministeerium (III lisa), föderaalne kaubanduskomisjon (IV lisa) ja transpordiministeerium (V lisa).

2.3.1. ***(Kordus) kinnitamine***

(48) ELi-USA andmekaitseraamistiku põhimõtete järgimise kinnitamiseks (või iga-aastaseks korduskinnitamiseks) peavad organisatsioonid avalikult deklareerima oma kohustust põhimõtteid järgida, tegema oma privaatsustingimused kättesaadavaks ja neid täielikult rakendama ([67]). Korduskinnituse taotluse osana peavad organisatsioonid esitama kaubandusministeeriumile teavet, muu hulgas asjaomase organisatsiooni nimi, eesmärgid, milleks organisatsioon isikuandmeid töötleb, isikuandmed, mida kinnitus hõlmab, samuti valitud kontrollimeetod, asjakohane sõltumatu kaebuste menetlemise mehhanism ja seadusjärgne asutus, kelle pädevuses on põhimõtete järgimise tagamine ([68]).

(49) Organisatsioonid võivad saada isikuandmeid ELi-USA andmekaitseraamistiku alusel alates kuupäevast, mil kaubandusministeerium on nad andmekaitseraamistikuga ühinenute nimekirja kandnud. Õiguskindluse tagamiseks ja nn valeväidete vältimiseks ei lubata esmakordselt põhimõtete järgimist kinnitavatel organisatsioonidel põhimõtete järgimisele avalikult viidata enne, kui kaubandusministeerium on kindlaks teinud, et organisatsiooni kinnitus on täielik, ja organisatsioon on lisatud andmekaitseraamistikuga ühinenute nimekirja ([69]). Selleks et organisatsioonil oleks õigus ELi-USA andmekaitseraamistikule tuginedes jätkuvalt liidust isikuandmeid saada, peab ta enda osalemise raamistikus igal aastal üle kinnitama. Kui organisatsioon lahkub mingil põhjusel ELi-USA andmekaitseraamistikust, peab ta eemaldama kõik avaldused, mis osutavad sellele, et organisatsioon jätkab andmekaitseraamistikus osalemist ([70]).

(50) Nagu nähtub III lisas sätestatud kohustustest, kontrollib kaubandusministeerium, kas organisatsioonid vastavad kõigile kinnitamise nõuetele ja kas nad on kehtestanud (avalikud) privaatsustingimused, mis sisaldavad *teate põhimõtte* kohaselt nõutavat teavet ([71]). Tuginedes andmekaitseraamistiku Privacy Shield kohase (kordus)kinnitamise protsessiga saadud kogemustele, teeb kaubandusministeerium mitu kontrolli, sealhulgas kontrollib, kas organisatsioonide privaatsustingimused sisaldavad hüperlinki õigele kaebuse esitamise vormile asjakohase vaidluste lahendamise mehhanismi veebisaidil, ja kui põhimõtete järgimise kinnitus hõlmab ühe organisatsiooni mitut üksust ja tütarettevõtjat, siis kas kõigi nende üksuste privaatsustingimused vastavad kinnitamise nõuetele ja on andmesubjektidele hõlpsasti kättesaadavad ([72]). Lisaks teeb kaubandusministeerium vajaduse korral ristkontrolli föderaalse kaubanduskomisjoni ja transpordiministeeriumiga, et kontrollida, kas organisatsioonid on allutatud nende (kordus)kinnitustes kindlaks määratud järelevalveorganile ja kas nad teevad koostööd alternatiivse vaidluste lahendamise organitega, et kontrollida, kas organisatsioonid on registreeritud nende (kordus)kinnituses märgitud sõltumatus kaebuste menetlemise mehhanismis ([73]).

([66]) I lisa III jao punkt 7.
([67]) I lisa I jao punkt 2.
([68]) I lisa III jao punkti 6 alapunkt b ja III lisa, vt jagu „Kinnitamise nõuetele vastavuse kontroll“.
([69]) I lisa, joonealune märkus 12.
([70]) I lisa III jao punkti 6 alapunkt h.
([71]) I lisa III jao punkti 6 alapunkt a ja joonealune märkus 12 ning III lisa, vt jagu „Kinnitamise nõuetele vastavuse kontroll“.
([72]) III lisa jagu „Kinnitamise nõuetele vastavuse kontroll“.
([73]) Samamoodi teeb kaubandusministeerium koostööd kolmanda isikuga, kes on andmekaitseasutuste kolleegiumi tasu kaudu kogutud rahaliste vahendite hoidja (vt põhjendus 73), et kontrollida, kas organisatsioonid, kes on valinud oma sõltumatu kaebuste menetlemise mehhanismiks andmekaitseasutused, on asjaomase aasta eest tasu maksnud. Vt III lisa jagu „Kinnitamise nõuetele vastavuse kontroll“.

(51) Kaubandusministeerium teavitab organisatsioone sellest, et (kordus)kinnitamise lõpuleviimiseks peavad nad lahendama kõik läbivaatamise käigus tuvastatud probleemid. Kui organisatsioon ei vasta kaubandusministeeriumi määratud aja jooksul (näiteks korduskinnituse puhul eeldatakse, et protsess viiakse lõpule 45 päeva jooksul) ([74]) või ei suuda muul viisil oma kinnitust valmis saada, loetakse, et esitamisest on loobutud. Sel juhul võib föderaalne kaubanduskomisjon või transpordiministeerium ELi-USA andmekaitseraamistikus osalemise või selle järgimise kohta esitatud valeväidete suhtes täitemeetmeid võtta ([75]).

(52) ELi-USA andmekaitseraamistiku nõuetekohase rakendamise tagamiseks peab huvitatud isikutel, nagu andmesubjektid, andmeeksportijad ja riiklikud andmekaitseasutused, olema võimalik kindlaks teha organisatsioonid, kes põhimõtteid järgivad. N-ö sisenemispunktis sellise läbipaistvuse tagamiseks on kaubandusministeerium võtnud kohustuse pidada nimekirja organisatsioonidest, kes on kinnitanud põhimõtete järgimist ning kes kuuluvad vähemalt ühe käesoleva otsuse IV ja V lisas osutatud täitevasutuse pädevusse, ([76]) ning see nimekiri üldsusele kättesaadavaks teha. Kaubandusministeerium uuendab seda nimekirja iga-aastaste korduskinnituste alusel ja iga kord, kui mõni organisatsioon loobub ELi-USA andmekaitseraamistikus osalemisest või ta eemaldatakse raamistikus osalejate hulgast. Läbipaistvuse tagamiseks ka n-ö väljumispunktis, kogub ja avalikustab kaubandusministeerium lisaks andmeid organisatsioonide kohta, kes on nimekirjast kustutatud, märkides igaühe kohta ära ka kustutamise põhjuse ([77]). Kõigele lisaks pakub ta linki föderaalse kaubanduskomisjoni ELi-USA andmekaitseraamistiku veebisaidile, kus on loetletud föderaalse kaubanduskomisjoni raamistiku alusel võetud täitemeetmed ([78]).

2.3.2. ***Nõuetele vastavuse järelevalve***

(53) Kaubandusministeerium jälgib erinevate mehhanismide kaudu pidevalt, kas ELi-USA andmekaitseraamistikus osalevad organisatsioonid järgivad põhimõtteid ka tegelikult ([79]). Eelkõige teeb ta juhuvaliku meetodil välja valitud organisatsioonide pistelisi kontrolle, samuti teatavate organisatsioonide *ad hoc* pistelisi kontrolle, kui on tuvastatud võimalikud vastavusprobleemid (nt kolmandad isikud on teatanud neist kaubandusministeeriumile), et kontrollida, kas i) kaebusi ja andmesubjekti taotlusi menetlevad kontaktpunktid on kättesaadavad ja valmis nõu andma; ii) organisatsiooni privaatsustingimused on hõlpsasti kättesaadavad nii tema veebisaidil kui ka kaubandusministeeriumi veebisaidile viiva hüperlingi kaudu; iii) organisatsiooni privaatsustingimused vastavad jätkuvalt kinnitamise nõuetele ja iv) organisatsioonide valitud sõltumatu vaidluste lahendamise mehhanism on kaebuste käsitlemiseks kättesaadav ([80]).

(54) Kui on usaldusväärseid tõendeid selle kohta, et organisatsioon ei täida oma kohustusi, mis tulenevad ELi-USA andmekaitseraamistikust (sealhulgas juhul, kui kaubandusministeeriumile esitatakse kaebus või kui organisatsioon ei anna kaubandusministeeriumi päringutele rahuldavat vastust), nõuab kaubandusministeerium, et organisatsioon täidaks ja esitaks üksikasjaliku küsimustiku ([81]). Organisatsiooniga, kes ei vasta küsimustikule rahuldavalt ja õigel ajal, hakkab võimalike täitemeetmete võtmiseks tegelema asjaomane asutus (föderaalne kaubanduskomisjon või transpordiministeerium) ([82]). Andmekaitseraamistiku Privacy Shield raames tehtud nõuetele vastavuse järelevalves tegi kaubandusministeerium korrapäraselt põhjenduses 53 nimetatud pistelisi kontrolle ja jälgis pidevalt avalikke

([74]) III lisa, joonealune märkus 2.
([75]) Vt III lisa jagu „Kinnitamise nõuetele vastavuse kontroll".
([76]) Teave andmekaitseraamistikuga ühinenute nimekirja kohta on esitatud III lisas (vt jao „Andmekaitseraamistiku programmi haldamine ja järelevalve kaubandusministeeriumi poolt" sissejuhatus) ja I lisas (I jao punkt 3, I jao punkt 4, III jao punkti 6 alapunkt d ja III jao punkti 11 alapunkt g).
([77]) III lisa, vt jao „Andmekaitseraamistiku programmi haldamine ja järelevalve kaubandusministeeriumi poolt" sissejuhatus.
([78]) Vt III lisa jagu „Andmekaitseraamistiku veebisaidi kohandamine sihtrühmade jaoks".
([79]) Vt III lisa jagu „Perioodilised omaalgatuslikud vastavuskontrollid ning andmekaitseraamistiku programmi hindamised".
([80]) Järelevalvetegevuses võib kaubandusministeerium kasutada erinevaid vahendeid, sealhulgas privaatsustingimuste katkiste viitelinkide kontrollimiseks või uudiste jälgimiseks, et leida teateid, mis annavad usaldusväärseid tõendeid mittevastavuse kohta.
([81]) Vt III lisa jagu „Perioodilised omaalgatuslikud vastavuskontrollid ning andmekaitseraamistiku programmi hindamised".
([82]) Vt III lisa jagu „Perioodilised omaalgatuslikud vastavuskontrollid ning andmekaitseraamistiku programmi hindamised".

teateid, mis võimaldas tal vastavusprobleeme tuvastada, käsitleda ja lahendada ([83]). Organisatsioonid, kes ei ole püsivalt põhimõtteid järginud, kustutatakse andmekaitseraamistikuga ühinenute nimekirjast ning nad peavad tagastama või kustutama isikuandmed, mille nad on raamistiku alusel saanud ([84]).

(55) Muudel nimekirjast kustutamise juhtudel, näiteks vabatahtliku lahkumise või korduskinnituse esitamata jätmise korral, peab organisatsioon andmed kas kustutama või tagastama või ta võib selliseid andmeid säilitada, kui ta kinnitab kaubandusministeeriumile igal aastal põhimõtetest kinnipidamist või tagab isikuandmetele asjakohase kaitse teiste lubatud meetoditega (näiteks kasutades lepingut, mis sisaldab komisjoni heaks kiidetud asjakohastes lepingu tüüptingimustes ette nähtud nõudeid täies ulatuses) ([85]). Sel juhul peab organisatsioon määrama ka oma organisatsioonis kontaktpunkti kõigi ELi-USA andmekaitseraamistikuga seotud küsimuste käsitlemiseks.

2.3.3. ***Osalemise kohta esitatud valeväidete kindlakstegemine ja nende suhtes meetmete võtmine***

(56) Kaubandusministeerium jälgib nii omal algatusel kui ka kaebuste alusel (nt andmekaitseasutustelt saadud kaebused) kõiki ELi-USA andmekaitseraamistikus osalemise kohta esitatud valeväiteid või andmekaitseraamistikule vastavust kinnitava tähise ebaõiget kasutamist ([86]). Eelkõige kontrollib kaubandusministeerium pidevalt, kas organisatsioonid, kes i) loobuvad ELi-USA andmekaitseraamistikus osalemisest, ii) ei vii lõpule iga-aastast korduskinnitamist (st organisatsioon kas alustas, kuid ei viinud iga-aastase korduskinnitamise protsessi õigel ajal lõpule, või isegi ei alustanud iga-aastase korduskinnitamise protsessi), iii) on osalejate hulgast eemaldatud, eelkõige „püsiva põhimõtete järgimata jätmise“ tõttu, või iv) põhimõtete järgimise algse kinnituse esitamata jätmise tõttu (st organisatsioon alustas, kuid ei viinud algse kinnitamise protsessi õigel ajal lõpule), eemaldavad kõigist asjakohastest avaldatud privaatsustingimustest viited ELi-USA andmekaitseraamistikule, mis osutavad sellele, et organisatsioon osaleb aktiivselt raamistikus ([87]). Kaubandusministeerium teeb ka interneti-otsinguid, et tuvastada organisatsioonide privaatsustingimustes viiteid ELi-USA andmekaitseraamistikule, sealhulgas selleks, et tuvastada selliste organisatsioonide esitatud valeväiteid, kes ei ole kunagi ELi-USA andmekaitseraamistikus osalenud ([88]).

(57) Kui kaubandusministeerium leiab, et viiteid ELi-USA andmekaitseraamistikule ei ole eemaldatud või neid kasutatakse valesti, teavitab ta organisatsiooni asja võimalikust edastamisest föderaalsele kaubanduskomisjonile või transpordiministeeriumile ([89]). Kui organisatsioon ei anna rahuldavat vastust, edastab kaubandusministeerium asja võimalike täitemeetmete võtmiseks asjaomasele asutusele ([90]). Kui organisatsioon esitab avalikkusele kas eksitavate väidete või tavade vormis valeandmeid põhimõtete järgimise kohta, võib föderaalne kaubanduskomisjon, transpordiministeerium või muu USA asjaomane täitevasutus võtta täitemeetmeid. Kaubandusministeeriumile valeandmete esitamise korral võidakse võtta täitemeetmeid valeandmete seaduse (False Statements Act, USA seadustiku 18. jaotise § 1001) alusel.

([83]) Andmekaitseraamistiku Privacy Shield teise iga-aastase läbivaatamise ajal teatas kaubandusministeerium, et kontrollis pisteliselt 100 organisatsiooni ja saatis 21 juhul nõuetele vastavuse küsimustikud (misjärel tuvastatud puudused parandati), vt komisjoni talituste töödokument SWD (2018) 497 final, lk 9. Samuti teatas kaubandusministeerium andmekaitseraamistiku Privacy Shield kolmandal iga-aastasel läbivaatamisel, et ta oli avalike teadete jälgimise abil avastanud kolm juhtumit ja võtnud kasutusele tava kontrollida iga kuu pisteliselt 30 ettevõtjat, mille tulemusel võeti vastavusküsimustikke kasutades järelmeetmeid 28 %-l juhtudest (misjärel avastatud probleemid viivitamata kõrvaldati ja kolmel juhul lahendati need pärast hoiatuskirja saamist), vt komisjoni talituse töödokument SWD (2019) 495 final, lk 8.

([84]) I lisa III jao punkti 11 alapunkt g. Püsiva põhimõtete järgimata jätmisega on tegemist eelkõige siis, kui organisatsioon keeldub täitmast eraelu puutumatuse iseregulatsiooni asutuse, sõltumatu vaidluste lahendamise organi või täitevasutuse lõplikku otsust.

([85]) I lisa III jao punkti 6 alapunkt f.

([86]) III lisa jagu „Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine“.

([87]) *Samas*.

([88]) *Samas*.

([89]) *Samas*.

([90]) Andmekaitseraamistiku Privacy Shield raames teatas kaubandusministeerium raamistiku kolmandal iga-aastasel läbivaatamisel, et oli tuvastanud osalemise kohta 669 valeväidet (2018. aasta oktoobrist 2019. aasta oktoobrini), millest enamik lahendati pärast kaubandusministeeriumi hoiatuskirja, 143 juhtumit anti üle föderaalsele kaubanduskomisjonile (vt põhjendus 62 allpool). Vt komisjoni talituste töödokument SWD(2019) 495 final, lk 10.

2.3.4. ***Täitmise tagamine***

(58) Selleks et tagada andmekaitse piisav tase ka praktikas, peaks olema loodud sõltumatu järelevalveasutus, millele on antud volitused jälgida vastavust andmekaitsenormidele ja tagada nende täitmine.

(59) ELi-USA andmekaitseraamistikus osalevad organisatsioonid peavad olema põhimõtete tõhusaks täitmiseks vajalike uurimis- ja täitmisvolitustega USA pädevate asutuste – föderaalse kaubanduskomisjoni ja transpordiministeeriumi – jurisdiktsiooni all ([91]).

(60) Föderaalne kaubanduskomisjon on sõltumatu asutus, mis koosneb viiest volinikust, kelle nimetab ametisse president USA Senati soovitusel ja nõusolekul ([92]). Volinikud nimetatakse ametisse seitsmeks aastaks ja president võib nad tagasi kutsuda vaid ebatõhususe, kohustuste täitmata jätmise või ametialaste rikkumiste tõttu. Föderaalses kaubanduskomisjonis võib olla kuni kolm volinikku samast parteist ja oma ametiajal ei tohi volinikud tegeleda muu äri-, kutse- või töise tegevusega.

(61) Föderaalne kaubanduskomisjon võib uurida põhimõtete järgimist, samuti valeväiteid põhimõtetest kinnipidamise või ELi-USA andmekaitseraamistikus osalemise kohta, mida esitavad organisatsioonid, kes ei ole enam andmekaitseraamistikuga ühinenute nimekirjas või ei ole kunagi põhimõtete järgimise kinnitust esitanudki ([93]). Föderaalne kaubanduskomisjon saab täitmist tagada, taotledes ajutiste või püsivate ettekirjutuste või muude õiguskaitsevahendite saamiseks haldus- või föderaalkohtult määrusi (sealhulgas kokkuleppemäärusi (*consent order*) kokkuleppemenetluse kaudu) ([94]) ning jälgib selliste kohtumääruste täitmist süstemaatiliselt ([95]). Kui organisatsioon selliseid kohtumäärusi ei täida, võib föderaalne kaubanduskomisjon taotleda tsiviilõiguslike sanktsioonide ja muude õiguskaitsevahendite rakendamist, sealhulgas ebaseadusliku tegevusega põhjustatud kahju suhtes. Iga ELi-USA andmekaitseraamistikus osalevale organisatsioonile väljastatav kokkuleppemäärus peab sisaldama aruandlussätteid ([96]) ja organisatsioonid peavad avalikustama föderaalsele kaubanduskomisjonile esitatavate vastavus- või hindamisaruannete asjakohased osad, mis käsitlevad ELi-USA andmekaitseraamistikku. Peale selle peab föderaalne kaubanduskomisjon internetis nimekirja organisatsioonidest, kellele föderaalne kaubanduskomisjon või kohtud on teinud ELi-USA andmekaitseraamistikuga seotud asjades ettekirjutusi või andnud määrusi ([97]).

(62) Seoses andmekaitseraamistikuga Privacy Shield võttis föderaalne kaubanduskomisjon täitemeetmeid ligikaudu 22 juhul, nii raamistiku konkreetsete nõuete rikkumise tõttu (nt suutmatus kinnitada kaubanduskomisjonile, et organisatsioon jätkab andmekaitseraamistiku Privacy Shield kaitsemeetmete rakendamist ka pärast raamistikust lahkumist, suutmatus kontrollida enesehindamise või välise vastavuskontrolli abil, kas organisatsioon järgis raamistikku) ([98]) kui ka valeväidete tõttu raamistikus osalemise kohta (nt organisatsioonid, kes ei viinud põhimõtete järgimise kinnitamiseks vajalikke samme lõpule või lasid oma kinnitusel aeguda, kuid lõid eksliku mulje, et osalevad jätkuvalt raamistikus) ([99]). Nende täitemeetmete tulemused tulenesid muu hulgas halduslike korralduste ennetavast kasutamisest, et saada teatavatelt andmekaitseraamistiku Privacy Shield osalejatelt materjale, et kontrollida, kas andmekaitseraamistikuga Privacy Shield seotud kohustusi on oluliselt rikutud ([100]).

([91]) ELi-USA andmekaitseraamistikus osalev organisatsioon peab avalikult deklareerima võetud kohustust põhimõtteid järgida, tegema kooskõlas kõnealuste põhimõtetega avalikuks oma privaatsustingimused ja rakendama neid täielikult. Nende järgimata jätmise korral saab võtta täitemeetmeid föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission (FTC) Act) paragrahvi 5 alusel, millega keelatakse äritegevuses või äritegevust mõjutav ebaõiglane tegevus ja pettus (USA seadustiku 15. jaotise § 45), ning USA seadustiku 49. jaotise § 41712 alusel, millega keelatakse vedajal või piletimüüjal rakendada lennutranspordis või lennutranspordi müügis ebaõiglasi või pettusel põhinevaid tavasid.

([92]) USA seadustiku 15. jaotise § 41.

([93]) IV lisa.

([94]) Föderaalselt kaubanduskomisjonilt saadud teabe alusel ei ole tal õigust teha eraelu puutumatuse kaitse valdkonnas 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.

([95]) Vt IV lisa jagu „Määruste taotlemine ja seire“.

([96]) Föderaalse kaubanduskomisjoni ettekirjutuse või kohtu määrusega võidakse kohustada ettevõtjaid rakendama eraelu puutumatuse programme ja tegema föderaalsele kaubanduskomisjonile korrapäraselt kättesaadavaks vastavusaruanded või sõltumatud hinnangud nende programmide kohta.

([97]) IV lisa jagu „Määruste taotlemine ja seire“.

([98]) Komisjoni talituste töödokument SWD(2019) 495 final, lk 11.

([99]) Vt föderaalse kaubanduskomisjoni veebisaidil loetletud juhtumid, mis on kättesaadavad aadressil https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Vt ka komisjoni talituste töödokument SWD(2017) 344 final, lk 17; komisjoni talituste töödokument SWD (2018) 497 final, lk 12 ja komisjoni talituste töödokument SWD (2019) 495 final, lk 11.

([100]) Vt nt esimees Joseph Simonsi koostatud märkused andmekaitseraamistiku Privacy Shield teisel iga-aastasel läbivaatamisel Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

(63) Üldisemalt on föderaalne kaubanduskomisjon võtnud viimastel aastatel täitemeetmeid mitmes juhtumis, mis on seotud vastavusega teatavatele andmekaitsenõuetele, mis on sätestatud ka ELi-USA andmekaitseraamistikus, nt eesmärgi piiramise ja andmete säilitamise, ([101]) võimalikult väheste andmete kogumise, ([102]) andmeturbe ([103]) ning andmete täpsuse ([104]) põhimõtte kohta.

(64) Transpordiministeeriumil on ainuõigus reguleerida lennuettevõtjate eraelu puutumatuse tavasid ja lennutranspordi müügis jagab ta piletimüügiagentide eraelu puutumatuse tavade suhtes pädevust föderaalse kaubanduskomisjoniga. Transpordiministeeriumi ametnike esmane eesmärk on jõuda kokkuleppele ja kui see ei ole võimalik, võivad nad algatada täitemenetluse, mis hõlmab tõenduslikku ärakuulamist transpordiministeeriumi halduskohtus, millel on õigus teha keelustamiskorraldusi ja määrata tsiviiltrahve ([105]). Halduskohtu kohtunikele on nende sõltumatuse ja erapooletuse tagamiseks kehtestatud haldusmenetluse seadusega (Administrative Procedure Act (APA)) mitu kaitsemeedet. Näiteks võib neid vallandada ainult mõjuval põhjusel; neile määratakse juhtumeid rotatsiooni korras; nad ei tohi täita ülesandeid, mis on vastuolus nende ülesannete ja kohustustega halduskohtunikuna; nende suhtes ei kohaldata neid palganud asutuse (antud juhul transpordiministeeriumi) uurimisrühma järelevalvet ning nad peavad täitma oma otsustus-/täitmisülesandeid erapooletult ([106]). Transpordiministeerium on kohustunud täitekorraldusi täitma ja tagama, et ELi-USA andmekaitseraamistiku juhtumitega korraldused on tema veebisaidil kättesaadavad ([107]).

2.4. **Õiguskaitse**

(65) Piisava kaitse tagamiseks ja eelkõige üksikisiku õiguste täitmise tagamiseks tuleks andmesubjektile tagada tõhus haldus- ja õiguskaitse, sealhulgas kahju hüvitamine.

(66) ELi-USA andmekaitseraamistiku *kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte* kohaselt peavad organisatsioonid nägema ette kaebuste menetlemise mehhanismi isikutele, keda põhimõtete järgimata jätmine mõjutab, ja seega võimaluse liidu andmesubjektidele esitada kaebusi seoses ELi-USA andmekaitseraamistikus osalevate organisatsioonide nõuetele mittevastavusega ning et saada neile kaebustele lahendus, vajaduse korral tõhusat õiguskaitset pakkuva otsusega ([108]). Osana põhimõtete järgimise kinnitamisest peavad organisatsioonid vastama selle põhimõtte nõuetele, nähes ette kergesti kättesaadavad sõltumatud kaebuste menetlemise mehhanismid, mille abil iga üksikisiku kaebusi ja vaidlusi uuritakse ja need lahendatakse tulemuslikult, mis toimub üksikisiku jaoks tasuta ([109]).

([101]) Vt nt föderaalse kaubanduskomisjoni korraldus juhtumis Drizly, LLC., millega muu hulgas nõutakse, et ettevõtja 1) hävitaks kõik kogutud isikuandmed, mis ei ole tarbijatele toodete või teenuste pakkumiseks vajalikud, 2) hoiduks isikuandmete kogumisest või säilitamisest, välja arvatud juhul, kui see on vajalik säilitamiskavas kirjeldatud erieesmärkidel.

([102]) Vt nt föderaalse kaubanduskomisjoni korraldus juhtumis CafePress (24. märts 2022), millega muu hulgas nõutakse kogutavate andmete hulga vähendamist.

([103]) Vt nt föderaalse kaubanduskomisjoni täitemeetmed juhtumites Drizzly, LLC ja CafePress, kus föderaalne kaubanduskomisjon nõudis asjaomastelt ettevõtjatelt spetsiaalse turvaprogrammi või spetsiifiliste turvameetmete kehtestamist. Andmetega seotud rikkumiste kohta vt lisaks ka föderaalse kaubanduskomisjoni 27. jaanuari 2023. aasta korraldus juhtumis Cheggis, kus 2019. aastal saavutati kokkulepe Equifaxiga (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Vt nt juhtum RealPage, Inc. (16. oktoober 2018), kus föderaalne kaubanduskomisjon võttis õiglase krediidiinfo seaduse alusel täitemeetmeid üürnike taustauuringuid tegeva ettevõtja vastu, kes esitas kinnisvaraomanikele ja kinnisvarahaldusettevõtjatele üksikisikute kohta taustauuringuid, kasutades selleks varasemaid üürimakseid käsitlevaid andmeid, avalike registrite teavet (sealhulgas karistusregister ja registreeritud väljatõstmised) ja krediiditeavet, mida kasutati tegurina eluaseme saamise tingimustele vastavuse kindlakstegemisel. Föderaalne kaubanduskomisjon leidis, et ettevõtja ei võtnud mõistlikke meetmeid oma automatiseeritud otsuste tegemise vahendi alusel esitatud teabe täpsuse tagamiseks.

([105]) Vt V lisa jagu „Täitmise tagamise tavad“.

([106]) Vt USA seadustiku 5. jaotise § 3105, § 7521 punkt a, § 554 punkt d ja § 556 punkti b alapunkt 3.

([107]) V lisa, vt jagu „ELi-USA andmekaitseraamistiku rikkumistega seotud täitekorralduste seire ja avalikustamine“.

([108]) I lisa II jao punkt 7.

([109]) I lisa III jao punkt 11.

(67) Organisatsioonid võivad valida kas liidus või Ameerika Ühendriikides paiknevad sõltumatud kaebuste menetlemise mehhanismid. Nagu põhjenduses 73 täpsemalt selgitatud, on võimalus võtta vabatahtlikult kohustus teha koostööd ELi andmekaitseasutustega. Kui organisatsioonid töötlevad personaliandmeid, on ELi andmekaitseasutustega koostöö tegemise kohustuse võtmine kohustuslik. Muud võimalused on sõltumatu alternatiivne vaidluste lahendamine või erasektori välja töötatud eraelu puutumatuse programmid, mille normide hulka on lisatud andmekaitseraamistiku põhimõtted. Programmid peavad kooskõlas *kaebuste menetlemise, nõuete täitmise tagamise ja vastutuse põhimõtte* nõuetega hõlmama tõhusaid nõuete täitmise tagamise mehhanisme.

(68) Seega annab ELi-USA andmekaitseraamistik andmesubjektidele mitu võimalust oma õiguste kaitsmiseks, ELi-USA andmekaitseraamistikus osalevate organisatsioonide nõuetele mittevastavuse kohta kaebuste esitamiseks ning neile kaebustele lahenduse saamiseks, vajaduse korral tõhusat õiguskaitset pakkuva otsusega. Üksikisikud võivad esitada oma kaebuse otse organisatsioonile, organisatsiooni osutatud sõltumatule vaidluste lahendamise organile, riiklikele andmekaitseasutustele, kaubandusministeeriumile või föderaalsele kaubanduskomisjonile. Juhul kui ühegi sellise kaebuste menetlemise või nõuete täitmise tagamise mehhanismi abil kaebusele lahendust ei leita, on üksikisikutel samuti õigus algatada siduv vahekohtumenetlus (käesoleva otsuse I lisa I 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 vahekohtu kolleegium, kus menetluse algatamise eeltingimuseks on teatavate õiguskaitsevahendite ammendumine.

(69) Esiteks võivad liidu andmesubjektid esitada kaebuse põhimõtete järgimata jätmise kohta ELi-USA andmekaitseraamistikus osalevatele organisatsioonidele otse ([110]). Selliste kaebuste lahendamise soodustamiseks peab organisatsioon nende menetlemiseks kehtestama tõhusa õiguskaitsemehhanismi. Organisatsiooni privaatsustingimustes tuleb seega esitada üksikisikutele selge teave, mis käsitleb kas organisatsioonisisest või -välist kontaktpunkti, mille kaudu kaebusi käsitletakse (selleks võib olla ka liidu ükskõik milline asjakohane asutus, kes on pädev järelepärimistele või kaebustele vastama), ning määratud sõltumatut vaidluste lahendamise organit (vt põhjendus 70). Üksikisiku kaebuse saamisel kas otse üksikisikult või kaubandusministeeriumilt, kellele andmekaitseasutus on selle edastanud, peab organisatsioon esitama liidu andmesubjektile vastuse 45 päeva jooksul ([111]). Samuti peavad organisatsioonid kiiresti vastama päringutele ja muudele teabenõuetele, mille on põhimõtete järgimise kohta esitanud kaubandusministeerium või andmekaitseasutus ([112]) (juhul kui organisatsioon on kohustunud andmekaitseasutusega koostööd tegema).

(70) 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 sisutühjad) ning osutab üksikisikutele tasuta vajalikku abi ([113]). Karistused ja heastamismeetmed, mida selline organ määrab, peavad olema piisavalt ranged, et tagada organisatsioonide vastavus põhimõtetele, ja nendega tuleks ette näha, et organisatsioon heastab mittevastavuse mõju, ning olenevalt olukorrast asjaomaste andmete töötlemise lõpetamine ja/või nende kustutamine, samuti avastatud põhimõtete järgimata jätmise avalikustamine ([114]). Organisatsiooni määratud sõltumatud vaidluste lahendamise organid peavad oma veebisaidil esitama asjakohase teabe ELi-USA andmekaitseraamistiku ja teenuste kohta, mida nad selle raames osutavad ([115]). Igal aastal peavad nad avaldama nende vaidluste lahendamise teenuse kohta koondstatistikat sisaldava aruande ([116]).

([110]) I lisa III jao punkti 11 alapunkti d alapunkt i.
([111]) I lisa III jao punkti 11 alapunkti d alapunkt i.
([112]) Selle menetleva asutuse määrab andmekaitseasutuste kolleegium, mis on ette nähtud täiendava põhimõttega „Andmekaitseasutuste roll“ (I lisa III jao punkt 5).
([113]) I lisa III jao punkti 11 alapunkt d.
([114]) I lisa II jao punkt 7 ja III jao punkti 11 alapunkt e.
([115]) I lisa III jao punkti 11 alapunkti d alapunkt ii.
([116]) Aastaaruanne peab sisaldama järgmist: 1) aruandeaastal seoses ELi-USA andmekaitseraamistikuga laekunud kaebuste koguarv; 2) laekunud kaebuste liigid; 3) vaidluste lahendamise kvaliteedinäitajad, näiteks kaebuste menetlemise aeg, ja 4) kaebuste lahendamise tulemused, eelkõige kohaldatud õiguskaitsevahendite ja sanktsioonide arv ning liigid.

(71) Osana oma vastavuskontrollimeetmetest võib kaubandusministeerium kontrollida, kas ELi-USA andmekaitseraamistikus osalevad organisatsioonid on ka tegelikkuses registreerinud end nende sõltumatute kaebuste menetlemise mehhanismide juures, mille juures registreerumist nad kinnitavad ([117]). Nii organisatsioonid kui ka vastutavad sõltumatud kaebuste menetlemise mehhanismid peavad kiiresti reageerima kaubandusministeeriumi päringutele ja nõuetele esitada ELi-USA andmekaitseraamistikuga seotud teavet. Kaubandusministeerium teeb koostööd sõltumatute kaebuste menetlemise mehhanismidega, et kontrollida, kas nende veebisaitidel on esitatud teave põhimõtete ja teenuste kohta, mida nad ELi-USA andmekaitseraamistikuga seoses pakuvad, ning et nad avaldavad aastaaruandeid ([118]).

(72) Kui organisatsioon ei täida vaidluste lahendamise või iseregulatsiooniorgani otsust, peab nimetatud organ teavitama sellest kaubandusministeeriumit ja föderaalset kaubanduskomisjoni (või muud USA ametiasutust, kellel on pädevus organisatsiooni nõuetele mittevastavust uurida) või pädevat kohut ([119]). Kui organisatsioon keeldub järgimast mis tahes eraelu puutumatuse iseregulatsiooni-, sõltumatu vaidluste lahendamise või valitsusorgani lõplikku otsust või kui selline organ otsustab, et organisatsioon ei ole korduvalt põhimõtteid järginud, võidakse see lugeda püsivaks põhimõtete järgimata jätmiseks ning kaubandusministeerium kustutab põhimõtteid mittejärginud organisatsiooni andmekaitseraamistikuga ühinenute nimekirjast, teatades sellest kõigepealt 30 päeva ette ja andes organisatsioonile võimaluse vastata ([120]). Kui organisatsioon väidab pärast nimekirjast kustutamist jätkuvalt, et ta tegutseb kooskõlas ELi-USA andmekaitseraamistiku põhimõtetega, edastab kaubandusministeerium asja föderaalsele kaubanduskomisjonile või muule täitevasutusele ([121]).

(73) Kolmandaks võivad üksikisikud esitada oma kaebuse ka liidus asuvale riiklikule andmekaitseasutusele, kes võib kasutada oma uurimis- ja õiguskaitsevolitusi määruse (EL) 2016/679 kohaselt. Organisatsioonidel on kohustus andmekaitseasutuse läbiviidaval uurimisel ja kaebuse lahendamisel koostööd teha, kui kaebus on seotud töösuhte raames kogutud personaliandmete töötlemisega või kui nad on vabatahtlikult nõustunud järelevalveasutuste järelevalvele alluma ([122]). Eelkõige peavad organisatsioonid vastama päringutele, täitma andmekaitseasutuse soovitusi, sealhulgas heastamis- ja hüvitamismeetmete kohta, ning andmekaitseasutusele kirjalikult kinnitama, et nimetatud meetmed on võetud ([123]). Kui andmekaitseasutuse nõuandeid ei järgita, edastab andmekaitseasutus sellised juhtumid kaubandusministeeriumile (kes võib organisatsioonid ELi-USA andmekaitseraamistikuga ühinenute nimekirjast kustutada) või võimalike täitemeetmete võtmiseks föderaalsele kaubanduskomisjonile või transpordiministeeriumile (andmekaitseasutustega koostöö tegemisest keeldumine või põhimõtete järgimata jätmine on USA õiguse alusel karistatav) ([124]).

(74) Selleks et hõlbustada kaebuste tõhusaks menetlemiseks tehtavat koostööd, on nii kaubandusministeerium kui ka föderaalne kaubanduskomisjon loonud spetsiaalse kontaktpunkti, mis vastutab andmekaitseasutustega otse suhtlemise eest ([125]). Need kontaktpunktid abistavad andmekaitseasutust päringutega organisatsiooni põhimõtete järgimise kohta.

(75) Andmekaitseasutuste nõuanded ([126]) väljastatakse pärast seda, kui kummalgi vaidluse poolel on olnud mõistlik võimalus esitada selgitused ja soovitud tõendid. Kolleegium võib saata nõuande nii kiiresti, kui nõuetekohase menetluse nõue võimaldab, üldjuhul 60 päeva jooksul alates kaebuse saamisest ([127]). Kui organisatsioon ei järgi nõuannet 25 päeva jooksul pärast selle saamist ning ei ole viivitust rahuldavalt põhjendanud, võib kolleegium teavitada oma kavatsusest suunata küsimus föderaalsele kaubanduskomisjonile (või muule USA pädevale

([117]) I lisa jagu „Kinnitamise nõuetele vastavuse kontroll".
([118]) Vt III lisa jagu „Koostöö hõlbustamine alternatiivse vaidluste lahendamise organitega, kes pakuvad põhimõtetega seotud teenuseid". Vt ka I lisa III jao punkt 11 alapunkti d alapunktid ii–iii.
([119]) Vt I lisa III jao punkti 11 alapunkt e.
([120]) Vt I lisa III jao punkti 11 alapunkt g, eriti selle alapunktid ii ja iii.
([121]) Vt III lisa jagu „Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine".
([122]) I lisa II jao punkti 7 alapunkt b.
([123]) I lisa III jao punkt 5.
([124]) I lisa III jao punkti 5 alapunkti c alapunkt ii.
([125]) III lisa (vt jagu „Andmekaitseasutustega tehtava koostöö hõlbustamine") ja IV lisa (vt jaod „Taotluse prioriseerimine ja uurimine" ning „Täitmise tagamise alane koostöö ELi andmekaitseasutustega").
([126]) Mitteametliku andmekaitseasutuste kolleegiumi töökorra peaksid kehtestama andmekaitseasutused vastavalt oma pädevusele oma töö korraldamisel ja omavahelises koostöös.
([127]) I lisa III jao punkti 5 alapunkti c alapunkt i.

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 ([128]). Teisel juhul teavitab kolleegium kaubandusministeeriumi, kes käsitab organisatsiooni keeldumist andmekaitseasutuste kolleegiumi nõuannet järgida püsiva järgimata jätmisena, mis toob kaasa organisatsiooni kustutamise andmekaitseraamistikuga ühinenute nimekirjast.

(76) Kui andmekaitseasutus, kellele kaebus on adresseeritud, ei ole kaebuse lahendamisega tegelenud või on seda teinud ebapiisavalt, on üksikisikust kaebuse esitajal võimalus vaidlustada nimetatud tegevus või tegevusetus vastava ELi liikmesriigi riiklikes kohtutes.

(77) Andmekaitseasutustele võivad kaebusi esitada ka üksikisikud, isegi kui organisatsioon ei ole määranud oma vaidluste lahendamise organiks andmekaitseasutuste kolleegiumi. Sellistel juhtudel võib andmekaitseasutus edastada kaebused kas kaubandusministeeriumile või föderaalsele kaubanduskomisjonile. Koostöö soodustamiseks ja elavdamiseks üksikisikute kaebuste ja ELi-USA andmekaitseraamistikus osalevate organisatsioonide poolse põhimõtete järgimata jätmise valdkonnas loob kaubandusministeerium spetsiaalse kontaktpunkti, kes peab sidet ja osutab andmekaitseasutustele abi organisatsioonide põhimõtetele vastavuse uurimisel ([129]). Ka föderaalne kaubanduskomisjon on võtnud kohustuse luua spetsiaalne kontaktpunkt ([130]).

(78) Neljandaks on kaubandusministeerium kohustunud võtma vastu, vaatama läbi ja püüdma parimal võimalikul viisil lahendada kaebusi põhimõtete järgimata jätmise kohta organisatsioonides ([131]). Selleks näeb kaubandusministeerium andmekaitseasutustele ette erikorra kaebuste edastamiseks spetsiaalsele kontaktpunktile, nende jälgimiseks ja organisatsioonidega suhtlemiseks, et lahendamisele kaasa aidata ([132]). Selleks et üksikisikute kaebuste menetlemist kiirendada, teeb kontaktpunkt vastavusküsimustes koostööd otse vastava andmekaitseasutusega ning eelkõige hoiab teda kursis kaebuste seisuga kuni 90 päeva jooksul nende esitamisest ([133]). See võimaldab andmesubjektidel esitada kaebusi ELi-USA andmekaitseraamistikus osalevate organisatsioonide mittevastavuse kohta otse oma riiklikule andmekaitseasutusele ja lasta saata need kaubandusministeeriumile kui ELi-USA andmekaitseraamistikku haldavale USA asutusele.

(79) Kui kaubandusministeerium omaalgatuslike kontrollide, kaebuste või muu teabe alusel leiab, et organisatsioon ei ole põhimõtteid püsivalt järginud, kustutab ta selle organisatsiooni andmekaitseraamistikuga ühinenute nimekirjast ([134]). Püsivaks põhimõtete järgimata jätmiseks loetakse ka eraelu puutumatuse iseregulatsiooni organi, sõltumatu vaidluste lahendamise organi või valitsusasutuse, sealhulgas andmekaitseasutuse lõpliku otsuse täitmisest keeldumist ([135]).

(80) Viiendaks peab ELi-USA andmekaitseraamistikus osalev organisatsioon olema põhimõtete tõhusaks täitmiseks vajalike uurimis- ja täitmisvolitustega asutuste, eelkõige föderaalse kaubanduskomisjoni ([136]) jurisdiktsiooni all. Föderaalne kaubanduskomisjon vaatab eelisjärjekorras läbi esildised, mille on põhimõtetele mittevastavuse kohta edastanud sõltumatud vaidluste lahendamise organid või iseregulatsiooniorganid, kaubandusministeerium ja andmekaitseasutused (omal algatusel või kaebuste põhjal), et teha kindlaks, kas föderaalse kaubanduskomisjoni seaduse (FTC Act) paragrahvi 5 on rikutud ([137]). Föderaalne kaubanduskomisjon on võtnud kohustuse luua esildiste käsitlemise standardmenetlus, luua andmekaitseasutuste edastatud esildiste jaoks asutusesisene kontaktpunkt ning vahetada tehtud esildistega seotud teavet. Lisaks võib ta kaebusi vastu võtta ka otse üksikisikutelt ning kohustub omal algatusel läbi viima ELi-USA andmekaitseraamistikuga seotud uurimisi, eelkõige eraelu puutumatuse kaitse küsimustega seotud laiema uurimise raames.

([128]) I lisa III jao punkti 5 alapunkti c alapunkt ii.
([129]) Vt III lisa jagu „Andmekaitseasutustega tehtava koostöö hõlbustamine“.
([130]) Vt IV lisa jaod „Taotluse prioriseerimine ja uurimine“ ning „Täitmise tagamise alane koostöö ELi andmekaitseasutustega“.
([131]) III lisa, vt nt jagu „Andmekaitseasutustega tehtava koostöö hõlbustamine“.
([132]) I lisa II jao punkti 7 alapunkt e ja III lisa jagu „Andmekaitseasutustega tehtava koostöö hõlbustamine“.
([133]) *Samas*.
([134]) I lisa III jao punkti 11 alapunkt g.
([135]) I lisa III jao punkti 11 alapunkt g.
([136]) ELi-USA andmekaitseraamistikus osalev organisatsioon peab avalikult deklareerima võetud kohustust põhimõtteid järgida, tegema kooskõlas kõnealuste põhimõtetega avalikuks oma privaatsustingimused ja rakendama neid täielikult. Järgimata jätmise korral saab võtta täitemeetmeid föderaalse kaubanduskomisjoni seaduse (FTC Act) paragrahvi 5 alusel, millega keelatakse äritegevuses või äritegevust mõjutav ebaõiglane tegevus ja pettus.
([137]) Vt ka transpordiministeeriumi võetud sarnased kohustused V lisas.

(81) Kuuendaks võib liidu andmesubjekt viimase võimalusena, juhul kui ükski muu ettenähtud õiguskaitsevahend ei ole üksikisiku kaebusele rahuldavat lahendust toonud, algatada siduva vahekohtumenetluse ELi-USA andmekaitseraamistiku kolleegiumis ([138]). Organisatsioonid peavad teavitama üksikisikuid võimalusest algatada vahekohtumenetlus ning neil on vastamiskohustus, kui üksikisik on nimetatud võimalust kasutanud ja esitanud asjaomasele organisatsioonile sellekohase teate ([139]).

(82) ELi-USA andmekaitseraamistiku kolleegium koosneb vähemalt kümnest vahekohtunikust, kelle määravad ametisse kaubandusministeerium ja Euroopa Komisjon lähtuvalt nende sõltumatusest, aususest ja kogemustest USA eraelu puutumatuse kaitse õiguse ja liidu andmekaitseõiguse alal. Iga vaidluse jaoks valivad pooled nimekirjast kolleegiumi ühe kuni kolm ([140]) vahekohtunikku.

(83) Kaubandusministeerium valis vahekohtumenetlusi haldama vaidluste lahendamise rahvusvahelise keskuse (International Centre for Dispute Resolution (ICDR)), mis on USA vahekohtute assotsiatsiooni (American Arbitration Association (AAA)) rahvusvaheline osakond. ELi-USA andmekaitseraamistiku kolleegiumi menetlusi reguleerivad kokkulepitud vahekohtureeglid ja ametisse nimetatud vahekohtunike käitumisjuhend. ICDR-AAA veebisait pakub üksikisikutele selget ja kokkuvõtlikku teavet vahekohtumenetluse ja vahekohtusse pöördumise menetluse kohta.

(84) Kaubandusministeeriumi ja komisjoni vahel kokku lepitud vahekohtureeglid täiendavad ELi-USA andmekaitseraamistikku, mis sisaldab mitut funktsiooni, mis parandavad liidu andmesubjektide juurdepääsu sellele mehhanismile: i) kolleegiumi jaoks nõude ettevalmistamisel võib andmesubjekti abistada tema riiklik andmekaitseasutus; ii) kuigi vahekohut peetakse Ameerika Ühendriikides, võivad liidu andmesubjektid otsustada osaleda video- või telefonikonverentsi teel, mida üksikisikule võimaldatakse tasuta; iii) kuigi vahekohtus kasutatakse üldjuhul inglise keelt, tagatakse vahekohtu istungil suuline tõlge ja kirjalikku tõlget pakutakse põhimõtteliselt siis, kui esitatakse põhjendatud taotlus, ja see on andmesubjektile tasuta; iv) kuigi kumbki pool peab kandma oma advokaaditasud ise, haldab kaubandusministeerium fondi, kuhu teevad igal aastal sissemakseid ELi-USA andmekaitseraamistikus osalevad organisatsioonid, kes peavad katma vahekohtumenetluse kulud maksimaalse summani, mille määravad kindlaks USA ametiasutused, konsulteerides komisjoniga ([141]).

(85) ELi-USA andmekaitseraamistiku kolleegiumil on õigus kehtestada „konkreetsele isikule sobivad asjakohased mitterahalised kaitsemeetmed“, ([142]) mis on vajalikud põhimõte järgimata jätmise heastamiseks. Kuigi kolleegium võtab otsustamisel arvesse ka teisi heastamismeetmeid, mis on ELi-USA andmekaitseraamistiku muude mehhanismide raames juba määratud, võivad üksikisikud siiski pöörduda vahekohtusse, kui nad peavad kõnealuseid muid heastamismeetmeid ebapiisavaks. See võimaldab liidu andmesubjektidel pöörduda vahekohtusse kõigil juhtudel, kus ELi-USA andmekaitseraamistikus osalevate organisatsioonide, sõltumatute kaebuste menetlemise mehhanismide või USA pädevate asutuste (näiteks föderaalse kaubanduskomisjoni) tegevus või tegevusetus ei ole toonud nende kaebustele rahuldavat lahendust. Vahekohtumenetlust ei või algatada, kui andmekaitseasutus ise on ELi-USA andmekaitseraamistikus osaleva organisatsiooni suhtes õiguslikult pädev kõnealust küsimust lahendama, nimelt siis, kui organisatsioon on kohustatud tegema andmekaitseasutustega 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 ettevõtja otsust ei täida.

([138]) Vt I lisa I lisa „Vahekohtumudel“.
([139]) Vt I lisa II jao punkti 1 alapunkti a alapunkt xi ja II jao punkti 7 alapunkt c.
([140]) Kolleegiumi moodustavate vahekohtunike arvu peavad kokku leppima vaidluse pooled.
([141]) I lisa I lisa, G jao punkt 6.
([142]) Üksikisikud ei saa vahekohtus kahjunõudeid esitada, ent vahekohtusse pöördumine ei mõjuta võimalust nõuda kahju hüvitamist USA tavakohtute kaudu.

(86) Seitsmendaks, kui organisatsioon ei täida oma kohustust järgida põhimõtteid ja avaldada privaatsustingimused, on USA õiguse kohaselt kättesaadavad täiendavad õiguskaitsevahendid, sealhulgas kahju hüvitamiseks. Näiteks võivad üksikisikud teatud tingimustel saada osariigi tarbijakaitseseaduste alusel kohtulikku õiguskaitset (sealhulgas kahju hüvitamine) valeandmete esitamise, ebaõiglaste ja pettusel põhinevate teguviiside ja tavade korral ([143]) ning lepinguvälist vastutust käsitlevate õigusnormide kohaselt (eelkõige eraellu sekkumise, ([144]) nime või sarnasuse omastamise ([145]) ning isiklike andmete avalikustamisega seotud rikkumiste korral ([146])).

(87) Eespool kirjeldatud erinevad õiguskaitsevahendid üheskoos tagavad, et iga kaebus, mis käsitleb ELi-USA andmekaitseraamistiku järgimist kinnitanud organisatsioonide mittevastavust andmekaitseraamistikule, lahendatakse ja heastatakse tõhusalt.

3. JUURDEPÄÄS EUROOPA LIIDUST EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE AMEERIKA ÜHENDRIIKIDES ASUVATE AVALIKU SEKTORI ASUTUSTE POOLT

(88) Komisjon on hinnanud ka piiranguid ja kaitsemeetmeid, sealhulgas Ameerika Ühendriikide õiguses kättesaadavaid järelevalve- ja individuaalse kaitse mehhanisme seoses USA avaliku sektori asutuste poolt avalikus huvis selliste isikuandmete kogumise ja järgneva kasutamisega, mida edastatakse Ameerika Ühendriikides asuvatele vastutavatele töötlejatele ja volitatud töötlejatele, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil (edaspidi „valitsuse juurdepääs“) ([147]). Selle hindamisel, kas tingimused, mille alusel pääseb valitsus juurde käesoleva otsuse alusel Ameerika Ühendriikidesse edastatud andmetele, vastavad määruse (EL) 2016/679 artikli 45 lõike 1 kohasele sisulise samaväärsuse kriteeriumile, nagu Euroopa Kohus on tõlgendanud põhiõiguste hartat silmas pidades, võttis komisjon arvesse mitut kriteeriumi.

(89) Eelkõige peavad kõik isikuandmete kaitse õiguse piirangud olema seadusega ette nähtud ja asjaomase õiguse piirangu ulatus peab olema määratletud sellise õiguse riivet võimaldavas õiguslikus aluses ([148]). Lisaks peab selles õiguslikus aluses olema selleks, et täita proportsionaalsuse nõuet, mille kohaselt tuleb erandeid ja piiranguid isikuandmete kaitsest kohaldada ainult niivõrd, kuivõrd see on demokraatlikus ühiskonnas vältimatult vajalik, et saavutada konkreetsed üldist huvi pakkuvad eesmärgid, mis on samaväärsed liidu tunnustatud eesmärkidega, sätestatud selged ja täpsed eeskirjad, mis reguleerivad kõnealuste meetmete ulatust ja kohaldamist, ning kehtestatud minimaalsed kaitsemeetmed, et isikutel, kelle andmeid on edastatud, oleksid piisavad tagatised oma isikuandmete tõhusaks kaitsmiseks kuritarvitamise riski eest ([149]). Samuti peavad need normid ja kaitsemeetmed olema õiguslikult siduvad

([143]) Vt nt osariigi tarbijakaitseseadused Californias (Cal. Civ. Code § 1750–1785 (West) Consumers Legal Remedies Act); Columbia ringkonnas (D.C. Code § 28–3901); Floridas (Fla. Stat. § 501.201–501.213, Deceptive and Unfair Trade Practices Act); Illinois's (815 Ill. Comp. Stat. 505/1–505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvanias (73 Pa. Stat. Ann. § 201-1–201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

([144]) St isiku eraasjadesse või probleemidesse tahtliku sekkumise korral viisil, mis oleks mõistlikule isikule väga solvav (Restatement (2nd) of Torts, § 652(b)).

([145]) Sellise õigusrikkumisega on tavaliselt tegemist üksikisiku nime või sarnasuse omastamise ja kasutamise korral ettevõtte või toote reklaamimiseks või mõnel sarnasel ärilisel eesmärgil (vt Restatement (2nd) of Torts, § 652C).

([146]) St kui üksikisiku eraelu puudutav teave avalikustatakse, kui see on mõistlikule isikule väga solvav ning see ei toimu avalikkuse seaduslikes huvides (Restatement (2nd) of Torts, § 652D).

([147]) See on asjakohane ka I lisa I jao punkti 5 seisukohast. Selle jao kohaselt ja sarnaselt isikuandmete kaitse üldmäärusega võivad eraelu puutumatuse põhimõtete hulka kuuluvate andmekaitsenõuete ja õiguste järgimise suhtes kehtida piirangud. Sellised piirangud ei ole aga absoluutsed, neile saab tugineda üksnes mitme tingimuse täitmise korral, näiteks ulatuses, mis on vajalik kohtumääruse täitmiseks või avaliku huvi, õiguskaitsega või riigi julgeolekuga seotud vajaduste täitmiseks. Selles kontekstis ja selguse huvides viidatakse käesolevas jaos ka korralduses EO 14086 sätestatud tingimustele, mida analüüsitakse muu hulgas põhjendustes 127–141.

([148]) Vt otsus kohtuasjas Schrems II, punktid 174–175 ja seal viidatud kohtupraktika. Vt ka liikmesriikide ametiasutuste juurdepääsu kohta kohtuasjas C-623/17, Privacy International, ECLI:EU:C:2020:790, punkt 65 ning otsus liidetud kohtuasjades C-511/18, C-512/18 ja C-520/18: La Quadrature du Net jt, ECLI:EU:C:2020:791, punkt 175.

([149]) Vt Schrems II, punktid 176 ja 181 ja seal viidatud kohtupraktika. Vt liikmesriikide ametiasutuste juurdepääsu kohta ka Privacy International, punkt 68 ja La Quadrature du Net jt, punkt 132.

ja üksikisikutele hagetavad ([150]). Eelkõige peab andmesubjektidel olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada ([151]).

3.1. **Juurdepääs andmetele ja andmete kasutamine USA avaliku sektori asutuste poolt kriminaalõiguskaitse eesmärkidel**

(90) Mis puudutab ELi-USA andmekaitseraamistiku alusel edastatud isikuandmete riivet kriminaalõiguskaitse eesmärkidel, on Ameerika Ühendriikide õiguses sätestatud isikuandmetele juurdepääsule ja nende kasutamisele mitu piirangut ning ette nähtud järelevalve- ja kahju hüvitamise mehhanismid, mis on kooskõlas käesoleva otsuse põhjenduses 89 osutatud nõuetega. Tingimusi, mille alusel selline juurdepääs võib toimuda, ja nende volituste kasutamisel kohaldatavaid kaitsemeetmeid hinnatakse üksikasjalikult järgmistes jagudes. Sellega seoses on USA valitsus (justiitsministeeriumi kaudu) esitanud kinnitavad avaldused ka kohaldatavate piirangute ja kaitsemeetmete kohta (käesoleva otsuse VI lisa).

3.1.1. ***Õiguslikud alused, piirangud ja kaitsemeetmed***

3.1.1.1. *Piirangud ja kaitsemeetmed seoses isikuandmete kogumisega kriminaalõiguskaitse eesmärkidel*

(91) Isikuandmetele, mida töötlevad põhimõtete järgimist kinnitanud USA organisatsioonid ja mis edastatakse liidust ELi-USA andmekaitseraamistiku alusel, võivad kriminaalõiguskaitse eesmärkidel juurde pääseda USA föderaalprokurörid ja föderaalse uurimisasutuse ametnikud erinevate menetluste alusel, nagu on üksikasjalikumalt selgitatud põhjendustes 92–99. Neid menetlusi kohaldatakse samamoodi, kui teavet saadakse mis tahes USA organisatsioonilt, olenemata asjaomaste andmesubjektide kodakondsusest või elukohast ([152]).

(92) Esiteks võib kohtunik föderaalse õiguskaitseasutuse ametniku või valitsuse advokaadi taotlusel anda välja läbiotsimis- või arestimismääruse (sealhulgas elektrooniliselt salvestatud teabe kohta) ([153]). Sellise määruse võib välja anda ainult siis, kui on küllaldane alus ([154]) arvata, et tõenäoliselt leitakse määruses osutatud kohast „arestitavaid esemeid“ (tõendid kuriteo kohta, ebaseaduslikult saadud esemed või vara, mida kavatsetakse kasutada või on kasutatud kuriteo toimepanemiseks). Määruses tuleb kindlaks määrata arestitav vara või ese ja märkida, millisele kohtunikule tuleb määrus tagastada. Isik, kelle suhtes läbiotsimist kohaldatakse või kelle vara läbi otsitakse, võib

([150]) Vt *Schrems II*, punktid 181–182.

([151]) Vt Schrems I, punkt 95 ja Schrems II, punkt 194. Sellega seoses on Euroopa Kohus eelkõige rõhutanud, et põhiõiguste harta artikli 47 järgimisel, mis tagab õiguse tõhusale õiguskaitsevahendile sõltumatus ja erapooletus kohtus, „on oma osa liidus nõutava kaitse taseme kujundamisel [ja] mille järgimise peab komisjon olema tuvastanud enne, kui ta saab vastu võtta otsuse määruse (EL) 2016/679 artikli 45 lõike 1 alusel“ (Schrems II, punkt 186).

([152]) Vt VI lisa. Vt näiteks pealtkuulamise seaduse (Wiretap Act), salvestatud sideandmete seaduse (Stored Communications Act) ja valitud telefoninumbrite salvestamise seaduse (Pen Register Act) kohta (üksikasjalikumalt käsitletud põhjendustes 95–98), Suzlon Energy Ltd *vs.* Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

([153]) Kriminaalmenetluse föderaaleeskirja (Federal Rules of Criminal Procedure) eeskiri 41. 2018. aasta otsuses kinnitas Ülemkohus, et õiguskaitseorganid vajavad läbiotsimismäärust või määruse erandit ka selleks, et pääseda juurde mobiilside varasematele asukohaandmetele, mis annavad igakülgse ülevaate kasutaja liikumisest, ja et kasutajal võib olla sellise teabe suhtes põhjendatud ootus eraelu puutumatusele (Timothy Ivory Carpenter *vs.* United States of America, nr 16–402, 585 U.S. (2018)). Seetõttu ei saa üldjuhul selliseid andmeid mobiilsideettevõtjatelt kohtumäärusega, mis tugineb põhjendatud kahtlusel, et teave on käimasoleva kriminaaluurimise seisukohast asjakohane ja oluline, vaid vaja on kasutada määrust, mis näitab küllaldase aluse olemasolu.

([154]) Ülemkohtu sõnul on „küllaldane alus“ „praktiline, mittetehniline“ standard, mis tugineb „igapäevaelu faktilistele ja praktilistele kaalutlustele, mille alusel mõistlikud ja kaalutletud inimesed […] tegutsevad“ (Illinois *vs.* Gates, 462 U.S. 213, 232 (1983)). Mis puudutab läbiotsimismäärust, siis on küllaldane alus olemas siis, kui on olemas piisav tõenäosus, et läbiotsimise tulemusel leitakse tõendeid kuriteo kohta.

võtta meetmeid, et ebaseadusliku otsimise teel saadud tõendusmaterjal loetaks kehtetuks, kui need tõendid esitatakse selle isiku vastu kriminaalmenetluses ([155]). Kui andmete valdaja (nt ettevõtja) on määruse alusel kohustatud andmed avalikustama, võib ta vaidlustada avalikustamise nõude kui põhjendamatult koormava ([156]).

(93) Teiseks võib vandemeeste kogu (*grand jury* ehk kohtuniku või kohtu-uurija kokku pandud uurimisorgan) väljastada teatavate raskete kuritegude uurimise kontekstis, ([157]) tavaliselt föderaalprokuröri taotlusel, kohtukorralduse, millega nõuda kelleltki äridokumentide, elektrooniliselt salvestatud teabe või muude materiaalsete esemed esitamist või kättesaadavaks tegemist. Lisaks on mitme põhimäärusega lubatud kasutada halduslikke korraldusi, et esitataks või tehtaks kättesaadavaks äridokumendid, elektrooniliselt säilitatud andmed või muud materiaalsed esemed uurimistes, mis hõlmavad tervishoiupettust, lapse väärkohtlemist, salateenistuse (Secret Service) kaitset, kontrollitavate ainete juhtumeid ning peainspektori uurimisi ([158]). Mõlemal juhul peab teave olema uurimise seisukohast asjakohane ja kohtukorraldus ei tohi olla ebamõistlik selle laia ulatuse või rõhuva või koormava laadi tõttu (ja kohtukorralduse saaja võib seda nendel põhjustel vaidlustada) ([159]).

(94) USA ettevõtjate valduses olevatele andmetele tsiviil- või regulatiivsetel eesmärkidel („avalikes huvides“) juurdepääsuks antavate halduslike korralduste tingimused on sellele väga sarnased. Tsiviil- ja regulatiivsete kohustustega asutuste volitused selliseid halduslikke korraldusi välja anda peavad olema sätestatud põhikirjas. Haldusliku korralduse kasutamist tuleb hinnata nn mõistlikkuse testiga, mille kohaselt on nõutav, et uurimine viidaks läbi õiguspärasel eesmärgil, haldusliku korraldusega nõutav teave on selle eesmärgi jaoks asjakohane, asutusel ei ole veel seda teavet, mida ta haldusliku korralduse abil soovib saada, ja haldusliku korralduse väljastamiseks vajalikud haldustoimingud on tehtud ([160]). Ülemkohtu praktikas on selgitatud ka vajadust saavutada tasakaal taotletava teabe avaliku huvi aspekti tähtsuse ning isiklike ja organisatsiooniliste eraelu puutumatuse kaitsega seotud huvide tähtsuse vahel ([161]). Kuigi haldusliku korralduse kasutamiseks ei ole vaja kohtu eelnevat heakskiitu, vaatab kohus selle läbi juhul, kui korralduse saaja selle eespool nimetatud põhjustel vaidlustab või kui korralduse väljastanud asutus soovib selle kohtu kaudu täitmisele pöörata ([162]). Lisaks neile üldistele piirangutele võivad eri põhimäärustest tuleneda (rangemad) erinõuded ([163]).

([155]) Mapp *vs.* Ohio, 367 U.S. 643 (1961).

([156]) Vt *vastus Ameerika Ühendriikide taotlusele*, 610 F.2d 1148, 1157 (3. Cir. 1979) (kus on öeldud, et „nõuetekohase menetluse jaoks on vajalik koormavuse küsimuse ärakuulamine, enne kui sundida telefoniettevõtet andmeid esitama“, kasutades selleks läbiotsimismäärust) ja *vastus Ameerika Ühendriikide taotlusele*, 616 F.2d 1122 (9th Cir. 1980).

([157]) USA põhiseaduse viienda paranduse kohaselt on nõutav, et mis tahes „raske või muidu alatu kuriteo eest“ esitab süüdistuse vandemeeste kogu. Vandemeeste kogu koosneb 16–23 liikmest ja otsustab, kas on küllaldane alus arvata, et toime on pandud kuritegu. Sellele järeldusele jõudmiseks on vandemeeste kogule antud uurimisvolitused, mis võimaldavad väljastada kohtukorraldusi.

([158]) Vt VI lisa.

([159]) Kriminaalmenetluse föderaaleeskirja (Federal Rules of Criminal Procedure) eeskiri 17.

([160]) Ameerika Ühendriigid *vs.* Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co. *vs.* Walling, 327 U.S. 186 (1946).

([162]) Ülemkohus on selgitanud, et halduslikku korralduse vaidlustamise korral peab kohus kaaluma, kas 1) uurimise eesmärk on seaduslik, 2) asjaomase halduslikku korralduse väljastanud asutus kuulub kongressi võimkonda ning 3) „taotletavad dokumendid on uurimise jaoks asjakohased“. Kohus märkis ka, et haldusliku korralduse nõue peab olema „mõistlik“, st nõutakse, et „esitatavate dokumentide täpsustus oleks asjaomase uurimise jaoks piisav, kuid mitte ülemäärane“, sealhulgas „läbiotsitava koha ning isikute või arestitavate esemete täpne kirjeldus“.

([163]) Näiteks annab finantspuutumatuse õiguse seadus (Right to Financial Privacy Act) valitsusasutusele õiguse saada halduslikku korralduse alusel finantsasutuse valduses olevad finantsdokumendid enda kätte ainult siis, kui 1) on põhjust arvata, et taotletavad dokumendid on seotud õiguspärase õiguskaitsealase uurimisega ja 2) kliendile on esitatud korralduse või kohtukutse koopia koos teatega, milles uurimise laadi on mõistliku täpsusega kirjeldatud (USA seadustiku 12. jaotise § 3405). Teine näide on õiglase krediidiaruandluse seadus (Fair Credit Reporting Act), mis keelab krediidiinfoasutustel avalikustada andmeid tarbijate kohta vastuseks halduslikku korralduse nõudele (ja lubab neil vastata ainult vandemeeste kogu korralduse nõuetele või kohtumäärustele, USA seadustiku 15. jaotise § 1681 jj). Sideteabele juurdepääsu, sealhulgas halduslike korralduste kasutamise võimaluse suhtes kehtivad salvestatud sideandmete seaduse erinõuded (vt üksikasjalik ülevaade põhjendustes 96–97).

(95) Kolmandaks võimaldavad mitu õiguslikku alust kriminaalõiguskaitseasutustel saada juurdepääsu sideandmetele. Kohus võib anda määruse, millega lubatakse koguda (pealtkuulamisseadmete abil) telefoninumbri või e-posti kohta reaalajas muid kui sisuandmeid seoses helistamise, marsruutimise, suunamise ja signaaliteabega, kui ta leiab, et asutus on tõendanud, et tõenäoliselt saadav teave on poolelioleva kriminaaluurimise jaoks asjakohane ([164]). Muu hulgas tuleb kohtumääruses täpsustada kahtlustatav isik, kui see on teada; sidevahendid, mille kohta määrus käib, ja märge süüteo kohta, millega kogutav teave on seotud. Pealtkuulamisseadme kasutamise loa võib anda kuni kuuekümneks päevaks, mida võib pikendada ainult uue kohtumäärusega.

(96) Lisaks võib salvestatud side seaduse alusel saada kriminaalõiguse täitmise eesmärgil juurdepääsu internetiteenuse osutajate, telefoniteenuse osutajate ja muude kolmandatest isikutest teenuseosutajate valduses olevatele abonendiandmetele, liiklusandmetele ja salvestatud andmesisule ([165]). Selleks et saada oma valdusse elektroonilise side salvestatud sisu, peavad kriminaalõiguskaitseasutused põhimõtteliselt saama kohtunikult määruse, mis põhineb küllaldasel alusel arvata, et asjaomasel kontol on tõendusmaterjal kuriteo kohta ([166]). Abonendi registreerimise andmete, IP-aadresside ja seotud ajatemplite ning arveldusandmete jaoks võivad kriminaalõiguskaitseasutused kasutada kohtukorraldust. Enamiku muude salvestatud ilma sisuta andmete (nt teemareata e-kirja päised) jaoks peab kriminaalõiguskaitseasutus saama kohtumääruse, mis väljastatakse, kui kohtunik on veendunud, et on alust arvata, et nõutav teave on käimasoleva kriminaaluurimise jaoks asjakohane ja oluline.

(97) Teenuseosutajad, kes saavad päringuid salvestatud side seaduse alusel, võivad vabatahtlikult teavitada klienti või abonenti, kelle teavet saada soovitakse, välja arvatud juhul, kui asjaomane kriminaalõiguskaitseasutus saab kaitsemääruse, millega selline teavitamine keelatakse ([167]). Selline kaitsemäärus on kohtumäärus, millega nõutakse, et elektroonilise side teenuste või kaugandmetöötlusteenuste osutaja, kellele määrus, kohtukorraldus või kohtumäärus on adresseeritud, ei teavitaks teisi isikuid määruse, kohtukorralduse või kohtumääruse olemasolust enne, kuni kohus seda vajalikuks peab. Kaitsemäärus väljastatakse, kui kohus leiab, et on alust arvata, et teavitamine ohustaks tõsiselt uurimist või viivitaks põhjendamatult kohtuprotsessi, nt seetõttu, et see tooks kaasa üksikisiku elu või füüsilise turvalisuse ohtu seadmise, kohtumõistmise eest põgenemise, võimalike tunnistajate hirmutamise jne. Asejustiitsministri memorandumiga (mis on siduv kõigile justiitsministeeriumi advokaatidele ja esindajatele) nõutakse, et prokurörid teeksid üksikasjaliku otsuse kaitsemääruse vajaduse kohta ja esitaksid kohtule põhjenduse selle kohta, kuidas on konkreetses juhtumis täidetud kaitsemääruse saamise seaduslikud kriteeriumid ([168]). Memorandum nõuab ka seda, et üldjuhul ei tohi kaitsemääruse taotlusega nõutada teavitamise edasilükkamist enam kui üheks aastaks. Kui erandjuhtudel võivad osutuda vajalikuks pikemaajalised määrused, võib selliseid määrusi taotleda ainult USA peaprokuröri või vastava justiitsministri abi määratud järelevalveametniku kirjalikul nõusolekul. Lisaks peab prokurör uurimise lõpus viivitamatult hindama, kas on alust jätta väljastatud kaitsemäärused kehtima, ning kui see nii ei ole, lõpetama kaitsemääruse kehtivuse ja tagama, et sellest teavitatakse teenuseosutajat ([169]).

([164]) USA seadustiku 18. jaotise § 3123.

([165]) USA seadustiku 18. jaotise § 2701–2713.

([166]) USA seadustiku 18. jaotise § 2701 punktide a–b alapunkti 1 alapunkt A. Kui asjaomast abonenti või klienti teavitatakse (kas ette või teatavatel juhtudel tagantjärele), võib kauem kui 180 päeva säilitatavaid sisuandmeid hankida ka halduslikku korralduse või vandemeeste kogu korralduse alusel (USA seadustiku 18. jaotise § 2701 punkti b alapunkti 1 alapunkt B või kohtumääruse alusel (kui on põhjendatud alust arvata, et teave on käimasoleva kriminaaluurimise jaoks asjakohane ja oluline (USA seadustiku 18. jaotise § 2701 punkt d). Samas föderaalse apellatsioonikohtu otsuse kohaselt saavad valitsuse alluvuses töötavad uurijad üldjuhul kohtunikelt läbiotsimismääruse, et koguda kommertssideteenuse osutajalt erasuhtluse sisu või talletatud andmeid. United States *vs.* Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) USA seadustiku 18. jaotise § 2705 punkt b.

([168]) Vt asejustiitsministri Rod Rosensteini 19. oktoobril 2017 välja antud memorandum kaitsemäärusi (või mitteavaldamise määrusi) piirava poliitika kohta, kättesaadav aadressil https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Asejustiitsminister Lisa Moncao 27. mail 2022 välja antud memorandum kaitsemääruse taotlemise lisatingimuste kohta kaitsemääruste taotlemisel vastavalt USA seadustikule (USA seadustiku 18. jaotise § 2705 punkt b).

(98) Ka võivad kriminaalõiguskaitseasutused kuulata reaalajas pealt telefonikõnesid, vestlusi või elektroonilist teabevahetust kohtumääruse alusel, milles kohtunik leiab muu hulgas, et on olemas küllaldane alus arvata, et telefoni või elektrooniline pealtkuulamine annab tõendusmaterjali föderaalse kuriteo kohta või süüdistuse eest põgeneva tagaotsitava isiku asukoha kohta ([170]).

(99) Täiendavat kaitset pakuvad justiitsministeeriumi erinevad põhimõtted ja suunised, sealhulgas justiitsministri suunised riigisiseste FBI operatsioonide kohta (AGG-DOM), milles on muu hulgas nõue, et föderaalne juurdlusbüroo (FBI) kasutaks võimalikult vähe sekkuvaid uurimismeetodeid, võttes arvesse mõju eraelu puutumatusele ja kodanikuvabadustele ([171]).

(100) USA valitsuse kinnituste kohaselt kohaldatakse eespool kirjeldatud samaväärset või tugevamat kaitset ka (osariikide seaduste alusel toimuvatele) osariikide õiguskaitseorganite uurimistele ([172]). Eelkõige kinnitavad põhiseaduse sätted, samuti osariigi tasandi põhimäärused ja kohtupraktika eespool nimetatud kaitsemeetmeid põhjendamatute läbiotsimiste ja arestimiste vastu nõudega, et väljastada tuleb läbiotsimismäärus ([173]). Sarnaselt föderaaltasandil pakutava kaitsega võib läbiotsimismääruse välja anda ainult küllaldase aluse tõendamise korral ning määruses tuleb kirjeldada läbiotsitavat kohta ja isikut või arestitavad eset ([174]).

([170]) USA seadustiku 18. jaotise § 2510–2522.

([171]) Justiitsministri suunised FBI riigisiseste operatsioonide kohta „Domestic Federal Bureau of Investigation (FBI) Operations“ (september 2008), kättesaadav aadressil http://www.justice.gov/archive/opa/docs/guidelines.pdf. Lisanormid ja meetmed, millega on ette nähtud piirangud föderaalprokuröride uurimisalasele tegevusele, on kehtestatud Ameerika Ühendriikide prokuröride juhendis (United States Attorneys' Manual), kättesaadav aadressil http://www.justice.gov/usam/united-states-attorneys-manual. Nendest suunistest kõrvale kaldumiseks tuleb saada eelnev heakskiit FBI direktorilt, asedirektorilt või direktori nimetatud tegevdirektori abilt, välja arvatud juhul, kui sellist heakskiitu ei ole võimalik saada vahetu ohu tõttu inimeste või vara ohutusele või riiklikule julgeolekule (sel juhul tuleb direktorit või muud volitusi andvat isikut võimalikult kiiresti teavitada). Kui suuniseid ei järgita, peab FBI sellest teatama justiitsministeeriumile, kes omakorda teavitab justiitsministrit ja asejustiitsministrit.

([172]) VI lisa, joonealune märkus 2. Vt ka nt Arnold *vs.* City of Cleveland, 67 Ohio St.3d 35, 616 NE2d 163, 169 (1993) („Üksikisikute õiguste ja kodanikuvabaduste valdkonnas näevad Ameerika Ühendriikide põhiseaduse sätted, kui need on kohaldatavad osariikide suhtes, ette alumise piiri, millest allapoole ei tohi osariigi kohtu otsused minna“); Cooper *vs.* California, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) („Mõistagi ei mõjuta meie seisukoht osariigi õigust kehtestada soovi korral läbiotsimistele ja arestimistele kõrgemaid standardeid, kui seda nõuab föderaalne põhiseadus.“); Petersen *vs.* City of Mesa, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Kuigi Arizona põhiseadusega võidakse kehtestada läbiotsimisele ja arestimisele rangemad standardid kui föderaalne põhiseadusega, ei saa Arizona kohtud pakkuda väiksemat kaitset, kui pakub neljas muudatus“).

([173]) Enamik osariike on neljandas muudatuses sätestatud kaitsemeetmed oma põhiseadusesse täpselt üle võtnud. Vt Alabama põhiseadus, artikkel I, § 5); Alaska põhiseadus, artikkel I, § 14; 1; Arkansase põhiseadus, artikkel II, § 15; California põhiseadus, artikkel I, § 13; Colorado põhiseadus, artikkel II, § 7; Connecticuti põhiseadus, artikkel I, § 7; Delaware'i põhiseadus, artikkel I, § 6; Florida põhiseadus, artikkel I, § 12; Georgia põhiseadus, artikkel I, § I, lõige XIII; Hawai põhiseadus, artikkel I, § 7; Idaho põhiseadus, artikkel I, § 17; Illinois' põhiseadus, artikkel I, § 6; Indiana põhiseadus, artikkel I, § 11; Iowa põhiseadus, artikkel I, § 8; Kansase põhiseadus, õiguste deklaratsioon Bill of Rights, § 15; Kentucky põhiseadus, § 10. Louisiana põhiseadus, artikkel I, § 5; Maine'i põhiseadus, artikkel I, § 5; Massachusetsi põhiseadus, õiguste deklaratsioon, artikkel 14; Michigani põhiseadus, artikkel I, § 11; Minnesota põhiseadus, artikkel I, § 10; Mississippi põhiseadus, artikkel III, § 23; Missouri põhiseadus, artikkel I, § 15; Montana põhiseadus, artikkel II, § 11; Nebraska põhiseadus, artikkel I, § 7; Nevada põhiseadus, artikkel I, § 18; New Hampshire' põhiseadus, 1. osa, artikkel 19; New Jersey põhiseadus, artikkel II, § 7; New Mexico põhiseadus, artikkel II, § 10; New Yorgi põhiseadus, artikkel I, § 12; Põhja-Dakota põhiseadus, artikkel I, § 8; Ohio põhiseadus, artikkel I, § 14; Oklahoma põhiseadus, artikkel II, § 30; Oregoni põhiseadus, artikkel I, § 9; Pennsylvania põhiseadus, artikkel I, § 8; Rhode Islandi põhiseadus, artikkel I, § 6; Lõuna-Carolina põhiseadus, artikkel I, § 10; Lõuna-Dakota põhiseadus, artikkel VI, § 11; Tennessee põhiseadus, artikkel I, § 7; Texase põhiseadus, artikkel I, § 9; Utah' põhiseadus, artikkel I, § 14; Vermonti põhiseadus, I peatükk, artikkel 11; Lääne-Virginia põhiseadus, artikkel III, § 6; Wisconsini põhiseadus, artikkel I, § 11; Wyomingi põhiseadus, artikkel I, § 4. Teised osariigid (nt Maryland, Põhja-Carolina ja Virginia) on oma põhiseaduses määruseid käsitlenud sellises erisõnastuses, mida kohtud on tõlgendanud nii, et see pakub neljanda muudatusega sarnast või kõrgemal tasemel kaitset (vt Marylandi õiguste deklaratsioon, artikkel 26; Põhja-Carolina põhiseadus, artikkel I, § 20; Virginia põhiseadus, artikkel I, § 10 ja asjakohane kohtupraktika, nt Hamel *vs.* State, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; State *vs.* Johnson, 861 S. E.2d 474, 483 (N.C. 2021) ning Lowe *vs.* Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)). Kõigele lisaks on Arizonal ja Washingtonil põhiseaduslikud sätted, mis kaitsevad eraelu puutumatust üldisemalt (Arizona põhiseadus, artikkel 2, § 8; Washingtoni põhiseadus, artikkel I, § 7), mida kohtud on tõlgendanud nii, et need pakuvad rohkem kaitset kui neljas muudatus (vt nt State *vs.* Bolt, 689 P.2d 519, 523 (Ariz. 1984), State *vs.* Ault, 759 P.2d 1320, 1324 (Ariz. 1988), State *vs.* Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , State *vs.* Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Vt nt California karistusseadustiku § 1524,3 punkt b; Alabama kriminaalmenetluse eeskirja reegel 3.6-3.13; punkt 10.79.035; Washingtoni läbivaadatud seadustik; Virginia kriminaalmenetluse seadustiku 5. peatüki jaotise 19.2 punkt 19.2-59.

3.1.1.2. *Kogutud teabe edasine kasutamine*

(101) Mis puudutab föderaalsete kriminaalõiguskaitseasutuste kogutud andmete edasist kasutamist, on erinevate põhimääruste, suuniste ja standarditega kehtestatud erikaitsemeetmed. Kui FBI tegevuse suhtes kohaldatavad eriõigusaktid (peaprokuröri suunised riigisiseste FBI operatsioonide kohta (AGG-DOM) ning FBI riigisiseste juurdluste ja operatsioonide juhend (Domestic Investigations and Operations Guide)) välja arvata, kehtivad selles jaos kirjeldatud nõuded üldiselt andmete edasisel kasutamisel mis tahes föderaalasutuse poolt, sealhulgas andmete puhul, millele on saadud juurdepääs tsiviil- või regulatiivsetel eesmärkidel. See hõlmab nõudeid, mis tulenevad juhtimis- ja eelarveosakonna (Office of Management and Budget (OMB)) memodest/määrustest, föderaalsest infoturbe juhtimise moderniseerimise seadusest (Federal Information Security Management Modernization Act), e-valitsuse seadusest (E-Government Act) ja föderaalregistrite seadusest (Federal Records Act).

(102) Kooskõlas Clinger-Coheni seaduses sätestatud volitustega (Clinger-Cohen Act; P.L. 104-106, Division E) ja 1987. aasta arvutiturbe seadusega (Computer Security Act of 1987; P.L. 100-235), saatis juhtimis- ja eelarveosakond (OMB) välja ringkirja nr A-130, et kehtestada üldised siduvad juhised, mis kehtivad kõigile föderaalasutustele (sealhulgas õiguskaitseasutustele), kui nad käitlevad isikuandmeid ([175]). Eelkõige on ringkirjas nõue, et kõik föderaalasutused „piirduksid isikuandmete loomisel, kogumisel, kasutamisel, töötlemisel, säilitamisel, hooldamisel, levitamisel ja avaldamisel seaduse alusel lubatud, volitatud asutuse ülesannete jaoks kohase ja mõistlikult vajalikuks peetava teabega“ ([176]). Lisaks peavad föderaalasutused nii suures ulatuses, kui on mõistlikult teostatav, tagama, et isikuandmed oleksid täpsed, asjakohased, õigeaegsed ja täielikud ning vähendatud asutuse ülesannete nõuetekohaseks täitmiseks vajaliku miinimumini. Üldisemalt peavad föderaalasutused looma tervikliku eraelu puutumatuse programmi, et tagada vastavus kohaldatavatele privaatsusnõuetele, töötada välja privaatsustingimused ja neid hinnata ning hallata privaatsusriske; hoidma töös menetlusi privaatsusnõuetega seotud intsidentide tuvastamiseks, dokumenteerimiseks ja nendest teatamiseks; töötama välja töötajatele ja töövõtjatele eraelu puutumatuse alase teadlikkuse suurendamise ja koolitusprogrammid ning kehtestama reeglid ja menetlused, millega tagatakse töötajate vastavus privaatsusnõutele ja -tingimustele ([177]).

(103) Lisaks nõuab e-valitsuse seadus (E-Government Act), ([178]) et kõik föderaalasutused (sealhulgas kriminaalõiguskaitseasutused) võtaksid kasutusele infoturbe kaitsemeetmed, mis on proportsionaalsed volitamata juurdepääsust, kasutamisest, avalikustamisest, häirest, muutmisest või hävitamisest tuleneva kahju ohu ja ulatusega; et neil oleks tööl infojuht, kes tagab infoturbe nõuete täitmise, ning igal aastal toimuks infoturbeprogrammi ja -tavade sõltumatu hindamine (mille teeb nt peainspektor, vt põhjendus 109) ([179]). Samamoodi on föderaalregistrite seaduse (Federal Records Act (FRA)) ([180]) ja täiendavate määruste ([181]) kohaselt nõutav rakendada föderaalasutuste valduses oleva teabe suhtes kaitsemeetmeid, mis tagavad teabe füüsilise terviklikkuse ja kaitsevad seda volitamata juurdepääsu eest.

(104) Kooskõlas oma föderaaltasandi õiguspädevusega, sealhulgas 2014. aasta föderaalse infoturbe moderniseerimise seadusega (Federal Information Security Modernisation Act), on OMB ja riiklik standardite ja tehnoloogia instituut (National Institute of Standards and Technologies (NIST)) välja töötanud standardid, mis on föderaalasutustele (sh kriminaalõiguskaitseasutustele) siduvad ja milles täpsustatakse teabeturbe miinimumnõudeid, mis tuleb kehtestada, sealhulgas juurdepääsu kontrolli meetmed, teadlikkuse ja koolituse tagamine, erandolukorra plaanimine, intsidentidele reageerimine, auditeerimis- ja aruandlusvahendid, süsteemi ja teabe terviklikkuse tagamine, eraelu puutumatuse ja turvalisuse riskide hindamine jne ([182]). Lisaks peavad kõik föderaalasutused

([175]) St „teave, mida saab kasutada üksikisiku identiteedi eristamiseks või jälgimiseks kas eraldi või koos muu teabega, mis on seotud või seostatav konkreetse isikuga“, vt OMB ringkiri nr A-130, lk 33 (isikuandmete määratlus).

([176]) OMB ringkiri nr A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information (Teabe haldamine kui strateegiline ressurss, II lisa. Isikuandmete haldamisega seotud kohustused), 81 Fed. Reg. 49,689 (28. juuli 2016), lk 17.

([177]) II liide, § 5 punktid a–h.

([178]) USA seadustiku 44. jaotise peatükk 36.

([179]) USA seadustiku 44. jaotise § 3544–3545.

([180]) FAC, USA seadustiku 44. jaotise § 3105.

([181]) CFRi 36. jaotise § 1228,150 jj, 1228,228 ning A liides.

([182]) Vt nt OMB ringkiri nr A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Infosüsteemide ja organisatsioonide turva- ja privaatsuskontroll) (10. detsember 2020) ning NIST, Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems (Föderaalsed teabetöötlusstandardid 200: föderaalsete teabe- ja infosüsteemide minimaalsed turbenõuded).

(sealhulgas kriminaalõiguskaitseasutused) kooskõlas OMB suunistega pidama ja rakendama andmetega seotud rikkumiste menetlemise kava, sealhulgas sellistele rikkumistele reageerimiseks ja kahjuriskide hindamiseks ([183]).

(105) Mis puudutab andmete säilitamist, siis on föderaalregistrite seaduses (FRA) ([184]) nõue, et USA föderaalasutused (sealhulgas kriminaalõiguskaitseasutused) kehtestaksid oma dokumentidele säilitamistähtajad (mille möödumisel tuleb dokumendid kõrvaldada), mille peab heaks kiitma Ameerika Ühendriikide rahvusarhiiv (National Archives and Records Administration) ([185]). Säilitamistähtaja pikkus määratakse kindlaks erinevate tegurite alusel, näiteks uurimise liik, see, kas tõendid on uurimise seisukohast endiselt asjakohased jne. FBI kohta on AGG-DOMis ette nähtud, et FBI-l peab selline dokumentide säilitamise kava paigas olema ja ta peab haldama süsteemi, mis võimaldab uurimiste seisu ja aluse viivitamatult teada saada.

(106) Peale selle sisaldab OMB ringkiri nr A-130 ka teatavaid nõudeid isikuandmete levitamise kohta. Põhimõtteliselt peab isikuandmete levitamine ja avalikustamine piirduma sellega, mis on seaduslikult lubatud, asjakohane ja asutuse ülesannete nõuetekohaseks täitmiseks mõistlikult vajalik ([186]). Kui USA föderaalasutused jagavad isikuandmeid teiste valitsusasutustega, peavad nad kehtestama vajaduse korral tingimused (sealhulgas konkreetsete turva- ja privaatsuskontrollimeetmete rakendamine), mis reguleerivad teabe töötlemist kirjalike lepingute kaudu (sh lepingud, andmete kasutamise kokkulepped, teabe vahetamise kokkulepped ja vastastikuse mõistmise memorandumid) ([187]). Mis puudutab põhjuseid, mille korral teavet levitada tohib, siis näiteks peaprokuröri suunistes riigisiseste FBI operatsioonide kohta ning FBI riigisiseste juurdluste ja operatsioonide juhendis ([188]) on ette nähtud, et FBI võib olla seadusega kohustatud seda tegema (nt rahvusvahelise lepingu alusel) või tal on lubatud teavet levitada teatavate asjaolude korral, nt teistele USA asutustele, kui avalikustamine on kooskõlas teabe kogumise eesmärgiga ja seostub nende kohustustega; kongressi komiteedele; välisriigi asutustele, kui teave on seotud nende kohustustega ja teabe levitamine on kooskõlas Ameerika Ühendriikide huvidega; teabe levitamine on eelkõige vajalik inimeste või vara ohutuse või turvalisuse kaitsmiseks või kuriteo või riigi julgeolekule tekkinud ohu eest kaitsmiseks või kuriteo või julgeolekuohu ärahoidmiseks ning avalikustamine on kooskõlas teabe kogumise eesmärgiga ([189]).

3.1.2. ***Järelevalve***

(107) Föderaalsete kriminaalõiguskaitseasutuste tegevust kontrollivad eri organid ([190]). Nagu on selgitatud põhjendustes 92–99, hõlmab see enamikul juhtudel eelkontrolli, mille teevad kohtunikud, kes peavad andmete kogumise üksikmeetmed enne nende kasutamist heaks kiitma. Lisaks jälgivad kriminaalõiguskaitseasutuste tegevuse eri etappe, sealhulgas isikuandmete kogumist ja töötlemist, teised organid. Üheskoos tagavad need kohtu- ja kohtuvälised organid, et õiguskaitseasutuste suhtes tehakse sõltumatut järelevalvet.

([183]) Memorandum 17-12, „Preparing for and Responding to a Breach of Personally Identifiable Information“ (Isikuandmete rikkumise vastu valmistumine ja sellele reageerimine), kättesaadav aadressil https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf ja OMB ringkiri nr A-130. Näiteks justiitsministeeriumi andmetega seotud rikkumistele reageerimise kord, vt https://www.justice.gov/file/4336/download.

([184]) FRA, USA seadustiku 44. jaotise § 3101 jj.

([185]) Ameerika Ühendriikide rahvusarhiivil on õigus hinnata asutuste dokumendihaldustavasid ja ta võib otsustada, kas teatavate dokumentide säilitamine on õigustatud (USA seadustiku 44. jaotise § 2904 punkt c, 2906).

([186]) OMB ringkiri nr A-130, jaotise 5.f.1 punkt d.

([187]) OMB ringkiri nr A-130, I liidese § 3 punkt d.

([188]) Vt ka FBI riigisiseste juurdluste ja operatsioonide juhendi (DIOG) 14. jaotis.

([189]) AGG-DOM, VI jao punktid B ja C; FBI riigisiseste juurdluste ja operatsioonide juhendi (DIOG) 14. jaotis.

([190]) Selles jaos nimetatud mehhanismid kehtivad ka siis, kui föderaalasutused koguvad ja kasutavad andmeid tsiviil- ja regulatiivsetel eesmärkidel. Föderaaltasandi tsiviil- ja reguleerivad asutused alluvad nende vastavate peainspektorite kontrollile ja kongressi järelevalvele, mida teevad muu hulgas valitsuse aruandluse eest vastutav amet (Government Accountability Office) ning kongressi auditi- ja uurimisasutus. Välja arvatud juhul, kui asutuses on ametis eraelu puutumatuse ja kodanikuvabaduste kaitse ametnik – ametikoht, mis on tavaliselt olemas sellistes asutustes nagu justiitsministeerium ja sisejulgeoleku ministeerium nende õiguskaitse- ja riikliku julgeolekuga seotud kohustuste tõttu –, on need ülesanded pandud asutuse eraelu kaitse vanemametnikule. Kõigil föderaalasutustel on seadusega sätestatud kohustus nimetada ametisse asutuse eraelu kaitse vanemametnik, kes vastutab selle eest, et asutus järgiks eraelu puutumatust käsitlevaid õigusakte, ja teeb seotud küsimuste üle järelevalvet. Vt nt OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

(108) Esiteks tegutsevad eri osakondades eraelu puutumatuse ja kodanikuvabaduste ametnikud, kellel on vastutus kriminaalõiguse täitmise eest ([191]). 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. Iga osakonna või asutuse juhid peavad tagama, et eraelu puutumatuse ja kodanikuvabaduste ametnikel on oma volituste täitmiseks vajalikud materjalid ja vahendid, neile antakse juurdepääs kõikidele ülesannete täitmiseks vajalikele materjalidele ja töötajatele ning et neid teavitatakse poliitika kavandatud muudatustest ning nendega konsulteeritakse ([192]). Privaatsus- ja kodanikuvabaduste ametnikud esitavad USA Kongressile korrapäraselt aruandeid, sealhulgas ministeeriumile/asutusele laekunud kaebuste arvu ja laadi kohta ning selliste kaebuste lahendamise kokkuvõtte ja korraldatud läbivaatamiste ja uurimiste ning ametniku tegevuse mõju kohta ([193]).

(109) Teiseks hoiab justiitsministeeriumi, sealhulgas FBI tegevusel silma peal sõltumatu peainspektor ([194]). Peainspektorid on seaduse järgi sõltumatud ([195]) ja nad vastutavad ministeeriumi programmide ja toimingute sõltumatu uurimise, auditite ja inspekteerimise eest. Neil on juurdepääs kõikidele andmetele, aruannetele, auditite, protokollidele, dokumentidele, poliitikamaterjalidele, soovitustele ja muudele materjalidele, vajaduse korral kohtukorralduse alusel, ning nad võivad võtta tunnistajatelt ütlusi ([196]). Ehkki peainspektorid annavad üksnes mittesiduvaid soovitusi parandusmeetmete võtmiseks, nende aruanded ja teave aruannete alusel võetud meetmete (või nende puudumise) ([197]) kohta üldiselt avalikustatakse ning saadetakse USA Kongressile, kes võib nende alusel ise järelevalvet teha (vt põhjendus 111) ([198]).

([191]) Vt USA seadustiku 42. jaotise § 2000ee-1. See hõlmab näiteks justiitsministeeriumi, sisejulgeoleku ministeeriumi ja FBI-d. Lisaks vastutab sisejulgeoleku ministeeriumis eraelu puutumatuse ametnik eraelu kaitse meetmete säilitamise ja tõhustamise ning läbipaistvuse edendamise eest ministeeriumis (USA seadustiku 6. jaotise § 142, paragrahv 222). Kõigi sisejulgeoleku ministeeriumi süsteemide, tehnoloogia, vormide ja programmide üle, millega kogutakse isikuandmeid või mis avaldavad mõju eraelu puutumatusele, teeb järelevalvet eraelu puutumatuse ametnik, kellel on juurdepääs kõikidele andmetele, aruannetele, auditite, protokollidele, dokumentidele, poliitikamaterjalidele, soovitustele ja muudele ministeeriumi käsutuses olevatele materjalidele, ja vajaduse korral kohtukorralduse alusel. Eraelu puutumatuse ametnik peab igal aastal kongressile aru andma ministeeriumi tegevusest, mis mõjutab eraelu puutumatust, sealhulgas kaebustest eraelu puutumatuse rikkumise kohta.

([192]) USA seadustiku 42. jaotise § 2000ee-1 punkt d.

([193]) Vt USA seadustiku 42. jaotise § 2000ee-1 punkti f alapunktid 1–2. Näiteks justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste juhtivametniku ning eraelu puutumatuse ja kodanikuvabaduste büroo aruanne, mis hõlmab ajavahemikku 2020. aasta oktoobrist 2021. aasta märtsini, näitab, et korraldati 389 eraelu puutumatuse kontrolli, sealhulgas infosüsteemides ja muudes programmides (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) 2002. aasta sisejulgeoleku seadusega (Homeland Security Act) loodi peainspektori büroo ka sisejulgeoleku ministeeriumis.

([195]) Need peainspektorid määratakse ametisse tähtajatult ning neid võib ametist vabastada üksnes president, kes peab ametist vabastamist USA Kongressile kirjalikult põhjendama.

([196]) Vt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 6.

([197]) Selle kohta vt näiteks justiitsministeeriumi peainspektori büroo koostatud ülevaade oma soovitustest ja sellest, mil määral on neid ministeeriumide ja asutuste järelmeetmetega rakendatud, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Vt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 4(5), 5. Näiteks avaldas justiitsministeeriumi peainspektori büroo hiljuti oma poolaastaaruande USA Kongressil (1. oktoober 2021 kuni 31. märts 2022, https://oig.justice.gov/node/23596), milles annab ülevaade oma audititest, hindamistest, kontrollidest, eriläbivaatamistest ning justiitsministeeriumi programmide ja toimingute uurimistest. Nende tegevuste hulgas oli ka üks käimasolev endise töövõtja uurimine seoses elektroonilise valve andmete ebaseadusliku avaldamisega (üksikisiku pealtkuulamine), mis viis töövõtja karistamiseni. Peainspektori büroo viis läbi ka justiitsministeeriumi asutuste infoturbeprogrammide ja -tavade uurimise, mis hõlmab asutuste süsteemide representatiivse alamhulga infoturbepoliitika, -menetluste ja -tavade tõhususe katsetamist.

(110) Kolmandaks, kui nad tegelevad terrorismivastase võitlusega, teeb kriminaalõiguse täitmisele pööramise ülesannetega ministeeriumide suhtes järelevalvet eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB), mis on täitevvõimu sõltumatu asutus, mis koosneb viiest haldusnõukogu liikmest, kelle president nimetab ametisse kahest parteist kuueks aastaks senati heakskiidul ([199]). Vastavalt selle asutamismäärusele on PCLOB-le usaldatud ülesanded terrorismivastase võitluse poliitika ja selle rakendamise valdkonnas, eesmärgiga kaitsta eraelu puutumatust ja kodanikuvabadusi. 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 ([200]). Ta saab aruandeid mitme föderaalministeeriumi/asutuse kodanikuvabaduste ja eraelu puutumatuse kaitse ametnikelt, ([201]) võib anda valitsusele ja õiguskaitseasutustele soovitusi ning annab korrapäraselt aru USA Kongressi komiteedele ja presidendile ([202]). Juhatuse aruanded, sealhulgas need, mis esitatakse USA Kongressile, peavad olema võimalikult suures ulatuses avalikult kättesaadavad ([203]).

(111) Lõpuks kontrollivad kriminaalõiguse täitmisele pööramist USA Kongressi erikomiteed (vastavalt esindajatekoja ja senati kohtukomitee). Kohtukomiteed teevad korrapärast järelevalvet eri viisidel, eelkõige kuulamiste, uurimiste, läbivaatamiste ja aruannete kaudu ([204]).

3.1.3. *Õiguskaitse*

(112) Nagu märgitud, peavad kriminaalõiguskaitseasutused enamikul juhtudel saama isikuandmete kogumiseks kohtult eelneva loa. Kuigi see ei ole nõutav halduslike korralduste puhul, on need piiratud konkreetsete olukordadega ja nende suhtes kohaldatakse sõltumatut kohtulikku kontrolli vähemalt siis, kui valitsus taotleb täitmist kohtus. Eelkõige võivad halduslike korralduste saajad need kohtus vaidlustada ebamõistlikkuse, st ülemäärasuse, ahistavuse või koormavuse alusel ([205]).

(113) Üksikisikud võivad esitada oma isikuandmete käitlemise kohta taotluse või kaebuse kõigepealt kriminaalõiguskaitseasutustele. Sealhulgas on võimalik taotleda juurdepääsu isikuandmetele ja nende parandamist ([206]). Mis puudutab terrorismivastase võitluse valdkonna meetmeid, võivad üksikisikud esitada kaebuse ka õiguskaitseasutuste eraelu puutumatuse ja kodanikuvabaduste ametnikele (või teistele eraelu puutumatuse ametnikele) ([207]).

(114) Lisaks on USA õigusega nähtud üksikisikutele ette mitu õiguskaitsevahendit kaitseks avaliku sektori asutuse või selle ametniku eest juhul, kui sellised asutused töötlevad isikuandmeid ([208]). Nimetatud vahendid, mille hulka kuulub haldusmenetluse seadus (Administrative Procedure Act (APA)), teabevabaduse seadus (Freedom of Information Act (FOIA)) ja elektroonilise side privaatsuse seadus (Electronic Communications Privacy Act (ECPA)), on kättesaadavad kõigile isikutele hoolimata nende kodakondsusest ja sõltuvalt kohaldatavatest tingimustest.

([199]) Juhatuse liikmed tuleb valida üksnes nende ametialase kvalifikatsiooni, saavutuste, avaliku maine, kodanikuvabaduste ja eraelu puutumatuse alaste teadmiste ning asjakohaste kogemuste alusel ning sõltumata poliitilistest veendumustest. Ühte parteisse kuuluvaid juhatuse liikmeid ei või ühelgi juhul olla rohkem kui kolm. Juhatuse liikmeks nimetatud isik ei tohi juhatuses töötamise ajal olla föderaalvalitsuse valitud ametnik, teenistuja või töötaja, muul viisil kui juhatuse liikmena. Vt USA seadustiku 42. jaotise § 2000ee punkt h.

([200]) USA seadustiku 42. jaotise § 2000ee punkt g.

([201]) Vt USA seadustiku 42. jaotise § 2000ee-1 punkti f alapunkti 1 alapunkti A alapunkt iii. Need on vähemalt justiitsministeerium, kaitseministeerium, sisejulgeoleku ministeerium ning lisaks muud ministeeriumid, asutused või täitevvõimu organid, kelle puhul PCLOB seda vajalikuks peab.

([202]) USA seadustiku 42. jaotise § 2000ee punkt e.

([203]) USA seadustiku 42. jaotise § 2000ee punkt f.

([204]) Näiteks korraldavad komiteed temaatilisi kuulamisi (vt nt esindajatekoja kohtukomitee hiljutine kuulamine „digitaalsete haarangute" teemal, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), ning korrapärased kuulamised, nt FBI ja justiitsministeeriumi kuulamised, vt https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 ja https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Vt VI lisa.

([206]) OMB ringkirja nr A-130 II liidese punkti 3 alapunktid a ja f, millega nõutakse föderaalasutustelt, et nad tagaksid üksikisikute nõudmisel asjakohase juurdepääsu ja andmete parandamise ning kehtestaksid eraelu puutumatust käsitlevate kaebuste ja taotluste vastuvõtmise ja käsitlemise menetlused.

([207]) Vt USA seadustiku 42. jaotise § 2000ee-1 nt justiitsministeeriumi ja sisejulgeoleku ministeeriumi kohta. Vt ka OMB memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy.*

([208]) Selles jaos nimetatud õiguskaitsemehhanismid kehtivad ka siis, kui föderaalasutused koguvad ja kasutavad andmeid tsiviil- ja regulatiivsetel eesmärkidel.

(115) Üldiselt on vastavalt APA ([209]) sätetele, mis käsitlevad kohtulikku läbivaatamist, „igal isikul, kelle õigusi on rikutud ametkonna tegevusega või keda on negatiivselt mõjutanud või kahjustanud ametkonna tegevus“ õigus pöörduda kohtusse ([210]). 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 ei ole muul viisil seadusega kooskõlas“ ([211]).

(116) ECPA ([212]) II jaotisega kehtestatud eraelu puutumatuse õiguste süsteem, mis reguleerib õiguskaitse juurdepääsu kolmandatest isikutest teenusepakkujate poolt säilitatud telefonikõnede, vestluste või elektroonilise teabevahetuse sisule ([213]). See kriminaliseerib ebaseadusliku (st ilma kohtu loata või muul viisil lubatud) juurdepääsu sellisele teabevahetusele ja annab puudutatud isikule võimaluse esitada tsiviilhagi USA föderaalkohtule, et mõista välja hüvitis tegeliku kahju eest ja karistuslik kahjuhüvitis, samuti õiglase hüvitise või tuvastushagi nimetatud ebaseaduslikud teod tahtlikult toime pannud valitsusametniku vastu või Ameerika Ühendriikide vastu.

(117) Lisaks sellele võimaldavad veel mitu õigusakti üksikisikutel esitada hagi USA avaliku sektori asutuse või ametniku vastu, näiteks pealtkuulamisseadus (Wiretap Act), ([214]) arvutipettuste ja sellealase kuritarvitamise seadus (Computer Fraud and Abuse Act), ([215]) föderaalne õigusvastaselt tekitatud kahju hüvitamise seadus (Federal Torts Claim Act), ([216]) finantsandmetega seotud eraelu puutumatuse seadus (Right to Financial Privacy Act) ([217]) ja õiglase krediidiinfo seadus (Fair Credit Reporting Act) ([218]).

([209]) USA seadustiku 5. jaotise § 702.

([210]) Üldiselt kohaldatakse kohtulikku läbivaatamist ainult asutuse „lõplikule“ tegevusele ja mitte selle „ettevalmistavale, menetluslikule ega vahepealsele“ tegevusele. Vt USA seadustiku 5. jaotise § 704.

([211]) USA seadustiku 5. jaotise § 706 punkti 2 alapunkt A.

([212]) USA seadustiku 18. jaotise § 2701–2712.

([213]) ECPA kaitseb teabevahetust, mille sisu säilitavad kaks selgelt määratletud liiki võrguteenuse osutajad ja täpsemalt teenuseosutajad, kes pakuvad: i) elektroonilise side teenuseid, näiteks telefoniside või e-post; ii) kaugandmetöötlusteenuseid nagu andmesalvestus või -töötlus.

([214]) USA seadustiku 18. jaotise § 2510 jj. Pealtkuulamisseaduse (USA seadustiku 18. jaotise § 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. Muude kui sisuandmete kogumise (näiteks IP-aadress, e-posti saaja ja saatja aadress) kohta vt ka väljamineva ja sissetuleva side jälgimise seadmeid käsitlev peatükk jaotises 18 (USA seadustiku 18. jaotise § 3121–3127 ja tsiviilmenetluse kohta § 2707).

([215]) USA seadustiku 18. jaotise § 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.

([216]) USA seadustiku 28. jaotise § 2671 jj. 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.

([217]) USA seadustiku 12. jaotise § 3401 jj. 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 kohtukorraldust või läbiotsimismäärust või piiratud juhtudel ametlikku kirjalikku taotlust ning isikut, kelle kohta käivat teavet taotletakse, teavitatakse sellisest taotlusest.

([218]) USA seadustiku 15. jaotise § 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.

(118) Samuti on teabevabaduse seaduse ([219]) sätete (USA seadustiku 5. jaotise § 552) kohaselt igal isikul õigus saada juurdepääs föderaalasutuste dokumentidele, sealhulgas juhul, kui need sisaldavad isiku isikuandmeid. Kui halduslikud õiguskaitsevahendid on ammendatud, võib üksikisik nõuda sellist juurdepääsuõigust kohtu kaudu, välja arvatud juhul, kui need andmed on kaitstud avalikustamise eest erandiga või õiguskorra tagamisega seonduva keeluga ([220]). Sellisel juhul hindab kohus, kas erand kehtib või kas asjaomane ametiasutus on sellele tuginenud seaduslikult.

3.2. **Juurdepääs andmetele ja nende kasutamine USA avaliku sektori asutuste poolt riikliku julgeoleku eesmärgil**

(119) Ameerika Ühendriikide õigusaktid sisaldavad erinevaid piiranguid ja kaitsemeetmeid seoses isikuandmetele juurdepääsu ja nende kasutamisega riigi julgeoleku eesmärgil ning näevad ette järelevalve- ja õiguskaitsemehhanismid, mis on kooskõlas käesoleva otsuse põhjenduses 89 osutatud nõuetega. Tingimusi, mille alusel selline juurdepääs võib toimuda, ja nende volituste kasutamisel kohaldatavaid kaitsemeetmeid hinnatakse üksikasjalikult järgmistes jagudes.

3.2.1. *Õiguslikud alused, piirangud ja kaitsemeetmed*

3.2.1.1. *Kohaldatav õigusraamistik*

(120) USA ametiasutused võivad koguda liidust ELi-USA andmekaitseraamistikus osalevatele organisatsioonidele edastatud isikuandmeid riikliku julgeoleku eesmärgil erinevate õiguslike vahendite alusel, võttes arvesse eritingimusi ja kaitsemeetmeid.

(121) Kui Ameerika Ühendriikides asuvad organisatsioonid on isikuandmed kätte saanud, võivad USA luureasutused taotleda juurdepääsu sellistele andmetele riikliku julgeoleku eesmärgil ainult vastavalt põhimäärusele, eriti välisluure jälitustegevuse seadusele (Foreign Intelligence Surveillance Act (FISA) võivad taotleda) või seadusesätetele, mis lubavad juurdepääsu riikliku julgeoleku teabenõuete (National Security Letter (NSL)) kaudu ([221]). FISA sisaldab mitut õiguslikku alust, mida võib kasutada ELi-USA andmekaitseraamistiku alusel edastatud liidu andmesubjektide isikuandmete kogumiseks (ja seejärel töötlemiseks) (FISA paragrahv 105, ([222]) FISA paragrahv 302, ([223]) FISA paragrahv 402, ([224]) FISA paragrahv 501 ([225]) ja FISA paragrahv 702 ([226])), nagu on üksikasjalikumalt kirjeldatud põhjendustes 142–152.

([219]) USA seadustiku 5. jaotise § 552.

([220]) Need erandid on aga piiratud. Näiteks USA seadustiku 5. jaotise § 552 punkti b alapunkti 7 kohaselt FOIA-st 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 täitemenetlust 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 kriminaalõiguskaitseasutus 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 täitemenetlust häirida] ja – A) uurimine või süüdistuse esitamine hõlmab võimalikku kriminaalõiguse rikkumist ning B) on alust arvata, et i) uurimise või süüdistuse esitamise subjekt ei ole menetlusest teadlik ja ii) andmete olemasolu avalikustamine võib põhjendatud eelduse kohaselt täitemenetlust häirida, võib amet ainult selle aja kestel, kui antud asjaolu eksisteerib, andmetele selle jao nõudeid mitte kohaldada.“ (USA seadustiku 5. jaotise § 552 punkti c alapunkti 1).

([221]) USA seadustiku 12. jaotise § 3414; USA seadustiku 15. jaotise § 1681u–1681v ja 18. jaotise § 2709. Vt põhjendus 153.

([222]) USA seadustiku 50. jaotise § 1804, mis käsitleb traditsioonilist individualiseeritud elektroonilist valvet.

([223]) USA seadustiku 50. jaotise § 1822, mis käsitleb välisluure eesmärgil tehtavaid füüsilisi läbiotsimisi.

([224]) USA seadustiku 50. jaotise § 1842 koos § 1841 punktiga 2 ja 18. jaotise paragrahviga 3127, mis käsitleb pealtkuulamisseadmete paigaldamist.

([225]) USA seadustiku 50. jaotise § 1861, millega antakse FBI-le luba esitada „taotlus, et saada kohtumäärus, mis lubab ühistransporditeenuse osutajal, avalikul majutusasutusel, füüsilisel hoidlal või sõidukite rendi asutusel avaldada tema valduses olevaid dokumente välisluureteabe kogumiseks või rahvusvahelise terrorismi uurimiseks“.

([226]) USA seadustiku 50. jaotise § 1881a, mis võimaldab USA luureühenduse üksustel taotleda USA ettevõtjatelt juurdepääsu teabele, sealhulgas internetisuhtluse sisule, milleks võetakse elektroonilise side ettevõtjaid abi andmisele kohustades sihikule teatavad väljaspool USAd asuvad USA-välised isikud.

(122) Samuti on USA luureasutustel võimalik koguda väljaspool Ameerika Ühendriike isikuandmeid, mis võivad hõlmata liidu ja Ameerika Ühendriikide vahel edastatavaid isikuandmeid. Andmete kogumine väljaspool Ameerika Ühendriike põhineb presidendi ([227]) täidesaatval korraldusel 12333 („korraldus EO 12333“) ([228]).

(123) Signaaliluureteabe kogumine on teabe kogumise vorm, mis on käesoleva kaitse piisavuse tuvastamise seisukohast kõige olulisem, sest see puudutab elektroonilise side ja andmete kogumist infosüsteemidest. Sellist kogumist võivad läbi viia USA luureasutused nii Ameerika Ühendriikides (FISA alusel) kui ka andmete Ameerika Ühendriikidesse edastamise ajal (korralduse EO 12333 alusel).

(124) 7. oktoobril 2022 andis USA president välja korralduse EO 14086 USA signaaliluure kaitsemeetmete tõhustamise kohta, millega kehtestati piirangud ja kaitsemeetmed kogu USA signaaliluuretegevusele. Nimetatud täidesaatev korraldus asendab suures osas presidendi poliitikasuunise (PPD-28), ([229]) tugevdab tingimusi, piiranguid ja kaitsemeetmeid, mis kehtivad igasugusele signaaliluuretegevusele (st FISA ja korralduse EO 12333 alusel), olenemata toimumiskohast, ([230]) ning loob uue õiguskaitsemehhanismi, mille kaudu üksikisikud saavad neid kaitsemeetmeid kasutada ja hageda ([231]) (vt üksikasjalikumalt põhjendused 176–194). Sellega rakendatakse USA õiguses ELi ja USA vahel peetud kõneluste tulemused pärast seda, kui Euroopa Kohus tunnistas kehtetuks komisjoni piisavusotsuse andmekaitseraamistiku Privacy Shield kohta (vt põhjendus 6). Seetõttu on see käesolevas otsuses hinnatud õigusraamistiku iseäranis oluline element.

(125) Korraldusega EO 14086 kehtestatud piirangud ja kaitsemeetmed täiendavad FISA paragrahviga 702 ja korraldusega EO 12333 sätestatud piiranguid ja kaitsemeetmeid. Allpool kirjeldatud nõudeid (punktides 3.2.1.2 ja 3.2.1.3) peavad luureasutused kohaldama oma signaaliluuretegevuses FISA paragrahvi 702 ja korralduse EO 12333 kohaselt, nt kui nad valivad / määravad kindlaks hangitava välisluureteabe kategooriaid FISA paragrahvi 702 kohaselt; koguvad välisluureteavet või vastuluureteavet korralduse EO 12333 kohaselt ning teevad individuaalseid sihtimisotsuseid FISA paragrahvi 702 ja korralduse EO 12333 kohaselt.

(126) Selles presidendi antud täidesaatvas korralduses sätestatud nõuded on siduvad kogu luureühendusele. Nõudeid tuleb edasi arendada asutuse põhimõtete ja menetluste kaudu, millega need võetakse üle igapäevaste toimingute konkreetsetesse juhistesse. Sellega seoses antakse korraldusega EO 14086 USA luureasutustele oma olemasolevate põhimõtete ja menetluste ajakohastamiseks, et viia need kooskõlla korralduse nõuetega, aega kuni üks aasta (st need peavad olema ajakohastatud 7. oktoobriks 2023). Sellised ajakohastatud põhimõtted ja menetlused tuleb välja töötada, konsulteerides justiitsministri, ODNI kodanikuvabaduste kaitse ametniku (ODNI CLPO) ning PCLOBga – sõltumatu järelevalveasutusega, kellel on volitus täitevvõimu põhimõtteid ja nende rakendamist eraelu puutumatuse ja kodanikuvabaduste kaitsmise eesmärgil läbi vaadata (PCLOBi rolli ja staatuse kohta vt põhjendus 110) –, ning üldsusele kättesaadavaks teha ([232]). Peale selle, kui ajakohastatud põhimõtted ja menetlused on paigas, vaatab PCLOB

([227]) USA põhiseaduse artikli II kohaselt kuulub vastutus riigi julgeoleku tagamise, sealhulgas eelkõige välisluureteabe kogumise eest presidendi kui relvajõudude ülemjuhataja pädevusse.

([228]) Korraldus EO 12333: United States Intelligence Activities, Federal Register, kd 40, nr 235 (8. detsember 1981, muudetud 30. juulil 2008). Korralduses EO 12333 on üldisemalt määratletud USA luuretegevuse eesmärgid, suunad, ülesanded ja vastutusalad (sealhulgas erinevate luureühenduse üksuste roll) ning sätestatud luuretegevuse üldised parameetrid.

([229]) Korraldus EO 14086 asendab presidendi varasema poliitikasuunise PPD-28, välja arvatud selle 3. jagu ja täiendav lisa (millega nõutakse, et luureasutused vaataksid oma signaaliluure prioriteedid ja nõuded igal aastal üle, võttes arvesse signaaliluuretegevusest saadavat kasu USA riiklikele huvidele ning nendest tegevustest tulenevat ohtu) ning 6. jagu (sisaldab üldsätteid), vt riikliku julgeoleku memorandum presidendi poliitikasuunise nr 28 osalise kehtetuks tunnistamise kohta, kättesaadav aadressil https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Vt korralduse EO 14086 5. jao punkt f, milles selgitatakse, et korralduse kohaldamisala on sama, mis PPD-28-l, mida selle joonealuse märkuse 3 kohaselt kohaldati signaaliluuretegevuse suhtes, mida tehti sideandmete või side kohta teabe kogumiseks, v.a signaaliluuretegevused, mida tehakse signaaliluure võimekuse katsetamiseks või arendamiseks.

([231]) Vt selle kohta nt korralduse EO 14086 5. jao punkt h, milles selgitatakse, et korralduses sätestatud kaitsemeetmed loovad juriidilise õiguse ja üksikisikud saavad nõuda nende täitmisele pööramist õiguskaitsemehhanismi kaudu.

([232]) Vt korralduse EO 14086 paragrahvi 2 punkti c alapunkti iv alapunkt C.

need läbi, et tagada nende vastavus täidesaatvale korraldusele. 180 päeva jooksul pärast PCLOBi asjaomase läbivaatamise lõpetamist peab iga luureasutus kõiki PCLOBi soovitusi hoolikalt kaaluma ja rakendama või nendega muul viisil edasi tegutsema. 3. juulil 2023 avaldas USA valitsus sellised ajakohastatud põhimõtted ja menetlused ([233]).

3.2.1.2. *Piirangud ja kaitsemeetmed seoses isikuandmete kogumisega riikliku julgeoleku eesmärgil*

(127) Korraldusega EO 14086 kehtestatakse mitu üldnõuet, mida kohaldatakse kõigi signaaliluuretegevuste suhtes (isikuandmete kogumine, kasutamine, levitamine jne).

(128) Esiteks peavad sellised tegevused põhinema õigusaktil või presidendi loal ning toimuma kooskõlas USA seadustega, sealhulgas põhiseadusega ([234]).

(129) Teiseks peavad olema kehtestatud asjakohased kaitsemeetmed tagamaks, et eraelu puutumatus ja kodanikuvabadused on selliste tegevuste kavandamisel lahutamatud kaalutlused ([235]).

(130) Eelkõige võib igasugust signaaliluuretegevust läbi viia alles pärast seda, kui „kõigi asjakohaste tegurite mõistliku hinnangu põhjal on tehtud kindlaks, et tegevus on vajalik kinnitatud luureprioriteedi edendamiseks“ („kinnitatud luureprioriteedi“ kohta vt põhjendus 135) ([236]).

(131) Lisaks võib selliseid tegevusi läbi viia ainult „sel määral ja viisil, mis on proportsionaalne kinnitatud luureprioriteediga, mille jaoks need on loa saanud“ ([237]). Teisisõnu tuleb õigesti tasakaalustada „luureprioriteedi tähtsust ja mõju, mida see avaldab mõjutatud isikute eraelu puutumatusele ja kodanikuvabadustele, olenemata nende rahvusest või elukohast“ ([238]).

(132) Kõigele lisaks, et tagada vastavus nendele üldnõuetele, mis kajastavad seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõtet, tehakse signaaliluuretegevuste üle järelevalvet (vt täpsem teave põhjendustes 3.2.2) ([239]).

(133) Neid üldisi nõudeid on seoses signaaliluureandmete kogumisega täiendavalt toetatud mitme tingimuse ja piiranguga, mis tagavad, et üksikisikute õigustesse sekkumine piirdub sellega, mis on vajalik ja proportsionaalne õiguspärase eesmärgi edendamiseks.

(134) Esiteks piiratakse korraldusega kahel viisil aluseid, millele tuginedes võib signaaliluuretegevuse raames andmeid koguda. Ühest küljest sätestatakse korralduses õiguspärased eesmärgid, mille jaoks võib signaaliluureandmeid koguda, nt eesmärk mõista või hinnata selliste välismaiste organisatsioonide, sealhulgas rahvusvaheliste terroriorganisatsioonide võimeid, kavatsusi või tegevust, mis kujutavad endast kohest või võimalikku ohtu Ameerika Ühendriikide riiklikule julgeolekule; kaitsta välisriikide sõjalise võimekuse ja tegevuse eest; mõista või hinnata rahvusvahelisi ohte, mis mõjutavad ülemaailmset julgeolekut, nagu kliima- ja muud ökoloogilised muutused, rahvatervise ohud ja humanitaarohud ([240]). Teisest küljest loetletakse korralduses teatavad eesmärgid, mida ei tohi signaaliluuretegevusega kunagi taotleda, nt kriitika, eriarvamuste või üksikisikute või ajakirjanduse ideede või

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkt i.

([235]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkt ii.

([236]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkti ii alapunkt A. Alati ei olegi nõutav, et signaaliluure oleks ainuke vahend kinnitatud luureprioriteedi aspektide edendamiseks. Näiteks võib signaaliluureandmete kogumist kasutada alternatiivsete valideerimisviiside tagamiseks (nt muudest luureallikatest saadud teabe kinnitamiseks) või samale teabele usaldusväärse juurdepääsu säilitamiseks (korralduse EO 14086 paragrahvi 2 punkti c alapunkti i alapunkt A).

([237]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkt ii alapunkt B.

([238]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkt ii alapunkt B.

([239]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkt iii koosmõjus paragrahvi 2 punktiga d.

([240]) Korralduse EO 14086 paragrahvi 2 punkti b alapunkt i. Kuna täidesaatvas korralduses on sätestatud õiguspäraste eesmärkide kindlapiiriline loetelu, mis ei hõlma võimalikke tulevasi ohte, nähakse korraldusega presidendile ette võimalus seda loetelu ajakohastada, kui ilmnevad uued riikliku julgeoleku nõuded, näiteks uued ohud riigi julgeolekule. Sellised ajakohastused tuleb põhimõtteliselt üldsusele avalikustada, välja arvatud juhul, kui president otsustab, et avalikustamine ohustab USA riiklikku julgeolekut (korralduse EO 14086 paragrahvi 2 punkti b alapunkti i alapunkt B).

poliitiliste arvamuste vaba väljendamise mahasurumiseks; isikute ebasoodsasse olukorda seadmiseks nende etnilise kuuluvuse, rassi, soo, soolise identiteedi, seksuaalse sättumuse või usutunnistuse tõttu või USA ettevõtjatele konkurentsieelise loomiseks ([241]).

(135) Peale selle ei saa luureasutused signaaliluureandmete kogumise põhjendamiseks korralduses EO 14086 sätestatud õiguspärastele eesmärkidele otse tugineda, vaid neid tuleb operatiivsetel eesmärkidel täiendavalt põhjendada konkreetsemate prioriteetidega, mille jaoks võib neid andmeid koguda. Teisisõnu võib andmeid tegelikult koguda ainult konkreetsema prioriteedi edendamiseks. Sellised prioriteedid kehtestatakse spetsiaalses protsessis, mille eesmärk on tagada vastavus kohaldatavatele õigusnõuetele, sealhulgas eraelu puutumatuse ja kodanikuvabadustega seotud nõuetele. Täpsemalt öeldes töötab luureprioriteedid esmalt välja riiklik luurejuht (nn riiklike luureprioriteetide raamistiku kaudu) ja esitab need kinnitamiseks presidendile ([242]). Enne luureprioriteetide presidendile esitamist peab riiklik luurejuht kooskõlas korraldusega EO 14086 saama riikliku luurejuhi kodanikuvabaduste kaitse ametnikult (ODNI CLPO) iga luureprioriteedi kohta hinnangu selle kohta, kas see 1) edendab üht või mitut täidesaatvas korralduses loetletud õiguspärast eesmärki; 2) ei ole kavandatud signaaliluureandmete kogumiseks korralduses loetletud keelatud eesmärgil ega põhjusta eeldatavasti seda ning 3) kehtestati, olles arvesse võtnud kõigi isikute eraelu puutumatust ja kodanikuvabadusi, olenemata nende kodakondsusest või elukohast ([243]). Kui direktor ei nõustu kodanikuvabaduste kaitse ametniku hinnanguga, tuleb presidendile esitada mõlemad seisukohad ([244]).

(136) Seetõttu tagab see protsess eelkõige selle, et eraelu puutumatuse kaalutlusi võetakse arvesse luureprioriteetide väljatöötamise algusest peale.

(137) Teiseks kehtib pärast luureprioriteedi kehtestamist mitu nõuet, mis reguleerivad otsust selle kohta, kas ja mil määral võib sellise prioriteedi edendamiseks koguda signaaliluureandmeid. Need nõuded rakendavad üldisi vajalikkuse ja proportsionaalsuse standardeid, mis on sätestatud täidesaatva korralduse paragrahvi 2 punktis a.

(138) Eelkõige võib signaaliluureandmeid koguda alles „pärast otsust, et kõigi asjakohaste tegurite mõistliku hinnangu põhjal on kogumine vajalik konkreetse luureprioriteedi edendamiseks“ ([245]). Selle üle otsustamisel, kas teatav signaaliluureandmete kogumine on vajalik kinnitatud luureprioriteedi edendamiseks, peavad USA luureasutused kaaluma muude, vähem sekkuvate allikate ja meetodite, sealhulgas diplomaatiliste ja avalike allikate kättesaadavust, teostatavust ja asjakohasust ([246]). Võimaluse korral tuleb eelistada selliseid alternatiivseid, vähem sekkuvaid allikaid ja meetodeid ([247]).

(139) Kui selliste kriteeriumide kohaldamise tulemusena peetakse signaaliluureandmete kogumist vajalikuks, peab see toimuma „võimalikult kohandatult“ ega tohi eraelu puutumatust ja kodanikuvabadusi ebaproportsionaalselt mõjutada ([248]). Tagamaks, et eraelu puutumatust ja kodanikuvabadusi ei mõjutata ebaproportsionaalselt – st et leida õige tasakaal riikliku julgeoleku vajaduste ning eraelu puutumatuse ja kodanikuvabaduste kaitse vahel –, tuleb nõuetekohaselt arvesse võtta kõiki olulisi tegureid, näiteks taotletava eesmärgi laadi; kogumistegevuse sekkuvust, sealhulgas selle kestust; kogumise tõenäolist panust taotletava eesmärgi saavutamisse; mõistlikult ettenähtavad tagajärgi üksikisikutele ning kogutavate andmete laadi ja tundlikkust ([249]).

([241]) Korralduse EO 14086 paragrahvi 2 punkti b alapunkt ii.
([242]) Riikliku julgeoleku seaduse (National Security Act) paragrahv 102A ja korralduse EO 14086 2. jao punkti b alapunkt iii.
([243]) Erandjuhtudel (eelkõige siis, kui sellist protsessi ei saa läbi viia uue või areneva luureandmete vajaduse tõttu), võib sellised prioriteedid määrata otse luureühenduse president või luureühenduse mõne üksuse juht, kes põhimõtteliselt peab kohaldama samu kriteeriume, mida on kirjeldatud paragrahvi 2 punkti b alapunkti iii alapunkti A alapunktides 1–3, vt korralduse EO 14086 4. jao alapunkt n.
([244]) Korralduse EO 14086 paragrahvi 2 punkti b alapunkti iii alapunkt C.
([245]) Korralduse EO 14086 paragrahvi 2 punkt b ja punkti c alapunkt i alapunkt A.
([246]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti i alapunkt A.
([247]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti i alapunkt A.
([248]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti i alapunkt B.
([249]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti i alapunkt B.

(140) Mis puudutab kogutavate signaaliluureandmete liiki, siis peab andmete kogumine Ameerika Ühendriikides, mis on praeguse kaitse piisavuse tuvastamise jaoks kõige olulisem, sest see puudutab USA organisatsioonidele edastatud andmeid, olema alati sihitud, nagu on üksikasjalikumalt selgitatud põhjendustes 142–153.

(141) „Masskogumist“ ([250]) võib kasutada ainult väljaspool Ameerika Ühendriike korralduse EO 12333 alusel andmete kogumisel. Korralduse EO 14086 kohaselt tuleb ka sellisel juhul eelistada sihitud kogumist ([251]). Seevastu masskogumine on lubatud ainult siis, kui kinnitatud luureprioriteedi edendamiseks vajalikku teavet ei ole võimalik saada sihtud kogmisega ([252]). Kui on vaja andmeid massiliselt koguda väljaspool Ameerika Ühendriike, kohaldatakse korralduse EO 14086 kohaseid erikaitsemeetmeid ([253]). Esiteks tuleb rakendada meetodeid ja tehnilisi meetmeid, et piirduda andmete kogumisel ainult sellega, mis on vajalik kinnitatud luureprioriteedi edendamiseks, minimeerides samas asjasse mittepuutuva teabe kogumist ([254]). Teiseks piiratakse korraldusega võimalikke masskogutud teabe kasutamise (sealhulgas päringute esitamist) erieesmärke kuuele, sealhulgas kaitsmine terrorismi ja pantvangide võtmise eest ning isikute vangistuses hoidmise eest välisriigi valitsuse, organisatsiooni või isiku poolt või nimel; kaitsmine välisriigi spionaaži, sabotaaži või tellitud mõrva eest; kaitsmine massihävitusrelvade või nendega seotud tehnoloogiate arendamisest, omamisest või levikust tulenevate ohtude eest jne ([255]). Kõigele lisaks võib masskogutud signaaliluureandmete päringuid teha ainult siis, kui see on vajalik kinnitatud luureprioriteedi edendamiseks, taotledes neid kuut eesmärki ning kooskõlas põhimõtete ja menetlustega, milles võetakse asjakohaselt arvesse päringute mõju kõigi isikute eraelu puutumatusele ja kodanikuvabadustele, olenemata nende kodakondsusest või elukohast ([256]).

(142) Lisaks korralduse EO 14086 nõuetele kehtivad USAs asuvale organisatsioonile edastatud andmete signaaliluure kaudu kogumisel teatavad piirangud ja kaitsemeetmed, mida reguleerib FISA paragrahv 702 ([257]). FISA paragrahv 702 võimaldab koguda välisluureteavet, võttes USA elektrooniliste sideteenuste osutajate kohustusliku abiga sihikule USA-välised isikud, kes usutavasti asuvad väljaspool Ameerika Ühendriike ([258]). Välisluureteabe

([250]) St signaaliluure andmete ulatuslik kogumine, mis tehnilistel või operatiivsetel kaalutlustel toimub ilma kategooriate kasutamiseta (nt kasutamata eritunnuseid, valikukriteeriume), vt korralduse EO 14086 paragrahvi 4 punkt b. Korralduse EO 14086 kohaselt ja nagu on selgitatud põhjenduses 141, toimub andmete masskogumine korralduse EO 12333 alusel ainult siis, kui see on vajalik spetsiifiliste kinnitatud luureprioriteetide edendamiseks, ning sellele kehtivad paljud piirangud ja kaitsemeetmed, mille eesmärk on tagada, et andmetele juurdepääs ei oleks valimatu. Seetõttu tuleb masskogumist vastandada üldisel alusel ja valimatult toimuvale kogumisele (massjälgimine) ilma piirangute ja kaitsemeetmeteta.

([251]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt A.

([252]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt A.

([253]) Korralduses EO 14086 sätestatud masskogumise reeglid kehtivad ka signaaliluure andmete sihitud kogumisele, mille puhul kasutatakse ajutiselt andmeid, mis saadi ilma kategooriateta (nt konkreetsed valikutingimused või identifikaatorid), st masskogumise teel (mis on võimalik ainult väljaspool Ameerika Ühendriikide territooriumi). See ei kehti juhul, kui selliseid andmeid kasutatakse ainult signaaliluure andmete sihitud kogumise algse tehnilise etapi toetamiseks, neid säilitatakse vaid lühikest aega, mis on vajalik selle etapi lõpuleviimiseks, ja kustutatakse seejärel kohe (korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt D). Sel juhul on esialgse, ilma kategooriateta kogumise ainus eesmärk võimaldada teabe sihipärast kogumist, rakendades konkreetset identifikaatorit või valikukriteeriumi. Sellise stsenaariumi korral sisestatakse valitsuse andmebaasidesse ainult teatavale kategooriale vastavad andmed, ülejäänud andmed aga hävitatakse. Seetõttu reguleerivad sellist sihitud kogumist endiselt signaaliluure andmete kogumise suhtes kehtivad üldreeglid, sh korralduse EO 14086 paragrahvi 2 punktid a–b ja paragrahvi 2 punkti c alapunkt i.

([254]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt A.

([255]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt B. Kui ilmnevad uued riikliku julgeoleku vajadused, näiteks uued ohud riiklikule julgeolekule, võib president seda nimekirja ajakohastada. Sellised ajakohastused tuleb põhimõtteliselt üldsusele avalikustada, välja arvatud juhul, kui president otsustab, et selline avalikustamine ohustab USA riiklikku julgeolekut (korralduse EO 14086 paragrahvi 2 punkti c alapunkti ii alapunkt C). Masskogutud andmete päringute kohta vt korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkt D.

([256]) Korralduse EO 14086 paragrahvi 2 punkti a alapunkti ii alapunkt A koostoimes paragrahvi 2 punkti c alapunkti iii alapunktiga D. Vt ka VII lisa.

([257]) USA seadustiku 50. jaotise § 1881.

([258]) USA seadustiku 50. jaotise § 1881a punkt a. Seega, nagu on märkinud eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (Privacy and Civil Liberties Oversight Board, PCLOB), on paragrahvi 702 alusel toimuv luure „suunatud üksnes konkreetsetele [USA-välistele] isikutele, kelle kohta on tehtud individuaalne otsus“ (eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (aruanne FISA paragrahvi 702 alusel läbi viidud luureprogrammi kohta), 2. juuli 2014, paragrahvi 702 kohane aruanne, lk 111). Vt ka NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act, paragrahv 702, 16. aprill 2014. Mõiste „elektroonilise side teenuse osutaja“ on määratletud USA seadustikus (USA seadustiku 50. jaotise § 1881 punkti a alapunkt 4).

kogumiseks vastavalt FISA paragrahvile 702 esitavad justiitsminister ja riiklik luurejuht välisluure järelevalve kohtule (Foreign Intelligence Surveillance Court (FISC)) igal aastal sertifikaadid, millega määratakse kindlaks hangitava välisluureteabe kategooriad ([259]). Sertifikaatidele tuleb lisada sihtimis-, minimeerimis- ja päringumenetlused, mille kiidab heaks ka kohus ja mis on USA luureasutustele õiguslikult siduvad.

(143) FISC on föderaalseaduse alusel loodud sõltumatu kohus, ([260]) mille otsuseid saab edasi kaevata välisluure järelevalve apellatsioonikohtusse (FISCR) ([261]) ja lõpuks ka Ameerika Ühendriikide ülemkohtusse ([262]). FISCd (ja FISCRi) abistab viiest advokaadist ja viiest tehnilisest eksperdist koosnev alaline kolleegium, millesse kuuluvad riikliku julgeoleku küsimuste ja kodanikuvabaduste eksperdid ([263]). 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 ([264]). See tagab eelkõige, et kohtu hinnangus võetakse nõuetekohaselt arvesse eraelu puutumatuse kaalutlusi. Kohus võib määrata mõne üksikisiku või organisatsiooni *amicus curiae* ülesannetesse, sealhulgas tehniliseks eksperdiks, kui ta seda vajalikuks peab, või anda seda taotlevale üksikisikule või organisatsioonile loa esitada *amicus curiae* memorandum ([265]).

(144) FISC vaatab üle sertifikaadid ja nendega seotud menetlused (eelkõige sihtimis- ja minimeerimismenetlused), et tagada vastavus FISA nõuetele. Kui kohus leiab, et nõuded ei ole täidetud, võib ta sertifitseerimisest täielikult või osaliselt keelduda ja nõuda menetluste muutmist ([266]). Sellega seoses on FISC korduvalt kinnitanud, et paragrahvi 702 kohaste sihtimis- ja minimeerimismenetluste läbivaatamine ei piirdu ainult kirjalike menetlustega, vaid hõlmab ka seda, kuidas valitsus neid menetlusi rakendab ([267]).

(145) Individuaalsed sihtimisotsused teeb riiklik julgeolekuasutus (NSA – luureasutus, kes vastutab sihtimise eest FISA paragrahvi 702 alusel) vastavalt FISC heakskiidetud sihtimismenetlustele, mis nõuavad, et NSA hindaks asjaolude kogumi põhjal, kas konkreetse isiku sihtmärgiks võtmisega on tõenäoline saada vastavuskinnituses määratletud kategooria välisluureteavet ([268]). See hinnang peab olema üksikasjalik ja faktidel põhinev, tuginema analüütilisele

([259]) USA seadustiku 50. jaotise § 1881a punkt g.

([260]) FISC koosneb kohtunikest, kelle nimetab ametisse Ameerika Ühendriikide ülemkohtu esimees USA ringkonnakohtu kohtunike hulgast, kelle on eelnevalt ametisse nimetanud president ja kinnitanud senat. Kohtunikud nimetatakse ametisse eluaegselt, neid saab ametist vabastada üksnes mõjuvatel põhjustel ning nende ametiaeg FISC-s kestab seitse aastat ega kattu teiste kohtunike ametiajaga. FISA kohaselt tuleb kohtunikud määrata vähemalt seitsmest erinevast USA kohturingkonnast. Vt USA seadustiku 50. jaotise § 1803 punkt a. Kohtunikke abistavad kogenud kohtunikuabid, kes moodustavad kohtu juriidilise personali ning valmistavad ette kogumistaotluste õiguslikud analüüsid. Vt USA välisluure järelevalve kohtu eesistuja Reggie B. Waltoni kiri USA senati kohtukomitee eesistujale Patrick J. Leahyle (29. juuli 2013) (edaspidi „Waltoni kiri“), lk 2, kättesaadav aadressil https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) FISCR koosneb kohtunikest, kelle nimetab ametisse Ameerika Ühendriikide ülemkohtu esimees USA ringkonna- või apellatsioonikohtute kohtunike hulgast, ja nende kohtunike ametiaeg kestab seitse aastat ega kattu teiste kohtunike ametiajaga. Vt USA seadustiku 50. jaotise § 1803 punkt b.

([262]) Vt USA seadustiku 50. jaotise § 1803 punkt b, § 1861 a punkt f, § 1881 a punkt h, 1881 a punkti i alapunkt 4.

([263]) USA seadustiku 50. jaotise § 1803 punkti i alapunkt 1, alapunkti 3 alapunkt A.

([264]) USA seadustiku 50. jaotise § 1803 punkti i alapunkti 2 alapunkt A.

([265]) USA seadustiku 50. jaotise § 1803 punkti i alapunkti 2 alapunkt B.

([266]) Vt nt FISC 18. oktoobri 2018. aasta arvamus, kättesaadav aadressil athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, mida välisluure järelevalve apellatsioonikohus kinnitas oma 12. juuli 2019. aasta arvamuses, mis on kättesaadav aadressil athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Vt nt FISC, Memorandum Opinion and Order at 35 (18. november 2020) (üldsusele avalikustamise luba antud 26. aprillil 2021) (D lisa).

([268]) USA seadustiku 50. jaotise § 1881a punkt a, Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 (Menetlused, mida riiklik julgeolekuasutus (NSA) kasutab välisluureteabe hankimiseks mitte-ameeriklastelt, kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike, 1978. aasta välisluure jälitustegevuse seaduse paragrahvi 702 kohaselt), muudetud redaktsioonis, märts 2018 (NSA sihtimismenetlused), kättesaadav aadressil https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, lk 1–4, täpsemad selgitused PCLOBi aruandes, lk 41–42.

hindamisele, analüütiku erikoolitusele ja kogemustele, samuti hangitava välisluureteabe laadile ([269]). Sihtimiseks selgitatakse välja nn identimistunnused, mis tuvastavad spetsiifilisi sidevahendid, nagu sihtmärgi e-posti aadress või telefoninumber, kuid mitte kunagi märksõnu või isikute nimesid ([270]).

(146) Kõigepealt teevad NSA analüütikud kindlaks välismaal asuvad USA-välised isikud, kelle jälgimine võimaldab analüütikute hinnangul saada sertifikaadis sätestatud vajalikke välisluureandmeid ([271]). Nagu on sätestatud NSA sihtimismenetlustes, võib NSA suunata jälgimise sihtmärgile alles siis, kui ta on sihtmärgi kohta juba midagi teada saanud ([272]). See võib tuleneda erinevatest allikatest pärit teabest, näiteks inimallikatelt hangitud luureandmetest. Nende muude allikate abil peab analüütik saama teada ka konkreetse identimistunnuse (st sidekonto), mida võimalik sihtmärk kasutab. Pärast nende üksikisikute kindlakstegemist ja nende sihtmärgiks võtmise kinnitamist NSA-sisese põhjaliku kontrollimehhanismi ([273]) abil võetakse sihtmärkide kasutatavate sidevahendite (nt e-posti aadressid) identimistunnused „ülesandeks“ (st neid arendatakse ja kasutatakse) ([274]).

(147) NSA peab dokumenteerima sihtmärgi valimise faktilise aluse ([275]) ja kinnitama korrapäraste ajavahemike järel pärast esialgset sihtimist, et sihtimisstandardi nõuded on jätkuvalt täidetud ([276]). Kui sihtimisstandard ei ole enam täidetud, tuleb andmete kogumine peatada ([277]). NSA iga sihtmärgi valimise ja iga tema dokumenteeritud sihtimishinnangu ja -põhjuse vastavust sihtimismenetlustele kontrollivad iga kahe kuu tagant justiitsministeeriumi luure järelevalve talituste ametnikud, kellel on kohustus teatada kõigist rikkumistest FISC-le ja USA Kongressile ([278]). NSA kirjalik dokumentatsioon hõlbustab FISC järelevalvet selle üle, kas konkreetsed isikud on FISA paragrahvi 702 alusel võetud sihtmärgiks nõuetekohaselt, kooskõlas tema järelevalvevolitustega, mida on kirjeldatud põhjendustes 173–174 ([279]). Lõpuks peab riiklik luurejuht avalikes iga-aastastes statistilistes läbipaistvusaruannetes teatama ka FISA paragrahvi 702 kohaste sihtmärkide koguarvu. Ettevõtjad, kes saavad FISA paragrahvi 702 kohased FISA direktiivid, võivad avaldada saadud taotluste kohta koondandmed (läbipaistvusaruannetes) ([280]).

([269]) NSA sihtimismenetlused, lk 4.

([270]) Vt PCLOB, paragrahvi 702 kohane aruanne, lk 32–33, 45 ja seal sisalduvad viited. Vt ka Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (välisluure jälitustegevuse seaduse paragrahvi 702 kohane poolaasta hindamine menetluste ja juhiste järgimise kohta), esitanud justiitsminister ja riiklik luurejuht, aruandeperiood: 1. detsember 2016 kuni 31. mai 2017, lk 41 (oktoober 2018), kättesaadav aadressil https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, paragrahvi 702 kohane aruanne, lk 42–43.

([272]) NSA sihtimismenetlused, lk 2.

([273]) PCLOB, paragrahvi 702 kohane aruanne, lk 46. Näiteks peab NSA kontrollima, et sihtmärgi ja identimistunnuse 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, Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014.

([274]) USA seadustiku 50. jaotise § 1881a punkt h.

([275]) NSA sihtimismenetlused, lk 8. Vt ka PCLOBi paragrahvi 702 kohane aruanne, lk 46. Kirjaliku põhjenduse esitamata jätmine on dokumenteerimise nõuetele mittevastavuse juhtum, millest tuleb teatada FISC-le ja USA Kongressile. Vt Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (välisluure jälitustegevuse seaduse paragrahvi 702 kohane poolaasta hindamine menetluste ja juhiste järgimise kohta), esitanud justiitsminister ja riiklik luurejuht, aruandeperiood: 1. detsember 2016 kuni 31. mai 2017, lk 41 (oktoober 2018), justiitsministeeriumi/ODNI vastavusaruanne FISC-le ajavahemiku 2016. aasta detsember kuni 2017. aasta mai kohta, lk A-6, kättesaadav aadressil https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Vt USA valitsuse esildis välisluure järelevalve kohtule, 2015 Summary of Notable Section 702 Requirements (2015. aasta kokkuvõte paragrahvi 702 olulistest nõuetest), lk 2–3 (15. juuli 2015) ja VII lisas esitatud teave.

([277]) Vt USA valitsuse esildis välisluure järelevalve kohtule, 2015 Summary of Notable Section 702 Requirements (2015. aasta kokkuvõte paragrahvi 702 olulistest nõuetest), lk 2–3 (15. juuli 2015), milles on märgitud, et „[kui] valitsus leiab hiljem, et sihtmärgi identimistunnuse jätkuva rakendamise tulemusena eeldatavasti välisluureteavet ei saa, tuleb seotud ülesanne kiiresti peatada ja sellega viivitamine võib põhjustada vastavusega seotud juhtumi, millest tuleb teatada“. Vt ka VII lisas esitatud teave.

([278]) PCLOB, paragrahvi 702 kohane aruanne, lk 70–72; Ameerika Ühendriikide välisluure jälitustegevuse kohtu kodukorra artikli 13 punkt b, kättesaadav aadressil https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Vt ka justiitsministeeriumi/ODNI vastavusaruanne FISC-le ajavahemiku 2016. aasta detsember kuni 2017. aasta mai kohta, lk A-6.

([280]) USA seadustiku 50. jaotise § 1874.

(148) USA organisatsioonidele edastatavate isikuandmete kogumise muude õiguslike aluste suhtes kehtivad erinevad piirangud ja kaitsemeetmed. Üldjuhul on andmete masskogumine FISA paragrahviga 402 (väljamineva ja sissetuleva side jälgimise seadmeid lubav norm) sõnaselgelt keelatud ning selle asemel tuleb riikliku julgeoleku teabenõuete kaudu ja kasutada spetsiifilisi valikukriteeriume ([281]).

(149) Traditsioonilise individualiseeritud elektroonilise jälgimise läbiviimiseks (kooskõlas FISA paragrahviga 105) peavad luureasutused esitama FISC-le taotluse ülevaatega faktidest ja asjaoludest, millega põhjendatakse küllaldast alust arvata, et rajatist kasutab või hakkab kasutama võõrvõim või võõrvõimu agent ([282]) . FISC hindab muu hulgas, kas esitatud faktidest lähtudes on olemas küllaldane alus arvata, et see tõepoolest nii on ([283]).

(150) Ruumide või vara läbiotsimiseks, mille kavandatud tulemus on teabe, materjali või vara (nt arvutiseadme) kontroll, arestimine vms FISA paragrahvi 301 alusel, tuleb taotleda FISC-lt vastavat määrust ([284]). Taotluses tuleb muu hulgas näidata, et on olemas küllaldane alus arvata, et läbiotsimise sihtmärk on võõrvõim või võõrvõimu agent; et läbiotsitav ruum või vara sisaldab välisluureteavet ja et läbiotsitav ruum on võõrvõimu (agendi) omanduses, kasutuses, valduses või talle või temalt üleandmise järgus ([285]).

(151) Samamoodi eeldab ka pealtkuulamisseadmete paigaldamine loataotlust (kooskõlas FISA paragrahviga 402) FISC kohtunikule (või USA föderaalkohtu magistraadile) ning konkreetse valikukriteeriumi kasutamist, st kriteerium, mis identifitseerib konkreetse isiku, konto vms ja mida kasutatakse tagamaks, et taotletava teabe maht oleks nii väike kui mõistlikult võimalik ([286]). See volitus ei puuduta side sisu, vaid on suunatud pigem teenust kasutava kliendi või kasutaja andmetele (nagu nimi, aadress, kasutajakood, kasutatud teenuse kestus/liik, maksete tegija / makseviis).

(152) FISC-le (või USA föderaalkohtu magistraadile) taotluse esitamine on nõutav ka FISA paragrahvi 501 ([287]) kohaselt, mis võimaldab koguda ühistranspordiettevõtja (st iga isik või üksus, kes transpordib tasu eest inimesi või vara, kasutades maismaa-, raudtee, vee- või lennutransporti), ühiskondliku majutusasutuse (nt hotell, motell või võõrastemaja), sõidukite rendileandja või füüsilise laoruumi (st pakub ruumi või kaupade ja materjalide ladustamisega seotud teenuseid) ([288]) äridokumente. Taotluses tuleb märkida, milliseid dokumente saada soovitakse ning konkreetsed ja selgelt väljendatavad faktid, mis annavad alust arvata, et isik, keda dokumendid puudutavad, on võõrvõim või võõrvõimu agent ([289]).

(153) Kõigele lisaks on erinevate põhimäärustega lubatud riikliku julgeoleku teabenõuded ja need võimaldavad uurimisasutustel hankida teatavatelt üksustelt (nt finantsasutused, krediidiinfoasutused, elektroonilise side pakkujad) teatavat teavet (välja arvatud suhtluse sisu), mis sisaldub krediidiaruannetes, finantsaruannetes, elektroonilistes tarbija- ja tehinguaruannetes ([290]). Riikliku julgeoleku teabenõuete põhimäärust, mis lubab juurdepääsu elektroonilisele sidele, võib kasutada ainult FBI ja see eeldab, et taotlustes kasutatakse kriteeriumit, mis identifitseerib konkreetselt isiku, üksuse, telefoninumbri või konto, ja kinnitakse, et teave on oluline sanktsioneeritud riikliku julgeolekuga seotud uurimises, mida viiakse läbi kaitseks rahvusvahelise terrorismi või salaluuretegevuse vastu ([291]). Riikliku julgeoleku teabenõude saanud isikutel on õigus see kohtus vaidlustada ([292]).

([281]) USA seadustiku 50. jaotise § 1842 punkti c alapunkt 3 ja mis puudutab riikliku julgeoleku teabenõudeid, siis USA seadustiku 12. jaotise § 3414 punkti a alapunkt 2; USA seadustiku 15. jaotise § 1681u; USA seadustiku 15. jaotise § 1681v punkt a ja USA seadustiku 18. jaotise § 2709 punkt a.

([282]) „Võõrvõimu agent“ võib olla USA-väline isik, kes on seotud rahvusvahelise terrorismi või massihävitusrelvade rahvusvahelise levikuga (sealhulgas ettevalmistav tegevus) (USA seadustiku 50. jaotise § 1801 punkti b alapunkt 1).

([283]) USA seadustiku 50. jaotise § 1804. Vt valikukriteeriumide kohta ka § 1841 lõige 4.

([284]) USA seadustiku 50. jaotise § 1821 lõige 5.

([285]) USA seadustiku 50. jaotise § 1823 punkt a.

([286]) USA seadustiku 50. jaotise § 1842 koos § 1841 lõikega 2 ning 18. jaotise paragrahv 3127.

([287]) USA seadustiku 50. jaotise § 1862.

([288]) USA seadustiku 50. jaotise § 1861–1862.

([289]) USA seadustiku 50. jaotise § 1862 punkt b.

([290]) USA seadustiku 12. jaotise § 3414; USA seadustiku 15. jaotise § 1681u–1681v ja 18. jaotise § 2709.

([291]) USA seadustiku 18. jaotise § 2709 punkt b.

([292]) nt USA seadustiku 18. jaotise § 2709 punkt d.

3.2.1.3. *Kogutud teabe edasine kasutamine*

(154) Kui USA luureasutused töötlevad signaaliluure teel kogutud isikuandmeid, kohaldatakse mitut kaitsemeedet.

(155) Esiteks peab iga luureasutus tagama asjakohase andmeturbe ja ennetama kõrvaliste isikute juurdepääsu signaaliluure teel kogutud isikuandmetele. Sellega seoses on eri õigusaktides, sealhulgas põhimääruses, suunistes ja standardites täpsustatud infoturbe miinimumnõudeid, mis tuleb kehtestada (nt mitmikautentimine, krüpteerimine jne) ([293]). Juurdepääs kogutud andmetele peab piirduma volitatud ja koolitatud töötajatega, kes vajavad seda teavet oma ülesannete täitmiseks ([294]). Üldisemalt peavad luureasutused pakkuma oma töötajatele asjakohast koolitust, sealhulgas õiguse (sealhulgas korralduse EO 14086) rikkumistest teatamise ja nende menetlemise korra kohta ([295]).

(156) Teiseks peavad luureasutused järgima luureühenduse täpsuse ja objektiivsuse standardeid, eelkõige seoses andmete kvaliteedi ja usaldusväärsuse tagamisega, alternatiivsete teabeallikate kaalumisega ja objektiivsusega analüüside tegemisel ([296]).

(157) Kolmandaks, mis puudutab andmete säilitamist, siis on korralduses EO 14086 selgitatud, et USA-väliste isikute isikuandmete suhtes kehtivad samad säilitamistähtajad nagu USA kodanike andmetele ([297]). Luureasutused on kohustatud määrama kindlaks konkreetsed säilitamistähtajad ja/või tegurid, mida tuleb kohaldatavate säilitamistähtaegade pikkuse kindlaksmääramisel arvesse võtta (nt kas teave on kuriteo tõendusmaterjal; kas teave on välisluureteave; kas teavet on vaja isikute või organisatsioonide, sealhulgas rahvusvahelise terrorismi ohvrite või sihtmärkide turvalisuse tagamiseks) ja mis on sätestatud eri õigusaktides ([298]).

(158) Neljandaks kehtivad signaaliluure teel kogutud isikuandmete levitamise suhtes erinormid. Üldnõude kohaselt võib isikuandmeid mitte-USA isikute kohta levitada ainult siis, kui see hõlmab sama liiki teavet, mida saab levitada USA kodanike kohta, nt teave, mis on vajalik isiku või organisatsiooni ohutuse kaitsmiseks (nt rahvusvaheliste terroriorganisatsioonide sihtmärgid, ohvrid või pantvangid) ([299]). Lisaks ei tohi isikuandmeid levitada üksnes isiku kodakondsuse või elukohariigi tõttu või korralduse EO 14086 nõuetest kõrvalehoidmise eesmärgil ([300]). USA valitsuse sisene levitamine võib toimuda ainult siis, kui volitatud ja koolitatud isikul on põhjendatud alust arvata

([293]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti B alapunkt 1. Vt ka riikliku julgeoleku seaduse VIII jaotis (salastatud teabele juurdepääsu nõuete kohta), korralduse EO 12333 paragrahv 1.5 (mis kohustab luureühenduse asutuste juhte järgima teabe jagamise ja infoturbe suuniseid, teabe privaatsuse ja muid õiguslikke nõudeid), riikliku julgeoleku poliitikasuunis nr 42 „National Policy for the Security of National Security Telecommunications and Information Systems“ (Riiklik julgeolekupoliitika telekommunikatsiooni- ja infosüsteemide turvalisuse tagamiseks) (mis juhendab riiklike julgeolekusüsteemide komiteed andma täitevametitele ja -asutustele suuniseid riiklike turvasüsteemide turvalisuse kohta) ja riikliku julgeoleku memorandum nr 8, „Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems“ (Riikliku julgeoleku, kaitseministeeriumi ja luureühenduse süsteemide küberturvalisuse parandamine) (kehtestatakse ajakavad ja juhised küberturvalisuse nõuete rakendamiseks riiklikes julgeolekusüsteemides, sealhulgas mitmikautentimine, krüpteerimine, pilvetehnoloogiad ja lõpp-punkti tuvastamise teenused).

([294]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti B alapunkt 2. Lisaks võib isikuandmetele, mille säilitamise kohta ei ole lõplikku otsust tehtud, pääseda juurde ainult selleks, et sellist otsust teha või selle tegemist toetada või täita volitatud haldus-, katsetamis-, arendus-, turva- või järelevalveülesandeid (korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti B alapunkt 3).

([295]) Korralduse EO 14086 paragrahvi 2 punkti d alapunkt ii.

([296]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkt C.

([297]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti A alapunkti 2 alapunktid a–c. Üldisemalt peab iga asutus kehtestama põhimõtted ja menetlused, mille eesmärk on minimeerida signaaliluure teel kogutud isikuandmete levitamist ja säilitamist (korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkt A).

([298]) Vt nt 2015. eelarveaastaks vastu võetud luuretegevuse lubamise seaduse (Intelligence Authorization Act) paragrahv 309; minimeerimismenetlused, mille eri luureasutused on vastu võtnud FISA paragrahvi 702 alusel ja mille FISC on heaks kiitnud; justiitsministri ja föderaalregistrite seadusega heaks kiidetud menetlused (mis nõuavad, et USA föderaalasutused, sealhulgas riiklikud julgeolekuasutused, kehtestaksid oma dokumentide säilitustähtajad, mille peab heaks kiitma Ameerika Ühendriikide rahvusarhiiv).

([299]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti A alapunkti 1 alapunkt a ja paragrahvi 5 punkt d koostoimes korralduse 12333 paragrahviga 2.3.

([300]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti A alapunkti 1 alapunktid b ja e.

vaja seda teavet teada ([301]) ja ta kaitseb seda asjakohaselt ([302]). Selleks et teha kindlaks, kas isikuandmeid võib levitada USA valitsuse välistele vastuvõtjatele (sh välisriigi valitsusele või rahvusvahelisele organisatsioonile), tuleb arvesse võtta levitamise eesmärki, levitatavate andmete laadi ja ulatust ning võimalikku kahjulikku mõju asjaomas(t)ele isiku(te)le ([303]).

(159) Kõigele lisaks ja sealhulgas selleks, et hõlbustada järelevalvet kohaldatavate juriidiliste nõuete järgimise üle ja tõhusat kahju hüvitamist, peavad kõik luureasutused korralduse EO 14086 kohaselt säilitama signaaliluureandmete kogumisega seotud asjakohaseid dokumente. Dokumenteerimise nõuded hõlmavad selliseid elemente nagu faktiline alus, millel põhineb hinnang, et konkreetne kogumistegevus on vajalik kinnitatud luureprioriteedi edendamiseks ([304]).

(160) Lisaks eespool nimetatud, korralduses EO 14086 signaaliluure teel kogutud teabe kasutamise suhtes sätestatud kaitsemeetmetele kehtivad kõikidele USA luureasutustele eesmärgi piiramise, võimalikult väheste andmete kogumise, andmete täpsuse, turvalisuse, säilitamise ja levitamise üldisemad nõuded, mis tulenevad eelkõige OMB ringkirjast nr A-130, e-valitsuse seadusest, föderaalregistrite seadusest (v (vt põhjendused 101–106) ja riiklike julgeolekusüsteemide komitee (CNSS) juhistest ([305]).

3.2.2. ***Järelevalve***

(161) USA luureasutuste tegevust kontrollivad erinevad organid.

(162) Esiteks nõutakse korraldusega EO 14086, et igal luureasutusel oleksid kõrged õigus-, järelevalve- ja vastavusametnikud, et tagada kohaldatava USA õiguse järgimine ([306]). Eelkõige peavad nad tegema perioodilist järelevalvet signaaliluuretegevuse üle ja tagama, et kõik mittevastavused parandatakse. Luureasutused peavad võimaldama sellistele ametnikele järelevalveülesannete täitmiseks juurdepääsu kogu asjakohasele teabele ega tohi võtta meetmeid nende järelevalvetegevuse takistamiseks või ebakohaseks mõjutamiseks ([307]). Peale selle tuleb järelevalveametniku või mõne muu töötaja tuvastatud olulisest mittevastavuse juhtumist ([308]) viivitamatult teatada luureasutuse juhile ja riiklikule luurejuhile, kes peavad tagama, et olulise rikkumisjuhtumi heastamiseks ja selle kordumise ennetamiseks võetakse kõik vajalikud meetmed ([309]).

(163) Seda järelevalvefunktsiooni täidavad ametnikud, kellel on määratud nõuetele vastavuse kontrolli ülesanne, samuti eraelu puutumatuse ja kodanikuvabaduste ametnikud ning peainspektorid ([310]).

([301]) Vt nt peaprokuröri suunised riigisiseste FBI operatsioonide kohta (AGG-DOM), kus on näiteks ette nähtud, et FBI võib teavet levitada ainult siis, kui teabe saajal on vaja seda teada oma ülesannete täitmiseks või üldsuse kaitsmiseks.

([302]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti A alapunkti 1 alapunkt c. Näiteks võivad luureasutused levitada teavet kriminaaluurimise või kuriteoga seotud asjaolude kohta, sealhulgas näiteks levitada hoiatusi tapmisähvarduste, raskete kehavigastuste tekitamise või inimröövi kohta; levitada teavet küberohtude, intsidentide või sissetungimisele reageerimise kohta ning teavitada ohvreid või potentsiaalseid ohvreid kuriteost.

([303]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkti A alapunkti 1 alapunkt d.

([304]) Korralduse EO 14086 paragrahvi 2 punkti c alapunkti iii alapunkt E.

([305]) Vt CNSSi poliitikasuunised nr 22, Küberturvalisuse riskijuhtimise poliitika (Cybersecurity Risk Management Policy) ja CNSSi juhis nr 1253, millega antakse üksikasjalikud juhised riiklikes turvasüsteemides rakendatavate turvameetmete kohta.

([306]) Korralduse EO 14086 paragrahvi 2 punkti d alapunkti i alapunktid A–B.

([307]) Korralduse EO 14086 paragrahvi 2 punkti d alapunkti i alapunktid B–C.

([308]) St USA kohaldatava õiguse süsteemne või tahtlik järgimata jätmine, mis võib kahtluse alla seada luureühenduse mõne üksuse maine või terviklikkuse või muul viisil seada kahtluse alla luureühenduse tegevuse asjakohasuse, sealhulgas mis tahes oluline mõju asjaomase isiku või asjaomaste isikute eraelu puutumatusele ja kodanikuvabadustega seotud huvidele, vt korralduse EO 14086 paragrahvi 5 punkt l.

([309]) Korralduse EO 14086 paragrahvi 2 punkti d alapunkt iii.

([310]) Korralduse EO 14086 paragrahvi 2 punkti d alapunkti i alapunkt B.

(164) Nagu kriminaalõiguskaitseasutustes on eraelu puutumatuse ja kodanikuvabaduste ametnikud olemas ka kõigis luureasutustes ([311]). Üldjuhul on nende ametnike pädevuses teha järelevalvet menetluste üle, millega tagatakse, et ministeeriumis/asutuses on eraelu puutumatuse ja kodanikuvabaduste kaitsega seotud küsimusega piisavalt arvestatud ning et asutus on kehtestatud nõuetekohased menetlused enda eraelu puutumatuse või kodanikuvabaduste rikkumise üle kaevanud üksikisikute kaebuste läbivaatamiseks (ning mõningatel asutustel, näiteks riikliku luurejuhi bürool (ODNI), on ka õigus kaebusi iseseisvalt uurida ([312])). Luureasutuste juhid peavad tagama, et eraelu puutumatuse ja kodanikuvabaduste ametnikel on oma volituste täitmiseks vajalikud vahendid, et neil on juurdepääs kõikidele oma ülesannete täitmiseks vajalikele materjalidele ja töötajatele ning et neid teavitatakse poliitika kavandatud muudatustest ning nendega konsulteeritakse ([313]). Privaatsus- ja kodanikuvabaduste ametnikud esitavad USA Kongressile ja eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjonile (PCLOB) korrapäraselt aruandeid, sealhulgas ministeeriumile/asutusele laekunud kaebuste arvu ja laadi kohta ning selliste kaebuste lahendamise kokkuvõtte ja korraldatud läbivaatamiste ja uurimiste ning ametniku tegevuse mõju kohta ([314]).

(165) Teiseks on igal luureasutusel oma sõltumatu peainspektor, kelle üks tööülesandeid on jälgida välisluuretegevust. Nende hulka kuulub ODNI koosseisu kuuluv luureühenduse peainspektori büroo, kellel 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 ([315]). Nagu kriminaalõiguskaitseasutuste puhul (vt põhjendus 109) on sellised peainspektorid seaduslikult sõltumatud ([316]) ja vastutavad vastava asutuse riikliku julgeolekuga seotud programmide ja tegevuste auditeerimise ja uurimise eest, sealhulgas kuritarvituste ja seaduserikkumiste puhul ([317]). Neil on juurdepääs kõikidele andmetele, aruannetele, audititele,

([311]) Vt USA seadustiku 42. jaotise § 2000ee-1. Nende hulgas on näiteks USA välisministeerium, justiitsministeerium, sisejulgeoleku ministeerium, kaitseministeerium, NSA, Luure Keskagentuur (CIA), FBI ja ODNI.

([312]) Vt korralduse EO 14086 paragrahvi 3 punkt c.

([313]) USA seadustiku 42. jaotise § 2000ee-1 punkt d.

([314]) Vt USA seadustiku 42. jaotise § 2000ee-1 punkti f alapunktid 1, 2. Näiteks NSA kodanikuvabaduste, eraelu puutumatuse ja läbipaistvuse büroo aruandest, mis hõlmab ajavahemikku 2021. aasta jaanuarist 2021. aasta juunini, tuleb välja, et asutus korraldas erinevates kontekstides 591 kodanikuvabadustele ja eraelu puutumatusele avalduva mõju läbivaatamist, nt seoses kogumistoimingute, teabe jagamise korralduse ja otsustega, andmete säilitamise otsustega jms, võttes arvesse erinevaid tegureid, nagu tegevusega seotud teabe hulk ja liik, kaasatud isikud, andmete eesmärk ja eeldatav kasutamine, kaitsemeetmed võimalike privaatsusriskide maandamiseks jne (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Samamoodi annavad CIA eraelu puutumatuse ja kodanikuvabaduste büroo aruanded, mis hõlmavad ajavahemikku 2019. aasta jaanuarist juunini, teavet büroo järelevalvetegevuse kohta, nt justiitsministri suunistele vastavuse kontroll vastavalt korraldusele EO 12333 seoses teabe säilitamise ja levitamisega, PPD-28 rakendamiseks antud juhised ning andmetega seotud rikkumiste tuvastamise ja kõrvaldamise nõuded ning isikuandmete kasutamise ja käitlemise läbivaatamised (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Peainspektori nimetab ametisse president ja kinnitab senat ning teda saab ametist vabastada ainult president.

([316]) 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, tegemise 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 seaduse (Inspector General Act of 1978) § 8 (kaitseministeeriumi kohta); § 8E (justiitsministeeriumi kohta), § 8G punkti d alapunkti 2 alapunktid A, B (NSA kohta); USA seadustiku 50. jaotise § 403q punkt b (CIA kohta); 2010. eelarveaastaks vastu võetud seadus luuretegevuse lubamise kohta (Intelligence Authorization Act For Fiscal Year 2010), paragrahvi 405 punkt f (luureühenduse kohta).

([317]) 1978. aasta peainspektori seadus (muudetud), Pub. L. 117–108, 8. aprill 2022. Näiteks nagu on selgitatud NSA peainspektori poolaastaaruannetes USA Kongressile ajavahemiku 1. aprillist 2021 kuni 31. märtsini 2022 kohta, hindas NSA peainspektor korralduse 12333 alusel kogutud USA isikuandmete käitlemist, signaaliluure andmete puhastamise protsessi, NSA kasutatavat automaatset sihtimisvahendit ning vastavust dokumenteerimise ja päringute tegemise reeglitele seoses FISA paragrahvi 702 kohase andmete kogumisega, ning andis sellega seoses mitu soovitust (vt https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, lk 5–8 ja https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, lk 10–13). Vt ka luureühenduse peainspektori hiljutised auditid ja uurimised infoturbe ja salastatud riikliku julgeolekuteabe loata avalikustamise kohta (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, lk 8, 11 ja https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, lk 19–20).

protokollidele, dokumentidele, poliitikamaterjalidele, soovitustele ja muudele materjalidele, vajaduse korral kohtukorralduse alusel, ning nad võivad võtta tunnistajatelt ütlusi ([318]). Peainspektorid edastavad kuriteokahtlusega juhtumid prokuratuurile ja annavad asutuste juhtidele soovitusi parandusmeetmete võtmiseks ([319]). Ehkki nad annavad üksnes mittesiduvaid soovitusi, nende aruanded ja teave aruannete alusel võetud meetmete (või nende puudumise) ([320]) kohta üldiselt avalikustatakse ning saadetakse USA Kongressile, kes saab nende alusel ise järelevalvet teha (vt põhjendused 168–169) ([321]).

(166) Kolmandaks jälgib USA luureorganite tegevuse vastavust põhiseadusele ja kõigile kehtivatele eeskirjadele presidendi luuretegevuse nõuandekogu (President's Intelligence Advisory Board (PIAB)) juurde loodud luuretegevuse järelevalve nõukogu (Intelligence Oversight Board (IOB)) ([322]). PIAB on presidendi kantselei koosseisu kuuluv nõuandev organ, mis koosneb 16 liikmest, kelle nimetab ametisse president väljastpoolt USA valitsust. IOB koosneb kuni viiest liikmest, kelle nimetab ametisse president PIAB liikmete hulgast. Korralduse EO 12333 kohaselt ([323]) on kõigi luureasutuste juhid kohustatud teavitama IOBd luuretegevusest, mille puhul on alust arvata, et see võib olla ebaseaduslik või vastuolus täidesaatva korralduse või presidendi suunisega. Selleks et tagada IOB-le juurdepääs oma ülesannete täitmiseks vajalikule teabele, paneb täidesaatev korraldus (EO) 13462 riiklikule luurejuhile ja luureasutuste juhtidele kohustuse anda seadusega lubatud piirides teavet ja abi, mida IOB peab oma ülesannete täitmiseks vajalikuks ([324]). IOB omakorda on kohustatud teavitama presidenti luuretegevusest, mis tema arvates võib rikkuda USA seadusi (sealhulgas täidesaatvaid korraldusi) ja millega justiitsminister, riiklik luurejuht või luureasutuse juht ei ole piisavalt tegelenud ([325]). Lisaks on IOB kohustatud teavitama justiitsministrit võimalikest kriminaalõiguse rikkumistest.

(167) Neljandaks alluvad luureasutused PCLOBi järelevalvele. Vastavalt selle asutamismäärusele on PCLOB-le usaldatud ülesanded terrorismivastase võitluse poliitika ja selle rakendamise valdkonnas, eesmärgiga kaitsta eraelu puutumatust ja kodanikuvabadusi. Luureasutuste 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 ([326]). Ta saab aruandeid mitme föderaalministeeriumi/asutuse kodanikuvabaduste ja eraelu puutumatuse kaitse ametnikelt, ([327]) võib anda valitsus- ja luureasutustele soovitusi ning annab korrapäraselt aru USA Kongressi komiteedele ja presidendile ([328]). Juhatuse aruanded, sealhulgas need, mis esitatakse USA Kongressile, peavad olema võimalikult suures ulatuses avalikult kättesaadavad ([329]). PCLOB on välja andnud mitu järelevalve- ja järelkontrolliaruannet, sealhulgas analüüs FISA paragrahvi 702 alusel käivitatud programmide ja eraelu puutumatuse kaitse kohta selles kontekstis, PPD-28 ja korralduse 12333 rakendamise kohta ([330]). PCLOBi ülesandeks on ka korralduse EO 14086

([318]) Vt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 6.

([319]) Vt samas § 4, 6–5.

([320]) Peainspektorite aruannete ja soovituste alusel võetud järelmeetmete kohta vt nt vastus justiitsministeeriumi peainspektori aruandele, milles leiti, et 2014.–2019. aastal FISC-le esitatud taotlustes ei olnud FBI piisavalt läbipaistev, mis tõi kaasa reformid nõuete täitmise, järelevalve ja aruandekohustuse tõhustamiseks FBIs (nt FBI direktor andis korralduse teha rohkem kui 40 parandusmeedet, sealhulgas 12 parandusmeedet, mis olid otseselt seotud FISA kohase dokumenteerimise, järelevalve, toimikute haldamise, koolituse ja auditite protsessiga) (vt https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance ja https://oig.justice.gov/reports/2019/o20012.pdf). Vt ka näiteks justiitsministeeriumi peainspektori audit FBI õigusnõuniku büroo rollide ja kohustuste kohta FBI riikliku julgeolekualase tegevusega seotud kohaldatavate seaduste, põhimõtete ja menetluste järgimise kontrollimisel ning 2. lisa, mis sisaldab FBI kirja, milles nõustutakse kõigi soovitustega. Sellega seoses annab 3. liide ülevaate järelmeetmetest ja teabest, mida peainspektor FBI-lt nõudis, et ta saaks oma soovituste menetluse lõpetada (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Vt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 4(5), 5.

([322]) Vt korraldus EO 13462.

([323]) Korralduse EO 12333 paragrahvi 1.6 punkt c.

([324]) Korralduse EO 13462 paragrahvi 8 punkt a.

([325]) Korralduse EO 13462 paragrahvi 6 punkt b.

([326]) USA seadustiku 42. jaotise § 2000ee punkt g.

([327]) Vt USA seadustiku 42. jaotise § 2000ee-1 punkti f alapunkti 1 alapunkti A alapunkt iii. Need on vähemalt justiitsministeerium, kaitseministeerium, sisejulgeoleku ministeerium, riiklik luurejuht ja Luure Keskagentuur ning lisaks muud ministeeriumid, asutused või täitevvõimu organid, kelle puhul PCLOB seda vajalikuks peab.

([328]) USA seadustiku 42. jaotise § 2000ee punkt e.

([329]) USA seadustiku 42. jaotise § 2000ee punkt f.

([330]) Kättesaadav aadressil https://www.pclob.gov/Oversight.

rakendamisega seotud konkreetsete järelevalveülesannete täitmine, eelkõige kontrollides, kas asutuse menetlused on korraldusega kooskõlas (vt põhjendus 126), ja hinnates õiguskaitsemehhanismi toimimist (vt põhjendus 194).

(168) Viiendaks on lisaks neile täitevvõimu järelevalvemehhanismidele järelevalvekohustused kogu USA välisluuretegevuse suhtes USA kongressi erikomiteedel, täpsemalt esindajatekoja ja senati luure- ja kohtukomiteel. Nimetatud komiteede liikmetel on juurdepääs salastatud teabele ning luuremeetoditele ja -programmidele ([331]). Komiteed täidavad järelevalveülesandeid eri viisidel, eelkõige kuulamiste, uurimiste, läbivaatamiste ja aruannete kaudu ([332]).

(169) Kongressi komiteed saavad korrapäraselt aruandeid luuretegevuse kohta, sealhulgas justiitsministrilt, riiklikult luurejuhilt, luureasutustelt ja muudelt järelevalveorganitelt (nt peainspektoritelt), vt põhjendused 164–165. Eelkõige peab president vastavalt riikliku julgeoleku seadusele (National Security Act) „tagama, et kongressi luurekomiteedel oleks täielik ja ajakohane teave Ameerika Ühendriikide luuretegevuse kohta, sealhulgas oluliste tulevikus kavandatavate luuretegevuste kohta vastavalt käesoleva alapeatüki nõuetele“ ([333]). Lisaks peab president „tagama, et kongressi luurekomiteesid teavitatakse viivitamata mis tahes ebaseaduslikust luuretegevusest ja ebaseadusliku tegevusega seoses võetud või kavandatavatest parandusmeetmetest“ ([334]).

(170) Lisaks tulenevad täiendavad aruandlusnõuded spetsiifilistest põhimäärustest. Eelkõige nõuab FISA, et justiitsminister peab senati ja esindajatekoja luure- ja kohtukomiteesid mõningate FISA paragrahvide alla kuuluvatest valitsuse tegevustest „täielikult teavitama“ ([335]). Samuti nõuab see, et valitsus esitaks kongressi komiteedele „koopiad kõikidest FISC või FISCR otsustest, määrustest ja arvamustest, millega „olulisel määral sisustatakse või tõlgendatakse“ FISA sätteid. Mis puudutab FISA paragrahvi 702 kohast jälgimist toimub parlamendi järelevalve luure- ja kohtukomiteedele seaduse alusel esitatavate aruannete ning sagedase teavitamise ja kuulamiste kaudu. Nende hulka kuulub kaks korda aastas esitatav justiitsministri aruanne FISA paragrahvi 702 kasutamise kohta koos tõendavate dokumentidega, sealhulgas justiitsministeeriumi ja ODNI vastavuskontrolli aruannetega ning mittevastavusjuhtumite kirjeldusega, ([336]) ning samuti kaks korda aastas esitatav justiitsministri ja riikliku luurejuhi hinnang, milles kirjeldatakse sihtimis- ja minimeerimismenetluste järgimist ([337]).

([331]) USA seadustiku 50. jaotise § 3091.

([332]) Näiteks korraldavad komiteed temaatilisi kuulamisi (vt nt esindajatekoja kohtukomitee hiljutine kuulamine „digitaalsete haarangute“ teemal, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, ning esindajatekoja luurekomitee kuulamine tehisintellekti kasutamise kohta luureühenduses, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), korrapäraseid järelevalveteemalisi kuulamisi, nt FBI ja justiitsministeeriumi riiklik julgeoleku osakonna kuulamised, vt https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 ja https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Uurimise näitena vt senati luurekomitee uurimist Venemaa sekkumise kohta 2016. aasta USA valimistesse, vt https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Aruandluse kohta vt nt ülevaade senatile komitee (järelevalve)tegevusest senati luurekomitee aruandes ajavahemiku 4. jaanuarist 2019 kuni 3. jaanuarini 2021 kohta, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Vt USA seadustiku 50. jaotise § 3091 punkti a alapunkt 1. See säte sisaldab üldnõudeid seoses kongressi järelevalvega riikliku julgeoleku valdkonnas.

([334]) Vt USA seadustiku 50. jaotise § 3091 punkt b.

([335]) Vt USA seadustiku 50. jaotise § 1808, 1846, 1862, 1871, 1881f.

([336]) Vt USA seadustiku 50. jaotise § 1881f.

([337]) Vt USA seadustiku 50. jaotise § 1881a lõike l punkt 1.

(171) Lisaks on FISAs kehtestatud USA valitsusele nõue avaldada igal aastal kongressile (ja üldsusele) muu hulgas taotletud ja saadud FISA kohaste kohtumääruste arv ning luuretegevuse subjektiks olnud USA isikute ja USA-väliste isikute hinnangulise arv ([338]). Kõnealune seadus nõuab ka välja antud riikliku julgeoleku teabenõuete arvu avalikustamist eraldi USA isikute ja USA-väliste isikute kohta (lubades samas FISA kohaste korralduste ja kinnituste ning riikliku julgeoleku teabenõuete saajatel avaldada teatavatel tingimustel läbipaistvusaruandeid) ([339]).

(172) Üldisemalt rakendab USA luureühendus oma (välis)luuretegevuse läbipaistvuse tagamiseks erinevaid meetmeid. Näiteks võttis ODNI 2015. aastal vastu luureandmete läbipaistvuse põhimõtted ja läbipaistvuse rakenduskava ning andis igale luureasutusele ülesande nimetada ametisse luureandmete läbipaistvuse ametnik, et edendada läbipaistvust ja juhtida läbipaistvusalgatusi ([340]). Nende meetmete raames on luureühendus avalikustanud ja avalikustab jätkuvalt poliitika, menetluste, järelevalvearuannete, FISA paragrahvi 702 ja korralduse 12333 kohaste tegevuste aruannete, FISC otsuste ja muude materjalide saladuse kaitse alt vabastatud osi, sealhulgas spetsiaalsel veebisaidil „IC on the Record", mida haldab ODNI ([341]).

(173) Lõpuks teeb FISA paragrahvi 702 kohase isikuandmete kogumise üle lisaks põhjendustes 162–168 nimetatud järelevalveorganite tehtavale järelevalvele järelevalvet ka FISC ([342]). Vastavalt FISC kodukorra artiklile 13 on USA luureasutuste järelevalveametnikud kohustatud teatama kõigist FISA paragrahvi 702 kohaste sihtimis-, minimeerimis- ja päringumenetluste rikkumistest justiitsministeeriumile ja ODNI-le, kes omakorda teatavad nendest FISC-le. Lisaks esitavad justiitsministeerium ja ODNI FISC-le kaks korda aastas ühised järelevalve hindamise aruanded, milles määratakse kindlaks sihtimisnõuetele vastavuse suundumused; esitatakse statistilised andmed; kirjeldatakse mittevastavuse juhtumite kategooriaid; kirjeldatakse üksikasjalikult põhjusi, miks teatavad sihtimisnõuete järgimisega seotud juhtumid aset leidsid, ja kirjeldatakse meetmeid, mida luureasutused on kordumise vältimiseks võtnud ([343]).

(174) Vajaduse korral (nt kui tuvastatakse sihtimismenetluse rikkumine) võib kohus anda asjaomasele luureasutusele korralduse võtta parandusmeetmeid ([344]). Kõnealused parandusmeetmed võivad ulatuda individuaalsetest kuni struktuurimeetmeteni, nt andmete kogumise lõpetamisest ja ebaseaduslikult saadud andmete kustutamisest kuni kogumistavade muutmiseni, sealhulgas töötajate juhendamine ja koolitamine ([345]). Lisaks võtab FISC paragrahvi 702 kohaste sertifikaatide iga-aastasel läbivaatamisel arvesse nõuetele mittevastavuse juhtumeid, et teha kindlaks, kas

([338]) USA seadustiku 50. jaotise § 1873 punkt b. Lisaks on paragrahvis 402 sätestatud, et „riiklik luurejuht korraldab justiitsministriga kooskõlastatult salastatusest vabastamise läbivaatamise kõikidele välisluure järelevalve kohtu 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".

([339]) USA seadustiku 50. jaotise § 1873 punkti b alapunkt 7 ja § 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Vt „IC on the Record", kättesaadav aadressil https://icontherecord.tumblr.com/.

([342]) Varem on FISC järeldanud, et „[kohtu] jaoks on ilmne, et rakendusasutused, nagu ka [ODNI] ja [justiitsministeeriumi riikliku julgeoleku osakond] pühendavad märkimisväärseid ressursse oma nõuetele vastavuse ja järelevalve kohustuste täitmiseks vastavalt paragrahvile 702. Üldjuhul tuvastatakse mittevastavuse juhtumid viivitamata ja võetakse asjakohaseid parandusmeetmeid, sealhulgas eemaldatakse teave, mis on saadud nõuetele mittevastavalt või mille suhtes kehtivad muul viisil hävitamisnõuded." FISA kohus, Memorandum Opinion and Order [pealkirja on muudetud] (2014), kättesaadav aadressil https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Vt nt justiitsministeeriumi/ODNI FISA paragrahvi 702 kohane vastavusaruanne FISC-le ajavahemiku 2018. aasta juuni kuni november kohta, lk 21–65.

([344]) USA seadustiku 50. jaotise § 1803 punkt h. Vt ka PCLOBi paragrahvi 702 kohane aruanne, lk 76. Vt lisaks FISC 3. oktoobri 2011. aasta memorandum arvamuse ja määruse kohta (Memorandum Opinion and Order), mis on näide puuduste kõrvaldamise korraldusest, millega pandi valitsusele kohustus tuvastatud puudused 30 päeva jooksul parandada. Kättesaadav aadressil https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Vt Waltoni kiri, punkt 4, lk 10–11. Vt ka FISC 18. oktoobri 2018. aasta arvamus, kättesaadav aadressil https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, mida välisluure järelevalve apellatsioonikohus kinnitas oma 12. juuli 2019. aasta arvamuses, kättesaadav aadressil https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, ja milles FISC andis muu hulgas valitsusele korralduse täita teatavad FISC teavitamise, dokumenteerimise ja aruandluse nõuded.

([345]) Vt nt FISC, Memorandum Opinion and Order 76 (6. detsember 2019) (avaldamine lubatud 4. septembril 2020), milles FISC tegi valitsusele ülesandeks esitada 28. veebruariks 2020 kirjalik aruanne sammude kohta, mida valitsus on astunud, et parandada nende aruannete kindlakstegemise ja eemaldamise protsesse, mis on koostatud FISA paragrahvi 702 kohase teabe põhjal ja mis kutsuti tagasi vastavuse põhjustel, samuti muude küsimuste kohta. Vt ka VII lisa.

esitatud sertifikaadid vastavad FISA nõuetele. Samamoodi võib FISC, kui ta leiab, et valitsuse sertifikaadid ei olnud piisavad, sealhulgas konkreetsete vastavusjuhtumite tõttu, anda välja nn puuduste kõrvaldamise korralduse, millega nõutakse, et valitsus parandaks rikkumise 30 päeva jooksul või et valitsus lõpetaks paragrahvi 702 kohase sertifikaadi rakendamise või ei alustaks selle rakendamist. Lõpuks hindab FISC suundumusi, mida ta täheldab vastavusküsimustes, ja võib nõuda vastavussuundumuste käsitlemiseks menetluste muutmist või lisajärelevalvet ja -aruandlust ([346]).

3.2.3. ***Õiguskaitse***

(175) Nagu selles jaos üksikasjalikumalt selgitatud, on liidu andmesubjektidel Ameerika Ühendriikides mitu võimalikku viisi, kuidas esitada hagi siduva pädevusega sõltumatusse ja erapooletusse kohtusse. Kõik need viisid koos võimaldavad üksikisikutel pääseda juurde oma isikuandmetele, lasta kontrollida, kas valitsuse juurdepääs nende andmetele on seaduslik, ja rikkumise avastamise korral lasta selline rikkumine heastada, sealhulgas oma isikuandmete parandamise või kustutamise kaudu.

(176) Esiteks luuakse korralduse EO 14086 alusel spetsiaalne õiguskaitsemehhanism, mida täiendab justiitsministri määrus, millega asutatakse andmekaitseasju läbivaatav kohus, et käsitleda ja lahendada üksikisikute kaebusi USA signaaliluuretegevuse kohta. Igal ELi üksikisikul on õigus esitada õiguskaitsemehhanismile kaebus USA signaaliluuretegevust reguleerivate seaduste (nt korraldus EO 14086, FISA paragrahv 702, korraldus EO 12333) väidetava rikkumise kohta, mis kahjustab nende eraelu puutumatust ja kodanikuvabadusi ([347]). See õiguskaitsemehhanism on kättesaadav üksikisikutele, kes on pärit riikidest või piirkondlikest majandusintegratsiooni organisatsioonidest, mille USA justiitsminister on tunnistanud „nõuetele vastavateks riikideks“ ([348]). 30. juunil 2023 määras justiitsminist korralduse EO 14086 paragrahvi 3 punkt f alusel Euroopa Liidu ja kolm Euroopa Vabakaubanduse Assotsiatsiooni riiki, mis koos moodustavad Euroopa Majanduspiirkonna, „nõuetele vastavateks riikideks“ ([349]). Kõnealune nimetus ei piira Euroopa Liidu lepingu artikli 4 lõike 2 kohaldamist.

(177) Liidu andmesubjekt, kes soovib sellise kaebuse esitada, peab esitama selle ELi liikmesriigi järelevalveasutusele, kes on pädev tegema järelevalvet isikuandmete töötlemise üle riigi ametiasutustes (DPA) ([350]). See tagab hõlpsa juurdepääsu õiguskaitsemehhanismile, võimaldades üksikisikutel pöörduda nii-öelda kodulähedase asutuse poole, kellega nad saavad suhelda oma emakeeles. Pärast põhjenduses 178 osutatud kaebuse esitamise nõuete kontrollimist suunab pädev andmekaitseasutus kaebuse Euroopa Andmekaitsenõukogu sekretariaadi kaudu õiguskaitsemehhanismi.

(178) Kaebuse esitamisel õiguskaitsemehhanismile kehtivad leebed vastuvõetavuse nõuded, sest üksikisikud ei pea tõendama, et nende andme suhtes on tõesti toimunud USA signaaliluuretegevus ([351]). Samal ajal tuleb õiguskaitsemehhanismile läbivaatamise lähtepunktina anda teatav põhiteave, nt isikuandmete kohta, mille puhul on alust arvata, et need on USAsse edastatud, ja vahendite kohta, mille abil need arvatavalt edastati; väidetava rikkumisega arvatavalt seotud USA valitsusüksuste andmed (kui need on teada); alus, mille põhjal väidetakse, et USA seadusi on rikutud (kuigi ka selle puhul ei ole vaja tõendada, et USA luureagentuurid tõepoolest kogusid isikuandmeid), ja millist abi taotletakse.

([346]) Vt VII lisa.

([347]) Vt korralduse EO 14086 paragrahvi 4 punkti k alapunkt iv, milles on sätestatud, et õiguskaitsemehhanismile peab kaebuse esitama kaebuse esitaja, kes tegutseb enda nimel (st mitte valitsuse, valitsusvälise või valitsustevahelise organisatsiooni esindajana). Mõiste „negatiivselt mõjutanud“ ei kohusta kaebuse esitajat hüvitamismehhanismidele juurdepääsu saamiseks teatavat künnist täitma (vt selle kohta põhjendus 178). Pigem selgitab see, et ODNI kodanikuvabaduste kaitse ametnikul ja andmekaitseasju läbivaataval kohtul on volitused heastada signaaliluuretegevust reguleerivate USA seaduste rikkumisi, mis kahjustavad kaebuse esitaja eraelu puutumatust ja kodanikuvabadusi. Seevastu ei kuulu ODNI kodanikuvabaduste kaitse ametniku ja andmekaitseasju läbivaatava kohtu pädevusse kohaldatava USA õiguse selliste nõuete rikkumised, mis ei ole mõeldud üksikisikute kaitsmiseks (nt eelarvenõuded).

([348]) Korralduse EO 14086 paragrahvi 3 punkt f.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Korralduse EO 14086 paragrahvi 4 punkti d alapunkt v.

([351]) Vt korralduse EO 14086 paragrahvi 4 punkti k alapunktid i–iv.

(179) Asjaomasele õiguskaitsemehhanismile esitatud kaebuste esialgse uurimise viib läbi ODNI kodanikuvabaduste kaitse ametnik, kelle kehtivat seadusjärgset rolli ja volitusi on laiendatud korralduse EO 14086 alusel võetud erimeetmetele ([352]). Luureühenduses vastutab kodanikuvabaduste kaitse ametnik muu hulgas selle eest, et kodanikuvabaduste ja eraelu puutumatuse kaitse oleks asjakohaselt lõimitud ODNI ja luureasutuste põhimõttesse ja menetlustesse; selle jälgimise eest, et ODNI tegutseks vastavuses kohaldatavate kodanikuvabaduste ja privaatsusnõuetega, ning eraelu puutumatusele avalduva mõju hindamise eest ([353]). ODNI kodanikuvabaduste kaitse ametniku võib riiklik luurejuht vallandada ainult mõjuval põhjusel, st üleastumise, rikkumiste, turvanõuete rikkumise, kohustuste eiramise või töövõimetuse korral ([354]).

(180) Kaebuse läbivaatamisel on ODNI kodanikuvabaduste kaitse ametnikul oma hinnangu andmiseks juurdepääs teabele ning ta võib kohustada eri luureasutuste eraelu puutumatuse ja kodanikuvabaduste kaitse ametnikke abi andma ([355]). Luureasutustel on keelatud ODNI kodanikuvabaduste kaitse ametniku läbivaatamist takistada või seda sobimatult mõjutada. See käib ka riikliku luurejuhi kohta, kes ei tohi läbivaatamisse sekkuda ([356]). Kaebuse läbivaatamisel peab ODNI kodanikuvabaduste kaitse ametnik kohaldama seadust erapooletult, võttes arvesse nii riigi julgeolekuhuve signaaliluuretegevuses kui ka eraelu puutumatuse kaitset ([357]).

(181) Läbivaatamise raames teeb ODNI kodanikuvabaduste kaitse ametnik kindlaks, kas kohaldatavaid USA seadusi on rikutud, ja kui see on nii, otsustab asjakohaste õiguskaitsemeetmete võtmise üle ([358]). Viimati nimetatu osutab meetmetele, millega tuvastatud rikkumine täielikult parandatakse, näiteks andmete ebaseadusliku hankimise lõpetamine, ebaseaduslikult kogutud andmete kustutamine, ebakorrektselt tehtud päringute või muul viisil ebaseaduslikult kogutud andmete tulemuste kustutamine, seaduslikult kogutud andmetele juurdepääsu piiramine asjakohaselt koolitatud töötajatega või seadusliku loata saadud või ebaseaduslikult levitatud andmeid sisaldavate luurearuannete tagasikutsumine ([359]). ODNI kodanikuvabaduste kaitse ametniku otsused üksikkaebuste kohta (sealhulgas õiguskaitsemeetmete kohta) on asjaomastele luureasutustele siduvad ([360]).

(182) ODNI kodanikuvabaduste kaitse ametnik peab säilitama oma läbivaatamise dokumendid ja esitama salastatud otsuse, milles selgitatakse tema faktiliste järelduste alust, selle kindlaksmääramist, kas käsitletud rikkumine toimus, ja asjakohaste õiguskaitsemeetmete määramist ([361]). Kui ODNI kodanikuvabaduste kaitse ametniku läbivaatamise käigus tuleb ilmsiks mõne FISC järelevalve alla kuuluva asutuse rikkumine, peab kodanikuvabaduste kaitse ametnik esitama salastatud aruande ka asejustiitsministrile riikliku julgeoleku küsimustes, kes omakorda on kohustatud rikkumisest teavitama FISCd, kes võib võtta täiendavaid täitemeetmeid (kooskõlas põhjendustes 173–174 kirjeldatud menetlusega) ([362]).

(183) Kui läbivaatamine on lõpule viidud, teatab ODNI kodanikuvabaduste kaitse ametnik kaebuse esitajale riigi ametiasutuse kaudu, et „läbivaatamise käigus ei tuvastatud ühtegi kaebuses hõlmatud rikkumist“ või et „ODNI kodanikuvabaduste kaitse ametnik tegi otsuse, millega nõutakse asjakohaste õiguskaitsemeetmete võtmist“ ([363]). See võimaldab kaitsta riigi julgeoleku kaitseks tehtud toimingute konfidentsiaalsust, andes samal ajal üksikisikutele otsuse, mis kinnitab, et nende kaebust on nõuetekohaselt uuritud ja lahendatud. Pealegi võib üksikisik selle otsuse vaidlustada. Selleks teavitatakse teda võimalusest esitada kodanikuvabaduste kaitse ametniku otsuste läbivaatamiseks kaebus andmekaitseasju läbivaatavale kohtule (vt põhjendus 184 jj) ning et juhul, kui kohtusse pöördutakse, valitakse kaebuse esitaja huvidest lähtuvalt eriadvokaat ([364]).

([352]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt iv. Vt ka 1947. aasta riikliku julgeoleku seadus (National Security Act), USA seadustiku 50. jaotise § 403-3d, paragrahv 103D, mis käsitleb kodanikuvabaduste kaitse ametniku rolli ODNIs.
([353]) USA seadustiku 50. jaotise § 3029 punkt b.
([354]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt iv.
([355]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt iii.
([356]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt iv.
([357]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkti i alapunkti B alapunktid i ja iii.
([358]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt i.
([359]) Korralduse EO 14086 paragrahvi 4 punkt a.
([360]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt d.
([361]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt i alapunktid F–G.
([362]) Vt korralduse EO 14086 paragrahvi 3 punkti c alapunkti i alapunkt D.
([363]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt E alapunkt 1.
([364]) Korralduse EO 14086 paragrahvi 3 punkti c alapunkt E alapunktid 2–3.

(184) Igal kaebuse esitajal ja kõigil luureühenduse üksustel on võimalik taotleda ODNI kodanikuvabaduste kaitse ametniku otsuse läbivaatamist andmekaitseasju läbivaatavas kohtus. Sellised läbivaatamistaotlused tuleb esitada 60 päeva jooksul pärast ODNI kodanikuvabaduste kaitse ametnikult teate saamist selle kohta, et läbivaatamine on lõpule viidud, ning need peavad sisaldama kogu teavet, mida isik soovib andmekaitseasju läbivaatavale kohtule esitada (nt argumendid õigusküsimuste või õiguse kohaldamise kohta juhtumi faktiliste asjaolude suhtes) ([365]). Liidu andmesubjektid võivad oma taotluse uuesti esitada pädevale andmekaitseasutusele (vt põhjendus 177).

(185) Andmekaitseasju läbivaatav kohus on sõltumatu kohus, mille asutas justiitsminister korralduse EO 14086 alusel ([366]). See koosneb vähemalt kuuest kohtunikust, kelle nimetab neljaks aastaks ametisse justiitsminister, konsulteerides eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoniga, kaubandusministri ja riikliku luurejuhiga ([367]). Kohtunike ametisse nimetamisel lähtub justiitsminister kriteeriumidest, mida täitevvõim kasutab föderaalkohtunike kandidaatide hindamisel, võttes arvesse eelnevat kohtunikukogemust ([368]). Lisaks peavad kohtunikud olema juristid (st advokatuuri aktiivsed liikmed, kellel on õigus advokaadina tegutseda) ning neil peab olema asjakohane kogemus eraelu puutumatuse ja riikliku julgeoleku valdkonnas. Justiitsminister peab püüdma tagada, et igal ajahetkel oleks vähemalt pooltel kohtunikest eelnev kohtukogemus ja kõik kohtunikud peavad olema läbinud julgeolekukontrolli, et pääseda juurde riigi salastatud riigi julgeolekuteabele ([369]).

(186) Andmekaitseasju läbivaatavasse kohtusse võib ametisse nimetada ainult isikud, kellel on põhjenduses 185 nimetatud kvalifikatsioon ja kes ei ole ametisse nimetamise ajal või sellele eelneva kahe aasta jooksul täitevvõimu asutuse töötajad. Samamoodi ei tohi kohtunikel andmekaitseasju läbivaatavas kohtus ametisoleku ajal olla USA valitsuses mingeid ametlikke kohustusi ega töösuhet (välja arvatud andmekaitseasju läbivaatava kohtu kohtunikuna) ([370]).

(187) Kohtuotsusprotsessi sõltumatus saavutatakse mitme tagatise abil. Eelkõige ei tohi täitevvõim (justiitsminister ja luureasutused) sekkuda andmekaitseasju läbivaatava kohtu tehtavasse läbivaatamisse või seda sobimatult mõjutada ([371]). Andmekaitseasju läbivaatav kohus ise on kohustatud kohtuasju erapooletult lahendama ([372]) ja ta tegutseb oma kodukorra kohaselt (võetakse vastu häälteenamusega). Peale selle võib andmekaitseasju läbivaatava kohtu kohtuniku ametist vabastada vaid justiitsminister ja üksnes mõjuval põhjusel (st üleastumise, rikkumiste, turvanõuete rikkumise, kohustuste täitmata jätmise või teovõimetuse tõttu) pärast seda, kui ta on võtnud nõuetekohaselt arvesse föderaalkohtunike suhtes kohaldatavaid standardeid, mis on sätestatud kohtunike käitumisjuhendis ja kohtunike teovõimetuse menetluse eeskirjas ([373]).

([365]) Justiitsministri määruse paragrahvi 201.6 punktid a–b.

([366]) Justiitsministri määruse paragrahvi 3 punkti d alapunkt i. Ameerika Ühendriikide ülemkohus on kinnitanud justiitsministri võimalust luua sõltumatuid otsustusõigusega organeid, sealhulgas üksikjuhtumite lahendamiseks, vt eelkõige United States ex rel. Accardi *vs.* Shaughnessy, 347 U.S. 260 (1954) ja United States *vs.* Nixon, 418 U.S. 683, 695 (1974). Korralduse EO 14086 erinevatele nõuetele vastavuse üle, nt andmekaitseasju läbivaatava kohtu kohtunike ametisse nimetamise ja ametist vabastamise kriteeriumid ja kord, teeb järelevalvet eelkõige justiitsministeeriumi peainspektor (vt ka põhjendus 109 peainspektorite seadusjärgsete volituste kohta).

([367]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt A ja justiitsministri määruse paragrahvi 201.3 punkt a.

([368]) Justiitsministri määruse paragrahvi 201.3 punkt b.

([369]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt B.

([370]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt A ja justiitsministri määruse paragrahvi 201.3 punktid a ja c. Andmekaitseasju läbivaatavasse kohtusse nimetatud isikud võivad osaleda kohtuvälises tegevuses, sealhulgas äritegevuses, finantstegevuses, mittetulunduslikus raha kogumises ja usaldusel põhinevas tegevuses, samuti advokaadipraktikas, kui selline tegevus ei sega nende kohustuste erapooletut täitmist või tõhusust või sõltumatust (justiitsministri määruse paragrahvi 201.7 punkt c).

([371]) Korralduse EO 14086 paragrahvi 3 punkti d alapunktid iii–iv ja justiitsministri määruse paragrahvi 201.7 punkt d.

([372]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt D ja justiitsministri määruse paragrahv 201.9.

([373]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkt iv ja justiitsministri määruse paragrahvi 201.7 punkt d. Vt ka kohtuasi Bumap *vs.* United States, 252 U.S. 512, 515 (1920), milles kinnitati USA õiguse kauaaegset põhimõtet, et ametist taandamise volitus on seotud ametisse nimetamise volitusega (nagu tuletas meelde ka justiitsministeeriumi õigusnõuniku büroo dokumendis „The Constitutional Separation of Powers Between the President and Congress“, 20 Op. O.L.C. 124, 166 (1996)).

(188) Andmekaitseasju läbivaatavale kohtule esitatud taotlused vaatavad läbi kolmest kohtunikust koosnevad kolleegiumid, sealhulgas eesistuja, kes peab tegutsema USA kohtunike käitumisjuhendi kohaselt ([374]). Iga kolleegiumi abistab eriadvokaat, ([375]) kellel on juurdepääs kogu juhtumiga seotud teabele, sealhulgas salastatud teabele ([376]). Eriadvokaadi ülesanne on tagada, et kaebuse esitaja huvid on esindatud ja et andmekaitseasju läbivaatava kohtu kohtunike kolleegium on kõigi asjakohaste õigus- ja faktiküsimustega hästi kursis ([377]). Selleks et saada lisateavet oma seisukoha kujundamiseks üksikisiku andmekaitseasju läbivaatavale kohtule esitatud läbivaatamistaotluse kohta võib eriadvokaat küsida kaebuse esitajalt teavet kirjalike küsimuste kaudu ([378]).

(189) Andmekaitseasju läbivaatav kohus vaatab ODNI kodanikuvabaduste kaitse ametniku tehtud otsused läbi (nii selle kohta, kas kohaldatava USA õiguse rikkumine toimus, kui ka asjakohaste õiguskaitsemeetmete kohta), tuginedes vähemalt ODNI kodanikuvabaduste kaitse ametniku uurimise andmetele, samuti kaebuse esitaja, eriadvokaadi või luureasutuse esitatud teabele ja esildistele ([379]). Andmekaitseasju läbivaatava kohtu kolleegiumil on juurdepääs kogu teabele, mis on vajalik läbivaatamiseks ja mida ta võib hankida ODNI kodanikuvabaduste kaitse ametniku kaudu (kolleegium võib näiteks nõuda, et kodanikuvabaduste kaitse ametnik täiendaks oma dokumenti lisateabe või faktiliste järeldustega, kui see on läbivaatamiseks vajalik) ([380]).

(190) Läbivaatamise lõpetamisel võib andmekaitseasju läbivaatav kohus 1) otsustada, et puuduvad tõendid selle kohta, et kaebuse esitaja isikuandmetega seotud signaaliluuretegevus leidis aset, 2) otsustada, et ODNI kodanikuvabaduste kaitse ametniku otsused olid õiguslikult korrektsed ja neid toetasid olulised tõendid, või 3) kui andmekaitseasju läbivaatav kohus ei nõustu ODNI kodanikuvabaduste kaitse ametniku otsustega (kohaldatava USA õiguse rikkumise toimumise või asjakohaste õiguskaitsemeetmetega), väljastab ta oma otsused ([381]).

([374]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt B ja justiitsministri määruse paragrahvi 201.7 punktid a–c. Justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste amet, kes vastutab andmekaitseasju läbivaatavale kohtule ja eriadvokaatidele haldustoe pakkumise eest (vt justiitsministri määruse paragrahv 201.5), valib rotatsiooni korras kolmeliikmelise kolleegiumi, püüdes tagada, et igas kolleegiumis on vähemalt üks kohtunik, kellel on eelnev kohtunikukogemus (kui ühelgi kohtunikel ei ole sellist kogemust, on eesistuja kohtunik, kelle justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste amet valib esimesena).

([375]) Justiitsministri määruse paragrahv 201.4. Justiitsminister määrab kaubandusministri, riikliku luurejuhi ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoniga konsulteerides ametisse vähemalt kaks eriadvokaati kaheks ametiajaks, mida saab pikendada. Eriadvokaatidel peab olema asjakohane kogemus eraelu puutumatuse ja riikliku julgeoleku õiguse valdkonnas, nad peavad olema kogenud advokaadid, advokatuuri aktiivsed liikmed ja neil peab olema nõuetekohane litsents advokaadina tegutsemiseks. Lisaks ei tohi nad esialgse ametisse nimetamise ajal olla olnud täitevvõimu töötajad kahe eelneva aasta jooksul. Igaks taotluse läbivaatamiseks valib kohtu eesistuja eriadvokaadi, kes abistab kolleegiumi, vt justiitsministri määruse paragrahvi 201.8 punkt a.

([376]) Justiitsministri määruse paragrahvi 201.8 punkti c ja paragrahv 201.11.

([377]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt C ja justiitsministri määruse paragrahvi 201.8 punkt e. Eriadvokaat ei tegutse kaebuse esitaja esindajana ja tal ei ole kaebuse esitajaga advokaadi-kliendi suhet.

([378]) Vt justiitsministri määruse paragrahvi 201.8 punkti d alapunkt e. Sellised küsimused vaatab kõigepealt läbi justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste amet, konsulteerides asjaomase luureühenduse üksusega, et tuvastada ja välistada salastatud või privilegeeritud või kaitstud teave enne selle edastamist kaebuse esitajale. Lisateave, mille eriadvokaat sellistele küsimustele vastuseks sai, lisatakse esildisse, mille eriadvokaat esitab andmekaitseasju läbivaatavale kohtule.

([379]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt D.

([380]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkt iii ja justiitsministri määruse paragrahvi 201.9 punkt b.

([381]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt E ja justiitsministri määruse paragrahvi 201.9 punktid c–e. Korralduse EO 14086 paragrahvi 4 punktis a sätestatud „asjakohaste õiguskaitsemeetmete“ määratluse kohaselt peab andmekaitseasju läbivaatav kohus, kui ta otsustab võtta rikkumise täielikuks kõrvaldamiseks parandusmeetme, võtma arvesse „viise, kuidas tuvastatud rikkumist on tavapäraselt käsitletud“, st andmekaitseasju läbivaatav kohus kaalub muu hulgas seda, kuidas sarnaseid vastavusprobleeme varem on lahendatud, et tagada parandusmeetme tõhusus ja asjakohasus.

(191) Kõigil juhtudel võtab andmekaitseasju läbivaatav kohus vastu kirjaliku otsuse häälteenamuse alusel. Kui läbivaatamisel ilmneb kohaldatavate normide rikkumine, määratakse otsuses asjakohased parandusmeetmed, mis hõlmavad ebaseaduslikult kogutud andmete kustutamist, ebakorrektselt tehtud päringute tulemuste kustutamist, seaduslikult kogutud andmetele juurdepääsu piiramist asjakohaselt koolitatud töötajatega või seadusliku loata saadud või ebaseaduslikult levitatud andmeid sisaldavate luurearuannete tagasikutsumist ([382]). Andmekaitseasju läbivaatava kohtu otsus on talle esitatud kaebuse suhtes siduv ja lõplik ([383]). Peale selle, kui kohtu läbivaatamise käigus tuleb ilmsiks mõne FISC järelevalve alla kuuluva asutuse rikkumine, peab andmekaitseasju läbivaatav kohus esitama salastatud aruande ka asejustiitsministrile riikliku julgeoleku küsimustes, kes omakorda on kohustatud rikkumisest teavitama FISCd, kes võib võtta täiendavaid täitemeetmeid (kooskõlas põhjendustes 173–174 kirjeldatud menetlusega) ([384]).

(192) Kõik andmekaitseasju läbivaatava kohtu kolleegiumi otsused edastatakse ODNI kodanikuvabaduste kaitse ametnikule ([385]). Juhul kui läbivaatamine andmekaitseasju läbivaatavas kohtus algatati kaebuse esitaja taotluse alusel, teavitatakse kaebuse esitajat riigi ametiasutuse kaudu, et andmekaitseasju läbivaatav kohtus on läbivaatamise lõpetanud ja et „läbivaatamise käigus ei tuvastatud ühtegi kaebuses hõlmatud rikkumist või et andmekaitseasju läbivaatav kohus tegi otsuse, millega nõutakse asjakohaste õiguskaitsemeetmete võtmist“ ([386]). Justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste kaitse amet peab registrit, mis sisaldab kogu andmekaitseasju läbivaatava kohtu poolt läbi vaadatud teavet ja kõiki tehtud otsuseid ning see tehakse tulevaste andmekaitseasju läbivaatava kohtu kolleegiumide jaoks mittesiduva kohtupraktikana kättesaadavaks ([387]).

(193) Ka justiitsministeerium peab iga kaebuse esitanud kaebuse esitaja kohta registrit pidama ([388]). Läbipaistvuse suurendamiseks peab justiitsministeerium asjaomaste luureasutustega vähemalt iga viie aasta järel ühendust võtma, et kontrollida, kas andmekaitseasju läbivaatava kohtu tehtud läbivaatamist puudutava teabe salastatus on kustutatud. ([389]). Sel juhul teavitatakse isikut, et selline teave võib olla kättesaadav kohaldatava õiguse alusel (st et ta võib taotleda juurdepääsu teabevabaduse seaduse alusel, vt põhjendus 199).

(194) Lisaks hinnatakse korrapäraselt ja sõltumatult selle õiguskaitsemehhanismi nõuetekohast toimimist. Täpsemalt öeldes vaatab korralduse EO 14086 kohaselt õiguskaitsemehhanismi toimimise igal aastal läbi sõltumatu organ eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) (vt põhjendus 110) ([390]). Selle läbivaatamise käigus hindab PCLOB muu hulgas, kas ODNI kodanikuvabaduste kaitse ametnik ja andmekaitseasju läbivaatav kohus on kaebusi menetlenud õigeaegselt; kas nad on saanud vajalikule teabele täieliku juurdepääsu; kas korralduses EO 14086 sätestatud olulisi kaitsemeetmeid on läbivaatamise käigus nõuetekohaselt arvesse võetud ja kas luureühendus on ODNI kodanikuvabaduste kaitse ametniku ja andmekaitseasju läbivaatava kohtu otsused täielikult täitnud. PCLOB koostab oma läbivaatamise tulemuste kohta aruande presidendile, justiitsministrile, riiklikule luurejuhile, luureasutuste juhtidele, ODNI kodanikuvabaduste kaitse ametnikulule ja kongressi luurekomiteedele, mis avalikustatakse ka salastamata versioonis – ja see omakorda annab teavet käesoleva otsuse toimimise perioodiliseks läbivaatamiseks, mille viib läbi komisjon. Justiitsminister, riiklik luurejuht, ODNI kodanikuvabaduste kaitse ametnik ja luureasutuste juhid on kohustatud kõiki sellistes aruannetes sisalduvaid soovitusi rakendama või muul viisil järgima. Lisaks annab PCLOB igal aastal välja avaliku sertifikaadi selle kohta, kas õiguskaitsemehhanism käsitleb kaebusi kooskõlas korralduse EO 14086 nõuetega.

([382]) Korralduse EO 14086 paragrahvi 4 punkt a.

([383]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkt ii ja justiitsministri määruse paragrahvi 201.9 punkt g. Arvestades, et andmekaitseasju läbivaatava kohtu otsus on lõplik ja siduv, ei saa ükski teine täitev- või haldusasutus/-organ (sealhulgas Ameerika Ühendriikide president) andmekaitseasju läbivaatava kohtu otsust tühistada. Seda on kinnitanud ka Ülemkohtu praktika, milles selgitati, et delegeerides justiitsministrile täitevvõimu raames antud siduvate otsuste väljastamise ainupädevuse sõltumatule organile, võtab justiitsminister endalt võimaluse selle organi otsust mis tahes viisil suunata (vt United States ex rel. Accardi *vs.* Shaughnessy, 347 U.S. 260 (1954).

([384]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt F ja justiitsministri määruse paragrahvi 201.9 punkt i.

([385]) Justiitsministri määruse paragrahvi 201.9 punkt h.

([386]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti i alapunkt H ja justiitsministri määruse paragrahvi 201.9 punkt h. Vt teate laadi kohta justiitsministri määruse paragrahvi 201.9 punkti h alapunkt 3.

([387]) Justiitsministri määruse paragrahvi 201.9 punkt j.

([388]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkti v alapunkt A.

([389]) Korralduse EO 14086 paragrahvi 3 punkti d alapunkt v.

([390]) Korralduse EO 14086 paragrahvi 3 punkt e. Vt ka https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Lisaks korralduse EO 14086 alusel kehtestatud konkreetsele õiguskaitsemehhanismidele on õiguskaitsevahendid kõigile üksikisikutele kättesaadavad (olenemata kodakondsusest või elukohast) ka USA tavakohtutes ([391]).

(196) Eelkõige annavad FISA ja sellega seotud põhimäärus üksikisikutele võimaluse esitada Ameerika Ühendriikide vastu tsiviilhagi, kui nende kohta käivaid andmeid on ebaseaduslikult ja tahtlikult kasutatud või avaldatud; ([392]) esitada rahalisi kahjunõudeid otse USA riigiametnike vastu ([393]) 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 ([394]). Üldisemalt, kui valitsus kavatseb kasutada kriminaalasjas kahtlustatava vastu luureoperatsioonide käigus saadud teavet, pannakse põhiseadusest ja seadusest tulenevate nõuetega ([395]) paika teatavad teabe avalikustamise kohustused, et kostjal oleks võimalik valitsusepoolse tõendite kogumise ja kasutamise seaduslikkus vaidlustada.

(197) Lisaks on mitu erivahendit õiguskaitse saamiseks valitsusametnike vastu isikuandmetele ebaseadusliku juurdepääsu või isikuandmete kasutamise korral, sealhulgas väidetava riikliku julgeoleku eesmärgi korral (st arvutipettuste ja sellealase kuritarvitamise seadus ([396]); elektroonilise side privaatsuse seadus ([397]) ja finantsandmetega seotud eraelu puutumatuse seadus ([398])). Kõik need õiguslikud meetmed 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).

(198) Üldisem õiguskaitsevõimalus on olemas APA ([399]) näol, mille kohaselt on „igal isikul, kelle õigusi on rikutud ametkonna tegevusega või keda on negatiivselt mõjutanud või kahjustanud ametkonna tegevus“, õigus pöörduda kohtusse ([400]). 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 ei ole muul viisil seadusega kooskõlas“ ([401]). Näiteks otsustas föderaalne apellatsioonikohus 2015. aastal APA kohase nõude kohta, et USA valitsuse poolne telefoniside metaandmete masskogumine ei olnud FISA paragrahvi 501 kohaselt lubatud ([402]).

([391]) Juurdepääs nendele vahenditele sõltub „kaebeõiguse“ tõendamisest. See standard, mis kehtib kõikidele isikutele sõltumata kodakondsusest, tuleneb USA konstitutsiooni III artiklis sätestatud põhjendatuse nõudest. Ülemkohtu hinnangul eeldab see, et 1) isik on kandnud „tegelikku kahju“ (st õiguslikult kaitstud huvi kahju, mis on konkreetne ja eristatav ning juba tekkinud või vahetult tekkiv), 2) kahju ja kohtus vaidlustatud tegevuse vahel on põhjuslik seos ning 3) on tõenäoline, mitte oletuslik võimalus, et kohtu soodne otsus parandab kahju (vt Lujan *vs.* Defenders of Wildlife, 504 U.S. 555 (1992)).

([392]) USA seadustiku 18. jaotise § 2712.

([393]) USA seadustiku 50. jaotise § 1810.

([394]) USA seadustiku 50. jaotise § 1806.

([395]) Vt vastavalt Brady *vs.* Maryland, 373 U.S. 83 (1963) ja Jencks Act, USA seadustiku 18. jaotise § 3500.

([396]) USA seadustiku 18. jaotise § 1030.

([397]) USA seadustiku 18. jaotise § 2701–2712.

([398]) USA seadustiku 12. jaotise § 3417.

([399]) USA seadustiku 5. jaotise § 702.

([400]) Üldiselt kohaldatakse kohtulikku läbivaatamist ainult asutuse „lõplikule“ tegevusele ja mitte selle „ettevalmistavale, menetluslikule ega vahepealsele“ tegevusele. Vt USA seadustiku 5. jaotise § 704.

([401]) USA seadustiku 5. jaotise § 706 punkti 2 alapunkt A.

([402]) ACLU *vs.* Clapper, 785 F.3d 787 (2d Cir. 2015). Nendes juhtumites vaidlustatud telefoniside andmete masskogumise programm lõpetati USA FREEDOM Actiga 2015. aastal.

(199) Lisaks põhjendustes 176–198 nimetatud õiguskaitsevahenditele on igal üksikisikul õigus taotleda juurdepääsu olemasolevatele föderaalasutuste dokumentidele FOIA alusel, sealhulgas juhul, kui need dokumendid sisaldavad tema isikuandmeid ([403]). Sellise juurdepääsu saamine võib hõlbustada ka hagi esitamist tavakohtusse, sealhulgas kaebeõiguse tõendamiseks. Asutused võivad teatavate loetletud erandite alla kuuluvat teavet, sealhulgas juurdepääsu riikliku julgeoleku huvides salastatud teabele ja õiguskaitseorganite uurimisinfole, kinni pidada, ([404]) kuid vastusega rahulolematutel kaebuse esitajatel on võimalus see vaidlustada, taotledes haldus- ja seejärel kohtulikku läbivaatamist (föderaalkohtutes) ([405]).

(200) Eelöeldust järeldub, et kui USA õiguskaitseorganid ja riiklikud julgeolekuasutused pääsevad juurde käesoleva otsuse kohaldamisalasse kuuluvatele isikuandmetele, reguleerib sellist juurdepääsu õigusraamistik, mis sätestab juurdepääsu tingimused ning tagab, et juurdepääs ja andmete edasine kasutamine piirdub sellega, mis on vajalik taotletava avaliku huvi eesmärgi saavutamiseks ja on sellega proportsionaalne. Nendele kaitsemeetmetele võivad tugineda isikud, kellel on tõhusad õiguskaitsevahendid.

4. **JÄRELDUS**

(201) Komisjon leiab, et Ameerika Ühendriigid on USA kaubandusministeeriumi välja antud põhimõtete kaudu taganud ELi-USA andmekaitseraamistiku alusel liidust põhimõtete järgimist kinnitanud USA organisatsioonidele edastatud isikuandmete kaitse taseme, mis on sisuliselt samaväärne sellega, mis on tagatud määrusega (EL) 2016/679.

(202) Lisaks on komisjon seisukohal, et põhimõtete tõhus kohaldamine on tagatud läbipaistvuskohustuste ja andmekaitseraamistiku haldamisega kaubandusministeeriumi poolt. Lisaks võimaldavad USA õiguses ette nähtud järelevalvemehhanismid ja õiguskaitsevahendid praktikas tuvastada andmekaitsenormide rikkumisi ja nende eest karistada ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu saamiseks ning vajaduse korral nende parandamiseks või kustutamiseks.

(203) Kõigele lisaks leiab komisjon USA õiguskorra kohta kättesaadava teabe, sealhulgas VI ja VII lisas sisalduva teabe põhjal, et USA avaliku sektori asutuste igasugune sekkumine avalikes huvides, eelkõige kriminaalõiguse täitmise tagamise ja riikliku julgeoleku eesmärgil, nende üksikisikute põhiõigustesse, kelle isikuandmeid liidust USAsse ELi-USA andmekaitseraamistiku alusel edastatakse, piirdub sellega, mis on rangelt vajalik kõnealuse õiguspärase eesmärgi saavutamiseks, ning et sellise sekkumise vastu on olemas tõhus õiguskaitse. Seetõttu tuleks eespool esitatud järeldusi silmas pidades otsustada, et Ameerika Ühendriigid tagavad isikuandmete kaitse piisava taseme määruse (EL) 2016/679 artikli 45 tähenduses, mida tõlgendatakse Euroopa Liidu põhiõiguste harta valguses, isikuandmete puhul, mis edastatakse Euroopa Liidust organisatsioonidele, kes on kinnitanud ELi-USA andmekaitseraamistiku põhimõtete järgimist.

(204) Arvestades, et korraldusega EO 14086 kehtestatud piirangud, kaitsemeetmed ja õiguskaitsemehhanism on komisjoni hinnangu aluseks oleva USA õigusraamistiku olulised elemendid, põhineb käesoleva otsuse vastuvõtmine eelkõige sellel, et kõik USA luureasutused on võtnud korralduse EO 14086 rakendamiseks vastu ajakohastatud põhimõtted ja menetlused ning liit on määratud organisatsiooniks, kellel on õigus kasutada õiguskaitsemehhanismi, vastavalt 3. juulil 2023 (vt põhjendus 126) ja 30. juunil 2023 (vt põhjendus 176).

([403]) USA seadustiku 5. jaotise § 552. Sarnased seadused on olemas osariikide tasandil.

([404]) 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). Salastatuse kriteeriumid ja kestus on sätestatud täidesaatvas korralduses EO 13526, millega sätestatakse üldreegel, et salastatuse kustutamiseks tuleb kindlaks määrata kindel kuupäev või sündmus, võttes aluseks teabe tundlikkuse riikliku julgeoleku seisukohast, millal või mille korral teabe salastatus tuleb automaatselt kustutada (vt täidesaatva korralduse EO 13526 paragrahv 1.5).

([405]) Kohus teeb uue otsuse selle kohta, kas andmeid hoitakse kinni seaduslikult, ja saab kohustada valitsust võimaldama andmetele juurdepääsu (USA seadustiku 5. jaotise § 552 punkti a alapunkti 4 alapunkt B).

5. KÄESOLEVA OTSUSE MÕJU JA ANDMEKAITSEASUTUSTE TEGEVUS

(205) Liikmesriigid ja nende organid peavad võtma liidu institutsioonide aktide järgimiseks vajalikud meetmed, sest 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.

(206) Seega on määruse (EL) 2016/679 artikli 45 lõike 3 alusel komisjoni vastu võetud otsus kaitse piisavuse kohta siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele. Eelkõige võib andmeid edastada liidus asuvalt vastutavalt või volitatud töötlejalt põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides ilma, et oleks vaja taotleda lisaluba.

(207) Tuleb meenutada, et vastavalt määruse (EL) 2016/679 artikli 58 lõikele 5 ja nagu Euroopa Kohus on selgitanud Schremsi kohtuotsuses, ([406]) peab samas olema liikmesriigi õigusega juhuks, kui riiklik andmekaitseasutus kahtleb (sh laekunud kaebuse põhjal) komisjoni tehtud kaitse piisavuse otsuse kooskõlas üksikisiku põhiõigustega eraelu puutumatusele ja andmekaitsele, ette nähtud õiguskaitsevahend, mis võimaldab tal edastada need vastuväited siseriiklikule kohtule, kellelt võidakse nõuda asja kohta Euroopa Kohtule eelotsusetaotluse esitamist ([407]).

6. KÄESOLEVA OTSUSE JÄRELEVALVE JA LÄBIVAATAMINE

(208) Euroopa Kohtu praktika ([408]) kohaselt ja nagu on tõdetud määruse (EL) 2016/679 artikli 45 lõikes 4, peaks komisjon pidevalt jälgima asjaomaseid muutusi kolmandas riigis pärast kaitse piisavuse otsuse vastuvõtmist, et hinnata, kas kolmas riik tagab endiselt sisuliselt samaväärse kaitsetaseme. Niisugune kontrollimine on igal juhul nõutav, kui komisjonile laekunud teave tekitab kõnealuse küsimuse suhtes põhjendatud kahtluse.

(209) Seetõttu peaks komisjon olukorda Ameerika Ühendriikides seoses käesolevas otsuses hinnatud isikuandmete töötlemise õigusliku raamistiku ja tegeliku tavaga pidevalt jälgima. Selle protsessi hõlbustamiseks peaksid USA ametiasutused viivitamatult teavitama komisjoni USA õiguskorra olulistest muudatustest, mis mõjutavad käesoleva otsuse esemeks olevat õigusraamistikku, samuti kõigist käesolevas otsuses hinnatud isikuandmete töötlemise tavadega seotud suundumustest nii selles, kuidas töötlevad isikuandmeid Ameerika Ühendriikides asuvad põhimõtete järgimist kinnitanud organisatsioonid, kui ka selles, millised piirangud ja kaitsemeetmed kehtivad isikuandmetele juurdepääsul avaliku sektori asutustele.

(210) Selleks et komisjonil oleks võimalik oma järelevalve ülesannet tõhusalt täita, peaksid liikmesriigid teavitama komisjoni kõikidest asjakohastest meetmetest, mida riiklikud andmekaitseasutused võtavad, eelkõige seoses ELi andmesubjektide päringute või kaebustega, mis puudutavad isikuandmete edastamist liidust Ameerika Ühendriikides asuvatele põhimõtete järgimist kinnitanud organisatsioonidele. Komisjoni tuleks teavitada ka võimalikest märkidest, et kuritegude ennetamise, uurimise, avastamise või nende eest süüdimõistmise või riigi julgeoleku eest vastutavate USA avaliku sektori asutuste tegevus, samuti järelevalveasutuste tegevus ei taga nõutavat kaitsetaset.

([406]) Schrems, punkt 65.

([407]) Schrems, punkt 65. „Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks“.

([408]) Schrems, punkt 76.

(211) Määruse (EL) 2016/679 artikli 45 lõike 3 ([409]) kohaldamisel peaks komisjon pärast käesoleva otsuse vastuvõtmist korrapäraselt kontrollima, kas järeldused ELi-USA andmekaitseraamistiku raames Ameerika Ühendriikide poolt tagatava kaitse piisava taseme kohta on endiselt faktiliselt ja õiguslikult põhjendatud. Kuna eelkõige korralduse EO 14086 ja justiitsministri määrusega nõutakse uute mehhanismide loomist ja uute kaitsemeetmete rakendamist, tuleks käesolev otsus läbi vaadata ühe aasta jooksul pärast selle jõustumist, et kontrollida, kas kõik asjakohased elemendid on täielikult rakendatud ja toimivad praktikas tõhusalt. Pärast esimest läbivaatamist ja olenevalt selle tulemustest teeb komisjon tihedas koostöös määruse (EL) 2016/679 artikli 93 lõike 1 alusel loodud komiteega ja Euroopa Andmekaitsenõukoguga otsuse tulevaste läbivaatamiste sageduse kohta ([410]).

(212) Läbivaatamiste tegemiseks peaks komisjon kohtuma kaubandusministeeriumi, föderaalse kaubanduskomisjoni ja transpordiministeeriumi esindajatega, kellega on vajaduse korral kaasas teiste ELi-USA andmekaitseraamistiku rakendamises osalevate ministeeriumide ja asutuste esindajad, ning valitsuse andmetele juurdepääsuga seotud küsimuste puhul justiitsministeeriumi, ODNI (sealhulgas kodanikuvabaduste kaitse ametnik), muude luureühenduse üksuste, andmekaitseasju läbivaatava kohtu esindajad ja eriadvokaadid. Sellel kohtumisel peaks olema lubatud osaleda ka Euroopa Andmekaitsenõukogu liikmete esindajatel.

(213) Läbivaatamine peaks hõlmama kõiki käesoleva otsuse toimimise aspekte, mis on seotud Ameerika Ühendriikides isikuandmete töötlemisega, eelkõige põhimõtete kohaldamist ja rakendamist, pöörates erilist tähelepanu andmete edasisaatmise korral pakutavale kaitsele; asjaomase kohtupraktika arengule; üksikisiku õiguste kasutamise tulemuslikkusele; põhimõtete järgimise seirele ja tagamisele ning piirangutele ja kaitsemeetmetele, mis puudutavad valitsuse juurdepääsu, eriti korraldusega EO 14086 kehtestatud kaitsemeetmete rakendamisele ja kohaldamisele, sealhulgas luureasutuste väljatöötatud poliitika ja menetluste kaudu; korralduse EO 14086 ning FISA paragrahvi 702 ja korralduse EO 12333 vastasmõjule ning järelevalvemehhanismide ja õiguskaitsevõimaluste tõhususele (sealhulgas korralduse EO 14086 alusel loodud uue õiguskaitsemehhanismi toimimisele). Selliste läbivaatamiste raames pööratakse tähelepanu ka andmekaitseasutuste ja Ameerika Ühendriikide pädevate asutuste vahelisele koostööle, sealhulgas põhimõtete kohaldamise ja raamistiku toimimise muude aspektide kohta suuniste ja muude tõlgendamisvahendite väljatöötamisele.

(214) Läbivaatamise alusel peab komisjon koostama avaliku aruande, mis esitatakse Euroopa Parlamendile ja nõukogule.

7. **KÄESOLEVA OTSUSE PEATAMINE, KEHTETUKS TUNNISTAMINE VÕI MUUTMINE**

(215) Kui kättesaadavast teabest, eriti käesoleva otsuse järelevalvest tulenevast või Ameerika Ühendriikide või liikmesriikide ametiasutuste esitatud teabest ilmneb, et käesoleva otsuse alusel edastatud andmete kaitse tase ei pruugi enam olla piisav, peaks komisjon viivitamata teavitama sellest Ameerika Ühendriikide pädevaid asutusi ning nõudma, et kindlaksmääratud mõistliku tähtaja jooksul võetakse asjakohaseid meetmeid.

(216) Kui Ameerika Ühendriikide pädevad asutused ei ole kindlaksmääratud ajavahemiku möödumisel neid meetmeid võtnud või muul viisil rahuldavalt tõendanud, et käesolev otsus põhineb endiselt kaitse taseme piisavusel, algatab komisjon direktiivi (EL) 2016/679 artikli 93 lõikes 2 osutatud menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks.

(217) Teise võimalusena algatab komisjon menetluse otsuse muutmiseks, et eelkõige kehtestada andmete edastamise lisatingimused või piirata kaitse piisavuse otsuse kohaldamisala selliselt, et selle alla kuuluks üksnes andmeedastus, mille puhul on kaitse piisav tase endiselt tagatud.

([409]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et „[r]akendusaktis nähakse ette korrapärase […] läbivaatamise mehhanism, milles võetakse arvesse kõiki asjaomaseid suundumusi kolmandas riigis või rahvusvahelises organisatsioonis".

([410]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et korrapärane läbivaatamine peaks toimuma „vähemalt iga nelja aasta tagant". Vt ka Euroopa Andmekaitsenõukogu, piisavuse viitedokument, WP 254 rev. 01.

(218) Komisjon peaks peatamise või kehtetuks tunnistamise algatama eelkõige juhul, kui:

a) on viiteid selle kohta, et organisatsioonid, kes on saanud liidult isikuandmeid käesoleva otsuse alusel, ei järgi põhimõtteid ning pädevad järelevalve- ja täitevasutused ei tegele sellise mittevastavustega tõhusalt;

b) on märke selle kohta, et USA ametiasutused ei järgi tingimusi ja piiranguid, mida kohaldatakse USA ametiasutuste juurdepääsul ELi-USA andmekaitseraamistiku alusel edastatud isikuandmetele õiguskaitse ja riikliku julgeoleku eesmärgil, või

c) kui teiste hulgas ODNI kodanikuvabaduste kaitse ametnik ja/või andmekaitseasju läbivaatav kohus ei menetle liidu andmesubjektide kaebusi tõhusalt.

(219) Komisjon peab kaaluma ka menetluse algatamist käesoleva otsuse muutmiseks, peatamiseks või kehtetuks tunnistamiseks, kui Ameerika Ühendriikide pädevad asutused ei esita teavet või selgitusi, mida on vaja liidust Ameerika Ühendriikidesse edastatud isikuandmetele võimaldatava kaitsetaseme hindamiseks või käesoleva otsuse täitmiseks. Sellega seoses peab komisjon võtma arvesse võimalusi saada asjakohast teavet muudest allikatest.

(220) Nõuetekohaselt põhjendatud, tungivalt vajalikul ja kiireloomulisel juhul, näiteks kui korraldust EO 14086 või justiitsministri määrust muudetakse viisil, mis kahjustab käesolevas otsuses kirjeldatud kaitsetaset, või kui justiitsministri otsus määrata liit organisatsiooniks, kellel on õigus kasutada õiguskaitsemehhanismi, tühistatakse, kasutab komisjon võimalust võtta kooskõlas direktiivi (EL) 2016/679 artikli 93 lõikes 3 osutatud menetlusega vastu viivitamata kohaldatavad rakendusaktid, millega otsus peatatakse või tunnistatakse kehtetuks või seda muudetakse.

8. **LÕPPMÄRKUSED**

(221) Euroopa Andmekaitsenõukogu avaldas arvamuse, ([411]) mida on käesoleva otsuse koostamisel arvesse võetud.

(222) Euroopa Parlament võttis vastu resolutsiooni ELi-USA andmekaitseraamistikuga pakutava kaitse piisavuse kohta ([412]).

(223) Käesoleva otsusega ette nähtud meetmed on kooskõlas määruse (EL) 2016/679 artikli 93 lõike 1 alusel loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku alusel määruse (EL) 2016/679 artikli 45 tähenduses kaitse piisava taseme isikuandmetele, mis edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele, mis on kantud andmekaitseraamistikuga ühinenute nimekirja, mida peab ja mille teeb avalikult kättesaadavaks USA kaubandusministeerium kooskõlas I lisa punkti I alapunktiga 3.

Artikkel 2

Kui liikmesriikide pädevad asutused kasutavad üksikisikute kaitsmiseks seoses nende isikuandmete töötlemisega määruse (EL) 2016/679 artiklist 58 tulenevaid volitusi seoses käesoleva otsuse artiklis 1 osutatud andmete edastamisega, teavitab asjaomane liikmesriik komisjoni viivitamata.

([411]) 28. veebruari 2023. aasta arvamus 5/2023 Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset ELi-USA andmekaitseraamistiku alusel.

([412]) Euroopa Parlamendi 11. mai 2023. aasta resolutsioon ELi-USA andmekaitseraamistikuga pakutava kaitse piisavuse kohta (2023/2501(RSP)).

Artikkel 3

1. Komisjon jälgib pidevalt käesolevas otsuses käsitletud õigusraamistiku kohaldamist, sealhulgas tingimusi, mille alusel andmeid edasi saadetakse, üksikisikute õigusi teostatakse ja USA ametiasutused saavad juurdepääsu käesoleva otsuse alusel edastatud andmetele, eesmärgiga hinnata, kas Ameerika Ühendriigid tagavad jätkuvalt artiklis 1 osutatud piisava kaitsetaseme.

2. Liikmesriigid ja komisjon teavitavad üksteist juhul, kui selgub, et I lisas esitatud põhimõtete täitmise tagamiseks seaduslikku volitust omavad Ameerika Ühendriikide ametiasutused ei taga tõhusaid avastamis- ja kontrollimehhanisme, mis võimaldavad I lisas sätestatud 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 seda, mis on vajalik ja proportsionaalne, ja/või puudub selliste riivete vastu tõhus õiguskaitse.

4. Komisjon hindab ühe aasta jooksul alates käesoleva otsuse liikmesriikidele teatavakstegemisest ning edaspidi sagedusega, mis otsustatakse tihedas koostöös määruse (EL) 2016/679 artikli 93 lõike 1 alusel loodud komiteega ja Euroopa Andmekaitsenõukoguga, artikli 1 lõikes 1 sätestatud järeldust kogu olemasoleva teabe, sealhulgas koos pädevate Ameerika Ühendriikide ametiasutustega tehtud läbivaatamise käigus saadud teabe alusel.

5. Kui komisjonil on andmeid, et piisav kaitsetase ei ole enam tagatud, teavitab komisjon Ameerika Ühendriikide pädevaid asutusi. Vajaduse korral otsustab ta vastavalt määruse (EL) 2016/679 artikli 45 lõikele 5 käesoleva otsuse peatada, seda muuta või see kehtetuks tunnistada või selle kohaldamisala piirata. Komisjon võib sellise otsuse vastu võtta ka siis, kui komisjonil ei ole USA valitsuse koostööst keeldumise tõttu võimalik kindlaks teha, kas USA tagab jätkuvalt kaitse piisava taseme.

Artikkel 4

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 10. juuli 2023

Komisjoni nimel
komisjoni liige
Didier REYNDERS

I LISA

ELi-USA ANDMEKAITSERAAMISTIKU PÕHIMÕTTED, MILLE ON VÄLJA ANDNUD AMEERIKA ÜHENDRIIKIDE KAUBANDUSMINISTEERIUM

I. ÜLEVAADE

1. Kuigi nii Ameerika Ühendriigid kui ka Euroopa Liit (edaspidi „EL“) on mõlemad pühendunud eraelu puutumatuse kaitse suurendamisele, ja õigusriigile ning mõistavad Atlandi-üleste andmevoogude tähtsust meie kodanikele, majandusele ja ühiskonnale, käsitlevad Ameerika Ühendriigid eraelu puutumatuse kaitset teisiti kui EL. Ameerika Ühendriikide lähenemisviis on sektoripõhine, see tugineb õigusnormide, regulatsiooni ja iseregulatsiooni kombinatsioonile. Ameerika Ühendriikide kaubandusministeerium (U.S. Department of Commerce) (edaspidi „ministeerium“) annab välja ELi-USA andmekaitseraamistiku põhimõtted, sealhulgas täiendavad põhimõtted (edaspidi koos „põhimõtted“) ja põhimõtete I lisa (edaspidi „lisa“), täites oma seadusest tulenevat ülesannet soodustada, edendada ja arendada rahvusvahelist kaubandust (USA seadustiku (U.S.C.) 15. jaotise § 1512). Põhimõtted töötati välja koostöös Euroopa Komisjoni (edaspidi „komisjon“), tööstuse ja muude sidusrühmadega kaubandustegevuse lihtsustamiseks Ameerika Ühendriikide ja ELi vahel. ELi-USA andmekaitseraamistiku põhikomponendiks olevad põhimõtted pakuvad Ameerika Ühendriikide organisatsioonidele usaldusväärset mehhanismi isikuandmete edastamisel EList USAsse ning tagavad, et seejuures rakendatakse ELi andmesubjektide huvides jätkuvalt tõhusaid kaitsemeetmeid ja kaitset, nagu on sätestatud Euroopa õigusaktides, mis käsitlevad kolmandatesse riikidesse edastatavate isikuandmete töötlemist. Need põhimõtted on mõeldud kasutamiseks ainult neile Ameerika Ühendriikide organisatsioonidele, kellel on õigus isikuandmeid EList vastu võtta, et saavutada vastavus ELi-USA andmekaitseraamistiku põhimõtetega ja saada seega kasu komisjoni kaitse piisavuse otsusest ([1]) . Põhimõtted ei mõjuta määruse (EL) 2016/679 (edaspidi „isikuandmete kaitse üldmäärus“) ([2]) kohaselt rakendatavaid norme, mida kohaldatakse isikuandmete töötlemisele ELi liikmesriikides. Samuti ei piira põhimõtted Ameerika Ühendriikide õiguse alusel eraelu puutumatuse suhtes kohaldatavaid muid kohustusi.

2. Selleks et toetuda ELi-USA andmekaitseraamistikule, mis võimaldab EList edastatud isikuandmeid vastu võtta, peab organisatsioon kinnitama põhimõtete järgimist ministeeriumile (või ministeeriumi määratud isikule). Organisatsiooni otsus ühineda ELi-USA andmekaitseraamistikuga 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 ELi-USA andmekaitseraamistikuga, peab organisatsioon a) tunnustama föderaalse kaubanduskomisjoni, USA transpordiministeeriumi või muu seadusjärgse asutuse (kes tagab tegelikult põhimõtete järgimise) volitusi uurimise läbiviimiseks ja nõuete täitmise tagamiseks *(muud USA seadusjärgsed asutused, keda EL tunnustab, võidakse lisada tulevikus juurde raamistiku lisana)*; b) avalikult kinnitama võetud kohustust põhimõtteid järgida; c) tegema avalikuks kõnealuste põhimõtetega kooskõlas olevad privaatsustingimused ning d) neid täielikult rakendama ([3]). Kui organisatsioon põhimõtteid ei järgi, saab võtta täitemeetmeid föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission (FTC) Act) paragrahvi 5 alusel, millega keelatakse äritegevuses või äritegevust mõjutav ebaõiglane tegevus või pettus (USA seadustiku 15. jaotise § 45); transpordiministeeriumile USA seadustiku 49. jaotise § 41712 alusel, millega keelatakse vedajal või piletimüügiagendil rakendada lennutranspordis või lennutranspordi müügis ebaõiglasi või pettusel põhinevaid tavasid, või selliseid tegusid keelava muu seaduse või määruse alusel.

([1]) Kui komisjoni otsust ELi-USA andmekaitseraamistiku alusel pakutava kaitse piisavuse kohta kohaldatakse ka Islandi, Norra ja Liechtensteini suhtes, katab ELi-USA andmekaitseraamistik nii ELi kui ka kolme kõnealust riiki. Seega loetakse seal, kus on viidatud ELile ja liikmesriikidele, nende hulka ka Island, Liechtenstein ja Norra.

([2]) EUROOPA PARLAMENDI JA NÕUKOGU 27. aprilli 2016. aasta MÄÄRUS (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

([3]) Nimetus „ELi-USA andmekaitseraamistiku Privacy Shield põhimõtted“ on muudetud nimetuseks „ELi-USA andmekaitseraamistiku põhimõtted“. (Vt täiendav põhimõte ise kinnitamise kohta).

3. Ministeerium peab nende USA organisatsioonide ametlikku nimekirja, kes on kinnitanud ministeeriumile, et nad järgivad andmekaitseraamistiku põhimõtteid ja kohustuvad neist kinni pidama („andmekaitseraamistikuga ühinenute nimekiri"), ning avalikustab selle. ELi-USA andmekaitseraamistiku hüved on tagatud sellest kuupäevast, mil ministeerium kannab organisatsiooni andmekaitseraamistikuga ühinenute nimekirja. Ministeerium kustutab andmekaitseraamistikuga ühinenute nimekirjast need organisatsioonid, kes lahkuvad vabatahtlikult ELi-USA andmekaitseraamistikust või ei esita ministeeriumile oma iga-aastast korduskinnitust; need organisatsioonid peavad kas jätkama põhimõtete rakendamist isikuandmete suhtes, mille nad on saanud ELi-USA andmekaitseraamistiku alusel, ning peavad seda ministeeriumile igal aastal kinnitama (st seni, kuni nad sellist teavet säilitavad), tagama teabele piisava kaitse muude heakskiidetud meetoditega (nt kasutades lepingut, mis sisaldab komisjoni vastu võetud asjakohastes lepingu tüüptingimustes ette nähtud nõudeid täies ulatuses) või andmed tagastama või kustutama. Ministeerium kustutab andmekaitseraamistikuga ühinenute nimekirjast ka need organisatsioonid, kes ei ole püsivalt põhimõtteid järginud; sellised organisatsioonid peavad tagastama või kustutama isikuandmed, mille nad on saanud ELi-USA andmekaitseraamistikus osalemise ajal. Organisatsiooni kustutamine andmekaitseraamistikuga ühinenute nimekirjast tähendab, et tal ei ole enam õigust saada komisjoni kaitse piisavuse otsuse alusel EList isikuandmeid.

4. Ministeerium säilitab ja avalikustab ka ametlikud andmed USA organisatsioonide kohta, kes on varasemalt ministeeriumile põhimõtete järgimist kinnitanud, ent kes on andmekaitseraamistikuga ühinenute nimekirjast kustutatud. Ministeerium annab selge hoiatuse, et need organisatsioonid ei osale ELi-USA andmekaitseraamistikus; et eemaldamine andmekaitseraamistikuga ühinenute nimekirjast tähendab, et selline organisatsioon ei saa väita, et ta vastab ELi-USA andmekaitseraamistikule , ja ta peab hoiduma mis tahes avaldustest või eksitavatest tavadest, mis osutavad tema osalemisele ELi-USA andmekaitseraamistikus, ning et sellistel organisatsioonidel ei ole enam õigust tugineda komisjoni kaitse piisavuse otsusele, et võtta vastu EList edastatud isikuandmeid. Sellise organisatsiooni suhtes, kes väidab, et ta osaleb jätkuvalt ELi-USA andmekaitseraamistikus või esitab muid ELi-USA andmekaitseraamistikuga seotud valeandmeid pärast seda, kui ta on andmekaitseraamistikuga ühinenute nimekirjast kustutatud, võivad föderaalne kaubanduskomisjon, transpordiministeerium või muud täitevasutused võtta täitemeetmeid.

5. Nende põhimõtete järgimist võib piirata a) kohtumääruse täitmiseks või avaliku huvi, õiguskaitse või riikliku julgeoleku vajaduste täitmiseks vajalikus ulatuses, sealhulgas juhul, kui põhimääruse või valitsuse määrusega kehtestatakse vastuolulisi kohustusi; b) põhimääruse, kohtumääruse või valitsuse määrusega, millega antakse otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon tõendada, et tema mittevastavus põhimõtetele on piiratud ainult sellega, mis on vajalik selliste volitustega talle pandud ülekaalukate õigustatud huvide kaitsmiseks, või c) kui isikuandmete kaitse üldmäärus lubab erandeid ja kõrvalekaldeid, tingimusel et selliseid erandeid või kõrvalekaldeid rakendatakse sarnastes olukordades. Selles kontekstis hõlmavad Ameerika Ühendriikide õiguses eraelu puutumatuse ja kodanikuvabaduste kaitseks ette nähtud kaitsemeetmed neid, mida nõutakse täidesaatvas korralduses (Executive Order) 14086 ([4]) selles sätestatud tingimustel (sealhulgas vajalikkuse ja proportsionaalsuse nõuded). Vastavalt eraelu puutumatuse kaitse suurendamise eesmärgile peaksid organisatsioonid püüdma neid põhimõtteid täielikult ja läbipaistvalt rakendada, sealhulgas püüdma sätestada oma privaatsustingimustes, kus kohaldatakse eespool punktis b nimetatud erandeid. Samal põhjusel eeldatakse, et kui on võimalik teha valik põhimõtete ja/või Ameerika Ühendriikide seaduste alusel, valivad organisatsioonid võimaluse korral kõrgema kaitse taseme.

6. Pärast seda, kui organisatsioonid on kõnealuse raamistikuga ühinenud, on nad kohustatud järgima põhimõtteid kõigi isikuandmete puhul, mis on edastatud ELi-USA andmekaitseraamistikule tuginedes. Organisatsioon, kes soovib ELi-USA andmekaitseraamistikust tulenevaid hüvesid laiendada EList töösuhte kontekstis edastatavatele personali puudutavatele isikuandmetele, peab sellest teatama ministeeriumile, kui ta esitab oma kinnituse põhimõtete järgimise kohta, ning peab järgima ise kinnitamist käsitleva täiendava põhimõtte nõudeid.

([4]) 7. oktoobri 2022. aasta täidesaatev korraldus USA signaaliluuretegevuse kaitsemeetmete tõhustamise kohta („Enhancing Safeguards for United States Signals Intelligence Activities").

7. Põhimõtete ja ELi-USA andmekaitseraamistikus osalevate organisatsioonide asjakohaste privaatsustingimuste tõlgendamise ja neile vastavuse küsimustes kohaldatakse Ameerika Ühendriikide seadusi, välja arvatud juhul, kui organisatsioonid on kohustunud tegema koostööd ELi andmekaitseasutustega. Kõiki põhimõtteid kohaldatakse vastavalt nende asjakohasusele, kui ei ole sätestatud teisiti.

8. Mõisted:

   a. „isikuandmed" – tuvastatud või tuvastatava füüsilise isiku kohta käivad isikuandmete kaitse üldmääruse kohaldamisalasse kuuluvad andmed, mida Ameerika Ühendriikides asuv organisatsioon EList saab ja mis tahes vormis salvestab;

   b. „(isikuandmete) töötlemine" – iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, 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 ja põhimõtete I lisa jõustumise kuupäev on Euroopa Komisjoni kaitse piisavuse otsuse jõustumise kuupäev.

II. PÕHIMÕTTED

1. TEADE

a. Organisatsioon peab üksikisikutele teada andma

   i. oma osalemisest ELi-USA andmekaitseraamistikus ja lisama lingi veebiaadressile, kus asub andmekaitseraamistikuga ühinenute nimekiri,

   ii. sellest, millist liiki isikuandmeid kogutakse ja, kui see on asjakohane, märkima ka USA organisatsiooni üksused või USA tütarettevõtjad, kes samuti põhimõtteid järgivad,

   iii. oma kohustusest järgida põhimõtteid kõikide EList ELi-USA andmekaitseraamistikule tuginedes saadud isikuandmete puhul,

   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. millist liiki kolmandatele isikutele ja mis eesmärkidel ta isikuandmed avalikustab,

   vii. üksikisikute õigus oma isikuandmetele juurde pääseda,

   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 see organ on 1) andmekaitseasutuste loodud kolleegium, 2) ELis asuv alternatiivne vaidluste lahendamise organ või 3) Ameerika Ühendriikides asuv alternatiivne vaidluste lahendamise organ,

   x. organisatsioon tunnustab föderaalse kaubanduskomisjoni, transpordiministeeriumi või muu Ameerika Ühendriikide seadusjärgse asutuse uurimis- ja nõuete täitmise tagamise pädevust,

   xi. teatavatel tingimustel on üksikisikul võimalus algatada siduv vahekohtumenetlus ([5]),

   xii. nõue avaldada isikuandmed seaduspärase taotluse alusel avaliku sektori asutustele, sealhulgas riikliku julgeoleku või õiguskaitse vajaduste täitmiseks, ning

   xiii. organisatsiooni kohustused andmete edasisaatmisel kolmandatele isikutele.

([5]) Vt nt kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte punkt c.

b. Kõnealune 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 (st *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 hiljem loa andis. Üksikisikutele tuleb võimaldada selge, hästi nähtavaks tehtud ja käepärane mehhanism valiku tegemiseks.

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

c. Tundliku teabe puhul (st isikuandmed, mis täpsustavad meditsiinilist või tervislikku seisundit, rassilist või etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi vaateid, ametiühingu liikmesust või teavet üksikisiku seksuaalelu kohta) peavad organisatsioonid saama üksikisikult sõnaselge kinnitava nõusoleku (st *opt in*), kui teave i) avalikustatakse kolmandale isikule või ii) seda kasutatakse muudel eesmärkidel kui see, milleks see algselt koguti või milleks üksikisik hiljem nõustuva valikuga loa andis. Lisaks peab organisatsioon käsitama tundliku teabena selliseid kolmandalt isikult vastu võetud isikuandmeid, mille kolmas isik määratleb ja mida ta käsitab tundliku teabena.

3. **VASTUTUS KOLMANDALE ISIKULE ANDMETE EDASISAATMISE EEST**

a. Isikuandmete edastamisel kolmandast isikust vastutavale töötlejale peavad organisatsioonid järgima teate ja valikuvõimaluse põhimõtet. Organisatsioonid peavad sõlmima vastutavast töötlejast kolmanda isikuga lepingu, milles nähakse ette, et asjaomaseid andmeid tohib töödelda ainult piiratud ja konkreetsetel eesmärkidel, kooskõlas isiku antud nõusolekuga, ning et saaja tagab põhimõtetes sätestatuga samal tasemel kaitse ja teatab organisatsioonile, kui ta jõuab otsusele, et ei suuda asjaomast kohustust enam täita. Lepingus sätestatakse, et kui selline otsus tehakse, siis lõpetab kolmandast isikust vastutav töötleja töötlemise või võtab heastamiseks muid mõistlikke ja asjakohaseid meetmeid.

b. Isikuandmete edastamisel kolmandale isikule, kes on tema esindaja, peab organisatsioon: i) edastama selliseid andmeid ainult piiratud ja konkreetsetel eesmärkidel; ii) tegema kindlaks, et esindaja on kohustatud tagama eraelu puutumatuse kaitse vähemalt põhimõtetes sätestatuga samal tasemel; iii) võtma mõistlikke ja asjakohaseid meetmeid tagamaks, et esindaja töötleb edastatud isikuandmeid ka tegelikult viisil, mis on kooskõlas kohustustega, mille organisatsioon on põhimõtete järgimiseks endale võtnud; iv) nõudma, et esindaja teataks organisatsioonile, kui ta teeb kindlaks, et ei suuda enam täita kohustust tagada kaitse põhimõtetes nõutaval tasemel; v) saades teada, sealhulgas alapunkti iv kohaselt, volitamata töötlemisest, võtab mõistlikke ja asjakohaseid meetmeid selle peatamiseks ja heastamiseks ning vi) esitab nõudmise korral ministeeriumile kokkuvõtte või teavitava koopia selle esindajaga sõlmitud lepingu asjaomastest eraelu puutumatust käsitlevatest sätetest.

4. **TURVALISUS**

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

5. **ANDMETE TERVIKLIKKUS JA EESMÄRGI PIIRAMINE**

a. Kooskõlas põhimõtetega peavad isikuandmed piirduma teabega, mis on töötlemise eesmärke arvesse võttes asjakohane ([6]). 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 kõnealused andmed on tema käsutuses.

b. Teavet võib säilitada kujul, mis võimaldab füüsilist isikut tuvastada või muuta isiku tuvastatavaks, ([7]) ainult nii kaua, kuni see on vajalik töötlemiseks punkti 5 alapunkti a tähenduses. Kõnealune kohustus ei takista organisatsioonidel töödelda isikuandmeid pikema aja vältel, kui töötlemine toimub mõistliku aja jooksul ja määral, mis vastab avalikes huvides arhiveerimise, ajakirjanduslikele, kirjanduse ja kunsti, teadusliku või ajalooalase uurimise ja statistilise analüüsi eesmärkidele. Sellistel juhtudel kehtivad sellise töötlemise suhtes ELi-USA andmekaitseraamistiku 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 põhimõtteid rikkudes, välja arvatud juhul, kui juurdepääsu võimaldamise tülikus või kulu asjaomasel juhul oleks üksikisiku eraelu puutumatust ähvardava ohuga ebaproportsionaalne või kui see rikuks teiste isikute õigusi.

7. **KAEBUSTE MENETLEMINE, TÄITMISE TAGAMINE JA VASTUTUS**

a. Tõhus eraelu 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. Miinimumina peavad need mehhanismid sisaldama

i. kergesti kättesaadavaid sõltumatuid kaebuste menetlemise mehhanisme, mille abil iga üksikisiku kaebusi ja vaidlusi uuritakse ja lahendatakse üksikisiku jaoks tulemuslikult ja kooskõlas põhimõtetega, ning määratakse kahjuhüvitis, kui see on ette nähtud kohaldatava õiguse või erasektori algatustega;

ii. järelmeetmeid kontrollimaks, et kinnitused ja väited, mida organisatsioonid oma eraelu puutumatuse tavade kohta on esitanud, vastavad tõele ja et kõnealuste tavade rakendamine vastab esitatule, eriti põhimõtete järgimata jätmise juhtumite puhul, ning

iii. põhimõtete järgimist kinnitanud organisatsioonide kohustust 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 valitud sõltumatud kaebuste menetlemise mehhanismid peavad reageerima kiiresti järelepärimistele ja ministeeriumi nõudmistele esitada ELi-USA andmekaitseraamistikuga seotud teavet. Kõik organisatsioonid peavad viivitamata reageerima põhimõtete järgimist käsitlevatele kaebustele, mille on esitanud ELi liikmesriikide ametiasutused ministeeriumi kaudu. Organisatsioonid, kes on otsustanud teha koostööd andmekaitseasutustega, sealhulgas organisatsioonid, kes töötlevad personali isikuandmeid, peavad uurimise ja kaebuste lahendamise küsimustes aru andma otse nendele asutustele.

([6]) Olenevalt olukorrast võivad nõuetele vastavad töötlemiseesmärgid hõlmata näiteks 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.

([7]) Kõnealuses kontekstis on üksikisik „tuvastatav“, kui tuvastamiseks mõistliku tõenäosusega kasutatavaid vahendeid (muu hulgas võttes arvesse tuvastamise raha- ja ajakulu ning töötlemise ajal kättesaadavat tehnoloogiat) ning andmete säilitamise vormi arvestades saaks organisatsioon või kolmas isik andmetele juurde pääsedes üksikisiku mõistliku tõenäosusega tuvastada.

c. Organisatsioonid on kohustatud kaebusi lahendama ning järgima I lisas sätestatud tingimusi, kui üksikisik soovib algatada siduva vahekohtumenetluse, saates sellekohase teate kõnealusele organisatsioonile, järgides menetlust ning kui I lisas sätestatud tingimused on täidetud.

d. Andmete edasisaatmise korral on andmekaitseraamistikus osalev organisatsioon vastutav nende isikuandmete töötlemise eest, mille ta saab ELi-USA andmekaitseraamistiku alusel ja edastab seejärel kolmandale isikule, kes tegutseb tema nimel tema esindajana. Andmekaitseraamistikus osalev organisatsioon jääb põhimõtete kohaselt vastutavaks ka siis, 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 kohus otsustab, et organisatsioon ei järgi põhimõtteid, või põhimõtetes või põhimõtete tulevases lisas loetletud Ameerika Ühendriikide seadusjärgne asutus (nt föderaalne kaubanduskomisjon või transpordiministeerium) otsustab, et organisatsioon ei järgi põhimõtteid, peab organisatsioon avalikustama kõik asjakohased ELi-USA andmekaitseraamistikuga seotud ning kohtule või USA seadusjärgsele asutusele esitatud vastavus- või hindamisaruannete osad konfidentsiaalsusnõuetega kooskõlas olevas ulatuses. Ministeerium on loonud andmekaitseasutuste jaoks kontaktpunkti, kuhu nad võivad pöörduda andmekaitseraamistikus osalevate organisatsioonide põhimõtetele mittevastavusega seotud probleemide korral. Föderaalne kaubanduskomisjon ja transpordiministeerium vaatavad eelisjärjekorras läbi ministeeriumi ja ELi liikmesriikide ametiasutuste esitatud kaebused põhimõtete mittejärgimise kohta ning vahetavad õigeaegselt teavet kaebuse kohta selle esitanud asutusega, järgides kehtivaid konfidentsiaalsuspiiranguid.

III. TÄIENDAVAD PÕHIMÕTTED

1. Tundlikud andmed

a. Organisatsioon ei ole kohustatud hankima kinnitavat sõnaselget nõusolekut (st *opt in*) tundlike andmete töötlemiseks, kui see:

i. toimub andmesubjekti või muu isiku elulistes huvides;

ii. on vajalik õigusnõuete koostamiseks või kaitsmiseks;

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, siis juhul, kui Ameerika Ühendriikide põhiseaduse esimeses paranduses sisalduvad vaba ajakirjanduse õigused ristuvad eraelu puutumatuse kaitse huvidega, lähtutakse selliste huvide tasakaalustamisel esimesest parandusest, kui on tegemist Ameerika Ühendriikide isikute või organisatsioonidega.

b. Ajakirjandusliku materjali trükis või eetris avaldamiseks või muul moel avalikuks edastamiseks kogutud isikuandmetele, sõltumata sellest, kas neid kasutatakse või mitte, samuti massiteabevahendite arhiivide levitatavast varem avaldatud materjalist leitud teabele põhimõtete nõuded ei laiene.

3. Teisene vastutus

a. Internetiteenuse osutajad, telekommunikatsiooniettevõtted või muud organisatsioonid ei ole andmekaitseraamistiku põhimõtete alusel vastutavad, kui nad teise organisatsiooni nimel vaid edastavad, marsruudivad või puhverdavad andmeid. ELi-USA andmekaitseraamistikust ei tulene teisest vastutust. 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. Aktsiaseltse ja osaühinguid, sealhulgas andmekaitseraamistikus osalevaid organisatsioone, auditeeritakse korrapäraselt. Enneaegne avalikustamine võib sellised auditid, eriti need, mille käigus kontrollitakse võimalikku õigusvastast tegevust, ohtu seada. Samuti peab andmekaitseraamistikus osalev organisatsioon, kes on seotud võimaliku ühinemise või ülevõtmisega, tegema 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 hoolsuse kontrolli tegevatel 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 avaliku huvist tulenevatel ning muudel juhtudel, mil nende põhimõtete rakendamine kahjustaks organisatsiooni õigustatud huve. Selliste õigustatud huvide hulka kuuluvad organisatsioonide kohustuste ja raamatupidamistoimingute tegemise vastavuse jälgimine ning konfidentsiaalsusvajadus, mis on seotud võimalike omandamiste, ühinemiste, ühisettevõtete või investeerimispankurite või audiitorite tehtavate muude sarnaste toimingutega.

5. **Andmekaitseasutuste roll**

a. Organisatsioonid täidavad oma kohustust teha koostööd andmekaitseasutustega, nagu allpool kirjeldatud. ELi-USA andmekaitseraamistiku alusel peavad EList isikuandmeid saavad Ameerika Ühendriikide organisatsioonid võtma kohustuse rakendada tõhusaid mehhanisme, et tagada vastavus põhimõtetele. Täpsemalt peavad osalevad organisatsioonid kooskõlas kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõttega tagama järgmise: a) i) kaebuste esitamise võimalus üksikisikutele, kellega andmed on seotud; a) ii) järelmeetmed, et kontrollida, kas kinnitused ja väited, mida nad on oma privaatsustingimuste kohta esitanud, vastavad tõele ning a) iii) kohustus heastada põhimõtete järgimata jätmisest tekkivad probleemid ning millised on 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 ELi-USA andmekaitseraamistiku põhimõtete järgimise kinnituses ministeeriumile (vt täiendav põhimõte ise kinnitamise kohta), et organisatsioon:

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

ii. teeb koostööd andmekaitseasutustega põhimõtete alusel esitatud kaebuste uurimisel ja lahendamisel ning

iii. järgib andmekaitseasutuste nõuandeid, kui need leiavad, et organisatsioon peab põhimõtete järgimiseks astuma konkreetseid samme, sealhulgas võtma meetmeid põhimõtete järgimata jätmise tõttu üksikisikutele tekitatud kahju heastamiseks või hüvitamiseks, ja esitab andmekaitseasutustele kirjaliku kinnituse selliste meetmete võtmise kohta.

c. Andmekaitseasutuste kolleegiumide tegevus

i. Andmekaitseasutuste koostöö toimub teabe ja nõuannete vormis järgmiselt.

1. Andmekaitseasutuste nõuanded edastatakse ELi tasandil moodustatud andmekaitseasutuste mitteametliku kolleegiumi kaudu, mis muu hulgas aitab tagada ühtlustatud ja ühtse lähenemisviisi.

2. Kolleegium nõustab Ameerika Ühendriikide organisatsioone üksikisikute lahendamata kaebuste asjus, mis on seotud ELi-USA andmekaitseraamistiku alusel edastatud isikuandmete käitlemisega. Nõustamise eesmärk on tagada põhimõtete õige kohaldamine ning see hõlmab heastamisvahendeid, mida andmekaitseasutused peavad asjakohas(t)ele isiku(te)le sobilikuks.

3. Kolleegium annab nõu vastuseks asjaomaste organisatsioonide taotluste ja/või otse üksikisikutelt saadud kaebustele organisatsioonide vastu, kes on kohustunud andmekaitseasutustega ELi-USA andmekaitseraamistiku raames koostööd tegema, julgustades selliseid üksikisikuid eelkõige kasutama sisemisi kaebuste käsitlemise menetlusi, mida organisatsioon võib pakkuda, ning vajaduse korral neid selles aidates.

4. Nõu antakse alles pärast seda, kui kummalgi vaidluse poolel on olnud mõistlik võimalus esitada selgitused ja soovitud tõendid. Kolleegium püüab esitada nõuande nii kiiresti, kui seda nõuetekohase menetluse nõue võimaldab. Üldjuhul püüab kolleegium esitada nõuande 60 päeva jooksul pärast kaebuse või taotluse saamist ning võimaluse korral kiiremini.

5. Kolleegium avalikustab talle läbivaatamiseks esitatud kaebuste tulemused, kui peab seda vajalikuks.

6. Sellest, et kolleegium esitab nõuandeid, ei tulene mitte mingisugust vastutust ei kolleegiumile 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 esitamist ning ei ole viivitust rahuldavalt põhjendanud, teavitab kolleegium oma kavatsusest saata materjal edasi kas föderaalsele kaubanduskomisjonile, transpordiministeeriumile või muule Ameerika Ühendriikide föderaalsele või valitsusasutusele, millel on seadusest tulenevad volitused võtta täitemeetmeid pettuse või valeandmete esitamise korral, või järeldada, et koostöökokkulepet on tõsiselt rikutud ning see loetakse seetõttu kehtetuks. Viimasel juhul teavitab kolleegium ministeeriumi, et andmekaitseraamistikuga ühinenute nimekirjas saaks nõuetekohased muudatused teha. Andmekaitseasutustega koostöö kohustuse mittetäitmist, samuti põhimõtete mittejärgimist käsitatakse pettusel põhineva tavana föderaalse kaubanduskomisjoni seaduse (FTC Act) paragrahvi 5 (USA seadustiku 15. jaotise § 45), USA seadustiku 49. jaotise § 41712 või muu sarnase põhimääruse alusel.

d. Organisatsioon, kes soovib tal ELi-USA andmekaitseraamistiku kohaselt olevaid hüvesid laiendada EList töösuhte kontekstis edastatavatele personali isikuandmetele, peab kohustuma tegema nende andmete käitlemisel koostööd andmekaitseasutustega (vt täiendav põhimõte personaliandmete kohta).

e. Sellise võimaluse valivad organisatsioonid peavad maksma aastatasu, mis läheb kolleegiumi tegevuskulude katmiseks. Neilt võidakse täiendavalt paluda nende vastu esitatud taotluste või kaebuste läbivaatamisel kolleegiumi vajatavate tõlgete kulude tasumist. Tasu suuruse määrab ministeerium pärast komisjoniga konsulteerimist. Tasu võib sisse nõuda ministeeriumi valitud kolmas isik, kes on selleks otstarbeks kogutud vahendite hoidja. Tasu kaudu kogutud vahendite jaotamise asjakohaste menetluste kehtestamisel ning kolleegiumi muude menetlus- ja haldusaspektide asjus teeb ministeerium tihedat koostööd komisjoni ja andmekaitseasutustega. Ministeerium ja komisjon võivad kokku leppida tasu kogumise sageduse muutmises.

6. **Põhimõtete järgimise kinnitamine**

a. ELi-USA andmekaitseraamistiku hüved on tagatud sellest päevast alates, mil ministeerium lisab organisatsiooni andmekaitseraamistikuga ühinenute nimekirja. Ministeerium lisab organisatsiooni andmekaitseraamistikuga ühinenute nimekirja alles pärast seda, kui on kindlaks teinud, et organisatsiooni algselt esitatud põhimõtete järgimise kinnitus on täielik, ja ta kustutab organisatsiooni sellest nimekirjast, kui organisatsioon lahkub vabatahtlikult andmekaitseraamistikust või jätab esitamata oma iga-aastase korduskinnituse või kui ta järjepidevalt eirab põhimõtteid (vt vaidluste lahendamise ja täitmise tagamise täiendav põhimõte).

b. ELi-USA andmekaitseraamistikus osalemiseks algse põhimõtete järgimise kinnituse või järgmiste korduskinnituste esitamiseks peab vastutav isik esitama organisatsiooni nimel ministeeriumile selle kohta, et organisatsioon kinnitab või kinnitab üle (olenevalt sellest, kummaga on tegemist) põhimõtete järgimist, ([8]) esildise, mis sisaldab vähemalt järgmist teavet:

([8]) Esildise peab ministeeriumi andmekaitseraamistiku veebisaidi kaudu esitama organisatsioonis töötav isik, kellele on antud volitus esindada organisatsiooni ja selle hõlmatud üksusi organisatsiooni põhimõtete järgimisega seotud küsimustes.

i. kinnitust või korduskinnitust esitava USA organisatsiooni nimi, samuti organisatsiooni nende USA üksuste või USA tütarettevõtjate nimi (nimed), mis samuti järgivad põhimõtteid, ja keda organisatsioon soovib kinnituses hõlmata;

ii. kirjeldus selle kohta, kuidas organisatsiooni tegevus on seotud isikuandmetega, mis saadakse EList ELi-USA andmekaitseraamistiku alusel;

iii. organisatsiooni selliste isikuandmete suhtes kohaldatavate asjaomaste privaatsustingimuste kirjeldus, sealhulgas järgmine:

1. kui organisatsioonil on olemas avalik veebisait, siis veebiaadress, kus tema privaatsustingimused on kättesaadavad, või kui organisatsioonil ei ole avalikku veebisaiti, siis teave selle kohta, kus üldsusel on võimalik tema privaatsustingimustega tutvuda, ning

2. rakendamise alguskuupäev;

iv. organisatsiooni kontaktandmed kaebuste, juurdepääsunõuete ning põhimõtete alusel tekkivate muude küsimuste käsitlemiseks, ([9]) sealhulgas:

1. (olenevalt olukorrast) organisatsiooni vastava(te) isiku(te) või asjaomas(t)e kontaktisiku(te) nimi (nimed), ametinimetus(ed), e-posti aadress(id) ja telefoninumber (-numbrid) ning

2. organisatsiooni asjaomane USA postiaadress;

v. seadusjärgne asutus, kellel on pädevus läbi vaadata mis tahes nõudeid organisatsiooni vastu seoses võimalike ebaõiglaste või pettusel põhinevate tavadega ja eraelu puutumatusele kohaldatavate (ning põhimõtetes või tulevases põhimõtete lisas loetletud) õigusnormide rikkumisega;

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

vii. kontrollimeetod (st enesehindamine või väline vastavuskontroll, sealhulgas kolmas isik, kes selliseid kontrolle teeb) ([10]) ning

viii. põhimõtetega seotud lahendamata kaebuste uurimiseks kättesaadavad asjakohased sõltumatud kaebuste menetlemise mehhanismid ([11]).

c. Organisatsioon, kes soovib tal ELi-USA andmekaitseraamistiku kohaselt olevaid hüvesid laiendada EList töösuhte kontekstis edastatavatele töötajate isikuandmetele, võib seda teha, kui olemas on seadusjärgne asutus, kes on loetletud põhimõtetes või tulevases põhimõtete lisas ja kellel on pädevus lahendada personaliandmete töötlemisest tulenevaid nõudeid organisatsiooni vastu. Lisaks peab organisatsioon sellele viitama oma algses põhimõtete järgimise kinnituses, samuti kõigis korduskinnitustes ja teatama, et kohustub tegema koostööd asjaomase ELi asutuse või asjaomaste asutustega personaliandmeid käsitleva täiendava põhimõtte ja andmekaitseasutuste rolli käsitleva täiendava põhimõtte alusel (vastavalt sellele, kumb on kohaldatav) ning järgima nimetatud asutuste nõuandeid. Organisatsioon peab esitama ministeeriumile ka koopia oma personaliandmetele kehtivatest privaatsustingimustest ning teatama, kus need on tutvumiseks kättesaadavad töötajatele, keda need puudutavad.

([9]) Peamine „organisatsiooni kontaktisik“ või „organisatsiooni vastutav isik“ ei tohi olla organisatsiooniväline isik (nt väline nõustaja või väline konsultant).

([10]) Vt täiendav põhimõte kontrolli kohta.

([11]) Vt täiendav põhimõte vaidluste lahendamise ja täitmise tagamise kohta.

d. Ministeerium peab andmekaitseraamistikuga ühinenute nimekirja organisatsioonide kohta, kes on esitanud tervikliku algse kinnituse, ning uuendab kõnealust nimekirja iga-aastaste korduskinnituste ning vaidluste lahendamist ja täitmise tagamist käsitleva täiendava põhimõtte kohaste teadete alusel. Sellised kinnitused tuleb esitada vähemalt kord aastas. Vastasel juhul kustutatakse organisatsioon andmekaitseraamistikuga ühinenute nimekirjast ja ELi-USA andmekaitseraamistikuga kaasnevad hüved ei ole enam tagatud. Kõik organisatsioonid, kelle ministeerium lisab andmekaitseraamistikuga ühinenute nimekirja, peavad olema kehtestanud teate põhimõttele vastavad privaatsustingimused ja nad peavad nendes avalikustatud privaatsustingimustes deklareerima, et järgivad põhimõtteid ([12]). Kui organisatsiooni privaatsustingimused on kättesaadavad internetis, peab seal olema ka hüperlink ministeeriumi andmekaitseraamistiku veebisaidile, samuti hüperlink põhimõtetega seotud lahendamata kaebuste uurimise ja sõltumatu kaebuste menetlemise mehhanismi veebisaidile või kaebuse vormile, ja seda üksikisikutele tasuta.

e. Põhimõtteid kohaldatakse pärast nende kinnitamist viivitamata. Osalevad organisatsioonid, kes on varem kinnitanud ELi-USA andmekaitseraamistiku Privacy Shield põhimõtete järgimist, peavad oma privaatsustingimusi ajakohastama, et asendada vastav viide nimetusega „ELi-USA andmekaitseraamistiku põhimõtted“. Asjaomased organisatsioonid lisavad selle viite võimalikult kiiresti ja igal juhul hiljemalt kolme kuu jooksul pärast ELi-USA andmekaitseraamistiku põhimõtete jõustumise kuupäeva.

f. Organisatsioon peab kohaldama põhimõtteid kõikide EList ELi-USA andmekaitseraamistikule tuginedes saadud isikuandmete suhtes. Kohustus järgida põhimõtteid ei ole ajaliselt piiratud andmete puhul, mida organisatsioon sai ajal, kui tal oli õigus ELi-USA andmekaitseraamistiku hüvedele; see 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 ELi-USA andmekaitseraamistikust lahkub. Organisatsioon, mis soovib ELi-USA andmekaitseraamistikust lahkuda, peab ministeeriumile sellest ette teatama. Ka tuleb kõnealuses teates märkida, mida organisatsioon teeb isikuandmetega, mille ta on ELi-USA andmekaitseraamistikule tuginedes saanud (st kas ta säilitab, tagastab või kustutab andmed ja kui ta säilitab andmeid, siis heakskiidetud vahendid, millega ta andmeid kaitseb). Organisatsioon, kes lahkub ELi-USA andmekaitseraamistikust, ent soovib selle raames saadud andmeid säilitada, peab kinnitama ministeeriumile igal aastal põhimõtete järgimist või andmetele piisava kaitse tagamist teiste heakskiidetud meetoditega (nt kasutades lepingut, mis sisaldab komisjoni vastu võetud asjakohasetes lepingu tüüptingimustes ette nähtud nõudeid täies ulatuses); vastasel korral peab organisatsioon teabe tagastama või kustutama ([13]). ELi-USA andmekaitseraamistikust lahkuv organisatsioon peab eemaldama kõikidest asjakohastest privaatsustingimustest kõik viited ELi-USA andmekaitseraamistikule, mis osutavad, et organisatsioon jätkab ELi-USA andmekaitseraamistikus osalemist ja tal on õigus sellest tulenevatele hüvedele.

([12]) Organisatsioon, kes esitab kinnituse esimest korda, ei tohi oma lõplikes privaatsustingimustes väita, et ta osaleb ELi-USA andmekaitseraamistikus, kuni ministeerium teavitab organisatsiooni, et ta võib seda teha. Kui organisatsioon esitab algse kinnituse, peab ta sellega koos esitama ministeeriumile privaatsustingimuste kavandi, mis on kooskõlas põhimõtetega. Kui ministeerium on kindlaks teinud, et organisatsiooni algne kinnitus on muus osas täielik, teatab ministeerium organisatsioonile, et ta peaks oma ELi-USA andmekaitseraamistikuga kooskõlas olevad privaatsustingimused lõplikult vormistama (nt vajaduse korral avaldama). Organisatsioon peab ministeeriumi viivitamatult teavitama niipea, kui vastavad privaatsustingimused on valmis. Siis kannab ministeerium organisatsiooni andmekaitseraamistikuga ühinenute nimekirja.

([13]) Kui organisatsioon otsustab andmekaitseraamistikust lahkumise ajal, et ta säilitab isikuandmeid, mille ta on saanud ELi-USA andmekaitseraamistikule tuginedes, ja kinnitab ministeeriumile, et ta kohaldab põhimõtteid nende andmete suhtes jätkuvalt, peab organisatsioon pärast raamistikust lahkumist kord aastas ministeeriumile aru andma (st välja arvatud juhul, kui ja kuni organisatsioon pakub sellistele andmetele piisavat kaitset mõne muu heakskiidetud meetodi kohaselt, või ta tagastab või kustutab kõik sellised andmed ning teatab sellest ministeeriumile) selle kohta, mida ta on nende isikuandmetega teinud, mida ta teeb nende isikuandmetega, mida ta jätkuvalt säilitab, ning kes hakkab tegutsema pideva kontaktpunktina põhimõtetega seotud küsimustes.

g. Organisatsioon, mis lakkab eksisteerimast eraldiseisva üksusena äriühingu staatuse muutumise tõttu nt ühinemise või ülevõtmise, pankroti või lõpetamise tulemusena, peab sellest ministeeriumi eelnevalt teavitama. Teates tuleb ka märkida, kas äriühingu staatuse muutumise tulemusel tekkiv üksus i) osaleb jätkuvalt ELi-USA andmekaitseraamistikus olemasoleva kinnituse alusel; ii) esitab kinnituse ELi-USA andmekaitseraamistiku uue osalejana (nt kui uuel üksusel või säilinud üksusel ei ole juba olemasolevat kinnitust, mille alusel ta saaks ELi-USA andmekaitseraamistikus osaleda) või iii) võtab kasutusele muud kaitsemeetmed, näiteks kirjaliku lepingu, mis tagab põhimõtete jätkuva kohaldamise kõigi isikuandmete suhtes, mille organisatsioon on ELi-USA andmekaitseraamistiku alusel saanud ja mida ta säilitab. Kui ei kohaldata ei punkti i, ii ega iii, tuleb ELi-USA andmekaitseraamistiku alusel saadud andmed viivitamatult tagastada või kustutada.

h. Kui organisatsioon lahkub mingil põhjusel ELi-USA andmekaitseraamistikust, peab ta eemaldama kõik väited, mis osutavad, et organisatsioon jätkab ELi-USA andmekaitseraamistikus osalemist või et tal on õigus ELi-USA andmekaitseraamistikust tulenevatele hüvedele. Eemaldada tuleb ka ELi-USA andmekaitseraamistikule vastavust kinnitav tähis, kui seda kasutatakse. Kui organisatsiooni esitab üldsusele valeandmeid põhimõtete järgimise kohta, võib föderaalne kaubanduskomisjon, transpordiministeerium või muu asjakohane valitsusasutus süüdistuse esitada. Ministeeriumile valeandmete esitamise korral võidakse kohaldada valeandmete seadust (False Statements Act, USA seadustiku 18. jaotise § 1001).

7. **Kontrollimine**

a. Organisatsioonid peavad ette nägema kontrollimeetmed tõendamaks, et kinnitused ja väited, mida nad oma ELi-USA andmekaitseraamistiku järgmise tavade kohta eraelu puutumatuse valdkonnas on esitanud, vastavad tõele ja asjaomaste tavade rakendamine vastab väidetele ning on kooskõlas põhimõtetega.

b. Kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte kontrollinõuete järgimiseks peab organisatsioon selliseid kinnitusi ja väiteid kontrollima enesehindamise või välise vastavuskontrolli kaudu.

c. Kui organisatsioon on valinud enesehindamise, peab selline kontroll näitama, et tema EList saadud isikuandmeid käsitlevad privaatsustingimused on täpsed, terviklikud, kergesti kättesaadavad, vastavuses põhimõtetega ja täielikult rakendatud (st neid järgitakse). Samuti peab kontroll näitama, et üksikisikuid teavitatakse sisemisest kaebuste lahendamise korrast ja sõltumatutest mehhanismidest, mille kaudu on võimalik nende kaebusi menetleda; et paika on pandud kord töötajatele selle korra rakendamise koolituse pakkumiseks ja nende suhtes kohaldatav distsiplinaarmenetlus juhul, kui nad korrast kinni ei pea, ning et paika on pandud sisekord perioodiliste objektiivsete kontrollide korraldamiseks eespool nimetatule vastavuse suhtes. Enesehindamise lõpuleviimise kinnitusele peaks alla kirjutama vastutav isik või organisatsiooni muu volitatud esindaja vähemalt kord aastas ning see peaks olema nõudmise korral kättesaadav üksikisikutele või kui tegemist on põhimõtete järgimata jätmise uurimise või sellekohase kaebusega.

d. Kui organisatsioon on valinud välise vastavuskontrolli, peab kontroll näitama, et tema EList saadud isikuandmeid käsitlevad privaatsustingimused on täpsed, terviklikud, kergesti kättesaadavad, vastavuses põhimõtetega ja täielikult rakendatud (st et neid järgitakse). Samuti peab see kontroll näitama, et üksikisikuid teavitatakse mehhanismidest, mille kaudu on võimalik nende kaebusi menetleda. Kontrolliviisideks võivad piiranguta olla auditeerimine, pisteline kontroll, „peibutiste“ kasutamine või vajaduse korral tehnoloogilised vahendid. Välise vastavuskontrolli eduka lõpuleviimise 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 kui tegemist on põhimõtete järgimata jätmise uurimise või sellekohase kaebusega.

e. Organisatsioonid peavad säilitama oma dokumente ELi-USA andmekaitseraamistiku kohaste puutumatustavade rakendamise kohta ja tegema need mittevastavuse uurimise või sellekohase kaebuse korral nõudmisel kättesaadavaks kaebuste läbivaatamise eest vastutavale vaidluste lahendamise sõltumatule organile või asutusele, kelle pädevuses on uurida ebaõiglaseid või pettusel põhinevaid tavasid. Organisatsioonid peavad viivitamata vastama ministeeriumi järelepärimistele ja muudele teabenõuetele, mis käsitlevad põhimõtete järgimist organisatsiooni poolt.

8. **Juurdepääs**

a. Juurdepääsu põhimõtte rakendamine

i. Põhimõtete kohaselt on juurdepääsuõigus eraelu puutumatuse kaitse jaoks on põhimõttelise tähtsusega. Eelkõige võimaldab see üksikisikutel kontrollida nende kohta säilitatavate andmete õigsust. Juurdepääsu põhimõte tähendab, et üksikisikutel on õigus järgmisele:

1. saada organisatsioonilt kinnitus selle kohta, kas organisatsioon töötleb või ei töötle nendega seotud isikuandmeid ([14]);

2. lasta selline teave endale edastada, et kontrollida selle täpsust ja töötlemise õiguspärasust ning

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

ii. Üksikisikud ei pea oma isikuandmetele juurdepääsu taotlusi põhjendama. Üksikisikute juurdepääsutaotlustele vastamisel 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 lisapäringute saatmiseks.

b. Juurdepääsu võimaldamise tülikus või kulud

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

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

c. Konfidentsiaalne äriinfo

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

([14]) Organisatsioon peaks vastama üksikisikute päringutele isikuandmete töötlemise eesmärgi, töödeldavate isikuandmete kategooriate ning selle kohta, kellele või millise kategooria vastuvõtjatele isikuandmed avalikustatakse.

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

d. Andmebaaside korraldus

i. Organisatsioon võib juurdepääsu võimaldada asjaomaste isikuandmete avalikustamise vormis ning üksikisiku juurdepääs organisatsiooni andmebaasile ei ole nõutav.

ii. Juurdepääs tuleb võimaldada ainult nende isikuandmete ulatuses, mida organisatsioon säilitab. Juurdepääsu põhimõttest endast ei teki kohustust isikuandmete faile säilitada, hooldada, ümber korraldada või restruktureerida.

e. Millal võib juurdepääsu piirata

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

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 kvaliteetse juhtimisega seotud järelevalve, kontrolli või regulatiivtoimingute tegemiseks 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 lisapäringutega pöörduda.

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

i. Üksikisikul on õigus nõuda kinnitust selle kohta, kas asjaomasel organisatsioonil on või ei ole tema kohta käivaid isikuandmeid. Üksikisikul on õigus ka sellele, 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, iseäranis 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

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

i. Vastuse andmise tähtaeg

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

9. **Personaliandmed**

a. Hõlmatus ELi-USA andmekaitseraamistikuga

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

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

b. Teate ja valikuvõimaluse põhimõtte rakendamine

i. Ameerika Ühendriikide organisatsioon, kes on saanud töötajate kohta andmeid EList ELi-USA andmekaitseraamistiku alusel, võib avalikustada need andmed kolmandatele isikutele või kasutada neid muudel eesmärkidel ainult kooskõlas teate ja valikuvõimaluse põhimõttega. Näiteks kui organisatsioon kavatseb kasutada töösuhte raames 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 seejärel loa andis. Lisaks ei tohi selliseid valikuvõimalusi kasutada töövõimaluste piiramiseks ega rakendada selliste töötajate suhtes karistusi.

ii. Tuleb märkida, et mõnest ELi liikmesriigist andmete edastamise teatavad üldiselt rakendatavad tingimused võivad välistada selliste andmete kasutamise muudel eesmärkidel isegi pärast edastamist EList väljapoole ning selliseid tingimusi tuleb täita.

iii. Lisaks peaksid tööandjad tegema mõistlikke pingutusi, et tulla vastu töötajate eraelu puutumatuse alastele eelistustele. See võib hõlmata näiteks isikuandmetele juurdepääsu piiramist, teatavatest andmetest 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

i. Täiendav põhimõte juurdepääsu kohta annab juhiseid põhjuste kohta, mis võivad õigustada juurdepääsu võimaldamisest keeldumist või selle piiramist personali kontekstis. Muidugi peavad tööandjad ELis järgima kohalikke õigusnorme ning tagama ELi töötajatele juurdepääsu sellistele andmetele, nagu nõuab nende koduriigi õigus, olenemata andmete töötlemise ja talletamise asukohast. ELi-USA andmekaitseraamistiku kohaselt teeb selliseid andmeid Ameerika Ühendriikides töötlev organisatsioon sellise juurdepääsu võimaldamisel koostööd kas otse või ELi tööandja kaudu.

d. Täitmise tagamine

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

ii. ELi-USA andmekaitseraamistikus osalev Ameerika Ühendriikide organisatsioon, kes kasutab ELi personaliandmeid, mis edastatakse EList töösuhte kontekstis, ja kes soovib selliseid edastusi teha ELi-USA andmekaitseraamistiku alusel, peab niisiis võtma sellisel juhul kohustuse teha uurimisalast koostööd ELi pädevate asutustega ning järgima nende nõuandeid.

e. Kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtte rakendamine

i. ELi-USA andmekaitseraamistikus osaleva organisatsiooni juhuslikeks töösuhtega seotud tegevusvajadusteks võib ELi-USA andmekaitseraamistikuga hõlmatud isikuandmeid, näiteks väikese arvu töötajate isikuandmeid lennupiletite broneerimiseks, hotellitoa või kindlustuse tellimiseks, edastada vastutavale töötlejale ilma juurdepääsu põhimõtte rakendamiseta või sõlmimata kolmandast isikust vastutava töötlejaga lepingut, mis tavaliselt on nõutav kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtte kohaselt, eeldusel et osalev organisatsioon on järginud teate ja valikuvõimaluse põhimõtet.

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

a. Andmete töötlemise lepingud

i. Kui isikuandmed edastatakse EList Ameerika Ühendriikidesse üksnes töötlemise eesmärgil, on selleks vaja lepingut, olenemata sellest, et volitatud töötleja osaleb ELi-USA andmekaitseraamistikus.

ii. ELi vastutavad töötlejad peavad lepingu sõlmima alati, kui edastamine toimub üksnes töötlemise eesmärgil, olenemata sellest, kas töötlemine toimub ELis või väljaspool seda ning kas volitatud töötleja osaleb või ei osale ELi-USA andmekaitseraamistikus. Lepingu eesmärk on tagada, et volitatud töötleja

1. tegutseb üksnes vastutava töötleja juhiste alusel;

2. rakendab vajalikke tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid juhusliku või ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest, ja saab aru, kas andmete edasisaatmine on lubatud, ning

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

iii. Kuna osalevad organisatsioonid tagavad piisava kaitse, ei ole selliste organisatsioonidega üksnes töötlemise eesmärgil sõlmitavate lepingute jaoks eelnevat luba vaja.

b. Andmete edastamine kontrollitavate äriühingute või üksuste grupis

i. Kui isikuandmeid edastatakse kahe vastutava töötleja vahel kontrollitavate äriühingute või üksuste grupis, ei ole kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtte kohaselt alati tarvis lepingut sõlmida. Vastutavad töötlejad kontrollitavate äriühingute või üksuste grupis võivad edastada andmeid, tuginedes muudele dokumentidele, nagu ELi siduvatele kontsernisisestele normidele või muudele grupisisestele vahenditele (nt vastavuse ja kontrolli programmid), tagades jätkuvalt põhimõtete kohase isikuandmete kaitse. Kõnealuste edastamiste puhul jääb osalev organisatsioon vastutavaks põhimõtete järgimise eest.

c. Andmete edastamine vastutavate töötlejate vahel

i. Vastutavate töötlejate vaheliste edastamiste puhul ei pea vastutav töötleja, kes on andmete vastuvõtja, olema osalev organisatsioon või omama sõltumatut kaebuste menetlemise mehhanismi. ELi-USA andmekaitseraamistikus osalev organisatsioon peab sõlmima vastuvõtjaga, kes on kolmandast isikust vastutav töötleja, lepingu, millega tagatakse ELi-USA andmekaitseraamistiku tingimustega samal tasemel kaitse, välja arvatud nõue, et kolmandast isikust vastutav töötleja peab olema osalev 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 ELi-USA andmekaitseraamistiku 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 olla vormilt erinevad, kuid peavad vastama kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte nõuetele. Organisatsioonid saavutavad nõuetega vastavuse järgmiselt: i) nad järgivad erasektori välja töötatud eraelu puutumatuse programme, mille reeglitele on lisatud põhimõtted ja mis 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 ELis 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 täitmisele pööratavad föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission Act) paragrahvi 5 alusel (USA seadustiku 15. jaotise § 45), millega keelatakse ebaõiglane tegevus ja pettus, USA seadustiku 49. jaotise § 41712 alusel, millega keelatakse vedajal või piletimüügiagendil rakendada lennutranspordis või lennutranspordi müügis ebaõiglasi või pettusel põhinevaid tavasid, või selliseid tegevusi keelava muu seaduse või määruse alusel.

c. Selleks et aidata tagada vastavust nende ELi-USA andmekaitseraamistiku suhtes võetud kohustustega ja et toetada programmi haldamist, peavad organisatsioonid ja nende sõltumatud kaebuste menetlemise mehhanismid andma nõudmise korral ministeeriumile ELi-USA andmekaitseraamistikuga seotud teavet. Lisaks peavad organisatsioonid viivitamata vastama kaebustele, mis käsitlevad nendepoolset põhimõtete järgimist ja mille on esitanud andmekaitseasutused ministeeriumi kaudu. Vastuses tuleb märkida, kas kaebus oli põhjendatud, ja kui oli, siis kuidas organisatsioon probleemi lahendab. Ministeerium kaitseb talle esitatud teabe konfidentsiaalsust kooskõlas Ameerika Ühendriikide õigusega.

d. Kaebuste menetlemise mehhanismid

i. Üksikisikuid tuleb julgustada esitama kaebusi asjaomasele organisatsioonile enne, kui nad pöörduvad sõltumatute kaebuste menetlemise mehhanismide poole. Organisatsioonid peavad vastama üksikisikule 45 päeva jooksul alates kaebuse saamisest. Kaebuste menetlemise mehhanismi sõltumatust võib tõendada eelkõige objektiivsuse, läbipaistva koosseisu ja rahastamise ning tõestatud varasemate otsuste abil. Kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte alusel peab üksikisikutele kättesaadav kaebuste menetlemine olema kergesti kättesaadav ja nende jaoks tasuta. Sõltumatud vaidluste lahendamise organid peaksid tutvuma kõikide üksikisikutelt saadud kaebustega, mis ei ole selgelt alusetud või sisutühjad. See ei takista kaebuste menetlemise mehhanismi eest vastutaval sõltumatul vaidluste lahendamise organil kehtestada vastuvõetavuse nõudeid, kuid sellised nõuded peaksid olema läbipaistvad ja põhjendatud (näiteks jätta kõrvale kaebused, mis ei mahu programmi kohaldamisalasse või mille peaks läbi vaatama mõni muu foorum) ning need 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 teave peaks sisaldama teadet mehhanismi eraelu puutumatuse tavade kohta kooskõlas põhimõtetega. Samuti peaksid nad kaebuste lahendamise protsessi hõlbustamiseks tegema koostööd näiteks kaebuste standardvormide väljatöötamisel.

ii. Sõltumatud kaebuste menetlemise mehhanismid peaksid oma veebisaitidel avaldama teabe põhimõtete ning teenuste kohta, mida nad ELi-USA andmekaitseraamistiku kohaselt osutavad. Kõnealune teave peab sisaldama järgmist: 1) teave põhimõtete kohastele sõltumatutele kaebuste menetlemise mehhanismidele esitatavate nõuete kohta või nimetatud teabe juurde viiv link; 2) link ministeeriumi andmekaitseraamistiku veebisaidile; 3) selgitus selle kohta, et nende vaidluste lahendamise teenus, mis on seotud ELi-USA andmekaitseraamistikuga, on üksikisikutele tasuta; 4) kirjeldus selle kohta, kuidas on võimalik esitada põhimõtetega seotud kaebust; 5) ajakava, mille jooksul põhimõtetega 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 järgmist: 1) aruandeaastal laekunud ja põhimõtetega seotud kaebuste koguarv; 2) laekunud kaebuste liigid; 3) vaidluste lahendamise kvaliteedinäitajad, näiteks kaebuste menetlemise aeg, ja 4) kaebuste lahendamise tulemused, eelkõige kohaldatud õiguskaitsevahendite ja sanktsioonide arv ning liigid.

iv. Nagu on sätestatud I lisas, on üksikisikul võimalik kasutada vahekohtumenetlust, et pöörduda lahendamata nõuetega vahekohtusse, kus teha kindlaks, kas osalev organisatsioon on rikkunud põhimõtetest tulenevaid kohustusi asjaomase üksikisiku suhtes ja kas selline rikkumine jääb täielikult või osaliselt heastamata. Kõnealust võimalust saab kasutada ainult nimetatud eesmärkidel. Seda võimalust ei saa kasutada näiteks põhimõtete suhtes tehtavate erandite ([15]) või väidete puhul, mis puudutavad ELi-USA andmekaitseraamistiku piisavust. Kõnealuse vahekohtu võimaluse raames on ELi-USA andmekaitseraamistiku kolleegiumil (mis koosneb kolmest vahekohtunikust, kelle pooled on kokku leppinud) volitused kehtestada konkreetse üksikisiku suhtes rakendatavad mitterahalised õiglased kaitsevahendid (näiteks üksikisiku kõnealustele andmetele juurdepääsu võimaldamine, andmete parandamine, kustutamine või tagastamine), mis on vajalikud põhimõtete rikkumise heastamiseks ainult asjaomasele üksikisikule. Föderaalse vahekohtu seaduse (Federal Arbitration Act) kohaselt on üksikisikutel ja osalevatel organisatsioonidel õigus taotleda kohtulikku läbivaatamist ning vahekohtu otsuste täitmisele pööramist Ameerika Ühendriikide seaduste alusel.

e. Õiguskaitsevahendid ja sanktsioonid

i. Sõltumatu vaidluste lahendamise organi pakutud mis tahes õiguskaitsevahendite tulemuseks peaks olema mittevastavuse mõju heastamine organisatsiooni poolt, kuivõrd see on teostatav, ning see, et organisatsioon järgib edasisel töötlemisel põhimõtteid, ja kui see on asjakohane, et kaebuse esitanud üksikisiku isikuandmete töötlemine lõpetatakse. Sanktsioonid peavad olema piisavalt ranged, tagamaks et organisatsioon järgib põhimõtteid. Paljud erineva rangusastmega sanktsioonid võimaldavad vaidluste lahendamise organitel asjakohaselt reageerida põhimõtete järgimata jätmisele olenevalt raskusastmest. Sanktsioonid peaksid hõlmama nii põhimõtete järgimata jätmise tuvastamise avalikustamist kui ka teatavatel asjaoludel nõuet andmed kustutada ([16]). Muud sanktsioonid võiksid hõlmata tunnuse

([15]) Põhimõtted, ülevaade, punkt 5.

([16]) Sõltumatud vaidluste lahendamise organid võivad omal äranägemisel otsustada, millistes olukordades nad neid sanktsioone rakendavad. Asjaomaste andmete tundlikkus on üks tegur, mida tuleb arvestada otsuse tegemisel selle kohta, kas tuleks nõuda andmete kustutamist, samuti kas organisatsioon on andmeid kogunud, kasutanud või avalikustanud põhimõtteid jõhkralt eirates.

kasutusõiguse peatamist ja eemaldamist, põhimõtete järgimata jätmise tagajärjel üksikisikutele tekitatud kahju hüvitamist ning keelavaid otsuseid. Kui osalevad organisatsioonid ei järgi vaidlusi lahendavate sõltumatute erasektori asutuste ja iseregulatsiooniasutuste korraldusi, peavad need asutused teavitama asjaomase pädevusega valitsusasutust või asjakohasel juhul kohtuid ning ministeeriumi.

f. Föderaalse kaubanduskomisjoni tegevus

i. Föderaalne kaubanduskomisjon on võtnud kohustuse vaadata eelisjärjekorras läbi kaebused põhimõtete väidetava eiramise kohta, mis on saadud: i) eraelu puutumatuse iseregulatsiooniorganitelt ja teistelt sõltumatutelt vaidluste lahendamise organitelt; ii) ELi liikmesriikidelt ning iii) ministeeriumilt, et otsustada, kas on rikutud föderaalse kaubanduskomisjoni seaduse paragrahvi 5, millega keelatakse ebaõiglased ja pettusel põhinevad teguviisid ja tavad äritegevuses. Kui föderaalne kaubanduskomisjon järeldab, et tal on alust kahtlustada paragrahvi 5 rikkumist, võib ta asja lahendada nii, et taotleb keelustavat halduskorraldust (*cease and desist order*), millega keelatakse kõnealune vaidlustatav tegevus, või esitab kaebuse föderaalsele ringkonnakohtule, mille tulemuseks õnnestumise korral võib olla samasisuline föderaalkohtu otsus. See hõlmab ka selliste organisatsioonide valeväiteid ELi-USA andmekaitseraamistiku põhimõtete järgimise või raamistikus osalemise kohta, kes kas ei ole enam andmekaitseraamistikuga ühinenute nimekirjas või ei ole kunagi ministeeriumile kinnitust esitanud. Föderaalne kaubanduskomisjon võib keelustava halduskorralduse eiramise eest määrata tsiviiltrahve ja taotleda föderaalkohtu määruse mittetäitmise eest vastutusele võtmist tsiviil- või kriminaalkorras. Föderaalne kaubanduskomisjon teavitab ministeeriumi sellistest meetmetest. Ministeerium julgustab teisi valitsusasutusi teda teavitama selliste kaebuste lõplikust lahendamisest või muudest põhimõtete järgimist puudutavatest lahenditest.

g. Püsiv põhimõtete järgimata jätmine

i. Kui organisatsioon ei järgi põhimõtteid püsivalt, kaotab ta õiguse ELi-USA andmekaitseraamistikust tulenevatele hüvedele. Ministeerium kustutab andmekaitseraamistikuga ühinenute nimekirjast organisatsioonid, kes ei järgi põhimõtteid püsivalt, ning nad peavad tagastama või kustutama isikuandmed, mille nad on saanud ELi-USA andmekaitseraamistiku alusel.

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, sealhulgas ministeerium, otsustab, et organisatsioon on jätnud korduvalt põhimõtted järgimata sellisel määral, et organisatsiooni kinnitus põhimõtete järgimise kohta ei ole enam usutav. Kui sellise otsuse teeb mõni muu asutus kui ministeerium, peab organisatsioon ministeeriumi sellistest asjaoludest viivitamata teavitama. Selle nõude täitmata jätmise korral võidakse kohaldada valeandmete seadust (False Statements Act, USA seadustiku 18. jaotise § 1001). Erasektori iseregulatsiooniprogrammist või sõltumatust vaidluste lahendamise mehhanismist loobumine ei vabasta organisatsiooni põhimõtete järgimise kohustusest ning tähendab püsivat põhimõtete järgimata jätmist.

iii. Ministeerium kustutab organisatsiooni andmekaitseraamistikuga ühinenute nimekirjast põhimõtete püsiva järgimata jätmise tõttu, sealhulgas vastuseks mis tahes teadetele, mida ta saab püsiva järgimata jätmise kohta kas organisatsioonilt endalt, eraelu puutumatuse iseregulatsiooniasutuselt või mõnelt muult sõltumatult vaidluste lahendamise organilt või valitsusasutuselt, kuid alles pärast põhimõtteid mittejärginud organisatsioonile 30päevast etteteatamist, millele organisatsioonil on võimalus vastata ([17]). Seega selgub ministeeriumi hallatavast andmekaitseraamistikuga ühinenute nimekirjast, millistele organisatsioonidele on või ei ole enam tagatud ELi-USA andmekaitseraamistiku kohased hüved.

iv. Organisatsioon, kes taotleb osalemist iseregulatsiooniorganis ELi-USA andmekaitseraamistikus osalemise õiguse taastamiseks, peab sellele organile esitama täieliku teabe oma varasema osalemise kohta ELi-USA andmekaitseraamistikus.

([17]) Ministeerium märgib teates tähtaja, mis on tingimata lühem kui 30 päeva, mille jooksul peab organisatsioon teatele vastama.

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

a. Üldiselt on valikuvõimaluse põhimõtte eesmärk tagada, et isikuandmeid kasutataks ja avalikustataks kooskõlas üksikisiku ootuste ja valikutega. Selle kohaselt peaks üksikisikul olema võimalus keelduda isikuandmete otseturunduses kasutamisest igal ajal organisatsiooni kehtestatud mõistlikes piirides, näiteks jättes organisatsioonile aega keeldumisvaliku rakendamiseks. Samuti võib organisatsioon nõuda piisavaid andmeid keeldumisvõimalust taotleva isiku kindlakstegemiseks. Ameerika Ühendriikides võivad üksikisikud selle valiku teha keskse keeldumisprogrammi abil. Igal juhul tuleks üksikisikule pakkuda käepärast ja taskukohast mehhanismi selle valiku tegemiseks.

b. Samamoodi võib organisatsioon kasutada andmeid teatavatel otseturunduseesmärkidel, kui enne andmete kasutamist oleks üksikisikule keeldumise võimaluse andmine teostamatu, kui organisatsioon annab samal ajal viivitamata (ning nõudmise korral igal ajal) üksikisikule võimaluse edaspidi keelduda (üksikisikule kulusid tekitamata) otseturundusteabe saamisest ning organisatsioon järgib üksikisiku soove.

13. **Reisiteave**

a. Väljaspool ELi asuvatele organisatsioonidele on paljudel 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. Isikuandmete kaitse üldmääruse kohaselt võib juhul, kui kaitse piisavuse otsust ei ole tehtud, edastada isikuandmeid kolmandasse riiki, kui isikuandmete kaitse üldmääruse artikli 46 kohaselt on ette nähtud asjakohased andmekaitsemeetmed, või konkreetsetes olukordades, kui täidetud on üks isikuandmete kaitse üldmääruse artikli 49 tingimustest (nt kui andmesubjekt on andnud edastamiseks sõnaselge nõusoleku). ELi-USA andmekaitseraamistikus osalevad Ameerika Ühendriikide organisatsioonid pakuvad isikuandmetele piisavat kaitset ja võivad seetõttu võtta vastu isikuandmete kaitse üldmääruse artikli 45 alusel EList edastatud andmeid, ilma kohustuseta võtta kasutusele isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend või vastata isikuandmete kaitse üldmääruse artikli 49 tingimustele. Kuna ELi-USA andmekaitseraamistik hõlmab erireegleid tundlike andmete kohta, võivad ELi-USA andmekaitseraamistiku alusel osalevatele organisatsioonidele edastatavad andmed sisaldada selliseid andmeid (mida võib olla vaja koguda näiteks seoses füüsilise abiga, mida tarbijad vajavad). Igal juhul peab andmeid edastav organisatsioon ikkagi järgima selle ELi liikmesriigi õigust, kus ta tegutseb ja kes võib muu hulgas kehtestada eritingimusi tundlike andmete kasutamisele.

14. **Farmaatsia- ja meditsiinitooted**

a. <u>ELi/liikmesriikide õigusaktide või põhimõtete rakendamine</u>

i. ELi/liikmesriigi õigust kohaldatakse isikuandmete kogumisele ja töötlemisele, mis leiab aset enne edastamist Ameerika Ühendriikidesse. Põhimõtteid kohaldatakse andmete suhtes siis, kui need on edastatud Ameerika Ühendriikidesse. Farmaatsiauuringuteks ja muudel eesmärkidel kasutatavatest andmetest tuleks võimaluse korral nimed kustutada.

b. <u>Tulevased teadusuuringud</u>

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 ELi-USA andmekaitseraamistikuga, võib asjaomane organisatsioon kasutada neid andmeid uuteks teadusuuringuteks, kui alguses esitati asjakohane teade ja anti valikuvõimalus. Selline teade peaks teavitama tulevastest andmete kasutusviisidest, näiteks korrapärased täiendamised, seonduvad uuringud või turundus.

ii. On arusaadav, et kõiki tulevasi andmete kasutamise viise ei ole võimalik nimetada, sest uute uuringute vajadus võib tekkida algandmete uuest tõlgendamisest, uutest meditsiinilistest avastustest ja meditsiini arengust ning tervishoiualasest ja regulatiivsest arengust. Kui see on asjakohane, peaks teade seega sisaldama 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

i. 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 selgitati osalejale antud teates sellel ajal, kui ta osalema nõustus.

d. Edastamine reguleerimise ja järelevalve eesmärkidel

i. Farmaatsia- ja meditsiiniseadmete ettevõtetel on lubatud ELis läbi viidud kliiniliste katsete isikuandmeid esitada Ameerika Ühendriikide seadusandjatele reguleerimise ja järelevalve eesmärkidel. Samuti on kooskõlas teate ja valikuvõimaluse põhimõttega lubatud edastada isikuandmeid muudele isikutele kui seadusandjad, 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. Kliinilistes katsetes (mida nimetatakse ka pimeuuringuteks) osalejatele 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 osalejatel olema võimalus soovi korral oma andmetele juurde pääseda. Seda peaksid nad taotlema eelkõige arstilt või muult tervishoiuteenuse osutajalt, kellelt nad kliinilise katse ajal ravi said, või siis sponsororganisatsioonilt.

f. Toote ohutuse ja tõhususe jälgimine

i. Farmaatsia- või meditsiiniseadmete ettevõte ei pea rakendama teate, valikuvõimaluse, kolmandale isikule andmete edasisaatmise eest vastutuse ja juurdepääsu põhimõtet 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 regulatiivsete nõuete täitmist. See kehtib näiteks tervishoiuteenuste osutajatelt farmaatsia- ja meditsiiniseadmete ettevõtetele, aga ka farmaatsia- ja meditsiiniseadmete ettevõtetelt sellisele valitsusasutusele nagu Food and Drug Administration (Ameerika Ühendriikide toidu- ja ravimiamet) esitatavate aruannete puhul.

g. Kodeeritud andmed

i. Põhiuurija kodeerib alati uurimisandmed päritolukohas ainulaadse koodiga, et üksikute andmesubjektide identiteeti mitte paljastada. Selliste uuringute sponsoriks olevad farmaatsiafirmad selle koodi võtit ei saa. Kordumatu koodi võti on ainult uurijal, et tal oleks võimalik uuritavaid eriolukordades tuvastada (nt kui on vajalik edaspidine meditsiiniline tähelepanu). Sellisel moel kodeeritud andmete edastamine EList Ameerika Ühendriikidesse ei käiks põhimõtete kohase isikuandmete edastamise alla.

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

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

b. Avalike registrite andmetele ei ole vaja rakendada teate, valikuvõimaluse ega kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtet, kui neid ei kombineerita mitteavalike registrite andmetega ning järgitakse asjakohase pädevuse alusel kehtestatud kasutustingimusi. Samuti ei ole teate, valikuvõimaluse või kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtet üldjuhul vaja rakendada avalikult kättesaadava teabe puhul, välja arvatud siis, kui Euroopa edastaja osutab, et selline teave allub piirangutele, mille kohaselt on nõutav, et organisatsioon rakendaks neid põhimõtteid 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 põhimõtteid rikkudes tahtlikult isikuandmed avalikustanud, et organisatsioon ise või keegi teine neist eranditest kasu võiks saada, lõpeb tema õigus ELi-USA andmekaitseraamistikust saadavatele hüvedele.

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 korraldamiseks; siiski tuleb järgida asjakohase pädevusega asutuse kehtestatud kasutustingimusi. Kui avalike registrite andmed on kombineeritud muude, mitteavalike registrite andmetega (muud kui eespool konkreetselt märgitud), peab organisatsioon siiski võimaldama juurdepääsu kõikidele sellistele andmetele, kui sellele ei kohaldata muid lubatud erandeid.

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

16. **Avaliku sektori asutuste juurdepääsutaotlused**

a. Selleks et tagada isikuandmetele juurdepääsuks avaliku sektori asutuste esitatavate seaduspäraste taotluste läbipaistvus, võivad osalevad 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 osalevad organisatsioonid asjaomastes aruannetes esitavad, koos luureühenduse avaldatud ja muu teabega, võib kasutada ELi-USA andmekaitseraamistiku selle toimimise perioodilise ühise läbivaatamise jaoks esitatava teabena kooskõlas põhimõtetega.

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

I LISA. VAHEKOHTUMUDEL

Käesolevas I lisas sätestatakse tingimused, mille alusel ELi-USA andmekaitseraamistikus osalevad organisatsioonid on kohustatud lahendama kaebusi vahekohtumenetluses kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte kohaselt. Allpool kirjeldatud siduvat vahekohtumenetluse kasutamise võimalust kohaldatakse ELi-USA andmekaitseraamistikuga hõlmatud isikuandmete suhtes esitatavate teatavate „jääknõuete" puhul. Kõnealuse valikuvõimaluse andmise eesmärk on pakkuda üksikisikutele kiiret, sõltumatut ja õiglast mehhanismi, mille nad võivad valida põhimõtete sellise väidetava rikkumise lahendamiseks, mida ei ole ELi-USA andmekaitseraamistiku muude võimalike mehhanismide abil lahendatud.

A. **Kohaldamisala**

Kõnealune võimalus on üksikisikule kättesaadav lahendamata ehk jääknõuetega vahekohtu poole pöördumiseks, et teha kindlaks, kas osalev organisatsioon on rikkunud põhimõtetest tulenevaid kohustusi asjaomase üksikisiku suhtes ja kas selline rikkumine on jäänud täielikult või osaliselt heastamata. Kõnealust võimalust saab kasutada ainult nimetatud eesmärkidel. Seda võimalust ei saa kasutada näiteks põhimõtete suhtes tehtavate erandite ([1]) või väidete puhul, mis puudutavad ELi-USA andmekaitseraamistiku piisavust.

B. **Kättesaadavad õiguskaitsevahendid**

Kõnealuse vahekohtu võimaluse raames on ELi-USA andmekaitseraamistiku kolleegiumil (kolleegium koosneb kolmest vahekohtunikust, kelle pooled on kokku leppinud) volitused kehtestada konkreetse üksikisiku suhtes rakendatavad mitterahalised õiglased kaitsevahendid (näiteks üksikisiku küsimuse all olevatele andmetele juurdepääsu võimaldamine, andmete parandamine, kustutamine või tagastamine), mis on vajalikud põhimõtete rikkumise heastamiseks ainult asjaomasele üksikisikule. Kõnealused volitused on ainsad, mis ELi-USA andmekaitseraamistiku kolleegiumil õiguskaitsevahendite suhtes on. Õiguskaitsevahendeid kaaludes peab ELi-USA andmekaitseraamistiku kolleegium võtma arvesse ka ELi-USA andmekaitseraamistiku teiste mehhanismide raames 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 vaidluste lahendamist ja täitmise tagamist käsitleva täiendava põhimõtte punkti d alapunktis i sätestatud ajavahemiku jooksul; 2) kasutama põhimõtete kohast sõltumatut kaebuste menetlemise mehhanismi, mis on üksikisikutele tasuta, ja 3) esitama juhtumi oma andmekaitseasutuse kaudu lahendamiseks ministeeriumile ning andma ministeeriumile võimaluse lahendada asi parimal moel aja jooksul, mis on sätestatud ministeeriumi väliskaubandusameti kirjas ja mis on üksikisikutele tasuta.

Kõnealuse vahekohtumenetluse võimalust ei saa kasutada, kui sama põhimõtete rikkumist, mida üksikisik väidab olevat toimunud, 1) on juba varem vahekohtumenetluses uuritud; 2) kui selle kohta on tehtud lõplik otsus kohtuasjas, mille pool kõnealune üksikisik oli, või 3) milles pooled on juba varem kokkuleppele jõudnud. Lisaks ei saa kõnealust võimalust kasutada, kui andmekaitseasutusel on 1) volitused andmekaitseasutuste rolli käsitleva täiendava põhimõtte või personali isikuandmeid käsitleva täiendava põhimõtte alusel, 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 puhul abi mõnelt muult foorumilt, välja arvatud juhul, kui mitterahalised õiglased õiguskaitsevahendid ei heasta täielikult väidetavat rikkumist, millisel juhul ei takista üksikisiku pöördumine vahekohtu poole kahjuhüvitise nõudmist, mida tavaliselt tehakse kohtu kaudu.

([1]) Põhimõtted, ülevaade, punkt 5.

E. **Läbivaatamine ja täitmise tagamine**

Föderaalse vahekohtu seaduse (Federal Arbitration Act) kohaselt on üksikisikutel ja osalevatel organisatsioonidel õigus taotleda kohtulikku läbivaatamist ning vahekohtu otsuste täitmisele pööramist Ameerika Ühendriikide seaduste alusel ([2]). Kõikidel sellistel juhtudel tuleb pöörduda föderaalsesse ringkonnakohtusse, mille territooriumil asub osaleva organisatsiooni peamine tegevuskoht.

Kõnealune 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. **Vahekohtunike kolleegium**

Pooled valivad ELi-USA andmekaitseraamistiku kolleegiumi liikmed allpool käsitletud vahekohtunike nimekirjast.

Kooskõlas kohaldatava õigusega koostavad ministeerium ja komisjon nimekirja vähemalt kümnest vahekohtunikust, kes valitakse nende sõltumatuse, aususe ja asjatundlikkuse alusel. Kõnealuse protsessi suhtes kohaldatakse alljärgnevat.

Vahekohtunikud:

1) jäävad nimekirja kolmeks aastaks, kui ei ilmne erandlikke asjaolusid või põhjuseid, ning ministeerium võib nende nimekirjas olemise aega pikendada üks kord täiendavaks kolmeaastaseks perioodiks, teavitades sellest eelnevalt komisjoni;

2) ei ole ühegi partei ega osaleva organisatsiooni, või USA või ELi või ELi liikmesriigi või muu valitsusasutuse, avalik-õigusliku asutuse või täitevasutusega seotud ega toimi nende juhiste järgi ning

3) peavad olema saanud loa töötada juristina Ameerika Ühendriikides ja olema asjatundjad USA eraelu puutumatust käsitlevate ning ELi isikuandmete kaitset käsitlevate õigusaktide alal.

([2]) Föderaalse vahekohtu seaduse (Federal Arbitration Act, FAA) 2. peatüki kohaselt „[k]uulub 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 [välisriigi vahekohtu otsuste tunnustamise ja täitmise kohta (10. juuni, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New Yorgi välisriigi vahekohtu otsuste tunnustamise ja täitmise“)].“ USA seadustiku 9. jaotise § 202. Lisaks sätestatakse FAAs, et „[k]okkuleppe või otsuse suhtes, mis tuleneb sellisest õigussuhtest ja mis jääb täies ulatuses Ameerika Ühendriikide kodanike vahele, ei kohaldata [New Yorgi] konventsiooni, välja arvatud, kui see õigussuhe hõlmab välismaal asuvat kinnisvara, see näeb 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 [New Yorgi] konventsioonis sätestatud põhjust otsuse tunnustamise või täitmise kinnitamisest keeldumiseks või edasilükkamiseks.“ Samas, § 207. Edasi sätestatakse 2. peatükis, et „Ameerika Ühendriikide ringkonna-kohtutel . . . on esimese kohtuastme pädevus . . . hagi või menetluse suhtes [New Yorki konventsiooni kohaselt], vaatamata vaidlusalusele summale“. Samas, § 203.
2. peatükis sätestatakse ka, et „1. peatükk kehtib käesoleva peatüki alusel esitatud nõuetele ja algatatud menetlustele sellises ulatuses, milles kõnealune peatükk ei ole vastuolus käesoleva peatükiga või [New Yorgi] konventsiooniga, mille Ameerika Ühendriigid on ratifitseerinud.“ Samas, § 208. 1. peatükis on omakorda sätestatud, et „[k]irjalik säte . . . lepingus, mis tõendab tehingut, mis on seotud äritegevusega, 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 täitmisele pööratav, välja arvatud põhjustel, mida näeb ette seadus või õiglane kohtumenetlus mis tahes lepingu ülesütlemiseks“. Samas, § 2. Edasi on 1. peatükis sätestatud, 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“. Samas, § 9.

G. **Vahekohtumenetlus**

Ministeerium ja komisjon on kooskõlas kohaldatava õigusega kokku leppinud, et võtavad vastu vahekohtu reeglid, millega reguleeritakse ELi-USA andmekaitseraamistiku kolleegiumi menetlusi ([3]). Kui menetlust reguleerivaid reegleid on vaja muuta, lepivad ministeerium ja komisjon kokku nende reeglite muutmises või vajaduse korral olemasolevate, kindlalt väljakujunenud USA vahekohtumenetluste kasutuselevõtmises, kui täidetud on kõik järgmised tingimused:

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

2. töötatakse välja menetluskord tagamaks, et üht ja sama rikkumist, mille üksikisik väidab olevat toime pandud, ei heastataks ega menetletaks kaks korda;

3. föderaalse kaubanduskomisjoni tegevus võib toimuda paralleelselt vahekohtumenetlusega;

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

5. vahekohtumenetlus toimub Ameerika Ühendriikides ning üksikisik võib valida osalemise video või telefoni teel, mis võimaldatakse talle tasuta. Isiklikult kohalviibimist ei nõuta;

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 ELi-USA andmekaitseraamistiku kolleegium leiab, et konkreetseid asjaolusid arvesse võttes oleksid kulud põhjendamatult ebaproportsionaalsed;

7. vahekohtunikele edastatavad materjalid hoitakse konfidentsiaalsena ning neid kasutatakse ainult seoses vahekohtu tegevusega;

8. konkreetset üksikisikut puudutavad menetluseelsed meetmed on vajaduse korral 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 teate laekumisest küsimuse all olevale organisatsioonile, kui pooled teisiti kokku ei lepi.

([3]) Ministeerium valis kooskõlas põhimõtete I lisaga vahekohtumenetlusi haldama ja põhimõtete I lisas määratletud vahekohtufondi haldama vaidluste lahendamise rahvusvahelise keskuse (International Centre for Dispute Resolution (ICDR)), mis on USA vahekohtute assotsiatsiooni (American Arbitration Association ((AAA)) rahvusvaheline osakond (edaspidi koos „ICDR-AAA"). 15. septembril 2017 leppisid ministeerium ja komisjon kokku, et võtavad vastu vahekohtu reeglite paketi, millega reguleeritakse põhimõtete I lisas kirjeldatud siduvaid vahekohtumenetlusi, ning vahekohtunike käitumisjuhendi, mis on kooskõlas kaubandusliku vahekohtu liikmete üldtunnustatud eetikastandardite ja põhimõtete I lisaga. Ministeerium ja komisjon leppisid kokku, et kohandavad vahekohtu reegleid ja käitumisjuhendit, et need kajastaksid ELi-USA andmekaitseraamistikus tehtavaid ajakohastusi, ning et ministeerium teeb nende ajakohastuste tegemiseks koostööd ICDR-AAAga.

H. **Kulud**

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

Kohaldatavatest õigusnormidest lähtudes aitab ministeerium hallata fondi, kuhu osalevad organisatsioonid peavad tegema 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, kes peab ministeeriumile fondi tegevuse kohta korrapäraselt aruandeid esitama. Ministeerium teeb koostööd kolmanda isikuga, et vaadata fondi tegevus perioodiliselt läbi, sealhulgas vajadus muuta sissemaksete suurust või tasude ülemmäärasid või vahekohtu kulude ülemmäärasid, ning võtavad muu hulgas arvesse peetud vahekohtumenetluste arvu ning seonduvaid kulusid ja ajalisi faktoreid, lähtudes arusaamast, et osalevaid organisatsioone ei või rahaliselt ülemäära koormata. Ministeerium teatab koos kolmanda isikuga tehtud läbivaatamiste tulemustest ja teavitab komisjoni sissemaksete suuruse muutmisest ette. Advokaaditasusid ei kaeta käesoleva sätte alusel ega mitte ühestki käesoleva sätte alusel tegutsevast fondist.

II LISA

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

6. juuli 2023

Austatud Didier Reynders
Õigusküsimuste volinik
Euroopa Komisjon
Rue de la Loi/Westraat 200
1049 Brüssel
Belgia

Lugupeetud volinik Reynders

Ameerika Ühendriikide nimel on mul hea meel käesolevaga edastada ELi-USA andmekaitseraamistiku materjalide pakett, mis koos täidesaatva korraldusega 14086 USA signaaliluuretegevuse kaitsemeetmete tõhustamise kohta ja USA föderaalsete õigusnormide kogumi (edaspidi „CFR“) 28. jaotise osaga 201, millega muudetakse justiitsministeeriumi määrusi ja luuakse andmekaitseasju läbivaatav kohus (Data Protection Review Court), kajastavad olulisi ja üksikasjalikke läbirääkimisi eraelu puutumatuse ja kodanikuvabaduste kaitse tugevdamiseks. Nende läbirääkimiste tulemusel on loodud uued kaitsemeetmed, tagamaks et USA signaaliluuretegevus on määratletud riikliku julgeoleku eesmärkide saavutamiseks vajalik ja proportsionaalne, ning uus mehhanism, mille abil Euroopa Liidu (edaspidi „EL“) üksikisikud saavad taotleda hüvitist, kui nad leiavad, et on sattunud signaaliluuretegevuse sihtmärgiks õigusvastaselt, ja mis üheskoos tagavad ELi isikuandmete privaatsuse. ELi-USA andmekaitseraamistik toetab kaasavat ja konkurentsivõimelist digitaalmajandust. Peaksime mõlemad olema uhked selles raamistikus kajastuvate edusammude üle, mis suurendavad eraelu puutumatuse kaitset kogu maailmas. Kõnealune pakett koos täidesaatva korralduse, määruste ja muude avalikest allikatest kättesaadavate materjalidega, on väga tugev alus komisjoni uuele kaitse piisavuse otsusele ([1]).

Lisatud on järgmised materjalid:

— ELi-USA andmekaitseraamistiku põhimõtted, sealhulgas täiendavad põhimõtted (edaspidi koos „põhimõtted“) ja põhimõtete I lisa (st lisa, milles on sätestatud tingimused, mille alusel andmekaitseraamistikus osalevad organisatsioonid on kohustatud lahendama teatavaid jääknõudeid, mis puudutavad põhimõtetega hõlmatud isikuandmeid);

— ministeeriumi andmekaitseraamistiku programmi haldava rahvusvahelise kaubanduse osakonna kiri, milles kirjeldatakse kohustusi, mille meie ministeerium on endale võtnud, et tagada ELi-USA andmekaitseraamistiku tõhus toimimine;

— föderaalse kaubanduskomisjoni kiri, milles kirjeldatakse tema tegevust põhimõtete täitmise tagamisel;

— transpordiministeeriumi kiri, milles kirjeldatakse tema tegevust põhimõtete täitmise tagamisel;

— riikliku luurejuhi büroo koostatud kiri kaitsemeetmete ja piirangute kohta, mida kohaldatakse USA riiklike julgeolekuasutuste suhtes, ning

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

([1]) Juhul kui komisjoni otsust ELi-USA andmekaitseraamistiku alusel pakutava kaitse piisavuse kohta kohaldatakse ka Islandi, Norra ja Liechtensteini suhtes, katab ELi-USA andmekaitseraamistiku pakett nii Euroopa Liitu kui ka kolme kõnealust riiki.

ELi-USA andmekaitseraamistiku täielik pakett avaldatakse ministeeriumi andmekaitseraamistiku veebisaidil ning põhimõtted ja põhimõtete I lisa jõustuvad Euroopa Komisjoni kaitse piisavuse otsuse jõustumise kuupäeval.

Võite olla kindel, et Ameerika Ühendriigid suhtuvad nimetatud kohustustesse tõsiselt. Soovime jätkata Teiega koostööd ELi-USA andmekaitseraamistiku rakendamisel ja selle protsessi järgmise etapi ühisel käivitamisel.

Lugupidamisega

Gina M. RAIMONDO

III LISA

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12. detsember 2022

Austatud Didier Reynders
Õigusküsimuste volinik
Euroopa Komisjon
Rue de la Loi/Westraat 200
1049 Brüssel
Belgia

Lugupeetud volinik Reynders

Väliskaubandusameti nimel on mul hea meel kirjeldada kaubandusministeeriumi (edaspidi „ministeerium“) võetud kohustusi, et tagada isikuandmete kaitse andmekaitseraamistiku programmi haldamise ja järelevalve kaudu. ELi-USA andmekaitseraamistiku väljakujundamine on suur saavutus eraelu puutumatuse ja äritegevuse huvides mõlemal pool Atlandi ookeani, sest see annab inimestele ELis kindlustunde, et nende andmed on kaitstud ning et neil on nende andmetega seotud probleemide lahendamiseks olemas õiguskaitsevahendid, ning see võimaldab tuhandetel ettevõtjatel jätkuvalt investeerida ning osaleda muul viisil Atlandi üleses äri- ja kaubandustegevuses, mis toob kasu kummagi poole majandusele ja kodanikele. ELi-USA andmekaitseraamistik peegeldab aastatepikkust tõhusat tööd Teie ja Teie kolleegidega Euroopa Komisjonis (edaspidi „komisjon“). Me loodame jätkata koostööd komisjoniga, tagamaks et see ühine jõupingutus toimib tõhusalt.

ELi-USA andmekaitseraamistik toob olulist kasu nii üksikisikutele kui ka ettevõtjatele. Esiteks määratakse selles kindlaks ELi üksikisikute Ameerika Ühendriikidesse edastatud isikuandmete puutumatuse kaitse abinõud. Selle kohaselt peavad USAs asuvad osalevad organisatsioonid välja töötama nõuetekohased privaatsustingimused, tegema avalikult teatavaks, et nad võtavad kohustuse järgida ELi-USA andmekaitseraamistiku põhimõtteid, sealhulgas täiendavaid põhimõtteid (edaspidi koos „põhimõtted“), ning põhimõtete I lisa (st lisa, milles on sätestatud tingimused, mille alusel ELi-USA andmekaitseraamistiku organisatsioonid on kohustatud lahendama teatavaid jääknõudeid, mis puudutavad põhimõtetega hõlmatud isikuandmeid), nii et selle täitmist saab USA õiguse alusel nõuda, ([1]) kinnitama igal aastal ministeeriumile uuesti asjaomaste põhimõtete järgimist, võimaldama ELi üksikisikutele tasuta sõltumatut vaidluste lahendamist ning alluma põhimõtetes loetletud USA seadusjärgse organi uurimis- ja täitevasutusele (nt föderaalse kaubanduskomisjoni (FTC) ja transpordiministeeriumi (DOT) või põhimõtete tulevases lisas loetletud USA seadusjärgsele asutusele. Äriühingu otsus kinnitada põhimõtete järgimist on küll vabatahtlik, ent kui ta on teinud avalikuks oma otsuse järgida ELi-USA andmekaitseraamistikku, võib tema võetud kohustuse täitmist USA õiguse alusel nõuda kas föderaalne kaubanduskomisjon või transpordiministeerium või muu USA seadusjärgne asutus, olenevalt sellest, kumma pädevusse osalev organisatsioon kuulub. Teiseks võimaldab ELi-USA andmekaitseraamistik USA äriühingutel, sealhulgas USAs asuvatel Euroopa äriühingute tütarettevõtjatel, saada Euroopa Liidust isikuandmeid, hõlbustamaks Atlandi-ülest äritegevust toetavate andmete edastamist.

([1]) Organisatsioonid, kes on kinnitanud, et nad võtavad kohustuse järgida ELi-USA andmekaitseraamistiku põhimõtted, ja soovivad saada ELi-USA andmekaitseraamistikus osalemisega kaasnevaid hüvesid, peavad vastama „ELi-USA andmekaitseraamistiku põhimõtetele“. Kõnealune kohustus järgida „ELi-USA andmekaitseraamistiku põhimõtteid“ tuleb lisada selliste osalevate organisatsioonide privaatsustingimustesse niipea kui võimalik ja igal juhul hiljemalt kolme kuu jooksul pärast „ELi-USA andmekaitseraamistiku põhimõtete“ jõustumise kuupäeva. (Vt täiendav põhimõte ise kinnitamise kohta, punkt e).

Ameerika Ühendriikide ja Euroopa Liidu vahelised andmevood on maailma suurimad ning toetavad USA ja ELi majandussuhet, mille maht on 7,1 triljonit dollarit ja mis toetab miljoneid töökohti mõlemal pool Atlandi ookeani. Ettevõtjaid, kes sõltuvad Atlandi-ülestest andmevoogudest, leidub kõikides majandusharudes, sealhulgas nii majandusajakirja Fortune Global 500 nimekirja kantud suurimate kui ka väikeste ja keskmise suurusega ettevõtjate hulgas. Atlandi-ülesed andmevood võimaldavad USA organisatsioonidel töödelda Euroopa üksikisikutele kaupade, teenuste ja töötamisvõimaluste pakkumiseks vajalikke andmeid.

Ministeerium kohustub tegema tihedat ja tulemuslikku koostööd meie ELi kolleegidega, et andmekaitseraamistiku programmi tõhusalt hallata ja jälgida. See kohustus väljendub selles, kuidas ministeerium arendab ja jätkuvalt täiustab mitmesuguseid ressursse, millega aidata organisatsioone kinnitamise protsessis, sidusrühmadele sihitud teabe pakkumiseks veebisaidi loomises, koostöös komisjoni ja Euroopa andmekaitseasutustega, et töötada välja ELi-USA andmekaitseraamistiku olulisi elemente selgitavad juhised, samuti teavitustöös, millega hõlbustada organisatsioonide andmekaitsekohustuste paremat mõistmist, ning programmi nõuete organisatsioonidepoolse täitmise järelevalves ja seires.

Meie jätkuv koostöö hinnatud ELi kolleegidega võimaldab ministeeriumil tagada, et ELi-USA andmekaitseraamistik toimib tõhusalt. Ameerika Ühendriikide valitsus on teinud komisjoniga pikka aega koostööd, et edendada ühiseid andmekaitsepõhimõtteid, millega ületada meie õiguslike lähenemisviiside erinevused ning edendada samal ajal Euroopa Liidus ja Ameerika Ühendriikides kaubandust ja majanduskasvu. Usume, et ELi-USA andmekaitseraamistik, mis on selle koostöö näiteks, võimaldab komisjonil teha kaitse piisavuse otsuse, millega antakse organisatsioonidele luba kasutada ELi-USA andmekaitseraamistikku isikuandmete edastamiseks Euroopa Liidust Ameerika Ühendriikidesse kooskõlas liidu õigusega.

Andmekaitseraamistiku programmi haldamine ja järelevalve kaubandusministeeriumi poolt

Ministeerium on võtnud endale kindla kohustuse hallata andmekaitseraamistiku programmi tulemuslikult ja teha selle üle tõhusat järelevalvet ja teeb selle tulemuse tagamiseks asjakohaseid jõupingutusi ning eraldab asjakohased vahendid. Ministeerium peab usaldusväärset nimekirja nende USA organisatsioonide kohta, kes on kinnitanud ministeeriumile, et nad järgivad andmekaitseraamistiku põhimõtteid ja kohustuvad neist kinni pidama (edaspidi „andmekaitseraamistikuga ühinenute nimekiri“), ning avalikustab selle ja ajakohastab seda osalevate organisatsioonide iga-aastaste korduskinnituste kohta tehtud esildiste alusel ning kustutab sellest organisatsioonid, kui need raamistikust vabatahtlikult lahkuvad, ei esita igal aastal korduskinnitust ministeeriumi menetluse kohaselt või kui leitakse, et nad eiravad põhimõtteid järjepidevalt. Ministeerium säilitab ka ametlikud andmed andmekaitseraamistikuga ühinenute nimekirjast kustutatud USA organisatsioonide kohta ja teeb need üldsusele kättesaadavaks, märkides igaühe kohta ka nimekirjast kustutamise põhjuse. Eespool nimetatud ametlik nimekiri ja ametlikud andmed jäävad üldsusele kättesaadavaks ministeeriumi andmekaitseraamistiku veebisaidil. Andmekaitseraamistiku veebisait sisaldab hästi nähtavale kohale paigutatud selgitust, et organisatsioon, kes on andmekaitseraamistikuga ühinenute nimekirjast kustutatud, peab lõpetama selliste väidete esitamise, et ta osaleb ELi-USA andmekaitseraamistikus või järgib selle nõudeid ning võib saada isikuandmeid ELi-USA andmekaitseraamistiku kohaselt. Sellegipoolest peab selline organisatsioon jätkama põhimõtete kohaldamist isikuandmete suhtes, mille ta on saanud ELi-USA andmekaitseraamistikus osalemise ajal, seni kuni ta sellist teavet säilitab. Ministeerium kohustub, edendades oma igakülgset ja jätkuvat pühendumist andmekaitseraamistiku programmi tõhusale haldamisele ja järelevalvele, tegema alljärgnevat.

Kinnitamise nõuetele vastavuse kontroll

— Ministeerium kontrollib enne organisatsiooni põhimõtete järgimise kinnituse või iga-aastase korduskinnituse (edaspidi koos „kinnitus“) lõpule viimist ja organisatsiooni lisamist andmekaitseraamistikuga ühinenute nimekirja või nimekirja jätmist, kas organisatsioon on vähemalt täitnud kinnitamist käsitlevas täiendavas põhimõttes sätestatud asjakohased nõuded selle kohta, millist teavet peab organisatsioon esitama oma kinnitust käsitleva esildise esitamisel ministeeriumile ja on esitanud õigel ajal asjakohased privaatsustingimused, millega teavitatakse üksikisikuid kõigist teate põhimõttes loetletud 13 elemendist. Ministeerium kontrollib, kas organisatsioon on

— esitanud selle organisatsiooni identimisandmed, kes kinnituse esitab, samuti kõik põhimõtete järgimist kinnitava organisatsiooni USA üksused või USA tütarettevõtjad, kes samuti järgivad põhimõtteid ja keda organisatsioon soovib oma kinnitusega hõlmata;

— esitatud nõutud kontaktteabe (nt põhimõtete järgimist kinnitava organisatsiooni selliste teatava(te) isiku(te) ja/või ametniku (ametnike) kontaktandmed, kes vastutavad kaebuste, juurdepääsutaotluste ja muude ELi-USA andmekaitseraamistikust tulenevate probleemide käsitlemise eest);

— kirjeldanud eesmärki (eesmärke), milleks organisatsioon kogub ja kasutab Euroopa Liidust saadud isikuandmeid;

— osutanud, milliseid isikuandmeid ELi-USA andmekaitseraamistikule tuginedes Euroopa Liidust saadakse ja mis on seega tema kinnitusega hõlmatud;

— kui organisatsioonil on olemas avalik veebisait, lisanud veebiaadressi, millelt leiab vaevata organisatsiooni asjaomased privaatsustingimused, või kui organisatsioonil ei ole avalikku veebisaiti, esitanud ministeeriumile koopia vastavatest privaatsustingimustest ja teabe selle kohta, kus need privaatsustingimused on vaatamiseks kättesaadavad mõjutatud isikutele (st mõjutatud töötajatele, kui asjaomased privaatsustingimused on personali privaatsustingimused, või üldsusele, kui asjaomased privaatsustingimused ei ole personali privaatsustingimused);

— lisanud õigel ajal oma asjaomastesse privaatsustingimustesse (st esialgu ainult privaatsustingimuste kavandisse, mis esitatakse koos esildisega, kui esildis tehakse algseks kinnitamiseks; muul juhul lõplikesse ja vajaduse korral avaldatud privaatsustingimustesse) kinnituse selle kohta, et ta järgib põhimõtteid, ja hüperlingi ministeeriumi andmekaitseraamistiku veebisaidile või selle veebisaidi aadressi (nt koduleht või andmekaitseraamistikuga ühinenute nimekirja veebisait);

— lisanud õigel ajal oma asjaomastesse privaatsustingimustesse teate põhimõttes loetletud 12 muud elementi (nt mõjutatud ELi üksikisikul teatavatel tingimustel olev võimalus tugineda siduvale vahekohtuotsusele; nõue avaldada isikuandmed avaliku sektori asutuste seaduspäraste taotluse alusel; sealhulgas riikliku julgeoleku või õiguskaitselisteks vajaduste täitmiseks, ning organisatsiooni kohustused kolmandatele isikutele andmete edasisaatmisel);

— määranud seadusjärgse asutuse, millel on pädevus läbi vaadata mis tahes nõudeid organisatsiooni vastu seoses võimalike ebaõiglaste või pettusel põhinevate tavadega ja puutumatusele kohaldatavate seaduste või normide rikkumisega (ja mis on loetletud põhimõtetes või tulevases põhimõtete lisas);

— esitanud kõik eraelu puutumatuse programmid, milles organisatsioon osaleb;

— teinud kindlaks, kas asjakohane meetod (st järelmeetmed, mille ta peab ette nägema) põhimõtetele vastavuse kontrollimiseks on „enesehindamine“ (st sisekontroll) või „väline vastavuskontroll“ (st kolmanda isiku kontroll) ja kui ta on märkinud asjakohase meetodina välise vastavuskontrolli, esitanud ka selle kontrolli teinud kolmanda isiku identimisandmed;

— on määranud kindlaks asjakohase sõltumatu kaebuste menetlemise mehhanismi, mis on kättesaadav põhimõtete alusel esitatud kaebuste lahendamiseks ja mille raames osutatakse vajalikku abi mõjutatud üksikisikutele tasuta.

  — Kui organisatsioon on valinud erasektori alternatiivse vaidluste lahendamise organi pakutava sõltumatu kaebuste menetlemise mehhanismi, lisab ta oma asjakohastesse privaatsustingimustesse hüperlingi asjaomasele veebisaidile või mehhanismiga ette nähtud kaebuste esitamise vormile, mis on kättesaadav põhimõtete alusel esitatud lahendamata kaebuste uurimiseks, või nende internetiaadressi.

  — Kui organisatsioon on kohustatud (st seoses Euroopa Liidust töösuhte raames edastatud personaliandmetega) või on otsustanud teha põhimõtete alusel esitatud kaebuste uurimisel ja lahendamisel koostööd asjaomaste andmekaitseasutustega, kas ta on teatanud võetud kohustusest andmekaitseasutustega sellist koostööd teha ja põhimõtete täitmiseks erimeetmete võtmise kohta nende antud nõuandeid järgida.

— Ministeerium kontrollib ka seda, kas organisatsiooni kinnitus põhimõtete järgimise kohta on kooskõlas tema asjakohaste privaatsustingimustega. Kui põhimõtete järgimist kinnitav organisatsioon soovib kinnitusega hõlmata oma USA üksusi või USA tütarettevõtjaid, millel on eraldi asjakohased privaatsustingimused, vaatab ministeerium läbi ka selliste hõlmatud üksuste või tütarettevõtjate asjakohased privaatsustingimused, tagamaks et need sisaldavad kõiki teate põhimõtte kohaselt nõutavaid elemente.

— Ministeerium teeb koostööd seadusjärgsete asutustega (nt föderaalne kaubanduskomisjon ja transpordiministeerium), et kontrollida, kas organisatsioonid kuuluvad nende kinnitamist käsitlevas esildises märgitud asjaomase seadusjärgse asutuse jurisdiktsiooni alla, kui ministeeriumil on põhjust selles kahelda.

— Ministeerium teeb koostööd erasektori alternatiivse vaidluste lahendamise organitega, et kontrollida, kas organisatsioonid on registreeritud nende kinnitamist käsitlevas esildises osutatud sõltumatu kaebuste menetlemise mehhanismi aktiivse kasutajana, ja teeb koostööd nende asutustega, et kontrollida, kas organisatsioonid on registreeritud tema kinnitamist käsitlevas esildises osutatud välise vastavuskontrolli aktiivse kasutajana, kui need asutused võivad pakkuda mõlemat liiki teenust.

— Ministeerium teeb koostööd enda valitud kolmanda isikuga, kes haldab andmekaitseasutuste kolleegiumi tasu (st andmekaitseasutuste kolleegiumi tegevuskulude katmiseks ette nähtud aastamaksu) kaudu kogutud rahalisi vahendeid, et kontrollida, kas organisatsioonid on maksnud selle tasu asjaomase aasta eest, kui organisatsioonid on märkinud, et asjaomase sõltumatu kaebuste menetlemise mehhanismina toimivad andmekaitseasutused.

— Ministeerium teeb koostööd enda valitud kolmanda isikuga, et hallata vahekohtumenetlusi ja juhtida põhimõtete I lisas sätestatud vahekohtufondi põhimõtete kohaselt, et kontrollida, kas organisatsioonid on vahekohtu fondi sissemakseid teinud.

— Kui ministeerium tuvastab organisatsioonide kinnitamist käsitlevates esildiste läbivaatamisel probleeme, teatab ta neile, et nad peavad kõik sellised probleemid lahendama ministeeriumi määratud asjakohase tähtaja jooksul ([2]). Ministeerium teavitab neid ka sellest, et kui nad ei vasta ministeeriumi määratud tähtaja jooksul või ei järgi kinnituse esitamisel muul moel ministeeriumi menetlusi, loetakse, et asjaomastest esildistest on loobutud, ning et valeandmete esitamise korral organisatsiooni ELi-USA andmekaitseraamistikus osalemise või sellele vastavuse kohta võib föderaalne kaubanduskomisjon, transpordiministeerium või muu asjaomane valitsusasutus võtta täitemeetmeid. Ministeerium teavitab organisatsioone nende ühenduse võtmise vahendite kaudu, mille organisatsioonid on ministeeriumile teatanud.

Koostöö hõlbustamine alternatiivse vaidluste lahendamise organitega, kes pakuvad põhimõtetega seotud teenuseid

— Ministeerium teeb koostööd erasektori alternatiivse vaidluste lahendamise organitega, kes pakuvad sõltumatuid kaebuste menetlemise mehhanisme, mis on kättesaadavad põhimõtete alusel esitatud lahendamata kaebuste uurimiseks, et kontrollida, kas need vastavad vähemalt nõuetele, mis on sätestatud vaidluste lahendamist ja täitmise tagamist käsitlevas täiendavas põhimõttes. Ministeerium kontrollib, kas

  — nende veebisaitidel on avaldatud teave ELi-USA andmekaitseraamistiku põhimõtete kohta ning teenuste kohta, mida nad andmekaitseraamistiku kohaselt osutavad, mis peab sisaldama järgmist: 1) teave põhimõtete kohastele sõltumatutele kaebuste menetlemise mehhanismidele esitatavate nõuete kohta või nimetatud teabe juurde viiv hüperlink; 2) hüperlink ministeeriumi andmekaitseraamistiku veebisaidile; 3) selgitus selle kohta, et nende vaidluste lahendamise teenus, mis on seotud ELi-USA andmekaitseraamistikuga, on üksikisikutele tasuta; 4) kirjeldus selle kohta, kuidas on võimalik esitada põhimõtetega seotud kaebust; 5) ajakava, mille jooksul põhimõtetega seotud kaebused läbi vaadatakse, ning 6) erinevate võimalike õiguskaitsevahendite kirjeldus. Ministeerium teavitab asutusi õigeaegselt olulistest muudatustest selles, kuidas ministeerium andmekaitseraamistiku programmi üle järelevalvet teeb ja seda haldab, kui sellised muudatused on peatsed või on juba tehtud ning need muudatused puudutavad rolli, mida asutused täidavad ELi-USA andmekaitseraamistikus;

([2]) Nt korduskinnituse puhul eeldatakse, et organisatsioonid lahendavad kõik sellised probleemid 45 päeva jooksul; ministeerium võib määrata ka teistsuguse asjakohase tähtaja.

— nad on avaldanud igal aastal nende vaidluste lahendamise teenuse kohta koondstatistikat sisaldava aruande, mis peab sisaldama järgmist: 1) aruandeaastal laekunud ja põhimõtetega seotud kaebuste koguarv; 2) laekunud kaebuste liigid; 3) vaidluste lahendamise kvaliteedinäitajad, näiteks kaebuste menetlemise aeg, ja 4) kaebuste lahendamise tulemused, eelkõige kohaldatud õiguskaitsevahendite ja sanktsioonide arv ning liigid. Ministeerium annab asutustele konkreetseid ja täiendavaid suuniseid selle kohta, millist teavet nad peaksid neid nõudeid käsitlevates aastaaruannetes esitama (nt loetelu erikriteeriumidest, millele kaebus peab vastama, et kaebust käsitletaks põhimõtetega seotud kaebusena, aastaaruandes), samuti määrab ta kindlaks muud liiki teabe, mida asutused peaksid esitama (nt kui asutus pakub ka põhimõtetega seotud kontrolliteenust, siis kirjeldus selle kohta, kuidas asutus väldib tegelikke või võimalikke huvide konflikte olukordades, kui ta pakub organisatsioonile nii kontrolliteenuseid kui ka vaidluste lahendamise teenuseid). Ministeeriumi antud lisasuunistes täpsustatakse ka kuupäev, millal asutuste vastava aruandeperioodi aastaaruanded peaksid olema avaldatud.

Järelmeetmed organisatsioonide suhtes, kes soovivad enda kustutamist andmekaitseraamistikuga ühinenute nimekirjast või on nimekirjast kustutatud

— Kui organisatsioon soovib ELi-USA andmekaitseraamistikust lahkuda, nõuab ministeerium, et organisatsioon eemaldaks kõikidest asjaomastest privaatsustingimustest kõik viited ELi-USA andmekaitseraamistikule, mis osutavad sellele, et ta osaleb jätkuvalt ELi-USA andmekaitseraamistikus ja et ta võib saada isikuandmeid ELi-USA andmekaitseraamistiku alusel (vt ministeeriumi kohustus otsida valeväiteid osalemise kohta). Ühtlasi nõuab ministeerium, et organisatsioon täidaks ja esitaks ministeeriumile teemakohase küsimustiku, et kontrollida järgmist:

  — tema soovi raamistikust lahkuda;

  — mida ta teeb nende isikuandmetega, mille ta on ELi-USA andmekaitseraamistikus osalemise ajal ELi-USA andmekaitseraamistikule tuginedes saanud: a) säilitab neid andmeid, jätkab nende andmete suhtes põhimõtete kohaldamist ja kinnitab ministeeriumile igal aastal, et ta kohustub põhimõtteid nende andmete suhtes kohaldama; b) säilitab neid andmeid ja tagab nendele andmetele piisava kaitse muude heakskiidetud meetodite abil või c) tagastab või kustutab andmed määratud kuupäevaks ning

  — kes on organisatsioonis alaline kontaktisik põhimõtetega seotud küsimustes.

— Kui organisatsioon on valinud eespool kirjeldatud vastuse a, nõuab ministeerium ka seda, et ta täidaks ja esitaks ministeeriumile igal aastal pärast raamistikust lahkumist (st lahkumise esimeseks aastapäevaks ning igaks järgnevaks aastapäevaks, välja arvatud juhul ja kuni organisatsioon kas pakub sellistele andmetele muude heakskiidetud meetoditega piisavat kaitset või tagastab või kustutab kõik sellised andmed ja teavitab sellest ministeeriumit) teemakohase küsimustiku, et kontrollida, mida ta jätkuvalt säilitatavate isikuandmetega on teinud ja mida ta nendega teeb, ja kes on organisatsioonis alaline kontaktisik põhimõtetega seotud küsimustes.

— Kui organisatsioon on lasknud oma kinnitusel aeguda (st ta ei ole esitanud põhimõtete järgimise kohta iga-aastast korduskinnitust ega ole andmekaitseraamistikuga ühinenute nimekirjast mõnel muul põhjusel, nt raamistikust lahkumise tõttu kustutatud), palub ministeerium tal täita ja esitada ministeeriumile teemakohase küsimustiku, et kontrollida, kas ta soovib raamistikust lahkuda või esitada korduskinnituse,

  — ning kui ta soovib lahkuda, kontrollib ministeerium lisaks, mida ta teeb isikuandmetega, mille ta on ELi-USA andmekaitseraamistikus osalemise ajal ELi-USA andmekaitseraamistikule tuginedes saanud (vt eespool kirjeldus selle kohta, mida organisatsioon peab kontrollima, kui ta soovib raamistikust lahkuda),

  — ning kui ta kavatseb esitada korduskinnituse, kontrollib ministeerium lisaks, kas kinnituse aegumise ajal kohaldas organisatsioon põhimõtteid ELi-USA andmekaitseraamistiku alusel saadud isikuandmete suhtes, ja täpsustab, milliseid meetmeid ta võtab, et lahendada lahendamata probleemid, mille tõttu on tema korduskinnituse esitamine viibinud.

— Kui organisatsioon kustutatakse andmekaitseraamistikuga ühinenute nimekirjast järgmistel põhjustel: a) loobumine ELi-USA andmekaitseraamistikus osalemisest, b) põhimõtete järgimise kohta iga-aastase korduskinnituse lõpule viimata jätmine (st organisatsioon kas alustas, kuid ei viinud iga-aastast korduskinnitamist õigel ajal lõpule või ei ole iga-aastast korduskinnitamise protsessi isegi alustanud) või c) „püsiv põhimõtete järgimata jätmine“, saadab ministeerium organisatsiooni kinnitamist käsitlevas esildises osutatud kontaktisiku(te)le teate, milles täpsustab kustutamise põhjuse ja selgitab, et organisatsioon ei tohi enam esitada ei otseseid ega kaudseid väiteid selle kohta, nagu ta osaleks või järgiks ELi-USA andmekaitseraamistikku ja nagu ta võiks saada isikuandmeid ELi-USA andmekaitseraamistiku kohaselt. Teates, mis võib sisaldada ka muud teavet, mis on kohandatud kustutamise põhjusega, märgitakse, et organisatsioonide suhtes, kes esitavad ELi-USA andmekaitseraamistikus osalemise või selle järgimise kohta valeandmeid, sealhulgas juhul, kui nad väidavad pärast andmekaitseraamistikuga ühinenute nimekirjast kustutamist, et nad osalevad ELi-USA andmekaitseraamistikus, võib föderaalne kaubanduskomisjon või transpordiministeerium või muu asjaomane valitsusasutus võtta täitemeetmeid.

Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine

— Kontrollib korrapäraselt, kui organisatsioon a) loobub ELi-USA andmekaitseraamistikus osalemisest, b) ei esita põhimõtete järgimise kohta iga-aastast korduskinnitust (st organisatsioon kas alustas, kuid ei viinud iga-aastast korduskinnitamist õigel ajal lõpule või ei ole iga-aastast korduskinnitamise protsessi isegi alustanud); c) on eemaldatud ELi-USA andmekaitseraamistikus osalejate hulgast, eelkõige „püsiva põhimõtete järgimata jätmise“ tõttu või d) kui ta ei esita algset kinnitust põhimõtete järgimise kohta (st organisatsioon küll alustas esialgse kinnituse esitamise protsessi, kuid ei viinud seda õigel ajal lõpule), võtab ministeerium omal algatusel meetmeid, et kontrollida ega organisatsiooni asjakohas avaldatud privaatsustingimustes ei ole selliseid viiteid ELi-USA andmekaitseraamistikule, millest loeb välja, et organisatsioon osaleb ELi-USA andmekaitseraamistikus ja et ta võib saada isikuandmeid ELi-USA andmekaitseraamistiku alusel. Kui ministeerium leiab selliseid viiteid, teavitab ta organisatsiooni, et edastab asja vajaduse korral asjakohasele asutusele võimalike täitemeetmete võtmiseks, kui organisatsioon jätkab ELi-USA andmekaitseraamistikus osalemise kohta valeväidete esitamist. Ministeerium kasutab organisatsiooni teavitamiseks vahendeid, mille organisatsioon on ministeeriumile teatanud, või vajaduse korral muid asjakohaseid vahendeid. Kui organisatsioon ei eemalda viiteid ega kinnita ELi-USA andmekaitseraamistiku põhimõtete järgimist kooskõlas ministeeriumi menetlusega, esitab ministeerium omal algatusel asja föderaalsele kaubanduskomisjonile, transpordiministeeriumile või muule asjakohasele täitevasutusele või võtab muid asjakohaseid meetmeid, et tagada ELi-USA andmekaitseraamistikule vastavust kinnitava tähise nõuetekohane kasutamine.

— Ministeerium teeb muidki jõupingutusi, et tuvastada valeväiteid ELi-USA andmekaitseraamistikus osalemise ja ELi-USA andmekaitseraamistikule vastavust kinnitava tähise ebaõige kasutamise kohta, sealhulgas organisatsioonide poolt, kes erinevalt eespool kirjeldatud organisatsioonidest ei ole kinnitamise protsessi üldse alustanudki (nt teeb asjakohaseid internetiotsinguid, et leida organisatsioonide privaatsustingimustes viiteid ELi-USA andmekaitseraamistikule). Kui ministeerium leiab selliste toimingute abil valeväiteid ELi-USA andmekaitseraamistikus osalemise kohta ja tuvastab ELi-USA andmekaitseraamistikule vastavust kinnitava tähise ebaõige kasutamise, teavitab ta organisatsiooni, et edastab asja vajaduse korral asjakohasele asutusele võimalike täitemeetmete võtmiseks, kui organisatsioon jätkab ELi-USA andmekaitseraamistikus osalemise kohta valeväidete esitamist. Ministeerium kasutab organisatsiooni teavitamiseks vahendeid, mille organisatsioon on ministeeriumile teatanud (kui on), või vajaduse korral muid asjakohaseid vahendeid. Kui organisatsioon ei eemalda viiteid ega kinnita ELi-USA andmekaitseraamistiku põhimõtete järgimist kooskõlas ministeeriumi menetlusega, esitab ministeerium omal algatusel asja föderaalsele kaubanduskomisjonile, transpordiministeeriumile või muule asjakohasele täitevasutusele või võtab muid asjakohaseid meetmeid, et tagada ELi-USA andmekaitseraamistikule vastavust kinnitava tähise nõuetekohane kasutamine.

— Ministeerium vaatab talle esitatud konkreetsed tõsiseltvõetavad kaebused ELi-USA andmekaitseraamistikus osalemist käsitlevate valeväidete kohta kiiresti läbi ja menetleb neid (nt andmekaitseasutustelt saadud kaebused, erasektori alternatiivse vaidluste lahendamise organite sõltumatute kaebuste menetlemise mehhanismide kaudu esitatud kaebused, andmesubjektide kaebused, ELi ja USA ettevõtjate ning muude kolmandate isikute kaebused) .

— Ministeerium võib võtta muid asjakohaseid parandusmeetmeid. Ministeeriumile valeandmete esitamise korral võidakse kohaldada valeandmete seadust (False Statements Act, USA seadustiku 18. jaotise § 1001).

Perioodilised omaalgatuslikud vastavuskontrollid ning andmekaitseraamistiku programmi hindamised

— Ministeerium teeb jätkuvalt jõupingutusi, et jälgida ELi-USA andmekaitseraamistiku organisatsioonide tegelikku põhimõtetele vastavust, et teha kindlaks probleemid, mis võivad nõuda järelmeetmeid. Eelkõige teeb ministeerium omal algatusel juhuvaliku alusel ELi-USA andmekaitseraamistiku organisatsioonide rutiinseid pistelisi kontrolle, samuti teatavate ELi-USA andmekaitseraamistiku organisatsioonide *ad hoc* pistelisi kontrolle, kui tuvastatakse võimalikud probleemid nõuetele vastavuses (nt võimalik puudus vastavuses, millele kolmandad isikud on ministeeriumi tähelepanu juhtinud), et kontrollida: a) kas kontaktpunktid, mis vastutavad kaebuste, juurdepääsutaotluste ja muude ELi-USA andmekaitseraamistiku kontekstis tekkivate küsimuste käsitlemise eest, on kättesaadavad; b) asjakohasel juhul seda, kas organisatsiooni üldsusele mõeldud privaatsustingimused on üldsusele vaatamiseks hõlpsasti kättesaadavad nii organisatsiooni avalikul veebisaidil kui ka andmekaitseraamistikuga ühinenute nimekirja juurde viiva hüperlingi kaudu; c) kas organisatsiooni privaatsustingimused vastavad jätkuvalt põhimõtetes kirjeldatud kinnitamisnõuetele ning d) kas organisatsiooni ELi-USA andmekaitseraamistiku alusel esitatud kaebuste lahendamiseks nimetatud sõltumatu kaebuste menetlemise mehhanism on kättesaadav. Ministeerium jälgib aktiivselt ka uudiseid, et leida teateid, mis annavad usaldusväärseid tõendeid ELi-USA andmekaitseraamistikus osalevate organisatsioonide mittevastavuse kohta.

— Vastavuskontrolli raames nõuab ministeerium, et ELi-USA andmekaitseraamistikus osalev organisatsioon täidaks ja esitaks ministeeriumile üksikasjaliku küsimustiku, kui: a) ministeerium on saanud konkreetse tõsiseltvõetava kaebuse, et organisatsioon ei järgi põhimõtteid, b) organisatsioon ei vasta rahuldavalt ministeeriumi järelepärimistele ELi-USA andmekaitseraamistiku puudutavates küsimustes või c) on olemas usutavad tõendid selle kohta, et organisatsioon ei järgi ELi-USA andmekaitseraamistiku alusel võetud kohustusi. Kui ministeerium on saatnud organisatsioonile kõnealuse üksikasjaliku küsimustiku ja organisatsioon ei vasta küsimustikule rahuldavalt, teatab ministeerium organisatsioonile, et vajaduse korral edastab ta asja asjaomasele asutusele võimalike täitemeetmete, kui ministeerium ei saa organisatsioonilt õigeaegset ja rahuldavat vastust. Ministeerium kasutab organisatsiooni teavitamiseks vahendeid, mille organisatsioon on ministeeriumile teatanud, või vajaduse korral muid asjakohaseid vahendeid. Kui organisatsioon ei anna õigeaegset ja rahuldavat vastust, edastab ministeerium asja omal algatusel föderaalsele kaubanduskomisjonile, transpordiministeeriumile või muule asjaomasele täitevasutusele või võtab nõuete täitmise tagamiseks muid asjakohaseid meetmeid. Ministeerium konsulteerib vastavuskontrollide osas pädevate andmekaitseasutustega, kui see on asjakohane.

— Ministeerium hindab perioodiliselt andmekaitseraamistiku programmi haldamist ja järelevalvet, tagamaks et tema järelevalvetegevus, sealhulgas kõik sellised otsinguvahendite abil tehtud toimingud (nt selleks, et leida ELi-USA andmekaitseraamistikus osalevate organisatsioonide privaatsustingimustele viitavaid mittetoimivaid linke), on olemasolevate ja uute tekkivate probleemide lahendamiseks asjakohased.

Andmekaitseraamistiku veebisaidi kohandamine sihtrühmade jaoks

Ministeerium kohandab andmekaitseraamistiku veebisaiti, et keskenduda järgmistele sihtrühmadele: ELi üksikisikud, ELi ettevõtjad, USA ettevõtjad ja andmekaitseasutused. Otse ELi üksikisikutele ja ELi ettevõtjatele mõeldud materjalide lisamine hõlbustab läbipaistvust mitmel viisil. ELi üksikisikute jaoks esitatakse veebisaidil selgelt järgmine teave: 1) õigused, mida ELi-USA andmekaitseraamistik annab ELi üksikisikutele; 2) ELi üksikisikutele kättesaadavad kaebuste menetlemise mehhanismid, juhuks kui nad leiavad, et mõni organisatsioon ei ole täitnud endale võetud kohustust põhimõtteid järgida, ning 3) kuidas leida teavet ühe organisatsiooni kinnituse kohta, et ta järgib ELi-USA andmekaitseraamistiku põhimõtteid. ELi ettevõtjate jaoks teeb veebisait hõlpsamaks järgmise teabe kontrollimise: 1) kas organisatsioon osaleb ELi-USA andmekaitseraamistikus; 2) millist liiki teavet sisaldab organisatsiooni kinnitus ELi-USA andmekaitseraamistiku põhimõtete järgimise kohta; 3) privaatsustingimused, mis hõlmatud teabe suhtes kohaldatakse ja 4) meetod, mida organisatsioon kasutab põhimõtete järgimise tõendamiseks. USA ettevõtjate jaoks esitatakse veebisaidil selgelt järgmine teave: 1) ELi-USA andmekaitseraamistikust tulenevad hüved; 2) kuidas ühineda ELi-USA andmekaitseraamistikuga ning kuidas ELi-USA andmekaitseraamistiku järgimist korduvkinnitada ja kuidas selle järgimisest loobuda ning 3) kuidas Ameerika Ühendriigid ELi-USA andmekaitseraamistikku haldavad ja selle täitmist tagavad. Otse andmekaitseasutustele adresseeritud materjali (nt teave kontaktpunkti kohta, mille ministeerium on andmekaitseasutuste jaoks määranud ja hüperlink põhimõtteid käsitleva sisu juurde föderaalse kaubanduskomisjoni veebisaidil) lisamine aitab kaasa nii koostööle kui ka läbipaistvusele. Samuti teeb ministeerium sihtotstarbelist koostööd komisjoni ja Euroopa Andmekaitsenõukoguga, et töötada välja teemakohaseid lisamaterjale (nt vastused korduma kippuvatele küsimustele), mida võiks kasutada andmekaitseraamistiku veebisaidil, kui selline teave hõlbustaks andmekaitseraamistiku programmi tõhusat haldamist ja järelevalvet.

Andmekaitseasutustega tehtava koostöö hõlbustamine

Andmekaitseasutustega tehtava koostöö võimaluste suurendamiseks hoiab ministeerium töös ministeeriumisisest spetsiaalset kontaktpunkti, mille kaudu hakkab toimuma sidepidamine andmekaitseasutustega. Kui andmekaitseasutus leiab, et ELi-USA andmekaitseraamistikus osalev organisatsioon ei järgi põhimõtteid, sealhulgas pärast kaebuse saamist ELi üksikisikult, võib andmekaitseasutus pöörduda määratud kontaktpunkti poole ministeeriumis, et organisatsiooni täiendavalt kontrollida. Ministeerium teeb kõik selleks, et aidata kaasa kaebuse lahendamisele koos ELi-USA andmekaitseraamistikus osaleva organisatsiooniga. 90 päeva jooksul pärast kaebuse saamist annab ministeerium andmekaitseasutusele tagasisidet. Spetsiaalsele kontaktpunktile antakse teada ka organisatsioonidest, kes esitavad valeväiteid osalemise kohta ELi-USA andmekaitseraamistikus. Määratud kontaktpunkt peab järge kõikide andmekaitseasutuste poolt ministeeriumile saadetud kaebuste üle ning allpool kirjeldatud ühisülevaates esitab ministeerium aruande, milles analüüsib kokkuvõtlikult aasta jooksul laekunud kaebusi. Spetsiaalne kontaktpunkt abistab andmekaitseasutusi, kes soovivad saada teavet konkreetse organisatsiooni antud kinnituse või eelneva osalemise kohta ELi-USA andmekaitseraamistikus, ka vastab spetsiaalne kontaktpunkt andmekaitseasutuste järelepärimistele ELi-USA andmekaitseraamistiku konkreetsete nõuete rakendamise kohta. Ministeerium teeb koostööd ka komisjoni ja Euroopa Andmekaitsenõukoguga andmekaitseasutuste kolleegiumi töö menetlus- ja haldusaspektide valdkonnas, sealhulgas andmekaitseasutuste kolleegiumi tasuna kogutud vahendite jaotamiseks asjakohaste menetluste kehtestamisel. Mõistame, et komisjon teeb ministeeriumiga koostööd, et hõlbustada nende menetlustega tekkida võivate probleemide lahendamist. Lisaks varustab ministeerium andmekaitseasutusi ELi-USA andmekaitseraamistiku kohta käivate materjalidega nende oma veebisaitidele lisamiseks, et suurendada läbipaistvust ELi üksikisikute ja ELi ettevõtjate jaoks. Suurenenud teadlikkus ELi-USA andmekaitseraamistiku ning sellega kaasnevate õiguste ja kohustuste kohta peaks hõlbustama probleemide ilmnemisel nende tuvastamist ja asjakohast lahendamist.

Täidab oma põhimõtete I lisa kohaseid kohustusi

Ministeerium täidab oma põhimõtete I lisa kohaseid kohustusi, sealhulgas peab koos komisjoniga sõltumatuse, aususe ja asjatundlikkuse alusel valitud vahekohtunike nimekirja, ning vajaduse korral toetab ministeerium enda valitud kolmandat isikut, kes haldab kooskõlas põhimõtetega vahekohtumenetlusi ja juhib põhimõtete I lisas nimetatud vahekohtufondi ([3]). Ministeerium teeb kolmanda isikuga koostööd, et muu hulgas kontrollida, kas kolmas isik haldab veebisaiti, mis sisaldab juhendavat teavet vahekohtuprotsessi kohta, sealhulgas järgmist: 1) kuidas menetlust algatada ja dokumente esitada; 2) vahekohtunike nimekiri, mida peab ministeerium, ja kuidas sellest nimekirjast vahekohtunikke valida; 3) ministeeriumi ja komisjoni vastu võetud vahekohtumenetlused ja vahekohtunike käitumisjuhend ([4]) ning 4) vahekohtunike tasude kogumine ja maksmine. Lisaks teeb ministeerium koostööd kolmanda isikuga, et vaadata vahekohtufondi tegevus perioodiliselt läbi, sealhulgas vajaduse muuta sissemaksete suurust või tasude ülemmäärasid (st maksimumsummasid) või vahekohtu kulude ülemmäärasid, ning võtta muu hulgas arvesse peetud vahekohtumenetluste arvu ning seonduvaid kulusid ja ajalisi faktoreid, lähtudes arusaamast, et ELi-USA andmekaitseraamistikus osalevaid organisatsioone rahaliselt ülemäära ei koormata. Ministeerium teatab koos kolmanda isikuga tehtud läbivaatamiste tulemustest ja teavitab komisjoni sissemaksete suuruse muutmisest ette.

ELi-USA andmekaitseraamistiku toimimise ühised läbivaatamised

Ministeerium ja vajaduse korral muud asutused korraldavad korrapäraselt komisjoni, huvitatud andmekaitseasutuste ja Euroopa Andmekaitsenõukogu asjaomaste esindajatega kohtumisi, kus ministeerium esitab ülevaated ELi-USA andmekaitseraamistikust. Iga-aastastel kohtumistel arutatakse muu hulgas jooksvaid küsimusi, mis on seotud andmekaitseraamistiku programmi toimimise, rakendamise, järelevalve ja täitmise tagamisega. Vajaduse korral võib kohtumistel arutada seotud teemasid, nagu muud andmeedastusmehhanismid, milles kasutatakse ELi-USA andmekaitseraamistiku kohaseid kaitsemeetmeid.

([3]) Ministeerium valis kooskõlas põhimõtete I lisaga vahekohtumenetlusi haldama ja põhimõtete I lisas määratletud vahekohtufondi haldama vaidluste lahendamise rahvusvahelise keskuse (International Centre for Dispute Resolution (ICDR)), mis on USA vahekohtute assotsiatsiooni (American Arbitration Association ((AAA)) rahvusvaheline osakond (edaspidi koos „ICDR-AAA“).

([4]) 15. septembril 2017 leppisid ministeerium ja komisjon kokku, et võtavad vastu vahekohtu reeglite paketi, millega reguleeritakse põhimõtete I lisas kirjeldatud siduvaid vahekohtumenetlusi, ning vahekohtunike käitumisjuhendi, mis on kooskõlas kaubandusliku vahekohtu liikmete üldtunnustatud eetikastandardite ja põhimõtete I lisaga. Ministeerium ja komisjon leppisid kokku, et kohandavad vahekohtu reegleid ja käitumisjuhendit, et need kajastaksid ELi-USA andmekaitseraamistikus tehtavaid ajakohastusi, ning et ministeerium teeb nende ajakohastuste tegemiseks koostööd ICDR-AAAga.

Seaduste ajakohastamine

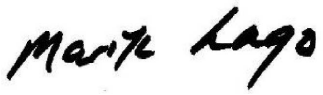
Ministeerium teeb mõistlikke jõupingutusi komisjoni informeerimiseks olulistest muudatustest Ameerika Ühendriikide seadustes, mis on asjakohased ELi-USA andmekaitseraamistiku raames isikuandmete kaitse ja USA ametiasutustele isikuandmetele juurdepääsuks ja nende edaspidiseks kasutamiseks rakendatavate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

USA valitsuse juurdepääs isikuandmetele

Ameerika Ühendriigid on välja andnud täidesaatva korralduse 14086 USA signaaliluuretegevuse kaitsemeetmete tõhustamise kohta ja CFRi 28. jaotise osa 201, millega muudetakse justiitsministeeriumi määrusi ja luuakse andmekaitseasju läbivaatav kohus (Data Protection Review Court (DPRC)), mis tagavad isikuandmete tugeva kaitse seoses valitsuse juurdepääsuga andmetele riikliku julgeoleku eesmärgil. Pakutav kaitse hõlmab järgmist: eraelu puutumatuse ja kodanikuvabaduste kaitsemeetmete tugevdamine eesmärgiga tagada, et USA signaaliluuretegevus on kindlaksmääratud riikliku julgeoleku eesmärkide saavutamiseks vajalik ja proportsionaalne; sõltumatu ja siduva õigusmõjuga uue õiguskaitsemehhanismi loomine ning USA signaaliluuretegevuse olemasoleva range ja mitmetasandilise järelevalve tugevdamine. Nende kaitsemeetmete kaudu võivad ELi üksikisikud taotleda hüvitist uuest mitmekihilisest õiguskaitsemehhanismist, kuhu kuulub sõltumatu andmekaitseasju läbivaatav kohus, mis koosneks USA valitsuse välistest valitud isikutest, kellel oleksid täielikud volitused nõudeid lahendada ja vajaduse korral parandusmeetmeid määrata. Ministeerium peab registrit ELi üksikisikute kohta, kes esitavad vastuvõetava kaebuse täidesaatva korralduse 14086 ja CFRi 28. jaotise osa 201 alusel. Viis aastat pärast käesoleva kirja kuupäeva ja seejärel iga viie aasta järel võtab ministeerium ühendust asjaomaste asutustega, et selgitada välja, kas teave, mis on seotud vastuvõetavate kaebuste läbivaatamisega või andmekaitseasju läbivaatavale kohtule esitatud läbivaatamistaotluste läbivaatamisega, on avalikustatud. Kui sellise teabe salastatus on kustutatud, teeb ministeerium ELi üksikisiku teavitamiseks koostööd asjaomase andmekaitseasutusega. Need täiustused kinnitavad, et USAsse edastatud ELi isikuandmeid käsitatakse viisil, mis on kooskõlas valitsuse juurdepääsu andmetele käsitlevate ELi õigusnõuetega.

Lähtudes põhimõtetest, täidesaatvast korraldusest 14086, CFRi 28. jaotise osast 201 ning lisatud kirjadest ja materjalidest, sealhulgas ministeeriumi andmekaitseraamistiku programmi haldamise ja järelevalvega seoses võetud kohustustest, loodame, et komisjon otsustab, et ELi-USA andmekaitseraamistik pakub liidu õiguse kohaselt piisavat kaitset, ning et jätkub andmete edastamine Euroopa Liidust nendele organisatsioonidele, kes osalevad ELi-USA andmekaitseraamistikus. Eeldame ka, et nende kokkulepete tingimused hõlbustavad veelgi USA organisatsioonidele andmete edastamist, mis toimub ELi lepingu tüüptingimuste või ELi siduvate kontsernisiseste eeskirjade alusel.

Lugupidamisega



Marisa LAGO

IV LISA

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

9. juuni 2023

Didier Reynders
Õigusküsimuste volinik
Euroopa Komisjon
Rue de la Loi / Wetstraat 200
1049 Brüssel
Belgia

Lugupeetud volinik Reynders

USA föderaalne kaubanduskomisjon (Federal Trade Commission – FTC) hindab võimalust selgitada oma rolli ELi-USA andmekaitseraamistiku täitmise tagamisel. Föderaalne kaubanduskomisjon on juba ammu võtnud endale kohustuse kaitsta tarbijaid ja eraelu puutumatust piiriüleselt ning oleme pühendunud selle raamistiku kaubandusvaldkonna aspektide täitmise tagamisele. Föderaalne kaubanduskomisjon on seda ülesannet täitnud alates 2000. aastast seoses USA-ELi raamistikuga Safe Harbor ja viimati alates 2016. aastast seoses ELi-USA andmekaitseraamistikuga Privacy Shield ([1]). 16. juulil 2020 tunnistas Euroopa Liidu Kohus (edaspidi „Euroopa Kohus“) kehtetuks ELi andmekaitseraamistiku Privacy Shield aluseks olnud Euroopa Komisjoni kaitse piisavuse otsuse muude küsimuste alusel kui kaubanduspõhimõtted, mille täimist föderaalne kaubanduskomisjon oli taganud. USA ja Euroopa Komisjon on pärast seda pidanud läbirääkimisi ELi-USA andmekaitseraamistiku üle, et kõnealust Euroopa Kohtu otsust arvesse võtta.

Kirjutan, et kinnitada föderaalse kaubanduskomisjoni võetud kohustust ELi-USA andmekaitseraamistiku põhimõtete täitmist jõuliselt tagada. Eelkõige kinnitame oma kohustusi kolmes põhivaldkonnas: 1) taotluse prioriseerimine ja uurimised; 2) korralduste taotlemine ja seire ning 3) täitmise tagamise alane koostöö ELi andmekaitseasutustega (edaspidi „andmekaitseasutused“).

I. **Sissejuhatus**

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

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

([1]) Esimees Edith Ramirezi kiri Euroopa Komisjoni õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinikule Věra Jourovále, milles kirjeldatakse, kuidas föderaalne kaubanduskomisjon tagab uue ELi-USA andmekaitseraamistiku Privacy Shield täitmist (29. veebruar 2016), *kättesaadav aadressil* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. Varem on föderaalne kaubanduskomisjon võtnud ka USA-ELi programmi Safe Harbor täitmise tagamise kohustuse. Föderaalse kaubanduskomisjoni esimehe Robert Pitofsky kiri Euroopa Komisjoni siseturu peadirektoraadi direktorile John Moggile (14. juuli 2000), *kättesaadav aadressil* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Käesolev kiri asendab nimetatud varasemad kohustused.

jõustatud esmase seadusega, föderaalse kaubanduskomisjoni seadusega, keelatakse ebaõiglased ja pettusel põhinevad tegevused või tavad, mis esinevad kaubandussektoris või mis seda mõjutavad ([2]). Samuti tagab föderaalne kaubanduskomisjon selliste sihipäraseid põhimääruste täitmise, mis kaitsevad andmeid, mis on seotud tervishoiu, laenude ja muude finantsküsimustega, samuti laste internetipõhise teabega, ning on andnud välja määrusi, millega kõiki neid põhimäärusi rakendatakse ([3]).

Ka on föderaalne kaubanduskomisjon teinud hiljuti mitu algatust meie eraelu puutumatuse kaitse valdkonnas tehtava töö tugevdamiseks. 2022. aasta augustis teatas föderaalne kaubanduskomisjon, et kaalub eeskirju kahjuliku kaubandusliku jälgimise ja lõdva andmeturbe ohjamiseks ([4]). Projekti eesmärk on luua tugev avalik register, et saada teavet selle kohta, kas föderaalne kaubanduskomisjon peaks andma välja normid kaubandusliku jälgimise ja andmeturbe tavade käsitlemiseks, ning selle kohta, millised need normid peaksid olema. Oleme palunud selle ja teiste algatuste kohta märkusi ELi sidusrühmadelt.

Juhtivad teadlased kogunevad jätkuvalt meie „PrivacyConi“ konverentsidel, et arutada tarbijate eraelu puutumatuse ja andmeturbega seotud uusimaid uuringuid ja suundumusi. Ka oleme suurendanud oma asutuse suutlikkust pidada sammu tehnoloogia arenguga, mis on enamiku meie eraelu puutumatuse valdkonnas tehtava töö keskmes, ning oleme selleks kokku pannud järjest suureneva meeskonna, mille moodustavad tehnoloogiaspetsialistid ja interdistsiplinaarsed teadustöötajad. Nagu teate, kuulutasime välja ka ühise dialoogi Teie ja Teie kolleegidega Euroopa Komisjonis muu hulgas sellistel eraelu puutumatusega seotud teemadel nagu tumemustrid ja ärimudelid, mida iseloomustab läbiv andmete kogumine ([5]). Samuti esitasime hiljuti kongressile aruande, et kongressi kindlaks tehtud internetiohtude puhul hoiatada selle eest, millised ohud on seotud sellega võitlemiseks tehisintellekti kasutamisega. Selles aruandes väljendati muret ebatäpsuse, erapoolikuse, diskrimineerimise ja kaubandusliku jälgimise hiiliva leviku pärast ([6]).

b. **USA õiguskaitse, millest saavad kasu ELi tarbijad**

ELi-USA andmekaitseraamistikku kohaldatakse USA eraelu puutumatuse laiemas kontekstis, mille raames kaitstakse mitmel viisil ka ELi tarbijaid. Föderaalse kaubanduskomisjoni seadusest tulenev ebaõiglaste ja pettusel põhinevate teguviiside ja tavade keelamine ei piirdu üksnes USA tarbijate kaitsmisega USA ettevõtjate eest, vaid hõlmab ka neid tavasid, mis 1) põhjustavad või võivad põhjustada mõistlikult ettearvatavat kahju Ameerika Ühendriikides või 2) on seotud konkreetse tegevusega Ameerika Ühendriikides. Lisaks sellele saab föderaalne kaubanduskomisjon kasutada välisriigi tarbijate kaitsmisel kõiki kodumaiste tarbijate kaitsmiseks olemasolevaid õiguskaitsevahendeid ([7]).

Samuti tagab föderaalne kaubanduskomisjon selliste muude sihtotstarbeliste seaduste täitmist, millest tulenev kaitse laieneb lisaks USA tarbijatele ka teistele 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 mõeldud veebisaitide ja internetipõhiste teenuste või alla 13-aastastelt lastelt teadlikult isikuandmeid koguvad üldkasutatavate kommertsveebisaitide haldajad teatavad sellest vanematele ning saavad tõestatava vanemate nõusoleku.

([2]) USA seadustiku 15. jaotise § 45 punkt a. Föderaalsel kaubanduskomisjonil ei ole pädevust kriminaalõiguse täitmisele pööramiseks ega riikliku julgeoleku küsimustes. Samuti ei ulatu föderaalse kaubanduskomisjoni pädevus enamiku muude valitsuse tegevuseni. Lisaks sellele on föderaalse kaubanduskomisjoni pädevusele kaubandustegevuse suhtes kehtestatud erandid, sealhulgas seoses pankade, lennuettevõtjate, kindlustusäri ja telekommunikatsiooniteenuste pakkujate ühiste vedajate tegevusega. Samuti ei ole föderaalsel kaubanduskomisjonil pädevust enamiku mittetulundusorganisatsioonide suhtes, kuid tal on pädevus pettuslike heategevusorganisatsioonide ja muude mittetulundusorganisatsioonide puhul, mis tegelikkuses tegutsevad kasumi saamise nimel. Samuti on föderaalsel kaubanduskomisjonil pädevus mittetulundusühingute suhtes, mis tegutsevad oma tulu teenivate liikmete kasumi nimel, pakkudes liikmetele sealhulgas olulisi majanduslikke hüvesid. Mõnel juhul kattub föderaalse kaubanduskomisjoni pädevus muude õiguskaitseorganite pädevusega. Oleme välja töötanud tugevad töösuhted föderaalsete ja osariikide asutustega ning teeme nendega tihedat koostööd, et koordineerida uurimisi ja esitada taotlusi, kui see on asjakohane.

([3]) *Vt* föderaalne kaubanduskomisjon – Privacy and Security (eraelu puutumatus ja turvalisus), https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Vt* pressiteade, föderaalne kaubanduskomisjon uurib norme, mis vähendavad kaubanduslikku jälgimist ja lõtvu andmeturbe tavasid (11. august 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Vt* Euroopa Komisjoni õigusküsimuste voliniku Didier Reyndersi ja Ameerika Ühendriikide föderaalse kaubanduskomisjoni esimehe Lina Khani ühine pressiavaldus (30. märts 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Vt* pressiteade, föderaalse kaubanduskomisjoni aruanne hoiatab veebiprobleemide ohjamiseks tehisintellekti kasutamise eest (16. juuni 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) USA seadustiku 15. jaotise § 45 punkti a alapunkti 4 alapunkt B. Lisaks hõlmavad „ebaõiglased ja pettusel põhinevad teguviisid ja tavad“ selliseid väliskaubandusega seotud teguviise või tavasid, mis i) põhjustavad või võivad põhjustada mõistlikult ettearvatavat kahju Ameerika Ühendriikides või ii) on seotud konkreetse tegevusega Ameerika Ühendriikides. USA seadustiku 15. jaotise § 45 punkti a alapunkti 4 alapunkt A.

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. Peale selle on lisaks USA föderaalseadustele, mille täitmist tagab föderaalse kaubanduskomisjon, tarbijakaitse, isikuandmetega seotud rikkumiste ja eraelu puutumatuse vallas veel muid föderaalseid ja osariikide seadusi, mis võivad anda ELi tarbijatele lisavõimalusi.

c. **Föderaalse kaubanduskomisjoni täitetoimingud**

Föderaalne kaubanduskomisjon on algatanud kohtuasju nii USA-ELi raamistiku Safe Harbor kui ka ELi-USA andmekaitseraamistiku Privacy Shield alusel ning jätkanud ELi-USA andmekaitseraamistiku Privacy Shield täitmise tagamist isegi pärast seda, kui Euroopa Kohus selle aluseks olnud kaitse piisavuse otsuse kehtetuks tunnistas ([8]). Mitu föderaalse kaubanduskomisjoni hiljutist kaebust on sisaldanud väiteid, et ettevõtjad on rikkunud ELi-USA raamistiku Privacy Shield sätted, sealhulgas Twitteri, ([9]) CafePressi ([10]) ja Flo ([11]) vastu algatatud menetlustes. Twitteri vastu võetud täitemeetmete raames nõudis föderaalne kaubanduskomisjon Twitterilt 150 miljonit dollarit trahvina selliste varasemat korraldust rikkuvate tavade eest, mis mõjutasid rohkem kui 140 miljonit klienti, sealhulgas ELi-USA raamistiku Privacy Shield 5. põhimõtte (andmete terviklikkus ja eesmärgi piiramine) rikkumine. Lisaks nõutakse asutuse korralduses, et Twitter lubaks kasutajatel kasutada turvalisi mitme teguriga autentimismeetodeid, mille puhul ei nõua kasutajatelt telefoninumbri esitamist.

CafePressi juhtumis väitis föderaalne kaubanduskomisjon, et ettevõtja ei suutnud turvata tarbijate tundlikku teavet, varjas suurt isikuandmetega seotud rikkumist ja rikkus ELi-USA raamistiku Privacy Shield 2. põhimõtet („Valikuvõimalus“), 4. põhimõtet („Turvalisus“) ja 6. põhimõtet („Juurdepääs“). Föderaalse kaubanduskomisjoni korraldusega pannakse ettevõtjale kohustus asendada ebapiisavad autentimismeetmed mitmikautentimisega, oluliselt piirata kogutavate ja säilitatavate andmete hulka, krüpteerida sotsiaalkindlustuse numbrid ja lasta kolmandal isikul hinnata oma infoturbe programme ning esitada föderaalsele kaubanduskomisjonile koopia, mille võib avalikustada.

Flo juhtumis väitis föderaalne kaubanduskomisjon, et viljakuse jälgimise rakendus avaldas pärast seda, kui oli võtnud endale kohustuse hoida kasutaja terviseteave privaatsena, selle siiski kolmandast isikust andmeanalüütika pakkujatele. Föderaalse kaubanduskomisjoni kaebuses märgitakse eraldi ära ettevõtte suhtlus ELi tarbijatega ning see, et Flo rikkus ELi-USA andmekaitseraamistiku Privacy Shieldi 1. põhimõtet („Teade“), 2. põhimõtet („Valikuvõimalus“), 3. põhimõtet („Vastutus kolmandale isikule andmete edasisaatmise eest“) ja 5. põhimõtet („Andmete terviklikkus ja eesmärgi piiramine“). Muu hulgas nõutakse kaubanduskomisjoni korralduses, et Flo teavitaks mõjutatud kasutajaid nende isikuandmete avalikustamisest ja annaks kõigile kasutajate terviseteavet saanud kolmandatele isikutele juhised need andmed hävitada. Oluline on see, et föderaalse kaubanduskomisjoni korraldustega kaitstakse ülemaailmselt kõiki tarbijaid, kes USA ettevõtjatega suhtlevad, mitte ainult neid tarbijaid, kes on esitanud kaebuse.

Paljudes USA-ELi raamistiku Safe Harbor ja ELi-USA andmekaitseraamistiku Privacy Shield täitmise tagamise juhtumites on olnud tegemist organisatsioonidega, kes esitasid kaubandusministeeriumi kaudu algse kinnituse põhimõtete järgimise kohta, kuid ei esitanud iga-aastast korduskinnitust, kuigi nad esitlesid end jätkuvalt raamistikus osalejana. Teistes juhtumites oli tegemist valeväidetega osalemise kohta, mida esitasid organisatsioonid, kes ei olnud kunagi kaubandusministeeriumi kaudu algset kinnitust esitanud. Edaspidi loodame oma ennetavates täitetoimingutes pöörata veelgi enam tähelepanu ELi-USA andmekaitseraamistiku põhimõtete sisulistele rikkumistele, mida on väidetud näiteks sellistes juhtumites nagu Twitter, CafePress ja Flo. Samal ajal haldab ja jälgib kaubandusministeerium kinnitamise protsessi ning peab ELi-USA andmekaitseraamistikuga ühinenute usaldusväärset nimekirja ja käsitleb muid programmis osalemise nõuetega seotud probleeme ([12]). Oluline on see, et organisatsioonide suhtes, kes väidavad, et osalevad ELi-USA andmekaitseraamistikus, võidakse kohaldada ELi-USA andmekaitseraamistiku põhimõtete sisulist täitmisele pööramist isegi siis, kui nad ei esita kinnitust põhimõtete järgimise kohta kaubandusministeeriumi kaudu või ei esita korduskinnitust.

([8]) Vt lisa A, kus on esitatud nimekiri föderaalse kaubanduskomisjoni programmiga Safe Harbor ja raamistikuga Privacy Shield seotud asjadest.

([9]) *Vt* pressiteade, föderaalne kaubanduskomisjon määrab Twitterile trahvi konto turvaandmete pettusliku kasutamise eest sihitud reklaamide müümiseks (25. mai 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Vt* pressiteade, föderaalne kaubanduskomisjon võtab CafePressi vastu meetmeid isikuandmetega seotud rikkumise varjamise tõttu (15. märts 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Vt* pressiteade, föderaalsel kaubanduskomisjonil on valmis korraldus viljakuse jälgimise rakendusele Flo Health, mis jagas tundlikke terviseandmeid Facebooki, Google'i ja teistega (22. juuni 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Kiri väliskaubandusameti aseriigisekretäri kohusetäitjalt rahvusvahelise kaubanduse alal Marisa Lagolt Euroopa Komisjoni õigusküsimuste volinikule austatud Didier Reyndersile (12. detsember 2022).

II. **Taotluste prioriseerimine ja uurimised**

Sarnaselt USA-ELi raamistikuga Safe Harbor ja ELi-USA andmekaitseraamistikuga Privacy Shield kohustub föderaalne kaubanduskomisjon menetlema kaubandusministeeriumilt ja ELi liikmesriikidelt saadud esildisi ELi-USA andmekaitseraamistiku põhimõtete kohta eelisjärjekorras. Eelisjärjekorras käsitleme ka eraelu puutumatuse kaitse iseregulatsiooniorganitelt ja muudelt sõltumatutelt vaidluste lahendamise organitelt saadud esildisi ELi-USA andmekaitseraamistiku põhimõtete rikkumise kohta.

Selleks et hõlbustada ELi liikmesriikide ELi-USA andmekaitseraamistiku kohaste taotluste esitamist, on föderaalne kaubanduskomisjon loonud standardse kaebemenetluse ning andnud ELi liikmesriikidele juhiseid selle teabe liigi kohta, mis võiks parimal viisil abistada föderaalset kaubanduskomisjoni taotlusega seotud päringu tegemisel. Osana sellest jõupingutusest on föderaalne kaubanduskomisjon määranud 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.

Kui kaubandusministeeriumilt, ELi liikmesriigilt või iseregulatsiooniorganisatsioonilt või muult sõltumatult vaidluste lahendamise organilt saadakse selline esildis, võib föderaalne kaubanduskomisjon võtta tõstatatud küsimuste käsitlemiseks erinevaid meetmeid. Näiteks võime läbi vaadata organisatsiooni privaatsustingimused, hankida lisateavet otse organisatsioonilt või kolmandatelt isikutelt, teha koostööd esildise esitanud üksusega, hinnata, kas rikkumised järgivad sarnast mustrit või rikkumine on mõjutatud märkimisväärset hulka tarbijaid, määrata kindlaks, kas esildis puudutab kaubandusministeeriumi haldusalasse jäävaid küsimusi, hinnata, kas oleks kasulik teha lisatööd turuosaliste teavitamiseks, ning algatada vajaduse korral täitemenetlus.

Lisaks kaubandusministeeriumilt, ELi liikmesriikidelt ja eraelu puutumatuse kaitse iseregulatsiooniorganitelt või muudelt sõltumatutelt vaidluste lahendamise organitelt ([13]) saadud ELi-USA andmekaitseraamistiku põhimõtteid käsitlevate esildiste eelisjärjekorras käsitlemisele jätkab föderaalne kaubanduskomisjon ELi-USA andmekaitseraamistiku põhimõtete oluliste rikkumiste uurimist vajaduse korral ka omal algatusel, kasutades mitmesuguseid vahendeid. Föderaalne kaubanduskomisjon on kaubandusorganisatsioone hõlmavate eraelu puutumatuse kaitse ja turvalisusega seotud küsimuste uurimise programmi osana korrapäraselt kontrollinud, kas kõnealune üksus on esitanud väiteid ELi-USA andmekaitseraamistikus osalemise kohta. Kui üksus esitas selliseid kinnitusi ja uurimise käigus selgus, et ELi andmekaitseraamistiku Privacy Shield põhimõtteid on ilmselgelt rikutud, lisas föderaalne kaubanduskomisjon väited ELi-USA andmekaitseraamistiku Privacy Shield rikkumiste kohta oma täitemeetmete hulka. Meil on kavas ELi-USA andmekaitseraamistiku põhimõtete alusel seda ennetavat lähenemisviisi jätkata.

III. **Korralduste taotlemine ja seire**

Samuti kinnitab föderaalne kaubanduskomisjon oma kohustust taotleda ja jälgida täitekorraldusi, et tagada vastavus ELi-USA andmekaitseraamistiku põhimõtetele. Nõuame ELi-USA andmekaitseraamistiku põhimõtetele vastavust seeläbi, et näeme tulevastes föderaalse kaubanduskomisjoni tehtavates ELi-USA andmekaitseraamistiku põhimõtetega seotud korraldustes ette mitmesugused sobivad keelavad sätted. Föderaalse kaubanduskomisjoni halduskorralduste rikkumine võib viia tsiviilõiguslike trahvideni summas kuni 50 120 USA dollarit rikkumise kohta või 50 120 USA dollarit päevas jätkuva rikkumise korral, ([14]) mis paljusid tarbijaid mõjutavate tavade korral võivad ulatuda miljonite dollariteni. Kõikidel kokkuleppemäärustel 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 süstemaatiliselt ELi-USA andmekaitseraamistiku Privacy Shield põhimõtteid käsitlevate olemasolevate korralduste täitmist, nagu ta teeb kõigi oma korralduste puhul, ja esitab vajaduse korral hagisid nende täitmisele pööramiseks ([15]). Oluline on see, et föderaalse kaubanduskomisjoni korraldustega jätkatakse ülemaailmselt kõikide tarbijate kaitsmist, kes ettevõtjatega suhtlevad, mitte ainult nende tarbijate kaitsmist, kes on esitanud kaebusi. Lisaks haldab föderaalne kaubanduskomisjon internetis nimekirja ettevõtetest, kelle kohta on tehtud ELi-USA andmekaitseraamistiku põhimõtete täitmise tagamisel korraldusi ([16]).

([13]) Kuigi föderaalne kaubanduskomisjon ei lahenda ega vahenda üksikuid tarbijakaebusi, kinnitab föderaalne kaubanduskomisjon, et seab ELi andmekaitseasutustest pärit ELi-USA andmekaitseraamistiku põhimõtetega 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 sama süsteemi, mis on kättesaadav USA tarbijatele: https://reportfraud.ftc.gov/. Siiski võib üksikute ELi-USA andmekaitseraamistiku põhimõtteid käsitlevate kaebuste korral olla ELi üksikisikutel kõige kasulikum esitada kaebused asjaomase liikmesriigi andmekaitseasutusele või sõltumatule vaidluste lahendamise organile.

([14]) USA seadustiku 15. jaotise § 45 punkt m; CFRi 16. jaotise § 1.98. Seda summat kohandatakse perioodiliselt inflatsiooni järgi.

([15]) Eelmisel aastal hääletas föderaalne kaubanduskomisjon korduvrikkujate uurimisprotsessi sujuvamaks muutmise poolt. *Vt* pressiteade, föderaalne kaubanduskomisjon annab loa peamiste täitetegevuse prioriteetide uurimiseks (1. juuli, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Vt* föderaalne kaubanduskomisjon, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Täitmise tagamise alane koostöö ELi andmekaitseasutustega**

Föderaalne kaubanduskomisjon tunnistab olulist rolli, mida ELi andmekaitseasutused võivad täita seoses ELi-USA andmekaitseraamistiku põhimõtete järgimisega ning julgustab pidama rohkem konsultatsioone ja tegema rohkem täitmisalast koostööd. Nimelt on praegusest digitaalse turu arengust ja andmemahukatest ärimudelitest tulenevate probleemide puhul üha otsustavama tähtsusega tegutseda koordineeritult. Föderaalne kaubanduskomisjon vahetab kaebusega seotud teavet kaebuse esitanud täitevasutustega, sealhulgas selle kohta, millises menetlusetapis kaebus on, kohaldades 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 ärahoidmisega seotud jõupingutuste tõhusust. Juhul kui taotlev täitevasutus otsib teavet teatava kaebuse menetlusetapi kohta oma täitemenetluse teostamise eesmärgil, vastab föderaalne kaubanduskomisjon 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 täitmist, millega keelatakse tavad, mis on sisuliselt sarnased nendega, mis on keelatud seadustega, mille täitmist föderaalse kaubanduskomisjon tagab ([17]). 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 seda volitust korrapäraselt, et abistada muid asutusi üle kogu maailma eraelu puutumatuse ja tarbijakaitsega seotud juhtumites.

Lisaks kõikidele konsultatsioonidele pöörduvate ELi andmekaitseasutustega juhtumipõhiste küsimuste kohta kohustub föderaalne kaubanduskomisjon osalema perioodilistel kohtumistel, millest võtavad osa Euroopa Andmekaitsenõukogu määratud esindajad, et arutada üldiselt, kuidas täitmise tagamise alast koostööd parandada. Lisaks osaleb föderaalne kaubanduskomisjon koos kaubandusministeeriumi, Euroopa Komisjoni ja Euroopa Andmekaitsenõukogu esindajatega ELi-USA andmekaitseraamistiku perioodilisel 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 täiteasutustega. Föderaalsel kaubanduskomisjonil on hea meel kinnitada oma tahet tagada ELi-USA andmekaitseraamistiku kaubandusvaldkonna aspektide täitmine. Peame partnerlust oma ELi kolleegidega nii meie kui ka Teie kodanike eraelu puutumatuse kaitse tagamise seisukohast ülimalt oluliseks.

Lugupidamisega

Lina M. KHAN
Esimees, föderaalne kaubanduskomisjon

([17]) Selle otsustamisel, kas kasutada oma USA turvalise võrgu seaduse (U.S. SAFE WEB Act) kohaseid volitusi, kaalub föderaalne kaubanduskomisjon muu hulgas järgmist: „A) kas taotlev asutus on nõustunud andma või annab tulevikus komisjonile vastastikust abi; B) kas taotluse rahuldamine kahjustaks Ameerika Ühendriikide avalikku huvi ning C) kas taotleva asutuse uurimis- või täitemenetlus on seotud seaduste või tavadega, mis kahjustavad või võivad kahjustada märkimisväärset hulka inimesi.“ USA seadustiku 15. jaotise § 46 punkti j alapunkt 3. Asjaomase volituse suhtes ei kohaldata konkurentsiõiguse rakendamise seadusi.

Liide A

Andmekaitseraamistiku Privacy Shield ja raamistiku Safe Harbor täitmise tagamine

	Viitenumber / FTC toimiku nr	Kohtuasi	Link
1	FTC toimik nr 2023062 Juhtum nr 3:22-cv-03070 (N.D. Cal.)	USA *vs.* **Twitter, Inc.**	Twitter
2	FTC toimik nr 192 3209	Asjas Residual Pumpkin Entity, LLC, varasema nimega d/b/a **CafePress**, ja PlanetArt, LLC, d/b/a **CafePress**	CafePress
3	FTC toimik nr 192 3133 Viitenumber C-4747	Asjas **Flo Health, Inc.**	Flo Health
4	FTC toimik nr 192 3050 Viitenumber C-4723	Asjas **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	FTC toimik nr 192 3092 Viitenumber C-4709	Asjas **T&M Protection, LLC**	T&M Protection
6	FTC toimik nr 192 3084 Viitenumber C-4704	Asjas **TDARX, Inc.**	TDARX
7	FTC toimik nr 192 3093 Viitenumber C-4706	Asjas **Global Data Vault, LLC**	Global Data
8	FTC toimik nr 192 3078 Viitenumber C-4703	Asjas **Incentive Services, Inc.**	Incentive Services
9	FTC toimik nr 192 3090 Viitenumber C-4705	Asjas **Click Labs, Inc.**	Click Labs
10	FTC toimik nr 182 3192 Viitenumber C-4697	Asjas **Medable, Inc.**	Medable
11	FTC toimik nr 182 3189 Viitenumber 9386	Asjas NTT Global Data Centers Americas, Inc., **RagingWire Data Centers, Inc.** õigusjärglasena	RagingWire
12	FTC toimik nr 182 3196 Viitenumber C-4702	Asjas **Thru, Inc.**	Thru
13	FTC toimik nr 182 3188 Viitenumber C-4698	Asjas **DCR Workforce, Inc.**	DCR Workforce
14	FTC toimik nr 182 3194 Viitenumber C-4700	Asjas **LotaData, Inc.**	LotaData
15	FTC toimik nr 182 3195 Viitenumber C-4701	Asjas **EmpiriStat, Inc.**	EmpiriStat

16	FTC toimik nr 182 3193 Viitenumber C-4699	Asjas 214 Technologies, Inc., samuti d/b/a **Trueface.ai**	Trueface.ai
17	FTC toimik nr 182 3107 Viitenumber 9383	Asjas **Cambridge Analytica, LLC**	Cambridge Analytica
18	FTC toimik nr 182 3152 Viitenumber C-4685	Asjas **SecureTest, Inc.**	SecurTest
19	FTC toimik nr 182 3144 Viitenumber C-4664	Asjas **VenPath, Inc.**	VenPath
20	FTC toimik nr 182 3154 Viitenumber C-4666	Asjas **SmartStart Employment Screening, Inc.**	SmartStart
21	FTC toimik nr 182 3143 Viitenumber C-4663	Asjas **mResourceLLC,** d/b/a Loop Works LLC	mResource
22	FTC toimik nr 182 3150 Viitenumber C-4665	Asjas **Idmission LLC**	IDmission
23	FTC toimik nr 182 3100 Viitenumber C-4659	Asjas **ReadyTech Corporation**	ReadyTech
24	FTC toimik nr 172 3173 Viitenumber C-4630	Asjas **Decusoft, LLC**	Decusoft
25	FTC toimik nr 172 3171 Viitenumber C-4628	Asjas **Tru Communication, Inc.**	Tru
26	FTC toimik nr 172 3172 Viitenumber C-4629	Asjas **Md7, LLC**	Md7.
30	FTC toimik nr 152 3198 Viitenumber C-4543	Asjas **Jhayrmaine Daniels (d/b/a California Skate-Line)**	Jhayrmaine Daniels
31	FTC toimik nr 152 3190 Viitenumber C-4545	Asjas **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	FTC toimik nr 152 3141 Viitenumber C-4540	Asjas **Golf Connect, LLC**	Golf Connect
33	FTC toimik nr 152 3202 Viitenumber C-4546	Asjas **Inbox Group, LLC**	Inbox Group
34	Toimik nr 152 3187 Viitenumber C-4542	Asjas **IOActive, Inc.**	IOActive
35	FTC toimik nr 152 3140 Viitenumber C-4549	Asjas **Jubilant Clinsys, Inc.**	Jubilant
36	FTC toimik nr 152 3199 Viitenumber C-4547	Asjas **Just Bagels Manufacturing, Inc.**	Just Bagels

37	FTC toimik nr 152 3138 Viitenumber C-4548	Asjas **NAICS Association, LLC**	NAICS
38	FTC toimik nr 152 3201 Viitenumber C-4544	Asjas **One Industries Corp.**	One Industries
39	FTC toimik nr 152 3137 Viitenumber C-4550	Asjas **Pinger, Inc.**	Pinger
40	FTC toimik nr 152 3193 Viitenumber C-4552	Asjas **SteriMed Medical Waste Solutions**	SteriMed
41	FTC toimik nr 152 3184 Viitenumber C-4541	Asjas **Contract Logix, LLC**	Contract Logix
42	FTC toimik nr 152 3185 Viitenumber C-4551	Asjas **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	FTC toimik nr 152 3051 Viitenumber C-4526	Asjas **American Int'l Mailing, Inc.**	AIM
44	FTC toimik nr 152 3015 Viitenumber C-4525	Asjas **TES Franchising, LLC**	TES
45	FTC toimik nr 142 3036 Viitenumber C-4459	Asjas **American Apparel, Inc.**	American Apparel
46	FTC toimik nr 142 3026 Viitenumber C-4469	Asjas **Fantage.com, Inc.**	Fantage
47	FTC toimik nr 142 3017 Viitenumber C-4461	Asjas **Apperian, Inc.**	Apperian
48	FTC toimik nr 142 3018 Viitenumber C-4462	Asjas **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	FTC toimik nr 142 3019 Viitenumber C-4463	Asjas **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	FTC toimik nr 142 3020 Viitenumber C-4464	Asjas **BitTorrent, Inc.**	BitTorrent
51	FTC toimik nr 142 3022 Viitenumber C-4465	Asjas **Charles River Laboratories, Int'l**	Charles River
52	FTC toimik nr 142 3023 Viitenumber C-4466	Asjas **DataMotion, Inc.**	DataMotion
53	FTC toimik nr 142 3024 Viitenumber C-4467	Asjas **DDC Laboratories, Inc.**, d/b/a DNA Diagnostics Center	DDC
54	FTC toimik nr 142 3028 Viitenumber C-4470	Asjas **Level 3 Communications, LLC**	Level 3

55	FTC toimik nr 142 3025 Viitenumber C-4468	Asjas **PDB Sports, Ltd.**, d/b/a the Denver Broncos Football Club, LLP	Broncos
56	FTC toimik nr 142 3030 Viitenumber C-4471	Asjas **Reynolds Consumer Products, Inc.**	Reynolds
57	FTC toimik nr 142 3031 Viitenumber C-4472	Asjas **Receivable Management Services Corporation**	Receivable Mgmt
58	FTC toimik nr 142 3032 Viitenumber C-4473	Asjas **Tennessee Football, Inc.**	Tennessee Football
59	FTC toimik nr 102 3058 Viitenumber C-4369	Asjas **Myspace LLC**	Myspace
60	FTC toimik nr 092 3184 Viitenumber C-4365	Asjas **Facebook, Inc.**	Facebook
61	FTC toimik nr 092 3081 Tsiviilhagi nr 09-CV-5276 (C.D. Cal.)	FTC *vs.* Javian Karnani ja **Balls of Kryptonite, LLC**, d/b/a Bite Size Deals, LLC ja Best Priced Brands, LLC	Balls of Kryptonite
62	FTC toimik nr 102 3136 Viitenumber C-4336	Asjas **Google, Inc.**	Google
63	FTC toimik nr 092 3137 Viitenumber C-4282	Asjas **World Innovators, Inc.**	World Innovators
64	FTC toimik nr 092 3141 Viitenumber C-4271	Asjas **Progressive Gaitways LLC**	Progressive Gaitways
65	FTC toimik nr 092 3139 Viitenumber C-4270	Asjas **Onyx Graphics, Inc.**	Onyx Graphics
66	FTC toimik nr 092 3138 Viitenumber C-4269	Asjas **ExpatEdge Partners, LLC**	ExpatEdge
67	FTC toimik nr 092 3140 Viitenumber C-4281	Asjas **Directors Desk LLC**	Directors Desk
68	FTC toimik nr 092 3142 Viitenumber C-4272	Asjas **Collectify LLC**	Collectify

V LISA

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. juuli 2023

Volinik Didier Reynders
Euroopa Komisjon
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgia

Lugupeetud volinik Reynders

Ameerika Ühendriikide transpordiministeerium (edaspidi „transpordiministeerium“) hindab võimalust kirjeldada oma rolli ELi-USA andmekaitseraamistiku põhimõtete täitmise tagamisel. ELi-USA andmekaitseraamistik täidab olulist rolli, et kaitsta isikuandmeid, 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 esimest korda avalikult oma pühendumust USA-ELi raamistiku Safe Harbor täitmise tagamisele Euroopa Komisjonile enam kui 22 aasta eest saadetud kirjas, kohustustele, mida korrati ja laiendati 2016. aasta kirjas, mis käsitles ELi-USA andmekaitseraamistikku Privacy Shield. Transpordiministeerium lubas nendes kirjades algselt USA-ELi programmi Safe Harbor põhimõtete täitmist ja hiljem ELi-USA andmekaitseraamistiku Privacy Shield põhimõtete täitmist jõuliselt tagada. Transpordiministeerium laiendab seda kohustust ELi-USA andmekaitseraamistiku põhimõtetele ja käesolev kiri tuletab seda kohustust meelde.

Eelkõige kinnitab transpordiministeerium järgmistes põhivaldkondades võetud kohustusi: 1) ELi-USA andmekaitseraamistiku põhimõtete väidetavate rikkumiste uurimine eelisjärjekorras; 2) asjakohaste täitemeetmete võtmine üksuste vastu, kes esitavad ELi-USA andmekaitseraamistikus osalemise kohta vale- või eksitavaid väiteid, ning 3) ELi-USA andmekaitseraamistiku rikkumistega seotud täitekorralduste seire ja avalikustamine. Anname teavet nende kõikide kohustuste kohta ning vajalikus kontekstis asjakohase tausta kohta seoses transpordiministeeriumi rolliga kaitsta tarbijate eraelu puutumatust ja tagada ELi-USA andmekaitseraamistiku põhimõtete täitmine.

1. **Taust**

A. Transpordiministeeriumi volitused eraelu puutumatuse valdkonnas

Transpordiministeerium on võtnud kindla kohustuse tagada tarbijatelt lennuettevõtjatele ja piletimüügiagentidele esitatud teabe privaatsus.

Transpordiministeeriumi pädevus võtta selles valdkonnas meetmeid on sätestatud õigusaktis USA seadustiku 49. jaotise § 41712, millega keelatakse vedajal või piletimüügiagendil rakendada lennutranspordis või lennutranspordi müügis ebaõiglasi või pettusel põhinevaid tavasid. Paragrahv 41712 on üles ehitatud föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission Act) paragrahvi 5 järgides (USA seadustiku 15. jaotise § 45).

Hiljuti andis transpordiministeerium välja määrused, milles määratletakse ebaõiglased ja pettusel põhinevad tavad kooskõlas nii transpordiministeeriumi kui ka föderaalse kaubanduskomisjoni praktikaga (CFRi 14. jaotise § 399.79). Täpsemalt on tava „ebaõiglane“, kui see põhjustab või tõenäoliselt põhjustab olulist kahju, mida ei ole mõistlikult võimalik vältida, ning kahju ei kaalu üles kasu tarbijatele või konkurentsile.

Tava on tarbijate jaoks „petlik“, kui see võib eksitada tarbijat, kes käitub asjaolusid arvestades mõistlikult, seoses olulise asjaoluga. Asjaolu on oluline, kui see on tõenäoliselt mõjutanud tarbija käitumist või otsust seoses toote või teenusega. Lisaks nendele üldpõhimõtetele tõlgendab transpordiministeerium paragrahvi 41712 spetsiifiliselt nii, et see keelab vedajatel ja piletimüüjatel: 1) rikkuda oma privaatsustingimusi; 2) rikkuda ministeeriumi sätestatud reegleid, mille kohaselt peetakse konkreetseid eraelu puutumatusega seotud tavasid ebaõiglaseks või pettusel põhinevaks või 3) rikkuda internetis laste eraelu puutumatuse kaitse seadust (Children's Online Privacy Protection Act – COPPA) või 4) eirata ELi-USA andmekaitseraamistiku osalisena ELi-USA andmekaitseraamistiku põhimõtteid ([1]).

Nagu eespool märgitud, on föderaalõiguse kohaselt transpordiministeeriumil ainuõigus reguleerida lennuettevõtjate eraelu puutumatuse tavasid, samuti jagab transpordiministeerium pädevust föderaalse kaubanduskomisjoniga seoses piletimüügiagentide eraelu puutumatuse tavadega lennutranspordi müügis.

Seega juhul, kui lennuettevõtja või lennutranspordi müüja on teinud avalikuks oma otsuse järgida ELi-USA andmekaitseraamistiku põhimõtteid, võib ministeerium kasutada paragrahvis 41712 kehtestatud seadusest tulenevaid volitusi, et tagada vastavus nendele põhimõtetele. Seega kui reisija annab andmeid vedajale või piletimüügiagendile, kes on kohustunud järgima ELi-USA andmekaitseraamistiku põhimõtteid, põhjustab see, kui vedaja või piletimüügiagent neid ei järgi, tõenäoliselt kahju tarbijale ning kujutab endast paragrahvi 41712 nõuete rikkumist.

B. Täitmise tagamise tavad

Ministeeriumi lennuamet (Office of Aviation Consumer Protection (OACP)) ([2]) uurib juhtumeid ja määrab karistusi USA seadustiku 49. jaotise paragrahvi 41712 alusel. Ta tagab paragrahvis 41712 ebaõiglaste ja pettusel põhinevate tavade vastu sätestatud seadusjärgse keelu täitmisele pööramise peamiselt läbirääkimiste kaudu, koostades keelustamiskorraldusi ja valmistades korraldusi ette, hinnates tsiviiltrahvide kohaldamist. Amet saab suures osas teavet võimalike rikkumiste kohta kaebuste kaudu, mis laekuvad üksikisikutelt, reisibüroodelt, lennuettevõtjatelt ning USA ja välisriikide valitusasutustelt. Tarbijad võivad kasutada lennuettevõtjate ja piletimüügiagentide vastu eraelu puutumatusega seotud kaebuste esitamiseks transpordiministeeriumi veebisaiti ([3]).

Kui juhtumis ei jõuta mõistliku ja asjakohase lahenduseni, on lennundusametil (OACP) pädevus algatada täitemenetlus, mis hõlmab ärakuulamist tõendite kogumiseks transpordiministeeriumi halduskohtus. Halduskohtul on pädevus anda välja keelustamiskorraldusi ja määrata tsiviiltrahve. Paragrahvi 41712 kohaste rikkumiste tulemuseks võivad olla keelustamiskorraldused ja tsiviiltrahvide määramine summas kuni 37 377 USA dollarit paragrahvi 41712 iga rikkumise kohta.

Transpordiministeeriumil puudub volitused määrata kahjutasu või rahalist hüvitist üksikutele kaebuse esitajatele. Samas on transpordiministeeriumil pädevus kiita heaks lennundusameti uurimiste tulemusel saadud lahendid, mis toob tarbijatele otsest kasu (nt raha, vautšerid), korvamaks rahalisi trahve, mida muidu tuleks maksta USA valitsusele. Seda on varem ette tulnud ning võib seda võib ette tulla ka ELi-USA andmekaitseraamistiku põhimõtete kontekstis, kui olukord seda nõuab. Paragrahvi 41712 korduv rikkumine lennuettevõtja poolt tõstataks ka küsimuse lennuettevõtja suhtumisest nõuete täitmisse, mis võib äärmisel juhul lõppeda sellega, et lennuettevõtjat ei peeta enam tegevuskõlblikuks ja ta kaotab seetõttu oma majandustegevuse loa.

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

Paragrahvi 41712 kohane ebaõiglaste või pettusel põhinevate tavade keeld lennutranspordis või lennutranspordi müügis kehtib nii USA kui ka välisriikide lennuettevõtjatele ja piletimüügiagentidele. Transpordiministeerium võtab sageli meetmeid USA ja välisriikide lennuettevõtjate vastu tavade tõttu, mis kahjustavad nii välisriigi kui ka USA tarbijaid, tuginedes sellele, et lennuettevõtjate tegevus toimus lennutranspordi ajal 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Varem lennundusjõustamise ja menetluste amet (Office of Aviation Enforcement and Proceedings).
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Ka pöörab transpordiministeerium lennuettevõtjate suhtes täitmisele muid sihipäraseid seadusi, millest tulenev kaitse laieneb lisaks USA tarbijatele ka teistele tarbijatele, näiteks internetis laste eraelu puutumatuse kaitse seadus (Children's Online Privacy Protection Act (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. **ELi-USA andmekaitseraamistiku põhimõtete täitmise tagamine**

Kui lennuettevõtja või piletimüügiagent otsustab osaleda ELi-USA andmekaitseraamistikus ja transpordiministeeriumile laekub kaebus, et see lennuettevõtja või piletimüügiagent on väidetavalt ELi-USA andmekaitseraamistiku põhimõtteid rikkunud, võtab ministeerium järgmised meetmed, et ELi-USA andmekaitseraamistiku põhimõtete täitmist jõuliselt tagada.

A. Väidetavate rikkumiste uurimine eelisjärjekorras

Transpordiameti lennundusamet (OACP) uurib kõiki kaebusi, milles väidetakse, et ELi-USA andmekaitseraamistiku põhimõtteid on rikutud, sealhulgas ELi andmekaitseasutustelt laekunud kaebusi, ning võtab täitemeetmed juhul, kui rikkumise kohta on tõendeid.

Lisaks sellele teeb lennundusamet koostööd föderaalse kaubanduskomisjoni ja kaubandusministeeriumiga ning seab esikohale nende väidete uurimise, mille kohaselt ei täida reguleeritud üksused oma ELi-USA andmekaitseraamistikust tulenevaid eraelu puutumatusega seotud kohustusi.

Kui saadakse kaebus ELi-USA andmekaitseraamistiku põhimõtete väidetava rikkumise kohta, võib lennundusamet võtta uurimise osana erinevaid meetmeid. Näiteks võib ta läbi vaadata piletimüügiagendi või lennuettevõtja privaatsustingimused, saada lisateavet otse piletimüügiagendilt või lennuettevõtjalt või kolmandatelt isikutelt, teha koostööd taotleva üksusega ning hinnata, kas rikkumised on korduvad või on mõjutatud tarbijate hulk märkimisväärne. Lisaks teeb ta kindlaks, kas asi on seotud kaubandusministeeriumi või föderaalse kaubanduskomisjoni haldusalasse jäävate küsimustega, hindab, kas tarbijate ja ettevõtjate koolitamisest oleks kasu, ning vajaduse korral algatab täitemenetluse.

Kui transpordiministeerium saab teada ELi-USA andmekaitseraamistiku põhimõtete võimalikust rikkumisest piletimüügiagentide poolt, kooskõlastab ta juhtumi käsitlemist föderaalse kaubanduskomisjoniga. Samuti nõustame föderaalset kaubanduskomisjoni ja kaubandusministeeriumi seoses kõikide ELi-USA andmekaitseraamistiku põhimõtete täitemeetmete tulemustega.

B. Osalemise kohta esitatud vale- või eksitavate väidetega tegelemine

Transpordiministeerium kohustub jätkuvalt uurima ELi-USA andmekaitseraamistiku põhimõtete rikkumisi, sealhulgas vale- või eksitavaid väiteid ELi-USA andmekaitseraamistikus osalemise kohta. Eelisjärjekorras võtame arvesse kaubandusministeeriumilt laekunud esildisi, mis käsitlevad organisatsioone, mille puhul on ministeerium avastanud, et nad väidavad end ebaseaduslikult olevat ELi-USA andmekaitseraamistiku praegused osalejad või kasutavad ELi-USA andmekaitseraamistikule vastavust kinnitavat tähist ilma loata.

Lisaks sellele märgime, et kui organisatsiooni privaatsustingimustes lubatakse, et organisatsioon täidab ELi-USA andmekaitseraamistiku põhimõtteid, siis see, kui organisatsioon ei esita kaubandusministeeriumi kaudu kinnitust põhimõtete järgimise kohta või ei esita korduskinnitust, iseenesest ei vabasta organisatsiooni täitemeetmetest, mida transpordiministeerium võib nende kohustuste täitmiseks tema suhtes võtta.

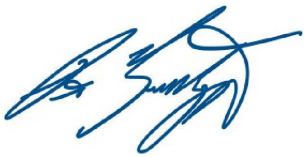
C. ELi-USA andmekaitseraamistiku rikkumistega seotud täitekorralduste seire ja avalikustamine

Transpordiministeeriumi lennundusamet kinnitab ka oma kohustust vajaduse korral täitekorraldusi jälgida, et tagada vastavus ELi-USA andmekaitseraamistiku põhimõtetele. Täpsemalt öeldes, kui amet annab välja korralduse, mille kohaselt tuleb lennuettevõtjal või piletimüügiagendil lõpetada ELi-USA andmekaitseraamistiku põhimõtete ja paragrahvi 41712 rikkumine ning hoiduda sellistest rikkumistest tulevikus, jälgib amet üksuse vastavust korralduses kehtestatud keelustamissättele. Lisaks tagab amet, et ELi-USA andmekaitseraamistiku põhimõtetega seotud juhtumitest tulenevad korraldused on kättesaadavad ameti veebisaidil.

Meil on hea meel jätkata ELi-USA andmekaitseraamistikuga seotud koostööd oma föderaaltasandi partnerite ja ELi sidusrühmadega.

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

Lugupidamisega



Pete BUTTIGIEG

VI LISA

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General Washington, D.C. 20530

23. juuni 2023

Ana Gallego Torres
Õigus- ja tarbijaküsimuste peadirektor
Euroopa Komisjon
Rue Montoyer/Montoyerstraat 59
1049 Brüssel
Belgia

Lugupeetud peadirektor Gallego Torres

Käesolevas kirjas antakse lühiülevaade peamistest uurimisvahenditest, mida kasutatakse selleks, et saada kaubanduslikke andmeid ja muid registriandmeid Ameerika Ühendriikide ettevõtjatelt kriminaalõiguse täitmise või avaliku huvi (tsiviil- ja regulatiivsel) eesmärgil, sealhulgas nende asutuste kehtestatud juurdepääsupiirangutest ([1]). Kõik selles kirjas kirjeldatud õiguslikud menetlused on mittediskrimineerivad selles suhtes, et neid kasutatakse teabe saamiseks Ameerika Ühendriikide ettevõtjatelt, sealhulgas ettevõtjatelt, kes esitavad ELi-USA andmekaitseraamistiku kaudu põhimõtete järgimise kinnituse, sõltumata andmesubjekti kodakondsusest või elukohast. Lisaks sellele võivad need ettevõtjad, kelle suhtes on Ameerika Ühendriikides algatatud kohtuasi, vaidlustada selle kohtus, nagu on allpool käsitletud ([2]).

Avaliku sektori asutuste võimaluse suhtes andmeid arestida on eriti oluline Ameerika Ühendriikide põhiseaduse neljas parandus, milles on ette nähtud, et „[k]eelatud on rikkuda inimeste õigust olla kaitstud iseenda, oma kodu, dokumentide ja vara põhjendamatu läbiotsimise ja arestimise eest ning vastav määrus antakse ainult küllaldase aluse korral, kui seda toetab vanne või ametlik kinnitus ja kirjeldatud on läbiotsitavat kohta, vahistatavat isikut või arestitavat eset“. USA põhiseaduse IV parandus. USA ülemkohus (United States Supreme Court) märkis kohtuasjas Berger *vs.* State of New York, et „selle paranduse peamine eesmärk, nagu on tunnistatud asjaomase kohtu loendamatutes otsustes, on kaitsta üksikisikute eraelu puutumatust ja turvalisust 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 parandusega üldjuhul õiguskaitseametnikelt seda, et nad hangiksid enne läbiotsimist selleks kohtu tehtud määruse. Vt Katz *vs.* Ameerika

([1]) Käesolevas ülevaates ei kirjeldata riikliku julgeoleku uurimisvahendeid, mida õiguskaitseasutused kasutavad võitluses terrorismi vastu ja muudes riikliku julgeoleku valdkonna uurimistes, sealhulgas riikliku julgeoleku teabenõudeid (National Security Letters – NSL) teatavate registriandmete kohta krediidiaruannetes, finantsaruannetes, elektroonilistes abonendi- ja tehinguaruannetes, USA seadustiku 12. jaotise § 3414; USA seadustiku 15. jaotise § 1681u; USA seadustiku 15. jaotise § 1681v; USA seadustiku 18. jaotise § 2709, USA seadustiku 50. jaotise § 3162 ning elektroonilise jälitustegevuse, läbiotsimismääruste, äridokumentide ja muude teabekogumite kohta vastavalt välisluure jälitustegevuse seadusele (Foreign Intelligence Surveillance Act – FISA), USA seadustiku 50. jaotise § 1801 jj.

([2]) Selles kirjas käsitletakse föderaalseid õiguskaitse- ja reguleerivaid asutusi. Osariigi õiguse rikkumisi uurivad osariigi õiguskaitseasutused ja neid rikkumisi arutatakse osariigi kohtutes. Osariikide õiguskaitseorganid kasutavad määrusi ja kohtukorraldusi, mis on välja antud osariigi õiguse kohaselt sisuliselt samal viisil, nagu on siin kirjeldatud, kuid võimalusega, et osariigi kohtumenetluse suhtes võidakse kohaldada osariigi põhiseaduses või põhimäärustes kehtestatud lisakaitset, mis on ületab USA põhiseaduses kehtestatud kaitset. Osariigi õiguskaitse peab olema vähemalt võrdne USA põhiseaduse järgse kaitsega, sealhulgas, aga mitte ainult, neljanda parandusega.

Ühendriigid, 389 U.S. 347, 357 (1967). Määruse väljaandmise standardid, näiteks küllaldase aluse ja täpsuse nõuded, kehtivad nii füüsilise läbiotsimise ja arestimise määruste kui ka salvestatud teabe vahetamise seaduse alusel välja antud elektroonilise side salvestatud sisu määruste suhtes, nagu on kirjeldatud allpool. Kui määruse nõue ei kehti, kohaldatakse valitsuse tegevuse suhtes siiski neljanda paranduse kohast mõistlikkuse kriteeriumi. Põhiseadusega on seega tagatud, et USA valitsusel ei ole piiramatut ega omavolilist võimu isikuandmeid koguda ([3]).

Kriminaalõiguskaitseasutused:

Föderaalprokurörid, 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 kriminaalse uurimise eesmärgil mitut liiki kohustuslike õigusprotsesside kaudu, sealhulgas vandemeeste kogu (grand jury) välja antud korraldused, halduslikud korraldused ja läbiotsimismäärused, ning nad võivad enda valdusesse saada muud teabevahetust vastavalt föderaalsele kriminaalmenetluse raames pealtkuulamise volitustele.

Vandemeeste kogu või kohtu tehtud kohtukorraldused: kriminaalkohtu korraldusi kasutatakse selleks, et toetada suunatud õiguskaitsega seotud uurimisi. Vandemeeste kogu tehtud kohtukorraldus on vandemeeste kogu välja antud ametlik taotlus (tavaliselt föderaalprokuröri taotlusel), et toetada vandemeeste kogu toimetatavat uurimist seoses kriminaalõiguse teatava rikkumise kahtlusega. Vandemeeste kogud on uurimisega tegelevad üksused kohtus ning need määrab kas kohtunik või magistraadikohtunik. Kohtukorraldusega võidakse isikult nõuda menetluses ütluste andmist või äridokumentide, elektrooniliselt säilitatud teabe või muude materiaalsete objektide koostamist või avaldamist. Teave peab olema uurimise seisukohast asjakohane ning kohtukorraldus ei saa olla ebamõistlik selle laia ulatuse või rõhuva või koormava laadi tõttu. Saajal on võimalik kohtukorraldus nendel põhjustel vaidlustada. Vt kriminaalmenetluse föderaaleeskirjade (Federal Rules of Criminal Procedure) eeskiri 17. Piiratud juhtudel võib kohus kasutada dokumentide saamiseks kohtukorraldusi pärast seda, kui vandemeeste kogu (*grand jury*) on esitanud süüdistuse.

Halduslikud korraldused: halduslikke korraldusi on õigus kasutada kriminaal- või tsiviiluurimises. Kriminaalõiguse täitmise kontekstis lubatakse mitme föderaalse põhimäärusega kasutada halduslikke korraldusi, et koostataks või tehtaks kättesaadavaks äridokumendid, elektrooniliselt säilitatud andmed või muud esemed uurimistes, mis on seotud tervishoiupettust, lapse väärkohtlemist, salateenistuse Secret Service kaitset käsitlevate juhtumite, kontrollitavate aine juhtumite ning peainspektori uurimistega, millesse kaasatakse valitsusasutusi. Juhul kui valitsus kavatseb nõuda halduslike korralduste täitmise pööramist kohtus, võib selle saaja, näiteks vandemeeste kogu (*grand jury*) välja antud korralduse saaja, väita, et nõue on ebamõistlik selle laia ulatuse või rõhuva või koormava laadi tõttu.

Pealtkuulamise kohtumäärused: pealtkuulamise kriminaalsätete alusel võivad õiguskaitseorganid saada kohtumääruse, et hankida telefoninumbri või e-posti kohta reaalajas muid kui sisuandmeid seoses helistamise, marsruutimise, suunamise ja signaaliteabega, kui nad tõendavad, et esitatud teave on käimasoleva kriminaaluurimise jaoks oluline. Vt USA seadustiku 18. jaotise § 3121–3127. Sellise seadme kasutamine või paigaldamine väljaspool seadust on föderaalne kuritegu.

Elektroonilise side privaatsuse seadus (Electronic Communications Privacy Act (ECPA)): lisanormid reguleerivad valitsuse juurdepääsu abonendi andmetele, liiklusandmetele ja salvestatud andmesisule, mida valdavad internetiteenuse osutajad, mobiilsideettevõtted ja muud kolmandast isikust teenuseosutajad, vastavalt ECPA II peatükile, mida nimetatakse ka salvestatud sideandmete seaduseks (Stored Communications Act – SCA), USA seadustiku 18. jaotise § 2701–2712. Salvestatud sideandmete seaduses kehtestatakse seadusjärgne eraelu puutumatuse õiguste süsteem, millega piiratakse õiguskaitseasutuste juurdepääsu internetiteenuse osutajate klientide ja abonentide andmetele osariigi õigusega nõutust enam. Salvestatud sideandmete seadus võimaldab olenevalt kogumise sekkuvusest järjest tugevamat eraelu puutumatuse kaitset. Abonendi registreerimise andmete, protokollide, internetiprotokolli ehk IP-aadresside ja seotud ajatemplite ning

([3]) Mis puudutab eespool käsitletud neljanda paranduse põhimõtteid eraelu puutumatuse ja turvalisuse huvide kaitsmise kohta, kohaldavad USA kohtud õiguskaitses tehnoloogia arenguga võimalikuks muutunud uut tüüpi uurimisvahendite suhtes neid põhimõtteid korrapäraselt. Näiteks 2018. aastal otsustas ülemkohus, et kui valitsus saab õiguskaitsealase uurimise käigus pikema aja jooksul mobiiltelefoniettevõttelt mobiilsideettevõtte varasemat mobiiltelefoni asukohal põhinevat asukohateavet, on tegemist „otsinguga“, mille suhtes kohaldatakse neljanda paranduse kohase määruse nõuet. Carpenter *vs.* United States, 138 S. Ct. 2206 (2018).

arveldusandmete jaoks tuleb kriminaalõiguskaitseasutustel saada kohtukorraldus. Enamiku muude salvestatud ilma sisuta andmete korral, nagu e-posti ilma teemareata päised, tuleb õiguskaitseorganil esitada kohtunikule konkreetsed asjaolud, mis näitavad, et taotletud teave on käimasoleva kriminaaluurimise jaoks vajalik ja oluline. Selleks et saada oma valdusse elektroonilise side salvestatud sisu, peavad kriminaalõiguskaitseasutused saama kohtunikult määruse, mis põhineb küllaldasel alusel arvata, et asjaomasel kontol on tõendusmaterjal kuriteo kohta. Samuti on salvestatud sideandmete seaduses kehtestatud tsiviilvastutus ja kriminaalkaristused ([4]).

Kohtumäärused jälgimise kohta vastavalt pealtkuulamise föderaalseadusele (Federal Wiretap Law): lisaks sellele võivad õiguskaitseorganid kuulata reaalajas pealt telefonikõnesid, vestlusi või elektroonilist teabevahetust kriminaalmenetluse eesmärgil vastavalt föderaalsele pealtkuulamise seadusele. Vt USA seadustiku 18. jaotise § 2510–2523. See volitus on saadaval üksnes vastavalt kohtumäärusele, millega kohtunik leiab muu hulgas, et on olemas küllaldane alus arvata, et telefoni või elektrooniline pealtkuulamine annab tõendusmaterjali föderaalse kuriteo kohta või süüdistuse eest põgeneva tagaotsitava isiku asukoha kohta. Põhimääruses on kehtestatud tsiviilvastutus ja kriminaalkaristused telefoni pealtkuulamise sätete rikkumise eest.

Läbiotsimismäärus – kriminaalmenetluse föderaaleeskirjade (Fed. R. Crim. P.) eeskiri 41: Ameerika Ühendriikides võivad õiguskaitseorganid ruumid füüsiliselt läbi otsida juhul, kui kohtunik on andnud selleks loa. Õiguskaitseorganid peavad kohtunikule tõendama küllaldasele alusele tuginedes, et kuritegu pandi toime või pannakse toime ning et kuriteoga seotud esemed leitakse tõenäoliselt kohast, mis on näidatud läbiotsimismääruses. Seda volitust kasutatakse sageli siis, kui politseil tekib vajadus valdus füüsiliselt läbi otsida, kui on oht, et kui ettevõttele esitatakse kohtukorraldus või muu andmeesitamismäärus, võidakse tõendusmaterjalid hävitada. Isik, kelle suhtes läbiotsimist kohaldatakse või kelle vara läbi otsitakse, võib võtta meetmeid, et ebaseadusliku otsimise teel saadud tõendusmaterjal loetaks kehtetuks, kui need tõendid esitatakse selle isiku vastu kriminaalmenetluses. Vt Mapp *vs.* Ohio, 367 U.S. 643 (1961). Kui andmete valdaja on määruse alusel kohustatud andmeid avalikustada, võib pool, kelle suhtes sunnimeedet kohaldatakse, vaidlustada avalikustamise nõude kui põhjendamatult koormava. Vt vastus Ameerika Ühendriikide taotlusele, 610 F.2d 1148, 1157 (3. Cir. 1979) (kus on öeldud, et „nõuetekohase menetluse jaoks on vajalik koormavuse küsimuse ärakuulamine, enne kui sundida telefoniettevõtet andmeid esitama“, kasutades selleks läbiotsimismäärust); vastuses Ameerika Ühendriikide taotlusele 616 F.2d 1122 (9. Cir. 1980) (milles jõuti samale järeldusele kohtu järelevalvevolituste põhjal).

Justiitsministeeriumi suunised ja põhimõtted: lisaks nendele põhiseadusega kooskõlas olevatele, seadusjärgsetele ja normidel põhinevatele piirangutele valitsuse andmetele juurdepääsu kohta, on justiitsminister (Attorney General) välja andnud suunised, millega pannakse õiguskaitseasutuste andmetele juurdepääsule lisapiirangud ning mis sisaldavad ka eraelu puutumatuse ja kodanikuvabaduste kaitset. Näiteks kehtestatakse justiitsministri suunistes riigisisese föderaalse juurdlusbüroo operatsioonide kohta (Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations) (september 2008) (edaspidi „AG FBI suunised“), kättesaadavad aadressil http://www.justice.gov/archive/opa/docs/guidelines.pdf, , piirangud uurimisvahendite suhtes, mida kasutatakse föderaaltasandi kuritegude uurimiste käigus teabe otsimiseks. Nende suunistega nõutakse, et FBI kasutaks võimalikult vähe sekkuvaid uurimismeetodeid, võttes arvesse eraelu puutumatusele ja kodanikuvabadustele avalduvat mõju ning võimalikku mainekahju. Lisaks on suunistes märgitud, et „on enesestmõistetav, et FBI peab tegutsema oma uurimistes ja muudes toimingutes seaduslikult ja põhjendatult, nii et austatakse vabadust ja eraelu puutumatust ning välditakse tarbetut sekkumist seaduskuulekate inimeste ellu.“ AG FBI suunised, 5. FBI on neid suuniseid rakendanud FBI riigisisese uurimise ja operatsioonide juhendi (FBI Domestic Investigations and Operations Guide – DIOG) kaudu, kättesaadav aadressil https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29; see on põhjalik käsiraamat, mis sisaldab üksikasjalikke piiranguid uurimisvahendite ja juhiste kasutamise kohta tagamaks, et kodanikuvabadused ja eraelu puutumatus oleksid igas uurimises kaitstud. Täiendavad eeskirjad ja meetmed, millega on ette nähtud piirangud föderaalprokuröride uurimisalase tegevuse suhtes, on kehtestatud Ameerika Ühendriikide prokuröride juhendis (United States Attorneys' Manual – USAM), kättesaadav ka internetiaadressil https://www.justice.gov/jm/justicemanual.

Tsiviil- ja reguleerivad asutused (avalik huvi):

([4]) Lisaks antakse salvestatud sideandmete seaduse paragrahviga 2705(b) valitsusele õigus saada tõendatud vajadusel kaitsta avalikustamise eest põhinev kohtumäärus, millega keelatakse sideteenuste osutajal vabatahtlikult teavitada oma kasutajaid salvestatud teabevahetuse seaduse kohase kohtumenetluse algatamisest. 2017. aasta oktoobris andis asejustiitsminister Rod Rosenstein justiitsministeeriumi advokaatidele ja agentidele välja memorandumi, mis sisaldas juhised tagamaks, et selliste kaitsemääruste taotlused on kohandatud uurimise konkreetsetele faktidele ja probleemidele, ning millega kehtestati sellele, kui kauaks võib taotlusega teavitamise edasilükkamist taotleda, üldine üheaastane ülempiir. 2022. aasta mais andis asejustiitsminister Lisa Monaco selle teema kohta välja lisajuhised, milles muu hulgas kehtestati justiitsministeeriumisisesed heakskiitmise nõuded taotlustele pikendada kaitsemäärust pärast esialgset üheaastast perioodi ja nõuti, et kaitsemäärused tühistatakse uurimise lõpetamisel.

Tsiviil- ja reguleerivate asutuste (st avalik huvi) juurdepääsu suhtes Ameerika Ühendriikide ettevõtetes säilitatavatele andmetele on samuti kehtestatud märkimisväärsed piirangud. Tsiviil- ja reguleerivad asutused võivad äriühingutelt välja nõuda äridokumente, elektrooniliselt säilitatud teavet või muid materiaalseid objekte. Nende asutuste suhtes kohaldatakse piiranguid seoses halduslike või tsiviilkorralduste esitamisega mitte üksnes nende enda põhimääruste alusel, vaid ka korralduste sõltumatu juriidilise läbivaatamise põhjal, mis toimub enne võimalikku juriidilist jõustamist. Vt nt kriminaalmenetluse föderaaleeskirjade eeskiri 45. Asutused võivad taotleda juurdepääsu üksnes nendele andmetele, mis on asjakohased nende reguleerimisalasse kuuluvate küsimuste puhul. Lisaks sellele võib halduslik korralduse saaja vaidlustada selle täitmise 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 võivad finantsasutused vaidlustada halduslikud korraldused, millega taotletakse teatavat liiki andmeid, näiteks pangasaladuse seaduse (Bank Secrecy Act) ja selle rakendusmääruste rikkumiste kohta. USA seadustiku 31. jaotise § 5318; CFR 31. jaotise X peatükk. Muud ettevõtjad võivad tugineda õiglase krediidiinfo seadusele (Fair Credit Reporting Act), vt USA seadustiku 15. jaotise § 1681b, või muudele asjaomast majandussektorit reguleerivatele õigusaktidele. Kui asutus korralduse tegemise õigust kuritarvitab, võib see viia asutuse vastutusele võtmiseni või asutuse ametnike vastutusele võtmiseni. Vt nt finantsandmetega seotud eraelu puutumatuse seadus (Right to Financial Privacy Act), USA seadustiku 12. jaotise § 3401–3423. Niisiis seisavad Ameerika Ühendriikide kohtud selle eest, et vältida mittenõuetekohaseid reguleerivaid taotlusi ning annavad sõltumatu ülevaate föderaalasutuse tegevusest.

Kõigele lisaks peavad haldusasutuste kõik seadusjärgsed volitused võtta Ameerika Ühendriikides asuva ettevõtja andmed pärast haldusotsingu tegemist oma valdusesse olema kooskõlas neljandal parandusel põhinevate 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 õiguskaitse- 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.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

VII LISA

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20511

9. detsember 2022

Leslie B. Kiernan
Õigusnõunik
USA kaubandusministeerium
1401 Constitution Ave., NW
Washington, DC 20230

Lugupeetud Leslie B. Kiernan

7. oktoobril 2022 allkirjastas president Biden täidesaatva korralduse 14086 *Ameerika Ühendriikide signaaliluuretegevuse kaitsemeetmete tõhustamise kohta*, millega tugevdatakse eraelu puutumatuse ja kodanikuvabaduste kaitsemeetmeid, mida kohaldatakse USA signaaliluuretegevuse suhtes. Nende kaitsemeetmete hulka kuulub järgmine: nõue, et signaaliluuretegevus vastaks ühele loetletud õiguspärastest eesmärkidest; selge keeld kasutada sellist tegevust teatavate keelatud eesmärkide saavutamiseks; uudsete menetluste kehtestamine, tagamaks et signaaliluuretegevus edendab neid õiguspäraseid eesmärke ega aita kaasa keelatud eesmärkide saavutamisele; nõue, et signaaliluuretegevus võetakse ette alles pärast seda, kui kõigi asjakohaste tegurite mõistlikul hindamise tulemusel on tehtud kindlaks, et tegevus on vajalik valideeritud luureprioriteedi edendamiseks, ning ainult sel määral ja viisil, mis on proportsionaalne kinnitatud luureprioriteediga, mille jaoks tegevusluba anti, ja luureühenduse suunamine oma põhimõtteid ja menetlusi ajakohastama, et need kajastaksid täidesaatva korralduse puhul nõutavaid signaaliluuretegevuse kaitsemeetmeid. Kõige olulisem on see, et korraldusega kehtestatakse ka sõltumatu ja siduv mehhanism, mis võimaldab korralduse kohaselt määratud „kvalifitseeruvatest osariikidest“ pärit isikutel taotleda hüvitist, kui nad leiavad, et nende suhtes on ebaseaduslikult kohaldatud USA signaaliluuretegevust, sealhulgas tegevust, millega rikutakse täidesaatvas korralduses sätestatud kaitset.

President Bideni täidesaatva korralduse 14086 väljaandmine tähistas Euroopa Komisjoni ja Ameerika Ühendriikide esindajate vahel enam kui aasta kestnud üksikasjalike läbirääkimiste kulminatsiooni ning see juhib samme, mida Ameerika Ühendriigid astuvad oma ELi-USA andmekaitseraamistiku kohaste kohustuste täitmiseks. Minu teadmiste järgi olete kooskõlas koostöövaimuga, tänu millele raamistik loodi, saanud Euroopa Komisjonilt kaks küsimuste paketti selle kohta, kuidas luureühendus kavatseb täidesaatvat korraldust rakendada. Ma käsitlen neid küsimusi selles kirjas hea meelega.

1978. aasta välisluure jälitustegevuse seaduse (Foreign Intelligence Surveillance Act (FISA)) paragrahv 702

Esimene küsimuste pakett puudutab FISA paragrahvi 702, mis võimaldab koguda välisluureteavet, võttes elektroonilise side teenuste osutajaid abile kohustades sihikule usutavasti väljaspool Ameerika Ühendriike asuvad USA-välised isikud. Täpsemalt puudutavad küsimused selle sätte ja täidesaatva korralduse 14086 koosmõju, aga ka muid kaitsemeetmeid, mida kohaldatakse FISA paragrahvi 702 kohaselt tehtavate toimingute suhtes.

Alustuseks võime kinnitada, et luureühendus rakendab FISA paragrahvi 702 kohaselt tehtavate toimingute suhtes täidesaatvas korralduses 14086 sätestatud kaitsemeetmeid.

Lisaks kohaldatakse juhul, kui valitsus kasutab FISA paragrahvi 702, palju muid kaitsemeetmeid. Näiteks peab kõigil FISA paragrahvi 702 kohastel sertifikaatidel olema nii peaprokuröri kui ka riikliku luurejuhi allkiri ning valitsus peab esitama kõik sellised sertifikaadid kinnitamiseks välisluure järelevalve kohtule (Foreign Intelligence Surveillance Court (FISC)), mis koosneb sõltumatutest eluaegsetest kohtunikest, kelle seitsmeaastast ametiaega selles ametis ei saa pikendada. Sertifikaatidega määratakse kindlaks ka kogutava välisluureteabe kategooriad, mis peavad vastama välisluureteabe seadusjärgsele määratlusele, võttes sihikule USA-välised isikud, kelle asukoht on põhjendatud arvamuse kohaselt väljaspool Ameerika Ühendriike. Sertifikaadid on sisaldanud teavet rahvusvahelise terrorismi ja muude teemade kohta, näiteks massihävitusrelvi puudutava teabe hankimise kohta. Iga aastane sertifikaat tuleb esitada FISC-le kinnitamiseks sertifitseerimistaotluse paketis, mis sisaldab peaprokuröri ja luurejuhi sertifikaate, teatavate luureagentuuride juhtide kirjalikke kinnitusi ning sihtimismenetlusi, minimeerimismenetlusi ja päringumenetlusi, mis on valitsusele siduvad. Sihtimismenetluste jaoks on vaja muu hulgas seda, et luureühendus hindaks kõigi asjaolude põhjal mõistlikult, kas sihtimine viib tõenäoliselt PISA paragrahvi 702 sertifikaadis määratletud välisluureteabe kogumiseni.

Lisaks peab luureühendus FISA paragrahvi 702 kohaselt tegema teabe kogumisel järgmist: põhjendama sihtimistegevuse ajal kirjaliku selgitusega oma hinnangut selle kohta, et sihtmärk eeldatavasti omab, eeldatavasti saab või tõenäoliselt edastab PISA paragrahvi 702 sertifikaadis määratletud välisluureteavet; kinnitama, et PISA paragrahvis 702 sätestatud sihtimisstandard on sihtimistegevuses jätkuvalt täidetud ja lõpetada kogumine, kui standardi nõuded ei ole enam täidetud. Vt USA Valitsuse avaldus välisluure järelevalve kohtule, *2015 Summcuy of Notable Section 702 Requirements,* lk 2–3 (15. juuli 2015).

FISC järelevalvet luureühenduse sihtimistegevuste üle hõlbustab nõue, et luureühendus registreeriks kirjalikult oma hinnangu selle kohta, et FISA paragrahvi 702 eesmärgid vastavad kohaldatavatele sihtimisstandarditele, ja kinnitaks selle kehtivust korrapäraselt. Justiitsministeeriumi luure järelevalve advokaadid, kes teevad järelevalvet välisluureoperatsioonidest sõltumatult, vaatavad iga registreeritud sihtimishinnangu ja põhjenduse kord kahe kuu tagant üle. Justiitsministeeriumi osakond, kes seda ülesannet täidab, vastutab seejärel FISC kauaaegse reegli kohaselt FISC-le kõigist kohaldatavate menetluste rikkumistest teatamise eest. See aruandlus koos FISC ja justiitsministeeriumi selle osakonna vaheliste korrapäraste kohtumistega paragrahvi 702 kohase sihtimise järelevalve teemal võimaldab FISC-l tagada FISA paragrahvi 702 kohase sihtimise ja muude menetluste järgimist ning üldse tagada, et valitsuse tegevus on seaduspärane. FISC saab seda teha mitmel viisil, sealhulgas siduvate parandusotsuste vastuvõtmisega, et lõpetada valitsuse volitused konkreetse sihtmärgi kohta FISA paragrahvi 702 kohaselt andmeid koguda või andmete kogumist muuta või see lõpetada. FISC võib ka nõuda, et valitsus esitaks täiendavaid aruandeid või teavet selle kohta, kuidas ta täidab sihtimis- ja muude menetluste nõudeid, või nõuda nende menetluste muutmist.

Signaaliluureandmete masskogumine

Teine küsimuste pakett puudutab signaaliluureandmete masskogumist, mis on täidesaatvas korralduses 14086 määratletud kui „suurtes kogustes signaaliluureandmete volitatud kogumine, mis tehnilistel või operatiivsetel kaalutlustel korraldatakse andmekategooriaid kasutamata (näiteks kasutamata konkreetseid identifikaatoreid või valikutingimusi)“.

Nendele küsimustele vastates märgime esmalt, et ei FISA ega riikliku julgeoleku teabenõuded ei luba andmete masskogumist. Seoses FISAga:

— FISA I ja III peatükk, mis lubavad teha vastavalt elektroonilist järelevalvet ja füüsilist otsingut, nõuavad kohtumäärust (väheste eranditega, näiteks eriolukorrad) ning alati on nõutav küllaldane alus arvata, et sihtmärk on võõrvõim või võõrvõimu agent. Vt USA seadustiku 50. jaotise § 1805, 1824;

— USA 2015. aasta vabaduse seadusega (USA Freedom Act) muudeti kohtumääruse kohast (välja arvatud erakorralistel asjaoludel) väljamineva ja sissetuleva side jälgimisseadmete kasutamist lubavat FISA IV jaotist, et nõuda valitsuselt taotluste esitamist „konkreetse valikutingimuse“ alusel. Vt USA seadustiku 50. jaotise § 1842 punkti c alapunkt 3;

— FISA V jaotis, mis lubab föderaalsel juurdlusbürool (Federal Bureau of Investigation (FBI)) hankida teatavat liiki äridokumente, eeldab kohtumäärust, mis põhineb taotlusel, milles täpsustakse, et „on olemas konkreetsed ja selgelt sõnastatavad faktid, mis annavad alust arvata, et isik, keda dokumendid puudutavad, on võõrvõim või võõrvõimu agent“. Vt USA seadustiku 50. jaotise § 1862 punkti b alapunkti 2 alapunkt B ([1]);

— lisaks lubab FISA paragrahv 702 „võtta välisluureteabe kogumise sihtmärgiks isikuid, kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike“. Vt USA seadustiku 50. jaotise § 188la punkt a. Seega, nagu on märkinud eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (Privacy and Civil Liberties Oversight Board (PCLOB)), seisneb valitsuse andmete kogumine FISA paragrahvi 702 alusel „täielikult nende üksikisikute sihtimises ja nende isikutega seotud teabe hankimises, kelle puhul valitsusel on põhjust eeldada teatavat liiki välisluureandmete saamist,“ nii et „programmis ei tehta sideandmete masskogumist“. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon, aruanne järelevalveprogrammi kohta, mida rakendatakse vastavalt välisluure jälitustegevuse seaduse paragrahvile 702 (*„Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act“)*, lk 103 (2. juuli 2014) ([2]).

Riikliku julgeoleku teabenõuete (National Security Letters) kohta on USA 2015. aasta vabaduse seaduses (USA Freedom Act) kehtestatud selliste teabenõuete kasutamise suhtes „konkreetne valikutingimus“. Vt USA seadustiku 12. jaotise § 3414 punkti a alapunkt 2; USA seadustiku 15. jaotise § 1681u; USA seadustiku 15. jaotise § 1681v punkt a; USA seadustiku 18. jaotise § 2709 punkt b.

Lisaks on täidesaatvas korralduses 14086 sätestatud, et „prioriteediks tuleb seada sihitud kogumine“ ja et kui luureühendus kogub andmeid hulgi, „lubatakse signaaliluureandmete masskogumist ainult juhul, kui on kindlaks tehtud, et kinnitatud luureprioriteedi edendamiseks vajalikku teavet ei ole võimalik saada sihitud kogumisega“. Vt täidesaatev korraldus 14086, § 2 punkti c alapunkti ii alapunkt A.

Veelgi enam, kui luureühendus teeb kindlaks, et masskogumine vastab nendele standarditele, on täidesaatva korraldusega 14086 sätestatud lisakaitsemeetmeid. Täpsemalt öeldes on täidesaatvas korralduses nõue, et luureühendus „rakendaks masskogumisel mõistlikke meetodeid ja tehnilisi meetmeid, et piirata kogutud andmeid ainult sellega, mis on vajalik kinnitatud luureprioriteedi edendamiseks, minimeerides samal ajal mitteasjakohase teabe kogumist“. Vt samas. Korralduses on ka märgitud, et „signaaliluuretegevus“, mille alla kuuluvad masskogumise teel saadud signaaliluureandmete päringuid, viiakse ellu alles pärast seda, kui kõigi asjakohaste tegurite mõistliku hindamise põhjal on kindlaks tehtud, et tegevused on vajalikud kinnitatud luureprioriteedi edendamiseks“. Vt samas § 2 punkti a alapunkti ii alapunkt A. Korraldusega täpsustatakse selle põhimõtte rakendamist, sätestades, et luureühendus võib kuue lubatud eesmärgi saavutamiseks küsida ainult masskogutud minimeerimata signaaliluureandmeid ning et sellised päringud tuleb teha kooskõlas põhimõtete ja menetlustega, milles „võetakse asjakohaselt arvesse [päringute] mõju kõigi isikute eraelu puutumatusele ja kodanikuvabadustele, olenemata nende kodakondsusest või elukohast“. Vt samas § 2 punkti c alapunkti iii alapunkt D. Kõigele lisaks on korralduses ette nähtud kogutud andmete käitlemise, turvalisuse ja juurdepääsu kontroll. Vt samas § 2 punkti c alapunkti iii alapunkt A ja § 2 punkti c alapunkti iii alapunkt B.

* * * * *

Loodame, et nendest selgitustest on abi. Võtke meiega julgesti ühendust, kui Teil on lisaküsimusi selle kohta, kuidas USA luureühendus kavatseb täidesaatvat korraldust 14086 rakendada.

([1]) Aastatel 2001–2020 lubas FISA V jaotis FBI-l taotleda FISC-lt luba, et hankida „käegakatsutavaid asju“, mis on seotud teatavate volitatud uurimistega. Vt USA sisejulgeoleku seadus (USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001)). See sõnastus, mis on aegunud ega ole seega enam seadus, andis volituse, mille kohaselt valitsus kogus omal ajal massiliselt telefoniside metaandmeid. Siiski juba enne sätte aegumist muudeti seda USA vabaduse seadusega, et kehtestada valitsusele nõue esitada FISC-le taotlus „konkreetse valikutingimuse“ alusel. Vt USA vabaduse seadus (USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015)).

([2]) Paragrahvid 703 ja 704, mille kohaselt võib luureühendus võtta sihikule välisriigis asuvaid USA kodanikke, nõuavad kohtumäärust (välja arvatud erakorralistel asjaoludel) ja alati on nõutav küllaldane alus arvata, et sihtmärk on võõrvõim, võõrvõimu agent või võõrvõimu ametnik või töötaja. Vt USA seadustiku 50. jaotise § 1881b, 1881c.

Sincerely,

Christopher C. FONZONE
Õigusnõunik

VIII LISA

Lühendite loetelu

Käesolevas otsuses kasutatakse alljärgnevaid lühendeid.

AAA	USA vahekohtute assotsiatsioon (American Arbitration Association)
Justiitsministri määrus	Justiitsministri määrus andmekaitseasju läbivaatava kohtu kohta
AGG-DOM	Justiitsministri suunised riigisiseste FBI operatsioonide kohta
APA	Haldusmenetluse seadus (Administrative Procedure Act)
CIA	Luure Keskagentuur (Central Intelligence Agency)
Euroopa Kohus	Euroopa Liidu Kohus
Otsus	Komisjoni rakendusotsus, mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete kaitse taseme piisavust ELi-USA andmekaitseraamistiku alusel
DPRC	Andmekaitseasju läbivaatav kohus (Data Protection Review Court)
ECOA	Võrdsete krediidivõimaluste seadus (Equal Credit Opportunity Act)
ECPA	Elektroonilise side privaatsuse seadus (Electronic Communications Privacy Act)
EMP	EMP
Korraldus EO 12333	Täidesaatev korraldus 12333 Ameerika Ühendriikide luuretegevuse kohta (United States Intelligence Activities)
Korraldus EO 14086	Täidesaatev korraldus 14086 USA signaaliluuretegevuse kaitsemeetmete tõhustamise kohta (Enhancing Safeguards for US Signals Intelligence Activities).
FBI	Föderaalne juurdlusbüroo (Federal Bureau of Investigation)
FISA	Välisluure jälitustegevuse seadus (Foreign Intelligence Surveillance Act)
FISC	Välisluure jälitustegevuse kohus (Foreign Intelligence Surveillance Court)
FISCR	Välisluure jälitustegevuse apellatsioonikohus (Foreign Intelligence Surveillance Court of Review)
FOIA	Teabevabaduse seadus (Freedom of Information Act)
FRA	Föderaalregistrite seadus (Federal Records Act)
FTC	USA föderaalne kaubanduskomisjon (U.S. Federal Trade Commission)
HIPAA	Ravikindlustuse teisaldatavuse ja vastutuse seadus (Health Insurance Portability and Accountability Act)
ICDR	Vaidluste lahendamise rahvusvaheline keskus
IOB	Luuretegevuse järelevalve nõukogu (Intelligence Oversight Board)
NIST	Riiklik standardite ja tehnoloogia instituut (National Institute of Standards and Technology)
NSA	Riiklik julgeolekuasutus (National Security Agency)
ODNI	Riikliku luurejuhi büroo (Office of the Director of National Intelligence)
ODNI kodanikuvabaduste kaitse ametnik, CLPO	Riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik
OMB	Juhtimis- ja eelarveosakond (Office of Management and Budget)
PCLOB	Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon
PIAB	Presidendi luuretegevuse nõuandekogu

PPD 28	Presidendi poliitikasuunis nr 28
Määrus (EL) 2016/679	Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta
Põhimõtted	ELi-USA andmekaitseraamistiku põhimõtted
USA	Ameerika Ühendriigid
Liit	Euroopa Liit