

KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2023/1795,**annettu 10 päivänä heinäkuuta 2023,****Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman tietosuojan tason riittävydestä***(tiedoksiannettu numerolla C(2023) 4745)***(ETA:n kannalta merkityksellinen teksti)**

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) ⁽¹⁾ ja erityisesti sen 45 artiklan 3 kohdan,

sekä katsoo seuraavaa:

1. JOHDANTO

- (1) Asetuksessa (EU) 2016/679 ⁽²⁾ vahvistetaan säännöt, joita sovelletaan henkilötietojen siirtoon unioniin sijoittautuneilta rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä kolmansiin maihin ja kansainvälisille järjestöille, siltä osin kuin tällaiset siirrot kuuluvat sen soveltamisalaan. Henkilötietojen kansainvälistä siirtoa koskevat säännöt vahvistetaan asetuksen V luvussa. Kansainvälisen yhteistyön ja kaupan kehittämiseksi on tarpeen siirtää henkilötietoja Euroopan unionin ulkopuolisiin maihin tai niistä unioniin. Samalla on kuitenkin varmistettava, että kolmansiin maihin tai kansainvälisille järjestöille tehtävien siirtojen yhteydessä ei heikennetä henkilötietojen suojan tasoa unionissa ⁽³⁾.
- (2) Asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukaan komissio voi päättää täytäntöönpanosäädöksellä, että jokin kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori varmistaa riittävän tietosuojan. Tämän edellytyksen täyttyessä henkilötietoja voidaan siirtää kyseiselle kolmannelle maalle ilman erillistä lupaa, kuten asetuksen (EU) 2016/679 45 artiklan 1 kohdassa ja johdanto-osan 103 kappaleessa säädetään.
- (3) Kuten asetuksen (EU) 2016/679 45 artiklan 2 kohdassa säädetään, tietosuojan riittävyttä koskevan päätöksen tekemisen on perustuttava kattavaan analyysiin kolmannen maan oikeusjärjestyksestä. Analyysissa on tarkasteltava sekä tietojen tuojia koskevia sääntöjä että niitä rajoituksia ja suojoitoimia, jotka koskevat viranomaisten pääsyä henkilötietoihin. Komission on arvioinnissaan määritettävä, vastaako kyseisen kolmannen maan takaama tietosuojan taso ”olennaisilta osin” unionissa taattua suojan tasoa (asetuksen (EU) 2016/679 johdanto-osan 104 kappale). Tätä on arvioitava suhteessa unionin lainsäädäntöön ja erityisesti asetukseen (EU) 2016/679 sekä Euroopan unionin tuomioistuimen, jäljempänä ’unionin tuomioistuin’, oikeuskäytäntöön ⁽⁴⁾.

⁽¹⁾ EUVL L 119, 4.5.2016, s. 1.

⁽²⁾ Viittausten helpottamiseksi liitteessä VIII on luettelo tässä päätöksessä käytetyistä lyhenteistä.

⁽³⁾ Ks. asetuksen (EU) 2016/679 johdanto-osan 101 kappale.

⁽⁴⁾ Ks. tuoreimpana tapauksena asia C-311/18, Facebook Ireland ja Schrems (Schrems II), ECLI:EU:C:2020:559.

- (4) Unionin tuomioistuin selvensi 6 päivänä lokakuuta 2015 asiassa C-362/14 Maximillian Schrems v. Data Protection Commissioner ⁽⁵⁾, jäljempänä 'Schrems', antamassaan tuomiossa, että tämä ei edellytä täysin samaa tietosuojan tasoa. Erityisesti keinot, joita kyseisellä kolmannella maalla on käytettävissään henkilötietojen suojaamiseksi, voivat erota unionissa käytetyistä menetelmistä, kunhan ne käytännössä varmistavat tehokkaasti tietosuojan riittävän tason ⁽⁶⁾. Tietosuojan tason riittävyyttä koskeva vaatimus ei sen vuoksi edellytä unionin sääntöjen kopiointia kohta kohdalta. Sen sijaan tarkastellaan, onko ulkomaisen järjestelmän antama suoja kokonaisuutena vaaditun tason mukainen. Tällöin selvitetään, mikä on yksityisyyteen liittyvien oikeuksien sisältö ja pannaanko ne täytäntöön ja valvotaanko niiden toteutumista tehokkaasti ⁽⁷⁾. Kyseisen tuomion mukaan komission olisi lisäksi tätä vaatimusta soveltaessaan arvioitava erityisesti, sisältääkö kyseisen kolmannen maan oikeudellinen kehys sääntöjä, joiden tarkoituksena on rajoittaa niiden henkilöiden perusoikeuksiin puuttumista, joiden tietoja siirretään unionista, kun puuttuminen olisi kyseisen maan valtiollisille elimille sallittua niiden pyrkiessä kansallisen turvallisuuden kaltaisiin legitimeihin tavoitteisiin, ja onko tällaista puuttumista vastaan olemassa tehokas oikeussuoja ⁽⁸⁾. Myös Euroopan tietosuojaneuvosto on antanut ohjeistusta tietosuojan riittävyyden tutkimisesta ⁽⁹⁾.
- (5) Unionin tuomioistuin selvensi tällaista yksityisyyden suojaa ja tietosuojaa koskeviin perusoikeuksiin puuttumista koskevaa vaatimusta 16 päivänä heinäkuuta 2020 asiassa C-311/18, Data Protection Commissioner v. Facebook Ireland Limited ja Maximillian Schrems, jäljempänä 'Schrems II', antamassaan tuomiossa, jolla mitätöitiin aikaisempaa transatlanttista tietovirtakehystä eli EU:n ja Yhdysvaltojen välistä Privacy Shield -järjestelyä, jäljempänä 'Privacy Shield -järjestely', koskeva komission täytäntöönpanopäätös (EU) 2016/1250 ⁽¹⁰⁾. Unionin tuomioistuin katsoi, että Yhdysvaltojen viranomaisten pääsyä henkilötietoihin, jotka on siirretty unionista Yhdysvaltoihin kansalliseen turvallisuuteen liittyviä tarkoituksia varten, ja näiden tietojen käyttöä koskevasta Yhdysvaltojen kansallisesta lainsäädännöstä johtuvia henkilötietojen suojan rajoituksia ei ole toteutettu tavalla, joka täyttäisi pääosiltaan unionin lainsäädäntöä vastaavat vaatimukset, siltä osin kuin on kyse tällaisen puuttumisen tarpeellisuudesta ja oikeasuhteisuudesta tietosuojaa koskevaan oikeuteen nähden ⁽¹¹⁾. Unionin tuomioistuin katsoi myös, että oikeussuojakeinoja ei ole saatavilla sellaisessa elimessä, joka antaa henkilölle, joiden tiedot on siirretty Yhdysvaltoihin, takeet, jotka pääosiltaan vastaavat oikeutta tehokkaisiin oikeussuojakeinoihin koskevassa perusoikeuskirjan 47 artiklassa edellytetyjä takeita ⁽¹²⁾.
- (6) Schrems II -asiassa annetun tuomion jälkeen komissio aloitti Yhdysvaltojen hallituksen kanssa neuvottelut mahdollisesta uudesta tietosuojan tason riittävyyttä koskevasta päätöksestä, joka olisi asetuksen (EU) 2016/679 45 artiklan 2 kohdan vaatimusten mukainen, sellaisina kuin unionin tuomioistuin on niitä tulkinnut. Näiden neuvottelujen tuloksena Yhdysvallat antoi 7 päivänä lokakuuta 2022 Yhdysvaltojen signaalitiedustelutoiminnan suojatoimien tehostamista koskevan toimeenpanoasetuksen (executive order) EO 14086, jäljempänä 'toimeenpanoasetus 14086', jota on täydennetty tietosuojaa käsittelevästä muutoksenhakutuomioistuimesta annetulla Yhdysvaltojen oikeusministerin asetuksella, jäljempänä 'oikeusministerin asetus' ⁽¹³⁾. Lisäksi on päivitetty tämän päätöksen nojalla unionista siirrettäviä tietoja käsitteleviin kaupallisiin toimijoihin sovellettavaa kehystä eli EU:n ja Yhdysvaltojen tietosuojakehystä, jäljempänä 'tietosuojakehys'.
- (7) Komissio on analysoinut huolellisesti Yhdysvaltojen lainsäädäntöä ja käytäntöä, mukaan lukien toimeenpanoasetus 14086 ja oikeusministerin asetus. Johdanto-osan 9–200 kappaleessa esitettyjen havaintojen perusteella komissio päättää, että Yhdysvallat takaa tietosuojan riittävän tason henkilötiedoille, jotka siirretään tietosuojakehysten puitteissa unioniin sijoittautuneelta rekisterinpitäjältä tai henkilötietojen käsittelijältä ⁽¹⁴⁾ Yhdysvalloissa sijaitseville varmennetuille organisaatioille.

⁽⁵⁾ Asia C-362/14, Maximillian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, 73 kohta.

⁽⁶⁾ Schrems, 74 kohta.

⁽⁷⁾ Ks. komission tiedonanto Euroopan parlamentille ja neuvostolle: Henkilötietojen vaihtaminen ja suojaaminen globalisoituneessa maailmassa, COM(2017) 7, 10.1.2017, 3.1 kohta, s. 6 ja 7.

⁽⁸⁾ Schrems, 88 ja 89 kohta.

⁽⁹⁾ Euroopan tietosuojaneuvosto: Tietosuojan riittävyyden viitearvot, WP 254 rev. 01, saatavilla osoitteessa https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

⁽¹⁰⁾ Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä (EUVL L 207, 1.8.2016, s. 1).

⁽¹¹⁾ Schrems II, 185 kohta.

⁽¹²⁾ Schrems II, 197 kohta.

⁽¹³⁾ 28 CFR osa 302.

⁽¹⁴⁾ Tämä päätös on ETA:n kannalta merkityksellinen. Euroopan talousalueesta tehdyn sopimuksen (ETA-sopimus) mukaan Euroopan unionin sisämarkkinat ulottuvat kolmeen ETA-valtioon (Islanti, Liechtenstein ja Norja). ETA:n sekakomitean 6 päivänä heinäkuuta 2018 antama päätös, jolla asetus (EU) 2016/679 otettiin osaksi ETA-sopimuksen liitettä XI, tuli voimaan 20 päivänä heinäkuuta 2018. Asetus kuuluu siis sopimuksen soveltamisalaan. Kyseistä päätöstä sovellettaessa viittauksia EU:hun ja EU:n jäsenvaltioihin olisi näin ollen pidettävä myös viittauksina ETA-valtioihin.

- (8) Tämän päätöksen seurauksena henkilötietojen siirrot unioniin sijoittautuneilta rekisterinpitäjiltä ja henkilötietojen käsittelijöiltä ⁽¹⁵⁾ Yhdysvaltoihin sijoittautuneille varmennetuille organisaatioille voidaan toteuttaa ilman eri hyväksyntää. Päätös ei rajoita asetuksen (EU) 2016/679 suoraa soveltamista tällaisiin organisaatioihin silloin, kun kyseisen asetuksen 3 artiklassa säädetyt alueellista soveltamista koskevat edellytykset täyttyvät.

2. EU:N JA YHDYSVALTOJEN TIETOSUOJAKEHYS

2.1 Henkilökohtainen ja aineellinen soveltamisala

2.1.1 Varmennetut organisaatiot

- (9) EU:n ja Yhdysvaltojen tietosuojakehys perustuu varmennusjärjestelmään, jolla yhdysvaltalaiset organisaatiot sitoutuvat tiettyihin yksityisyyden suojaa koskeviin tietosuojakehyksen periaatteisiin, mukaan lukien täydentävät periaatteet, jäljempänä yhdessä 'järjestelyn periaatteet', jotka on antanut Yhdysvaltojen kauppaministeriö ja jotka sisältyvät tämän päätöksen liitteeseen I ⁽¹⁶⁾. Jotta organisaatio voisi antaa tietosuojakehyksen mukaisen varmennuksen, sen on oltava liittovaltion kauppakomission tai liikenneministeriön tutkinta- ja täytäntöönpanovallan alainen ⁽¹⁷⁾. Järjestelyn periaatteita sovelletaan välittömästi varmennuksen jälkeen. Kuten johdanto-osan 48–52 kappaleessa tarkennetaan, tietosuojakehykseen kuuluvien organisaatioiden on vuosittain varmennettava uudelleen sitoutumisensa järjestelyn periaatteisiin ⁽¹⁸⁾.

2.1.2 Henkilötietojen määritelmä ja rekisterinpitäjän ja edustajan käsitteet

- (10) Tietosuojakehyksen tarjoama suoja kattaa kaikki henkilötiedot, jotka siirretään unionista Yhdysvalloissa sijaitseville organisaatioille, jotka ovat varmentaneet Yhdysvaltojen kauppaministeriölle sitoutuvansa järjestelyn periaatteisiin, lukuun ottamatta tietoja, jotka kerätään julkaisemista, radio- ja tv-lähetystoimintaa tai muuta journalistisen aineiston julkista viestintää varten, ja tietoja, jotka löytyvät aikaisemmin julkaistusta tiedotusvälineiden arkistoista levitetystä aineistosta ⁽¹⁹⁾. Viimeksi mainittuja tietoja ei näin ollen voida siirtää tietosuojakehyksen puitteissa.
- (11) Järjestelyn periaatteissa henkilötiedoilla tarkoitetaan asetuksen (EU) 2016/679 tapaan jossakin muodossa rekisteröityjä tunnistetun tai tunnistettavan henkilön tietoja, joihin sovelletaan yleistä tietosuojaa-asetusta ja jotka yhdysvaltalainen organisaatio on vastaanottanut EU:sta ⁽²⁰⁾. Ne kattavat myös pseudonymisoidut (tai "avainkoodatut") tutkimustiedot (myös silloin, kun avainta ei jaeta vastaanottavan yhdysvaltalaisen organisaation kanssa) ⁽²¹⁾. Henkilötietojen käsittelyllä tarkoitetaan kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen tai levittäminen sekä poistaminen tai tuhoaminen ⁽²²⁾.
- (12) Tietosuojakehystä sovelletaan Yhdysvalloissa organisaatioihin, jotka voidaan katsoa rekisterinpitäjiksi (henkilö tai organisaatio, joka yksin tai yhdessä muiden kanssa määrittää henkilötietojen käsittelyn tarkoitukset ja keinot) ⁽²³⁾ tai henkilötietojen käsittelijöiksi (rekisterinpitäjän puolesta toimiva edustaja) ⁽²⁴⁾. Yhdysvaltoihin sijoittautuneiden henkilötietojen käsittelijöiden on oltava sopimuksen nojalla velvollisia toimimaan ainoastaan EU:n rekisterinpitäjän

⁽¹⁵⁾ Tämä päätös ei vaikuta asetuksen (EU) 2016/679 vaatimuksiin, joita sovelletaan unioniin sijoittautuneisiin tietoja siirtäviin elimiin (rekisterinpitäjiin ja henkilötietojen käsittelijöihin). Näitä vaatimuksia ovat esimerkiksi käyttötarkoitussidonnaisuus, tietojen minimointi, läpinäkyvyys ja tietoturvallisuus (ks. myös asetuksen (EU) 2016/679 44 artikla).

⁽¹⁶⁾ Ks. tältä osin asiassa Schrems annetun tuomion 81 kohta, jossa unionin tuomioistuin vahvistaa, että tietosuojan riittävä taso voidaan varmistaa oman varmennuksen järjestelmällä.

⁽¹⁷⁾ Liite I, I jakson 2 kohta. Liittovaltion kauppakomissiolla (FTC) on laaja toimivalta suhteessa kaupalliseen toimintaan joitakin poikkeuksia lukuun ottamatta; poikkeuksiin kuuluvat esimerkiksi pankit, lentoyhtiöt, vakuutustoiminta ja televiestintäpalvelujen tarjoajien yleiset operaattoripalvelut (tosin Yhdysvaltojen yhdeksännen piirin muutoksenhakutuomioistuimen 26. helmikuuta 2018 tekemä päätös asiassa FTC v. AT&T vahvistaa, että liittovaltion kauppakomissiolla on toimivaltaa suhteessa tällaisten yhteisöjen muihin kuin yleisiin operaattoripalveluihin). Ks. myös liitteen IV alaviite 2. Yhdysvaltain liikennevirastolla (DoT) on toimivalta valvoa, että lentoyhtiöt ja lipunvälittäjät noudattavat vaatimuksia (lentoliikenteen osalta), ks. liitteessä V oleva A jakso.

⁽¹⁸⁾ Liite I, I jakson 6 kohta.

⁽¹⁹⁾ Liite I, III jakson 2 kohta.

⁽²⁰⁾ Liite I, I jakson 8 kohdan a alakohta.

⁽²¹⁾ Liite I, III jakson 14 kohdan g alakohta.

⁽²²⁾ Liite I, I jakson 8 kohdan b alakohta.

⁽²³⁾ Liite I, I jakson 8 kohdan c alakohta.

⁽²⁴⁾ Ks. esim. liitteessä I oleva II.2.b kohta ja kohdat II.3.b ja 7.d, joissa tehdään selväksi, että edustajat toimivat rekisterinpitäjän puolesta tämän ohjeiden mukaisesti ja erityisten sopimusvelvoitteiden sitomina.

ohjeiden perusteella ja avustamaan sitä vastattaessa henkilöille, jotka käyttävät järjestelyn periaatteiden mukaisia oikeuksiaan ⁽²⁵⁾. Lisäksi henkilötietojen käsittelijän on alihankintana teetettävän tietojen käsittelyn osalta tehtävä alihankkijan kanssa sopimus, jossa taataan samantasoinen suoja kuin järjestelyn periaatteissa, ja varmistettava sen asianmukainen täytäntöönpano ⁽²⁶⁾.

2.2 EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteet

2.2.1 Käyttötarkoitussidonnaisuus ja valintaperiaate

- (13) Henkilötietojen käsittelyn olisi oltava lainmukaista ja asianmukaista. Henkilötietoja olisi kerättävä tiettyä tarkoitusta varten ja käytettävä myöhemmin vain siltä osin kuin käyttö ei ole ristiriidassa kyseisen tarkoituksen kanssa.
- (14) Tietosuojakehyksessä tämä on varmistettu erilaisilla periaatteilla. Ensinnäkin tietojen eheyden ja käyttötarkoitussidonnaisuuden periaatteen (Data Integrity and Purpose Limitation Principle), samoin kuin asetuksen (EU) 2016/679 5 artiklan 1 kohdan b alakohdan mukaan, organisaatio ei saa käsitellä henkilötietoja tavalla, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta tai tarkoitusta, johon kyseinen rekisteröity oli myöhemmin antanut suostumuksensa ⁽²⁷⁾.
- (15) Jotta organisaatio voisi käyttää henkilötietoja uuteen (muutettuun) tarkoitukseen, joka poikkeaa olennaisesti alkuperäisestä tarkoituksesta mutta on edelleen sen kanssa yhteensopiva, tai luovuttaa henkilötiedot kolmannelle osapuolelle, organisaatiolla on oltava selkeä, helposti havaittava ja käytettävä mekanismi, jonka avulla rekisteröidyt voivat halutessaan kieltää tietojen siirtämisen valintaperiaatteen (Choice Principle) ⁽²⁸⁾ mukaisesti. Valintaperiaate ei kuitenkaan korvaa periaatteiden vastaisen tietojen käsittelyn nimenomaista kieltä ⁽²⁹⁾.

⁽²⁵⁾ Liite I, III jakson 10 kohdan a alakohta. Ks. myös Yhdysvaltojen kauppaministeriön Privacy Shield -järjestelyn puitteissa yhteistyössä Euroopan tietosuojaneuvoston kanssa laatima ohjeistus, jossa selvennetään yhdysvaltalaisen käsittelijöiden velvoitteita niiden vastaanottaessa henkilötietoja unionista. Koska säännöt eivät ole muuttuneet, tämä ohjeistus ja kysymys/vastaus-neuvonta ovat edelleen relevantteja EU:n ja Yhdysvaltojen välisen tietosuojakehyksen yhteydessä (<https://www.privacyshield.gov/article?id=Processing-FAQs>).

⁽²⁶⁾ Liite I, II jakson 3 kohdan b alakohta.

⁽²⁷⁾ Liite I, II jakson 5 kohdan a alakohta. Asianmukaisia tarkoituksia voivat olla muun muassa tarkastus, petostentorjunta tai muut tarkoitukset, jotka vastaavat sitä, mitä järkevä ja huolellinen henkilö voi odottaa tiedonkeruutilanteessa (ks. liite I, alaviite 6).

⁽²⁸⁾ Liite I, II jakson 2 kohdan a alakohta. Tätä ei sovelleta, kun organisaatio antaa henkilötietoja sen puolesta ja sen ohjeiden mukaisesti toimivalle henkilötietojen käsittelijälle (liite I, II jakson 2 kohdan b alakohta). Tässä tapauksessa organisaatiolla on oltava sopimus ja sen on varmistettava, että noudatetaan henkilötietojen edelleen siirtämiseen liittyvää vastuuvollisuusperiaatetta (Accountability for Onward Transfer Principle), kuten johdanto-osan 43 kappaleessa tarkemmin kuvataan. Lisäksi valintaperiaatetta (sekä ilmoitusperiaatetta (Notice Principle)) voidaan rajoittaa silloin, kun henkilötietoja käsitellään due diligence -tarkastuksen yhteydessä (osana mahdollista sulautumista tai yritysostoa) tai muun tarkastuksen yhteydessä, siinä määrin ja niin kauan kuin se on tarpeen lakisääteiden tai yleisen edun mukaisten vaatimusten täyttämiseksi, tai siinä määrin ja niin kauan kuin näiden periaatteiden soveltaminen vaarantaisi organisaation oikeutetut edut due diligence -tarkastuksen tai muun tarkastuksen yhteydessä (liite I, III jakson 4 kohta). Täydentävässä periaatteessa (Supplemental Principle) nro 15 (liite I, III jakson 15 kohdan a ja b alakohta) säädetään myös poikkeuksesta valintaperiaatteen (kuten myös ilmoitusvelvollisuutta ja henkilötietojen edelleen siirtämiseen liittyvää vastuuvollisuutta koskevaan periaatteen) silloin, kun henkilötiedot ovat peräisin julkisesti saatavilla olevista lähteistä (jollei EU:n tiedonviejä ilmoita, että tietoihin sovelletaan rajoituksia, jotka edellyttävät kyseisten periaatteiden soveltamista) tai kun ne on kerätty yleisesti yleisön käytettävissä olevista asiakirjoista (kunhan niihin ei liity ei-julkisia tietoja ja käytön ehtoja noudatetaan). Vastaavasti täydentävä periaate 14 (liite I, III jakson 14 kohdan f alakohta) sisältää vapautuksen valintaperiaatteesta (sekä ilmoitusperiaatteesta ja siirtoon liittyvää vastuuvollisuutta koskevasta periaatteesta), kun henkilötietoja käsitellään lääkkeitä ja lääkintälaitteita valmistavassa yrityksessä tuotteiden turvallisuuden ja tehokkuuden seuranta varten, siltä osin kuin järjestelyn periaatteiden noudattaminen haittaa sääntelyvaatimusten noudattamista.

⁽²⁹⁾ Tämä koskee kaikkia tietosuojakehyksen puitteissa tehtyjä tiedonsiirtoja, myös silloin, kun ne koskevat työsuhteen yhteydessä kerättyjä tietoja. Vaikka varmennettu yhdysvaltalainen organisaatio voi siksi periaatteessa käyttää henkilötietoja muihin kuin työsuhteeseen liittyviin tarkoituksiin (esimerkiksi tietynlainen markkinointiviestintä), sen on noudatettava käyttötarkoituksen vastaisen käsittelyn kieltä, ja lisäksi se voi tehdä näin ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Organisaatio voi poikkeuksellisesti käyttää henkilötietoja muuhun yhteensopivaan tarkoitukseen noudattamatta ilmoitus- ja valintaperiaatetta, mutta vain siinä määrin ja niin kauan kuin on tarpeen, jotta organisaation kyky toteuttaa ylennyksiä, nimityksiä tai muita vastaavia työsuhteeseen liittyviä päätöksiä ei vaarannu (ks. liite I, III jakson 9 kohdan b alakohdan iv alakohta). Yhdysvaltalaiselle organisaatiolle asetettu kiello ryhtyä rankaisutoimiin työntekijää vastaan valinta-oikeuden käyttämisestä, mukaan lukien kaikki työllistymismahdollisuuksia koskevat rajoitukset, takaa, että alisteisuus- ja riippuvuussuhteesta huolimatta työntekijään ei kohdistu paineita, vaan hän voi käyttää valinta-oikeuttaan vapaasti. Ks. liite I, III jakson 9 kohdan b alakohdan i alakohta.

2.2.2 Erityisiä henkilötietoryhmiä koskeva käsittely

- (16) ”Erityisiä tietoryhmiä” käsiteltäessä olisi sovellettava erityisiä suoja-toimia.
- (17) Valintaperiaatteen mukaisesti on sovellettava erityisiä suoja-toimia silloin, kun käsitellään ”arkaluonteisia tietoja” eli henkilötietoja, jotka koskevat henkilön terveydentilaa, rotua tai etnistä alkuperää, poliittista kantaa, uskonnollista tai eettistä vakaumusta, kuulumista ammattiliittoon, sukupuolielämää tai mitä tahansa muita kolmannelta osapuolelta saatuja tietoja, joita kyseinen osapuoli pitää ja käsittelee arkaluontoisina ⁽³⁰⁾. Tämä tarkoittaa, että varmennetut organisaatiot käsittelevät kaikkia unionin tietosuojalainsäädännössä arkaluonteisiksi katsottuja tietoja (mukaan lukien seksuaalista suuntautumista ja perimää koskevat tiedot ja biometriset tiedot) arkaluonteisina myös EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa.
- (18) Organisaatioiden on pääsääntöisesti saatava henkilöltä nimenomainen suostumus voidakseen käyttää arkaluonteisia tietoja muihin tarkoituksiin kuin niihin, joita varten ne on alun perin kerätty tai joita varten henkilö on antanut suostumuksensa, tai voidakseen luovuttaa ne kolmansille osapuolille ⁽³¹⁾.
- (19) Tällaista suostumusta ei tarvita unionin tietosuojalainsäädännössä säädettyihin poikkeuksiin verrattavissa olevissa rajoitetuissa olosuhteissa, esimerkiksi silloin, kun arkaluonteisten tietojen käsittely on henkilön elintärkeiden etujen mukaista tai se on tarpeen oikeudellisen vaatimuksen laitimista taikka lääketieteellisen hoidon antamista tai diagnoosin tekemistä varten ⁽³²⁾.

2.2.3 Tietojen täsmällisyys, minimointi ja turvallisuus

- (20) Tietojen on oltava täsmällisiä, ja ne on tarvittaessa pidettävä ajan tasalla. Tietojen on myös oltava asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään, ja periaatteessa niitä pitäisi säilyttää ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.
- (21) Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteen ⁽³³⁾ mukaan henkilötiedot on rajoitettava siihen, mikä on käsittelyn tarkoituksen kannalta merkityksellistä. Organisaation on myös toteutettava tarvittavat kohtuulliset toimet sen varmistamiseksi, että henkilötiedot ovat käyttötarkoitukseensa nähden luotettavia sekä lisäksi tarkkoja, täydellisiä ja ajantasaisia.
- (22) Lisäksi henkilökohtaiset tiedot voidaan valintaperiaatteen mukaan säilyttää muodossa, jossa henkilö tunnistetaan tai voidaan tunnistaa (eli henkilötietojen muodossa) ⁽³⁴⁾ ainoastaan niin kauan kuin on tarpeen sitä tarkoitusta varten, johon tiedot alun perin kerättiin tai johon henkilö on myöhemmin antanut luvan. Tämä velvoite ei estä organisaatioita käsittelemästä henkilötietoja pidempää aikaa mutta ainoastaan niin kauan ja siinä määrin kuin tällainen käsittely kohtuudella palvelee jotakin seuraavista tarkoituksista, jotka ovat verrattavissa unionin tietosuojalainsäädännössä säädettyihin poikkeuksiin: arkistointi yleisen edun nimissä, journalismi, kirjallisuus ja taide, tieteellinen ja historiantutkimus ja tilastollinen analyysi ⁽³⁵⁾. Jos henkilötietoja säilytetään jotakin tällaista tarkoitusta varten, niiden käsittely edellyttää järjestelyn periaatteiden mukaisia suoja-toimia ⁽³⁶⁾.
- (23) Henkilötietoja olisi myös käsiteltävä tavalla, jolla varmistetaan niiden turvallisuus, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tätä varten rekisterinpitäjien ja henkilötietojen käsittelijöiden olisi toteutettava asianmukaisia teknisiä tai organisatorisia toimenpiteitä henkilötietojen suojaamiseksi mahdollisilta uhkilta. Näitä toimenpiteitä arvioitaessa olisi otettava huomioon uusin tekniikka, toimenpiteisiin liittyvät kustannukset sekä käsittelyn luonne, laajuus, konteksti ja tarkoitus sekä yksilöiden oikeuksiin kohdistuvat riskit.

⁽³⁰⁾ Liite I, II jakson 2 kohdan c alakohta.

⁽³¹⁾ Liite I, II jakson 2 kohdan c alakohta.

⁽³²⁾ Liite I, III jakson 1 kohta.

⁽³³⁾ Liite I, II jakson 5 kohta.

⁽³⁴⁾ Ks. liitteessä I oleva alaviite 7, jonka mukaan henkilön katsotaan olevan tunnistettavissa, jos organisaatio tai kolmas osapuoli voi kohtuudella tunnistaa kyseisen henkilön, ottaen huomioon kohtuullisen todennäköisesti käytettävät tunnistusmenetelmät (samalla on otettava huomioon muun muassa tunnistamisen kustannukset ja siihen käytettävä aika sekä käsittelyhetkellä käytettävissä oleva tekniikka).

⁽³⁵⁾ Liite I, II jakson 5 kohdan b alakohta.

⁽³⁶⁾ Ks. edellinen alaviite.

- (24) Tietosuojakehyksessä tämä varmistetaan turvallisuusperiaatteella (Security Principle), jossa edellytetään asetuksen (EU) 2016/679 32 artiklan tavoin, että on toteutettava kohtuullisia ja asianmukaisia turvallisuustoimenpiteitä ottaen huomioon käsittelyyn liittyvät riskit ja tietojen luonne ⁽³⁷⁾.

2.2.4 Läpinäkyvyys

- (25) Rekisteröidyille olisi ilmoitettava heidän henkilötietojensa käsittelyn pääkohdat.
- (26) Tämä varmistetaan ilmoitusperiaatteella ⁽³⁸⁾, jolla organisaatiot veloitetaan asetuksen (EU) 2016/679 läpinäkyvyysvaatimusten tapaan ilmoittamaan rekisteröidyille muun muassa i) organisaation osallistumisesta tietosuojakehykseen, ii) kerättyjen tietojen tyyppi, iii) käsittelyn tarkoitus, iv) minkä tyyppisille kolmansille osapuolille henkilötietoja voidaan luovuttaa ja keitä nämä kolmannet osapuolet ovat sekä mitä tarkoitusta varten tiedot luovutetaan, v) rekisteröidyn oikeudet, vi) organisaation yhteystiedot ja vii) käytettävissä olevat oikeussuojamekanismit.
- (27) Ilmoituksessa käytetyn kielen on oltava selkeää, ja ilmoituksen on oltava henkilön helposti havaittavissa. Ilmoitus on annettava, kun henkilöä pyydetään ensimmäistä kertaa antamaan henkilötietoja organisaatiolle, tai niin pian kuin ilmoituksen antaminen on käytännössä mahdollista. Ilmoitus on annettava joka tapauksessa ennen henkilötietojen käyttämistä olennaisesti poikkeavaan (mutta yhteensopivaan) tarkoitukseen kuin siihen, jota varten ne on alun perin kerätty, tai ennen niiden luovuttamista ensimmäisen kerran kolmannelle osapuolelle ⁽³⁹⁾.
- (28) Lisäksi organisaatioiden on julkistettava tietosuojaperiaatteensa, joissa otetaan huomioon järjestelyn periaatteet (tai henkilöstötietojen tapauksessa asetettava ne asianomaisten helposti saataville), ja annettava linkit kauppaministeriön verkkosivustolle (jolla on lisätietoja varmennuksesta, rekisteröityjen oikeuksista ja käytettävissä olevista muutoksenhakumenettelyistä), tietosuojakehykseen osallistuvien organisaatioiden luetteloon, jäljempänä 'tietosuojakehyksen osallistujaluettelo', ja asianmukaisen vaihtoehtoisen riitojenratkaisuelimen verkkosivustolle ⁽⁴⁰⁾.

2.2.5 Yksilön oikeudet

- (29) Rekisteröidyillä olisi oltava tietyt oikeudet, joihin voidaan vedota rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, kuten oikeus saada pääsy tietoihin, oikeus vastustaa niiden käsittelyä ja oikeus saada tiedot oikaistuiksi ja poistetuiksi.
- (30) Tietosuojakehykseen sisältyvä tiedonsaantiperiaate (Access Principle) ⁽⁴¹⁾ takaa yksilöille nämä oikeudet. Rekisteröidyllä on erityisesti oikeus saada organisaatiolta ilman perusteluja tieto siitä, käsitteleekö organisaatio häneen liittyviä henkilötietoja, oikeus saada tiedot itselleen ja oikeus saada tietoa käsittelyn tarkoituksesta, käsiteltävien henkilötietojen ryhmistä sekä vastaanottajista (ryhmistä), joille tietoja luovutetaan ⁽⁴²⁾. Organisaatioiden on vastattava tietopyyntöihin kohtuullisessa ajassa ⁽⁴³⁾. Organisaatio voi asettaa kohtuulliset

⁽³⁷⁾ Liite I, II jakson 4 kohdan a alakohta. Lisäksi tietosuojakehyksessä edellytetään henkilöstötietojen osalta, että työnantajien olisi otettava huomioon työntekijöiden esittämät yksityisyyttä koskevat toiveet rajoittamalla pääsyä henkilöstötietoihin, muuttamalla määrättyt tiedot tunnistamattomiksi tai käyttämällä koodeja tai salanimiä (liite I, III jakson 9 kohdan b alakohdan iii alakohta).

⁽³⁸⁾ Liite I, II jakson 1 kohta.

⁽³⁹⁾ Liite I, II jakson 1 kohdan b alakohta. Täydentävässä periaatteessa 14 (liite I, III jakson 14 kohdan b ja c alakohta) vahvistetaan säännökset, joita sovelletaan henkilötietojen käsittelyyn terveystutkimusten ja kliinisten tutkimusten yhteydessä. Tämä periaate mahdollistaa erityisesti sen, että organisaatiot voivat käsitellä kliinisen tutkimuksen tietoja myös sen jälkeen, kun henkilö on vetäytynyt tutkimuksesta, jos asia on ilmoitettu selvästi henkilölle hänen suostuessaan osallistumaan tutkimukseen. Vastaavasti jos tietosuojakehykseen osallistuva organisaatio saa henkilötietoja terveystutkimusta varten, se saa käyttää niitä uudessa tutkimuksessa ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Tällöin henkilölle olisi periaatteessa kerrottava tietojen mahdollisesta tulevasta käytöstä (esimerkiksi asiaan liittyvissä tutkimuksissa). Jos tietojen kaikkia tulevia käyttötarkoituksia ei vielä alussa voida ilmoittaa, koska niitä ei tunneta (tarve uusille tutkimuksille voi syntyä uusien havaintojen tai lääketieteen tai tutkimuksen kehittymisen myötä), on kerrottava, että tietoja saatetaan käyttää mahdollisissa tulevaisuudessa lääketieteellisissä ja farmaseuttisissa tutkimuksissa. Jos tällainen myöhempi käyttö ei ole niiden yleisten tutkimustarkoitusten mukaista, joita varten tiedot kerättiin (eli jos uudet käyttötarkoitukset ovat olennaisesti erilaisia mutta edelleen yhteensopivia alkuperäisen tarkoituksen kanssa, ks. johdanto-osan 14–15 kappale), on hankittava uusi nimenomainen suostumus. Ks. myös alaviitteessä 28 kuvatut ilmoitusperiaatetta koskevat erityiset rajoitukset ja poikkeukset.

⁽⁴⁰⁾ Liite I, III jakson 6 kohdan d alakohta.

⁽⁴¹⁾ Ks. myös tietoihin pääsyä koskeva täydentävä periaate (liite I, III jakson 8 kohta).

⁽⁴²⁾ Liite I, III jakson 8 kohdan a alakohdan i ja ii alakohta.

⁽⁴³⁾ Liite I, III jakson 8 kohdan i alakohta.

rajoitukset sille, miten usein yhden henkilön tietopyyntöihin vastataan tietyllä ajanjaksolla, ja se voi periä kohtuullisen maksun esimerkiksi silloin, kun tietopyyntöjä tehdään kohtuuttoman usein ⁽⁴⁴⁾.

- (31) Oikeutta saada pääsy tietoihin voidaan rajoittaa vain poikkeuksellisissa olosuhteissa, jotka ovat samankaltaisia kuin unionin tietosuojalainsäädännössä säädetty olosuhteet. Näin on erityisesti silloin, kun tiedonsaantioikeus loukkaisi muiden henkilöiden laillisia oikeuksia, kun oikeuden myöntämisestä aiheutuva rasitus tai siitä syntyvät kustannukset olisivat suhteettoman suuria verrattuina henkilön tietosuojaan kohdistuviin riskeihin kyseisissä olosuhteissa (pelkkien kustannusten ja rasituksen perusteella ei kuitenkaan päätetä, onko tietojen luovuttaminen kohtuullista), kun tietojen luovuttaminen todennäköisesti vaarantaisi vastakkaisen tärkeän yleisen edun, kuten kansallisen turvallisuuden, yleisen turvallisuuden tai maanpuolustuksen, kun tietoihin sisältyy luottamuksellisia kaupallisia tietoja tai kun tietoja käsitellään ainoastaan tutkimus- tai tilastotarkoituksia varten ⁽⁴⁵⁾. Tiedonsaantioikeuden epäämisen tai rajoittamisen on oltava välttämätöntä ja se on perusteltava asianmukaisesti, ja organisaation on osoitettava näiden vaatimusten täyttäminen ⁽⁴⁶⁾. Tätä arviointia tehdessään organisaation on otettava erityisesti huomioon kyseisen yksilön etu ⁽⁴⁷⁾. Jos tiedot on mahdollista erottaa muista, rajoituksen piiriin kuuluvista tiedoista, organisaation on erotettava suojatut tiedot jäljelle jäävistä tiedoista, jotka luovutetaan niiden pyytäjälle ⁽⁴⁸⁾.
- (32) Rekisteröidyllä on lisäksi oikeus vaatia virheellisten tietojen oikaisemista tai muuttamista sekä sellaisten tietojen poistamista, joita on käsitelty järjestelyn periaatteiden vastaisesti ⁽⁴⁹⁾. Kuten johdanto-osan 15 kappaleessa selitetään, henkilöllä on lisäksi oikeus vastustaa tietojen käsittelyä tai kieltää se, kun käyttötarkoitus (vaikka se olisikin hyväksyttävä) poikkeaa olennaisesti tarkoituksesta, jota varten tiedot on kerätty, sekä oikeus vastustaa tietojen luovuttamista kolmansille osapuolille tai kieltää se. Jos henkilötietoja käytetään suoramarkkinointiin, henkilöllä on yleinen oikeus kieltää niiden käsittely milloin tahansa ⁽⁵⁰⁾.
- (33) Järjestelyn periaatteissa ei erityisesti käsitellä rekisteröityyn vaikuttavia päätöksiä, jotka perustuisivat yksinomaan henkilötietojen automaattiseen käsittelyyn. Unionissa kerättyjen henkilötietojen osalta mahdollisen automatisoitua käsittelyyn perustuvan päätöksen tekee kuitenkin yleensä unionissa toimiva rekisterinpitäjä (jolla on suora suhde kyseiseen rekisteröityyn), ja näin ollen kyseiseen päätökseen sovelletaan suoraan asetusta (EU) 2016/679 ⁽⁵¹⁾. Tähän kuuluvat siirtotilanteet, joissa tietojen käsittelyn suorittaa ulkomainen (esimerkiksi yhdysvaltalainen) toiminnanharjoittaja, joka toimii unionin rekisterinpitäjän puolesta (käsittelijänä) (tai unionin käsittelijän alihankkijana vastaanotettuaan tiedot ne keränneeltä unionin rekisterinpitäjältä); päätöksen tekee tämän perusteella unionin rekisterinpitäjä.
- (34) Tämä vahvistettiin komission vuonna 2018 teettämässä tutkimuksessa Privacy Shield -järjestelyn toiminnan toisen vuotuisen uudelleentarkastelun yhteydessä ⁽⁵²⁾. Tutkimuksessa todettiin, että tuolloin ei ollut näyttöä siitä, että Privacy Shield -järjestelyyn kuuluvat organisaatiot normaalisti soveltaisivat automatisoitua päätöksentekoa Privacy Shield -järjestelyssä siirrettyjen henkilötietojen perusteella.

⁽⁴⁴⁾ Liite I, III jakson 8 kohdan f alakohdan i ja ii alakohta ja 8 kohdan g alakohta.

⁽⁴⁵⁾ Liite I, III jakson 4 kohta, 8 kohdan b, c ja e alakohta, 14 kohdan e ja f alakohta sekä 15 kohdan d alakohta.

⁽⁴⁶⁾ Liite I, III jakson 8 kohdan e alakohdan ii alakohta. Organisaation on ilmoitettava henkilölle epäämisen tai rajoituksen syyt sekä yhteyspiste mahdollisia lisätiedusteluja varten (III jakson 8 kohdan a alakohdan iii alakohta).

⁽⁴⁷⁾ Liite I, III jakson 8 kohdan a alakohdan ii ja iii alakohta.

⁽⁴⁸⁾ Liite I, III jakson 8 kohdan a alakohdan i alakohta.

⁽⁴⁹⁾ Liite I, II jakson 6 kohta ja III jakson 8 kohdan a alakohdan i alakohta.

⁽⁵⁰⁾ Liite I, III jakson 8 kohdan 12 alakohta.

⁽⁵¹⁾ Vastaavasti siinä poikkeuksellisessa tapauksessa, että yhdysvaltalaisella organisaatiolla on suora suhde unionin rekisteröityyn, tämä on tyypillisesti seurausta siitä, että yhdysvaltalainen toiminnanharjoittaja on kohdentanut toimiaan unionissa olevaan henkilöön tarjoamalla tälle tavaroita tai palveluja tai seuraamalla tämän käyttäytymistä. Tässä tapauksessa yhdysvaltalainen organisaatio itse kuuluu asetuksen (EU) 2016/679 (3 artiklan 2 kohta) soveltamisalaan, minkä vuoksi sen on suoraan noudatettava unionin tietosuojalainsäädäntöä.

⁽⁵²⁾ SWD(2018) 497 final, 4.1.5 kohta. Tutkimuksessa keskityttiin i) siihen, missä määrin Privacy Shield -järjestelyyn Yhdysvalloissa osallistuvat organisaatiot tekevät yksilöihin vaikuttavia päätöksiä, jotka perustuvat Privacy Shield -järjestelyn nojalla EU:ssa toimivilta yrityksiltä siirrettyjen henkilötietojen automaattiseen käsittelyyn, ja ii) henkilöitä koskeviin suojatoimiin, joita Yhdysvaltain liittovaltion lainsäädännössä on tällaisia tilanteita varten, ja näiden suojatoimien soveltamisedellytyksiin.

- (35) Aloilla, joilla yritykset todennäköisimmin käyttävät henkilötietojen automatisoitua käsittelyä, kun ne tekevät henkilöön vaikuttavia päätöksiä (esimerkiksi luotonanto, asuntolainatarjoukset, työllisyys, asuminen ja vakuutukset), Yhdysvaltojen lainsäädäntö tarjoaa erityisiä suojatoimia kielteisiä päätöksiä vastaan ⁽⁵³⁾. Kyseisten säädösten mukaan henkilöillä on yleensä oikeus saada tietoonsa päätöksen (esimerkiksi luoton hylkääminen) perustana olleet syyt, riittauttaa puutteelliset tai virheelliset tiedot (sekä lainvastaisten perusteiden käyttö) ja hakea muutosta. Kulutusluottojen osalta luottokelpoisuusraportointia koskeva laki (Fair Credit Reporting Act) ja yhtäläisiä luotonsaantimahdollisuuksia koskeva laki (Equal Credit Opportunity Act) sisältävät suojatoimia, jotka antavat kuluttajille oikeuden selitykseen ja oikeuden riittauttaa päätös. Nämä lait ovat merkityksellisiä useiden kysymysten, kuten luotonannon, työllisyyden, asumisen ja vakuutusten kannalta. Lisäksi tietyissä syrjinnän vastaisissa laeissa, kuten kansalaisoikeuslain (Civil Rights Act) VII osastossa ja oikeudenmukaista asumista koskevassa laissa (Fair Housing Act), henkilöille tarjotaan suojaa automatisoidussa päätöksenteossa käytettäviä malleja vastaan, sillä ne voivat johtaa syrjintään tiettyjen ominaisuuksien perusteella. Henkilöille myönnetään oikeus riittauttaa tällaiset päätökset, automatisoidut päätökset mukaan lukien. Sairausvakuutuslain (Health Insurance Portability and Accountability Act) yksityisyyden suojaa koskevalla säännöllä (Privacy Rule) luodaan terveystietoja koskevia oikeuksia, jotka vastaavat asetuksen (EU) 2016/679 henkilökohtaisten terveystietojen saatavuutta koskevia oikeuksia. Lisäksi terveydenhuoltopalvelujen tarjoajien on Yhdysvaltojen viranomaisten ohjeiden mukaan saatava tietoja, joiden avulla ne voivat kertoa henkilöille lääketieteen alalla käytettävistä automatisoiduista päätöksentekojärjestelmistä ⁽⁵⁴⁾.
- (36) Näin ollen nämä säännöt tarjoavat samanlaisia suojatoimia kuin unionin tietosuojalainsäädännössä säädetty suojatoimet siinä epätodennäköisessä tilanteessa, että tietosuojakehykseen osallistuva organisaatio tekisi itse automatisoituja päätöksiä.

2.2.6 Tietojen edelleen siirtämistä koskevat rajoitukset

- (37) Unionista Yhdysvalloissa oleville organisaatioille siirrettyjen henkilötietojen suojan tasoa ei saa heikentää siirtämällä näitä tietoja edelleen Yhdysvalloissa tai muussa kolmannessa maassa sijaitseville vastaanottajille.
- (38) Tietojen edelleen siirtämiseen liittyvää vastuuvuolisuutta koskevan periaatteen ⁽⁵⁵⁾ mukaan on sovellettava erityisiä sääntöjä niin sanottuun "tietojen edelleen siirtämiseen" eli henkilötietojen siirtämiseen tietosuojakehykseen osallistuvalla organisaatiolla rekisterinpitäjänä tai henkilötietojen käsittelijänä toimivalle kolmannelle osapuolelle, riippumatta siitä, sijaitseeko viimeksi mainittu Yhdysvalloissa vai Yhdysvaltojen (ja unionin) ulkopuolisessa kolmannessa maassa. Tietoja voidaan siirtää edelleen vain i) rajoitettuihin ja täsmennettyihin tarkoituksiin, ii) tietosuojakehykseen osallistuvan organisaation ja kolmannen osapuolen välisen sopimuksen perusteella ⁽⁵⁶⁾ (tai vastaavan konsernin sisäisen järjestelyn perusteella ⁽⁵⁷⁾) ja iii) ainoastaan, jos sopimuksessa edellytetään, että kolmannen osapuolen on tarjottava suojan taso, joka vastaa järjestelyn periaatteiden takaamaa suojan tasoa.
- (39) Velvollisuus tarjota samantasoinen tietosuojaa kuin järjestelyn periaatteissa, luettuna yhdessä tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteen (Data Integrity and Purpose Limitation Principle) kanssa, tarkoittaa erityisesti sitä, että kolmas osapuoli voi käsitellä sille toimitettuja henkilötietoja ainoastaan sellaisia tarkoituksia varten, jotka eivät ole ristiriidassa niiden tarkoitusten kanssa, joita varten tiedot on alun perin kerätty tai joihin henkilö on myöhemmin antanut luvan (valintaperiaatteen mukaisesti).

⁽⁵³⁾ Ks. esimerkiksi Equal Credit Opportunity Act (15 U.S.C. 1691 § ja sitä seuraavat pykälät), Fair Credit Reporting Act (15 U.S.C. 1681 § ja sitä seuraavat pykälät) tai Fair Housing Act (42 U.S.C. 3601 § ja sitä seuraavat pykälät). Lisäksi Yhdysvallat on sitoutunut Taloudellisen yhteistyön ja kehityksen järjestön OECD:n puiteissa laadittuihin tekoälyn periaatteisiin, joihin sisältyvät muun muassa läpinäkyvyyden, selitettävyyden, turvallisuuden ja vastuuvuolisuuden periaatteet.

⁽⁵⁴⁾ Ks. esimerkiksi ohjeistus 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⁾ Ks. liite I, II jakson 3 kohta, ja täydentävä periaate "tietojen edelleen siirtämistä koskevat pakolliset sopimukset" (liite I, III jakson 10 kohta).

⁽⁵⁶⁾ Tästä yleisestä periaatteesta poiketen organisaatio voi siirtää edelleen pienen työntekijäjoukon henkilötietoja ilman, että sen tarvitsee tehdä tietojen saajan kanssa sopimus, kun tietoja tarvitaan satunnaisesti työhön liittyviin operatiivisiin toimiin, kuten lennon tai hotellihuoneen varaamiseen tai vakuutuksen hankkimiseen. Tässäkin tapauksessa organisaation on kuitenkin edelleen noudatettava ilmoitus- ja valintaperiaatteita (ks. liite I, III jakson 9 kohdan a alakohta).

⁽⁵⁷⁾ Ks. täydentävä periaate tietojen edelleen siirtämistä koskevasta pakollisista sopimuksista (liite I, III jakson 10 kohdan b alakohta). Vaikka tämä periaate mahdollistaa myös muihin kuin sopimuksellisiin välineisiin perustuvat siirrot (esimerkiksi konsernin sisäiset periaatteiden noudattamista ja valvontaa koskevat ohjelmat), tekstissä tehdään selväksi, että näillä välineillä on aina "varmistettava henkilötietojen suojan jatkuvuus periaatteiden mukaisesti". Kun otetaan lisäksi huomioon, että vastuu järjestelyn periaatteiden noudattamisesta säilyy varmennuksen antaneella yhdysvaltalaisella organisaatiolla, sillä on voimakas kannustin käyttää välineitä, jotka todella ovat tehokkaita käytännössä.

- (40) Tietojen edelleen siirtämiseen liittyvää vastuuvollisuutta koskevaa periaatetta olisi luettava yhdessä myös ilmoitusperiaatteen kanssa ja, kun kyseessä on tietojen siirtäminen rekisterinpitäjänä toimivalle kolmannelle osapuolelle ⁽⁵⁸⁾, valintaperiaatteen kanssa, jonka mukaan rekisteröidyille on ilmoitettava (muun muassa) mahdollisen kolmannen vastaanottajan tyyppi/nimi, edelleensierroin tarkoitus ja tarjottu valintaoikeus. Rekisteröidyille on myös ilmoitettava mahdollisuudesta kieltää tiedonsiirto ja arkaluonteisten tietojen tapauksessa myös tieto siitä, että niiden on annettava tietojen siirrolle "nimenomainen myönteinen suostumus".
- (41) Vastuuvollisuutta tarjota periaatteissa vaadittua vastaava suoja sovelletaan kaikkiin kolmansiin osapuoliin, jotka osallistuvat siirrettyjen tietojen käsittelyyn sijainnistaan (Yhdysvalloissa tai muussa kolmannessa maassa) riippumatta, samoin kuin silloin, kun alkuperäinen kolmantena osapuolena toimiva vastaanottaja itse siirtää kyseisiä tietoja toiselle kolmantena osapuolena olevalle vastaanottajalle esimerkiksi alihankintana teetetävää käsittelyä varten.
- (42) Kolmantena osapuolena olevan vastaanottajan kanssa tehdyssä sopimuksessa on kaikissa tapauksissa määrättävä siitä, että kyseinen osapuoli ilmoittaa tietosuojakehykseen osallistuvalla organisaatiolla, jos se toteaa, ettei se voi enää täyttää vastuuvollisuutta. Kun tällaiseen toteamukseen on päädytty, kolmannen osapuolen on lopetettava tietojen käsittely tai ryhdyttävä muihin kohtuullisiin ja asianmukaisiin toimiin tilanteen korjaamiseksi ⁽⁵⁹⁾.
- (43) Lisäsuojatoimia sovelletaan, kun tietoja siirretään edelleen edustajana toimivalle kolmannelle osapuolelle (eli henkilötietojen käsittelijälle). Tällaisessa tapauksessa kyseisen yhdysvaltalaisen organisaation on varmistettava, että edustaja toimii ainoastaan sen ohjeiden mukaisesti, ja toteutettava kohtuullisia ja asianmukaisia toimia i) sen varmistamiseksi, että edustaja todella käsittelee siirretyt henkilötiedot tavalla, joka vastaa järjestelyn periaatteissa vahvistettuja organisaation velvoitteita, ja ii) luvattoman käsittelyn lopettamiseksi ja tilanteen korjaamiseksi, kun se on saanut tätä koskevan ilmoituksen ⁽⁶⁰⁾. Yhdysvaltojen kauppaministeriö voi vaatia organisaatiota toimittamaan yhteenvedon tai olennaiset osat sisältävän jäljennöksen sopimuksen yksityisyyden suojaa koskevista määräyksistä ⁽⁶¹⁾. Jos (alihakinnan) käsittelyketjussa esiintyy periaatteiden noudattamiseen liittyviä ongelmia, rekisterinpitäjänä toimivan organisaation on todistettava, että se ei ole vastuussa vahingon aiheuttaneesta tapahtumasta, tai muuten se joutuu vastuuseen muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti ⁽⁶²⁾.

2.2.7 Vastuuvollisuus

- (44) Vastuuvollisuutta koskevan periaatteen mukaan tietoja käsittelevien yksiköiden on otettava käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta ne voivat tehokkaasti noudattaa tietosuojavelvoitteitaan ja osoittaa erityisesti toimivaltaiselle valvontaviranomaiselle niiden noudattamisen.
- (45) Kun organisaatio on vapaaehtoisesti päättänyt antaa varmennuksen ⁽⁶³⁾ tietosuojakehyksen puitteissa, järjestelyn periaatteiden noudattamisesta tulee pakollista, ja sen noudattamista voidaan vaatia oikeudessa. Muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen ⁽⁶⁴⁾ mukaan tietosuojakehykseen osallistuvien organisaatioiden on tarjottava tehokkaat mekanismit periaatteiden noudattamisen varmistamiseksi. Organisaatioiden on myös toteutettava toimenpiteitä sen varmistamiseksi ⁽⁶⁵⁾, että niiden tietosuojaperiaatteet vastaavat järjestelyn periaatteita ja että niitä tosiasiallisesti noudatetaan. Tämä voidaan tehdä joko itsearviointijärjestelmän avulla, jonka tulee sisältää sisäiset menettelyt, joilla varmistetaan, että työntekijät saavat koulutusta organisaation tietosuojaperiaatteiden täytäntöönpanosta ja että periaatteiden noudattamista tarkastellaan säännöllisesti ja puolueettomasti, tai ulkoisen uudelleentarkastelun avulla, mihin voi sisältyä tarkastuksia, pistokokeita ja teknisten välineiden käyttöä.

⁽⁵⁸⁾ Henkilöillä ei ole oikeutta kieltää tietojen siirtoa, jos tiedot siirretään sellaiselle kolmannelle osapuolelle, joka toimii edustajana ja suorittaa tehtävänsä kyseisen yhdysvaltalaisen organisaation puolesta ja sen ohjeiden mukaisesti. Tämä edellyttää kuitenkin sopimusta edustajan kanssa, ja kyseisen yhdysvaltalaisen organisaation on taattava järjestelyn periaatteiden mukaiset suojatoimet käyttämällä ohjeistuksen antamiseen liittyviä valtuuksiaan.

⁽⁵⁹⁾ Tilanne vaihtelee sen mukaan, onko kolmas osapuoli rekisterinpitäjä vai henkilötietojen käsittelijä (edustaja). Ensimmäisessä skenaariossa kolmannen osapuolen kanssa tehtävässä sopimuksessa on määrättävä, että viimeksi mainittu lopettaa tietojen käsittelyn tai ryhtyy muihin kohtuullisiin ja asianmukaisiin toimiin tilanteen korjaamiseksi. Toisessa skenaariossa tietosuojakehykseen kuuluvan organisaation on toteutettava nämä toimet, sillä se vastaa ohjeidensa mukaisesti toimivan edustajan suorittamasta tietojen käsittelystä. Ks. liite I, II jakson 3 kohta.

⁽⁶⁰⁾ Liite I, II jakson 3 kohdan b alakohta.

⁽⁶¹⁾ Ks. edellinen alaviite.

⁽⁶²⁾ Liite I, II jakson 7 kohdan d alakohta.

⁽⁶³⁾ Ks. myös omaa varmennusta koskeva täydentävä periaate (liite I, III jakson 6 kohta).

⁽⁶⁴⁾ Ks. riitojenratkaisua ja täytäntöönpanoa koskeva täydentävä periaate (liite I, III jakson 11 kohta).

⁽⁶⁵⁾ Ks. myös tarkastusta koskeva täydentävä periaate (liite I, III jakson 7 kohta).

- (46) Organisaatioiden on lisäksi dokumentoitava tietosuojakehyksen mukaisten käytäntöjen täytäntöönpano ja toimitettava pyynnöstä asiaa koskeva dokumentaatio periaatteiden noudattamista koskevan tutkimuksen tai valitusmenettelyn yhteydessä riippumattomalle riitojenratkaisuelimelle tai toimivaltaiselle lainvalvontaviranomaiselle ⁽⁶⁶⁾.

2.3 Hallinnointi, valvonta ja täytäntöönpano

- (47) Tietosuojakehystä hallinnoi ja seuraa kauppaministeriö. Tietosuojakehyksessä määrätään valvonta- ja täytäntöönpanomekanismeista, jotta voidaan tarkastaa ja varmistaa, että tietosuojakehykseen osallistuvat organisaatiot noudattavat järjestelyn periaatteita ja että mahdolliseen periaatteiden noudattamatta jättämiseen puututaan. Nämä mekanismit on esitetty järjestelyn periaatteissa (liite I) sekä kauppaministeriön (liite III), liittovaltion kauppakomission (liite IV) ja liikenneministeriön (liite V) antamissa sitoumuksissa.

2.3.1 (Uudelleen)varmennus

- (48) Tietosuojakehykseen osallistuvien organisaatioiden varmennus (tai vuosittainen uudelleenvarmennus) edellyttää, että organisaatiot sitoutuvat julkisesti noudattamaan järjestelyn periaatteita, asettavat tietosuojaperiaatteensa saataville ja panevat ne kaikilta osin täytäntöön ⁽⁶⁷⁾. Organisaatioiden on osana (uudelleen)varmennushakemustaan toimitettava kauppaministeriölle tiedot muun muassa seuraavista: organisaation nimi, organisaation suorittaman henkilötietojen käsittelyn tarkoitus, varmennuksen kattamat henkilötiedot sekä valittu tarkastamismenetelmä, sovellettava riippumaton muutoksenhakumekanismi ja lakisääteinen elin, jolla on toimivalta valvoa järjestelyn periaatteiden noudattamista ⁽⁶⁸⁾.
- (49) Organisaatio voi vastaanottaa henkilötietoja tietosuojakehyksen puitteissa siitä päivästä alkaen, jona kauppaministeriö on lisännyt sen tietosuojakehyksen osallistujaluetteloon. Oikeusvarmuuden takaamiseksi ja totuudenvastaisten väitteiden välttämiseksi ensimmäistä kertaa varmennuksen antavat organisaatiot eivät saa ilmoittaa julkisesti noudattavansa järjestelmän periaatteita ennen kuin kauppaministeriö on todennut, että organisaation varmennus on saatettu päätökseen, ja lisännyt organisaation osallistujaluetteloon ⁽⁶⁹⁾. Jotta organisaatio voi jatkaa osallistumistaan tietosuojakehykseen voidakseen vastaanottaa henkilötietoja unionista, sen on varmennettava osallistumisensa järjestelyyn uudelleen vuosittain. Kun organisaatio vetäytyy tietosuojakehyksestä mistä tahansa syystä, sen on poistettava kaikki maininnat, joista voisi päätellä, että se osallistuu edelleen tietosuojakehykseen ⁽⁷⁰⁾.
- (50) Liitteessä III esitettyjen sitoumusten mukaisesti kauppaministeriö tarkastaa, täyttävätkö organisaatiot kaikki varmennusta koskevat vaatimukset ja ovatko ne ottaneet käyttöön (julkiset) tietosuojaperiaatteet, jotka sisältävät ilmoitusperiaatteen edellyttämät tiedot ⁽⁷¹⁾. Kauppaministeriö tekee Privacy Shield -järjestelyn mukaisesta (uudelleen)varmennusprosessista saatujen kokemusten perusteella useita tarkastuksia muun muassa sen toteamiseksi, sisältävätkö organisaatioiden tietosuojaperiaatteet linkin oikeaan valituslomakkeeseen asianomaisen riitojenratkaisumekanismiin verkkosivustolla. Kun varmennukseen sisältyy useita saman organisaation yksiköitä ja tytäryhtiöitä, se tarkastaa, täyttävätkö kunkin yksikön tietosuojaperiaatteet varmennusvaatimukset ja ovatko ne helposti rekisteröityjen saatavilla ⁽⁷²⁾. Lisäksi kauppaministeriö tekee tarvittaessa liittovaltion kauppakomission ja liikenneministeriön kanssa ristiintarkastuksia sen varmistamiseksi, että organisaatioita valvovat niiden (uudelleen) varmennuksessa nimetyt valvontaelimet. Kauppaministeriö tekee myös yhteistyötä vaihtoehtoisten riitojenratkaisuelinten kanssa sen varmistamiseksi, että organisaatiot on rekisteröity niiden (uudelleen)varmennuksessa yksilöityyn riippumattomaan muutoksenhakumekanismiin ⁽⁷³⁾.

⁽⁶⁶⁾ Liite I, III jakson 7 kohta.

⁽⁶⁷⁾ Liite I, I jakson 2 kohta.

⁽⁶⁸⁾ Liite I, III jakson 6 kohdan b alakohta, ja liite III, ks. jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

⁽⁶⁹⁾ Liite I, alaviite 12.

⁽⁷⁰⁾ Liite I, III jakson 6 kohdan h alakohta.

⁽⁷¹⁾ Liite I, III jakson 6 kohdan a alakohta ja alaviite 12, sekä liite III, ks. jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

⁽⁷²⁾ Liite III, jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

⁽⁷³⁾ Vastaavasti kauppaministeriö tekee yhteistyötä kolmannen osapuolen kanssa, joka toimii tietosuojaviranomaisten paneelia varten suoritetuilla maksuilla kerättyjen varojen säilyttäjänä (ks. johdanto-osan 73 kappale). Näin kauppaministeriö tarkastaa, ovatko tietosuojaviranomaisen riippumattomaksi muutoksenhakumekanismiksi valinneet organisaatiot suorittaneet maksun kyseisen vuoden osalta. Ks. liite III, jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

- (51) Kauppaministeriö ilmoittaa organisaatioille, että niiden on (uudelleen)varmennuksen päätökseen saattamiseksi korjattava kaikki arvioinnin aikana havaitut ongelmat. Jos organisaatio ei vastaa kauppaministeriön asettamassa määräajassa (esimerkiksi uudelleenvarmennus olisi saatettava päätökseen 45 päivän kuluessa) ⁽⁷⁴⁾ tai se ei muutoin saata varmennustaan päätökseen, sen katsotaan luopuneen varmennuksesta. Mikäli tietosuojakehykseen osallistumisesta tai sen määräysten noudattamisesta on annettu vääriä tietoja, kauppakomissio tai liikenneministeriö voi ryhtyä asiassa lainvalvontatoimiin ⁽⁷⁵⁾.
- (52) Tietosuojakehyksen asianmukaisen soveltamisen varmistamiseksi asianomaisten osapuolten, kuten rekisteröityjen, tiedonviejien ja kansallisten tietosuojaviranomaisten, on voitava tunnistaa järjestelyn periaatteita noudattavat organisaatiot. Jotta tämä läpinäkyvyys voitaisiin varmistaa tietosuojakehykseen osallistuvien organisaatioiden osalta, kauppaministeriö on sitoutunut pitämään yllä ja saattamaan yleisön saataville luettelon organisaatioista, jotka ovat varmentaneet noudattavansa järjestelyn periaatteita ja jotka kuuluvat ainakin yhden tämän päätöksen liitteissä IV ja V tarkoitetun lainvalvontaviranomaisen toimivallan piiriin ⁽⁷⁶⁾. Kauppaministeriö päivittää luettelon organisaatioiden vuosittain antamien uudelleenvarmennusten perusteella ja aina, kun organisaatio peruuttaa osallistumisensa tietosuojakehykseen tai se poistetaan tietosuojakehyksen piiristä. Jotta läpinäkyvyys voitaisiin taata myös tietosuojakehyksestä poistuneiden organisaatioiden osalta, kauppaministeriö pitää yllä ja saattaa yleisön saataville luettelon organisaatioista, jotka on poistettu luettelosta, ja ilmoittaa kussakin tapauksessa poistamisen syyn ⁽⁷⁷⁾. Lisäksi se ilmoittaa linkin tietosuojakehystä koskevalle liittovaltion kauppakomission verkkosivustolle, jossa on luettelo tietosuojakehyksen puitteissa toteutetuista kauppakomission lainvalvontatoimista ⁽⁷⁸⁾.

2.3.2 Vaatimusten noudattamisen seuranta

- (53) Kauppaministeriö seuraa jatkuvasti erilaisten mekanismien avulla, miten organisaatiot noudattavat tietosuojakehyksen järjestelyn periaatteita ⁽⁷⁹⁾. Se tekee erityisesti tarkastuksia paikan päällä satunnaisesti valituissa organisaatioissa sekä tapauskohtaisesti paikan päällä tietyissä organisaatioissa, jos niissä on havaittu mahdollisia vaatimusten noudattamiseen liittyviä ongelmia (esimerkiksi sellaisia, joista kolmas osapuoli on ilmoittanut kauppaministeriölle). Tarkastuksilla pyritään toteamaan, i) ovatko rekisteröityjen valituksia ja pyyntöjä käsittelevät yhteyspisteet käytettävissä ja vastaavtko ne yhteydenottoihin, ii) ovatko organisaatioiden tietosuojaperiaatteet helposti saatavilla sekä niiden verkkosivustoilla että kauppaministeriön verkkosivustolla olevan linkin kautta, iii) ovatko organisaatioiden tietosuojaperiaatteet edelleen varmennuksen vaatimusten mukaiset ja iv) onko organisaatioiden valitsema riippumaton riitojenratkaisumekanismi saatavilla valitusten käsittelyä varten ⁽⁸⁰⁾.
- (54) Jos on luotettava näyttöä siitä, että organisaatio ei noudata tietosuojakehyksen vaatimuksia (esimerkiksi jos kauppaministeriöön toimitetaan valituksia tai organisaatio ei anna tyydyttävää vastausta kauppaministeriön tietopyyntöön), kauppaministeriö vaatii organisaatiota täyttämään ja toimittamaan yksityiskohtaisen kyselyn ⁽⁸¹⁾. Jos organisaatio ei vastaa kyselyyn tyydyttävästi tai ajoissa, tapaus siirretään toimivaltaiselle viranomaiselle (liittovaltion kauppakomissio tai liikenneministeriö) mahdollisia lainvalvontatoimia varten ⁽⁸²⁾. Kauppaministeriö on tehnyt osana Privacy Shield -järjestelyn mukaista vaatimusten noudattamisen seurantaa säännöllisesti johdanto-osan 53

⁽⁷⁴⁾ Liite III, alaviite 2.

⁽⁷⁵⁾ Ks. liite III, jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

⁽⁷⁶⁾ Tietoa tietosuojakehyksen osallistujaluettelon hallinnoinnista on liitteessä III (ks. johdanto kohdassa "Kauppaministeriön toteuttama tietosuojakehyksen hallinto ja valvonta") ja liitteessä I (I jakson 3 kohta, I jakson 4 kohta, III jakson 6 kohdan d alakohta ja III jakson 11 kohdan g alakohta).

⁽⁷⁷⁾ Ks. liite III, johdanto kohdassa "Kauppaministeriön toteuttama tietosuojakehyksen hallinto ja valvonta".

⁽⁷⁸⁾ Ks. liite III, jakso "Kauppaministeriö räättää tietosuojakehyksen verkkosivuston eri kohdeyleisöille".

⁽⁷⁹⁾ Ks. liite III, jakso "Kauppaministeriö tarkastelee määräajoin viran puolesta periaatteiden noudattamista ja arvioi tietosuojakehystä".

⁽⁸⁰⁾ Kauppaministeriö voi osana seuranta-toimiaan muun muassa tarkistaa tietosuojaperiaatteiden toimimattomat linkit tai seurata aktiivisesti uutisia, jotka antavat luotettavaa näyttöä vaatimusten noudattamatta jättämisestä.

⁽⁸¹⁾ Ks. liite III, jakso "Kauppaministeriö tarkastelee määräajoin viran puolesta periaatteiden noudattamista ja arvioi tietosuojakehystä".

⁽⁸²⁾ Ks. liite III, jakso "Kauppaministeriö tarkastelee määräajoin viran puolesta periaatteiden noudattamista ja arvioi tietosuojakehystä".

kappaleessa mainittuja tarkastuksia paikan päällä ja seurannut jatkuvasti julkisia raportteja, joiden avulla se on pystynyt tunnistamaan, käsittelemään ja ratkaisemaan vaatimusten noudattamiseen liittyviä ongelmia⁽⁸³⁾. Organisaatiot, jotka jatkuvasti jättävät noudattamatta järjestelyn periaatteita, poistetaan tietosuojakehyksen osallistujaluettelosta, ja niiden on palautettava tai poistettava henkilötiedot, jotka ne ovat vastaanottaneet tietosuojakehyksen puitteissa⁽⁸⁴⁾.

- (55) Muissa luettelosta poistamista koskeissa tapauksissa, esimerkiksi silloin, kun organisaatio vetäytyy järjestelystä vapaaehtoisesti tai ei anna uutta varmennusta, organisaation on joko poistettava tai palautettava henkilötiedot tai se voi säilyttää ne, jos se vahvistaa kauppaministeriölle vuosittain sitoumuksensa jatkaa periaatteiden soveltamista tai tarjoaa henkilötiedoille riittävän suojan muiden hyväksyttyjen keinojen avulla (esimerkiksi käyttämällä sopimusta, joka vastaa täysin komission hyväksymien vakiomuotoisten sopimuslausekkeiden vaatimuksia)⁽⁸⁵⁾. Tällöin organisaation on nimettävä organisaatiossaan yhteyspiste kaikkia tietosuojakehykseen liittyviä kysymyksiä varten.

2.3.3 Tietosuojakehykseen osallistumista koskevien totuudenvastaisten väitteiden havaitseminen ja niihin puuttuminen

- (56) Kauppaministeriö seuraa, väittävätkö organisaatiot totuudenvastaisesti osallistuvansa tietosuojakehykseen tai käyttävätkö ne väärin tietosuojakehyksen varmennusmerkkiä, sekä viran puolesta että (esimerkiksi tietosuojaviranomaisten tekemien) valitusten perusteella⁽⁸⁶⁾. Kauppaministeriö tarkastaa jatkuvasti erityisesti, että organisaatiot, jotka i) vetäytyvät tietosuojakehyksestä, ii) eivät anna vuotuista uudelleenvarmennusta (eli ovat aloittaneet uudelleenvarmennuksen mutta eivät ole saattaneet sitä ajoissa päätökseen tai eivät ole edes aloittaneet vuotuista uudelleenvarmennusta), iii) on poistettu osallistujaluettelosta periaatteiden ”jatkuvan noudattamatta jättämisen” vuoksi tai iv) eivät ole saattaneet päätökseen ensimmäistä varmennusta (eli ovat aloittaneet ensimmäisen varmennuksen mutta eivät ole saattaneet sitä ajoissa päätökseen), poistavat kaikista asiaa koskevista julkaisuista tietosuojaperiaatteistaan sellaiset viittaukset tietosuojakehykseen, joista saa sen käsityksen, että organisaatio olisi tietosuojakehyksessä aktiivisesti mukana⁽⁸⁷⁾. Kauppaministeriö myös hakee internetissä organisaatioiden tietosuojaperiaatteista viittauksia tietosuojakehykseen, muun muassa havaitakseen sellaisten organisaatioiden totuudenvastaiset väitteet, jotka eivät ole koskaan osallistuneet tietosuojakehykseen⁽⁸⁸⁾.
- (57) Jos kauppaministeriö toteaa, että viittauksia tietosuojakehykseen ei ole poistettu tai niitä käytetään väärin, se ilmoittaa organisaatiolle asian mahdollisesta siirtämisestä liittovaltion kauppakomission tai liikenneministeriön käsiteltäväksi⁽⁸⁹⁾. Jos organisaatio ei anna tyydyttävää vastausta, kauppaministeriö saattaa asian toimivaltaisen viranomaisen käsiteltäväksi mahdollisia lainvalvontatoimia varten⁽⁹⁰⁾. Liittovaltion kauppakomissio, liikenneministeriö tai muut asiaankuuluvat Yhdysvaltojen lainvalvontaviranomaiset voivat ryhtyä toimiin sellaisten virheellisten tietojen johdosta, jotka organisaatio on antanut yleisölle järjestelyn periaatteiden noudattamista koskevien harhaanjohtavien lausumien tai käytäntöjen muodossa. Kauppaministeriölle toimitetut väärät tiedot voivat johtaa toimiin totuudenvastaisia lausuntoja koskevan lain (False Statements Act, 18 U.S.C. 1001 §) nojalla.

⁽⁸³⁾ Privacy Shield -järjestelyn toisen vuotuisen tarkastelun yhteydessä kauppaministeriö ilmoitti tehneensä paikan päällä tarkastuksen sadassa organisaatiossa ja lähettäneensä 21 tapauksessa noudattamista koskevan kyselyn (minkä jälkeen havaitut ongelmat korjattiin), ks. komission yksiköiden valmisteluasiakirja SWD(2018) 497 final, s. 9. Kauppaministeriö myös kertoi Privacy Shield -järjestelyn kolmannen vuotuisen tarkastelun aikana, että se oli havainnut julkisten raporttien seurannan yhteydessä kolme tapausta ja ryhtynyt suorittamaan 30 yrityksessä paikan päällä kuukausittaisia tarkastuksia, jotka johtivat kyselymuotoiseen seurantaan 28 prosentissa tapauksista (minkä jälkeen havaitut ongelmat korjattiin heti, tai kolmessa tapauksessa varoituskirjeen jälkeen), ks. komission yksiköiden valmisteluasiakirja SWD(2019) 495 final, s. 8.

⁽⁸⁴⁾ Liite I, III jakson 11 kohdan g alakohta. Periaatteiden jatkuva noudattamatta jättäminen tarkoittaa erityisesti sitä, että organisaatio kieltäytyy noudattamasta yksityisyyden suojan itsesääntelystä vastaavan elimen, riippumattoman riitojenratkaisuelimen tai lainvalvontaviranomaisen lopullista päätöstä.

⁽⁸⁵⁾ Liite I, III jakson 6 kohdan f alakohta.

⁽⁸⁶⁾ Ks. liite III, jakso ”Tietosuojakehykseen osallistumista koskevien totuudenvastaisten väitteiden havaitseminen ja niihin puuttuminen”.

⁽⁸⁷⁾ Ks. edellinen alaviite.

⁽⁸⁸⁾ Ks. edellinen alaviite.

⁽⁸⁹⁾ Ks. edellinen alaviite.

⁽⁹⁰⁾ Kauppaministeriö ilmoitti Privacy Shield -järjestelyn kolmannen vuotuisen tarkastelun yhteydessä, että se oli havainnut 669 totuudenvastaista väitettä osallistumisesta tietosuojakehykseen (lokakuun 2018 ja lokakuun 2019 välisenä aikana). Suurin osa niistä korjattiin kauppaministeriön varoituskirjeen jälkeen, mutta 143 tapausta siirrettiin liittovaltion kauppakomission käsiteltäväksi (ks. jäljempänä oleva johdanto-osan 62 kappale). Ks. komission yksiköiden valmisteluasiakirja SWD(2019) 495 final, s. 10.

2.3.4 Täytäntöönpano

- (58) Sen varmistamiseksi, että tietosuojan riittävä taso taataan käytännössä, tarvitaan riippumaton valvontaviranomainen, jonka tehtävänä on seurata tietosuojasääntöjen noudattamista ja varmistaa niiden täytäntöönpano.
- (59) Tietosuojakehykseen osallistuvien organisaatioiden on kuuluttava Yhdysvaltojen toimivaltaisten viranomaisten eli liittovaltion kauppakomission ja liikenneministeriön toimivaltaan. Näillä viranomaisilla on tarvittavat tutkinta- ja täytäntöönpanovaltuudet, joiden ansiosta ne voivat tehokkaasti varmistaa järjestelyn periaatteiden noudattamisen ⁽⁹¹⁾.
- (60) Liittovaltion kauppakomissio on riippumaton viranomainen, joka koostuu viidestä jäsenestä. Presidentti nimittää kauppakomission senaattia kuullen ja sen suostumuksella ⁽⁹²⁾. Komission jäsenet nimitetään seitsemäksi vuodeksi, ja presidentti voi erottaa heidät vain työn tehottomuuden, velvollisuuksien laiminlyömisestä tai virka-aseman väärinkäytön vuoksi. Liittovaltion kauppakomissiossa voi olla enintään kolme jäsentä samasta poliittisesta puolueesta, eivätkä komission jäsenet voi nimityksensä aikana harjoittaa muuta liiketoimintaa, ammattia tai työtä.
- (61) Liittovaltion kauppakomissio voi tutkia periaatteiden noudattamista sekä totuudenvastaisia väitteitä järjestelyn periaatteiden noudattamisesta tai osallistumisesta tietosuojakehykseen sellaisissa organisaatioissa, jotka eivät ole enää tietosuojakehyksen osallistujaluettelossa tai jotka eivät ole koskaan antaneet varmennusta ⁽⁹³⁾. Liittovaltion kauppakomissio voi toteuttaa täytäntöönpanotoimia hakemalla väliaikaisia tai pysyviä kieltokanteita tai muita korjaavia toimenpiteitä koskevia hallinnollisia tai liittovaltion tuomioistuimen määräyksiä (mukaan lukien sovintoratkaisujen kautta annetut "suostumusmääräykset") ⁽⁹⁴⁾, ja se seuraa järjestelmällisesti tällaisten määräysten noudattamista ⁽⁹⁵⁾. Jos organisaatio ei noudata tällaisia määräyksiä, liittovaltion kauppakomissio voi hakea siviilioikeudellisia seuraamuksia ja muita korjaavia toimenpiteitä, mukaan lukien seuraamukset lainvastaisen toiminnan aiheuttamasta vahingosta. Tietosuojakehykseen osallistuvalla organisaatiolla annettuun suostumusmääräykseen liittyy omatoimista raportointia koskevia säännöksiä ⁽⁹⁶⁾, ja organisaatioiden on julkaistava kaikki liittovaltion kauppakomissiolle toimitettuun, periaatteiden noudattamista koskevaan kertomukseen tai arviointikertomukseen sisältyvät tietosuojakehykseen liittyvät osuudet. Lisäksi liittovaltion kauppakomissio pitää verkossa yllä luetteloa organisaatioista, joille on annettu kauppakomission tai tuomioistuimen määräys tietosuojakehykseen liittyvissä tapauksissa ⁽⁹⁷⁾.
- (62) Privacy Shield -järjestelyn puitteissa liittovaltion kauppakomissio toteutti lainvalvontatoimia noin 22 tapauksessa sekä järjestelyn erityisvaatimusten noudattamatta jättämisen takia (kun organisaatio esimerkiksi ei ollut toimittanut kauppaministeriölle vahvistusta siitä, että se oli jatkanut Privacy Shield -järjestelyn suoja-toimien soveltamista järjestelystä poistumisensa jälkeen, tai organisaatio ei ollut tarkastanut tai antanut ulkopuolisen tahon tarkastaa periaatteiden noudattamista) ⁽⁹⁸⁾ että järjestelyyn osallistumista koskevien totuudenvastaisten väitteiden takia (kun organisaatio esimerkiksi ei ollut saattanut kaikkia varmennuksen edellyttämiä vaiheita päätökseen tai organisaatio oli antanut varmennuksensa raueta mutta esitti virheellisiä lausumia osallistumisensa jatkumisesta) ⁽⁹⁹⁾. Nämä lainvalvontatoimet johtuivat muun muassa hallinnollisten haasteiden ennakoivasta käyttämisestä näytön saamiseksi tietyiltä Privacy Shield -järjestelyn osallistujilta, jotta voitaisiin tarkastaa, onko Privacy Shield -järjestelyn velvoitteita rikottu olennaisesti ⁽¹⁰⁰⁾.

⁽⁹¹⁾ Tietosuojakehykseen osallistuvan organisaation on ilmoitettava julkisesti, että se on sitoutunut noudattamaan järjestelyn periaatteita, julkistettava tietosuojaperiaatteensa järjestelyn periaatteiden mukaisesti ja pantava ne kaikilta osin täytäntöön. Jos organisaatio ei noudata periaatteita, siihen voidaan kohdistaa toimia liittovaltion kauppakomissiosta annetun lain (FTC Act) 5 §:n nojalla. Kyseisessä säännöksessä kielletään kaupankäynnissä toteutettavat tai kaupankäyntiin vaikuttavat epäoikeudenmukaiset ja harhaanjohtavat toimet (15 U.S.C. 45 §). Lisäksi organisaatioon sovelletaan 49 U.S.C. 41712 §:ää, jossa kielletään liikenteenharjoittajaa tai lipunvälittäjää harjoittamasta epäoikeudenmukaista tai harhaanjohtavaa menettelyä lentoliikenteessä tai lentokuljetusten myynnissä.

⁽⁹²⁾ 15 U.S.C. 41 §.

⁽⁹³⁾ Liite IV.

⁽⁹⁴⁾ Liittovaltion kauppakomissiolta saatujen tietojen mukaan sillä ei ole toimivaltaa tehdä yksityisyyden suojaan liittyviä tarkastuksia paikan päällä. Sillä on kuitenkin valta velvoittaa organisaatiot esittämään asiakirjoja ja antamaan todistajanlausuntoja (ks. liittovaltion kauppakomissiosta annetun lain 20 §), ja se voi viedä asian tuomioistuimeen, jos tällaisia määräyksiä ei noudateta.

⁽⁹⁵⁾ Ks. liite IV, jakso "Määräysten hakeminen ja niiden noudattamisen valvonta".

⁽⁹⁶⁾ Kauppakomission tai tuomioistuimen määräyksissä voidaan vaatia yrityksiä toteuttamaan yksityisyydensuojaa koskevia ohjelmia ja antamaan kauppakomissiolle säännöllisesti kertomus järjestelyn periaatteiden noudattamisesta tai riippumattoman kolmannen osapuolen arviointi kyseisistä ohjelmista.

⁽⁹⁷⁾ Liite IV, jakso "Määräysten hakeminen ja niiden noudattamisen valvonta".

⁽⁹⁸⁾ Ks. komission yksiköiden valmisteluasiakirja SWD(2019) 495 final, s. 11.

⁽⁹⁹⁾ Ks. liittovaltion kauppakomission verkkosivustolla oleva tapausluettelo osoitteessa <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. Ks. myös komission yksiköiden valmisteluasiakirjat SWD(2017) 344 final, s. 17, SWD(2018) 497 final, s. 12, ja SWD(2019) 495 final, s. 11.

⁽¹⁰⁰⁾ Ks. esimerkiksi Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

- (63) Yleisesti ottaen liittovaltion kauppakomissio on viime vuosina toteuttanut useissa tapauksissa täytäntöönpanotoimia, jotka koskevat myös EU:n ja Yhdysvaltojen tietosuojakehykseen sisältyvien yksittäisten tietosuojavaatimusten noudattamista. Näissä on ollut kyse esimerkiksi käyttötarkoituksen rajoittamisen ja tietojen säilyttämisen periaatteista ⁽¹⁰¹⁾, tietojen minimoinnista ⁽¹⁰²⁾, tietoturvasta ⁽¹⁰³⁾ ja tietojen täsmällisyydestä ⁽¹⁰⁴⁾.
- (64) Liikenneministeriöllä on yksinomainen toimivalta säännellä lentoyhtiöiden yksityisyydensuojakäytäntöjä, ja se jakaa toimivallan liittovaltion kauppakomission kanssa niiden yksityisyydensuojakäytäntöjen osalta, joita lipunkirjoittajat soveltavat lentoliikennepalvelujen myynnissä. Liikenneministeriön virkamiehet pyrkivät asiassa sovintoon, ja jos sitä ei saavuteta, heillä on valtuudet panna vireille täytäntöönpanomenettely. Menettelyyn kuuluu istunto, jossa esitetään todisteita ja jota johtaa liikenneministeriön hallintolainkäytöstä vastaava tuomari, jolla on valtuudet antaa kieltomääräyksiä ja määrätä siviilioikeudellisia seuraamuksia ⁽¹⁰⁵⁾. Hallintolainkäytöstä vastaavat tuomarit hyötyvät useista hallintomenettelylain (Administrative Procedure Act, APA) mukaisista suojatoimista, jotka takaavat heidän riippumattomuutensa ja puolueettomuutensa. Heidät voidaan esimerkiksi erottaa vain hyvästä syystä, tapaukset jaetaan heille vuorotteluperiaatteella, he eivät saa suorittaa tehtäviä, jotka ovat ristiriidassa hallintolainkäytöstä vastaavan tuomarin tehtävien ja velvollisuuksien kanssa, he eivät kuulu sen viranomaisen tutkintaryhmän valvonnan piiriin, jonka palveluksessa he ovat (tässä tapauksessa liikenneministeriö), ja heidän on hoidettava päätäntä-/lainvalvontatehtävänsä puolueettomasti ⁽¹⁰⁶⁾. Liikenneministeriö on sitoutunut seuraamaan täytäntöönpanomääräysten noudattamista ja varmistamaan, että tietosuojakehykseen liittyvissä asioissa annetut määräykset ovat saatavilla sen verkkosivustolla ⁽¹⁰⁷⁾.

2.4 Oikeussuojakeinot

- (65) Jotta voidaan varmistaa yksilön oikeuksien asianmukainen suojelu ja täytäntöönpano, rekisteröidyllä olisi oltava tehokkaat hallinnolliset ja oikeudelliset oikeussuojakeinot.
- (66) Tietosuojakehykseen sisältyvässä muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteessa (Recourse, Enforcement and Liability Principle) edellytetään, että organisaatiot tarjoavat henkilöille, joihin järjestelyn periaatteiden noudattamatta jättäminen on vaikuttanut, mahdollisuuden muutoksenhakuun. Näin unionin rekisteröidyillä on mahdollisuus tehdä valitus, kun tietosuojakehykseen kuuluvat organisaatiot eivät noudata periaatteita, ja saada valitukseen ratkaisu, tarvittaessa päätöksellä, jossa määrätään tehokkaista korjaustoimenpiteistä ⁽¹⁰⁸⁾. Varmennuksen osana organisaatioiden on täytettävä muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen vaatimukset ottamalla käyttöön tehokkaat ja helposti saatavilla olevat riippumattomat muutoksenhakumekanismit, jotta kunkin henkilön valitukset ja riitapaukset voidaan tutkia ja ratkaista nopeasti ilman kyseiselle henkilölle aiheutuvia kuluja ⁽¹⁰⁹⁾.

⁽¹⁰¹⁾ Ks. esim. liittovaltion kauppakomission määräys asiassa Drizly, LLC., jossa muun muassa vaaditaan yritystä 1) tuhoamaan keräämänsä henkilötiedot, jotka eivät ole tarpeen tuotteiden tai palvelujen tarjoamiseksi kuluttajille, ja 2) pidättäytymään keräämästä tai tallentamasta henkilökohtaista tietoa, paitsi jos se on tarpeen säilytysaikataulussa mainittuja erityisiä tarkoituksia varten.

⁽¹⁰²⁾ Ks. esim. liittovaltion kauppakomission määräys asiassa CafePress (24. maaliskuuta 2022), jossa vaaditaan muun muassa minimoimaan kerättävien tietojen määrä.

⁽¹⁰³⁾ Ks. esim. liittovaltion kauppakomission täytäntöönpanotoimet asioissa Drizzly, LLC ja CafePress, joilla se vaati asianomaisia yrityksiä ottamaan käyttöön erityisen tietoturvaohjelman tai toteuttamaan tiettyjä tietoturvatavoitteita. Tietosuojaloukkauksista ks. myös liittovaltion kauppakomission 27. tammikuuta 2023 antama määräys asiassa Chegg, Equifaxin kanssa vuonna 2019 saavutettu sovintoratkaisu (<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⁾ Ks. esim. asia RealPage, Inc (16. lokakuuta 2018), jossa liittovaltion kauppakomissio toteutti luottokelpoisuusraportointia koskevan lain (FCRA) nojalla täytäntöönpanotoimia vuokralaisten seulontaa harjoittavaa yritystä vastaan. Yritys toimitti yksityishenkilöistä kiinteistöjen omistajille ja kiinteistöyhtiöille taustaraportteja, jotka perustuivat vuokrahistoriatietoihin, julkisiin rekisteritietoihin (mukaan lukien rikos- ja häätöhistoriat) ja luottotietoihin ja joita käytettiin vuokralaisten valinnassa. Kauppakomissio totesi, että yritys ei ollut toteuttanut kohtuullisiksi katsottavia toimenpiteitä varmistaa automaattisen päätöksentekosovelluksen pohjalta toimittamiensa tietojen paikkansapitävyyden.

⁽¹⁰⁵⁾ Ks. liite V, jakso "Täytäntöönpanokäytännöt".

⁽¹⁰⁶⁾ Ks. 5 U.S.C. 3105 §, 7521 §:n a momentti, 554 §:n d momentti ja 556 §:n b momentin 3 kohta.

⁽¹⁰⁷⁾ Liite V, jakso "EU:n ja Yhdysvaltojen tietosuojakehyksen rikkomisen vuoksi annettujen täytäntöönpanomääräysten seuranta ja julkistaminen".

⁽¹⁰⁸⁾ Liite I, II jakson 7 kohta.

⁽¹⁰⁹⁾ Liite I, III jakson 11 kohta.

- (67) Organisaatiot voivat valita joko unionissa tai Yhdysvalloissa toimivan riippumattoman muutoksenhakumekanismin. Kuten johdanto-osan 73 kappaleessa tarkennetaan, tähän sisältyy mahdollisuus sitoutua vapaaehtoisesti yhteistyöhön EU:n tietosuojaviranomaisten kanssa. Kun organisaatiot käsittelevät henkilöstötietoja, sitoutuminen yhteistyöhön EU:n tietosuojaviranomaisten kanssa on pakollista. Muita vaihtoehtoja ovat riippumaton vaihtoehtoinen riitojenratkaisu ja yksityisellä sektorilla laaditut yksityisyydensuojaohjelmat, joiden sääntöihin järjestelyn periaatteet sisältyvät. Viimeksi mainittujen tulee sisältää myös tehokkaat täytäntöönpanomekanismit muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti.
- (68) Näin ollen tietosuojakehys tarjoaa rekisteröidyille useita mahdollisuuksia käyttää oikeuksiaan ja tehdä valituksia, kun EU:n ja Yhdysvaltojen organisaatiot eivät noudata järjestelyn periaatteita, sekä saada valitukseensa ratkaisu, tarvittaessa päätöksellä, jossa määrätään tehokkaasta korjaustoimenpiteestä. Henkilöt voivat tehdä valituksen suoraan organisaatiolle, organisaation nimeämälle riippumattomalle riitojenratkaisuelimelle, kansallisille tietosuojaviranomaisille, kauppaministeriölle tai liittovaltion kauppakomissiolle. Jos valitusta ei ole voitu ratkaista millään näistä muutoksenhaku- tai täytäntöönpanomekanismeista, henkilöillä on myös oikeus turvautua sitovaan välimiesmenettelyyn (tämän päätöksen liitteen I liite I). Lukuun ottamatta välimiespaneelia, joka edellyttää, että tietyt oikeussuojakeinot on jo käytetty, henkilöt voivat vapaasti turvautua mihin tahansa valitsemaansa oikeussuojakeinoon tai niihin kaikkiin, eikä heidän tarvitse valita mitään tiettyä menettelyä jonkin toisen sijaan tai käyttää niitä tietyssä järjestyksessä.
- (69) Unionin rekisteröidyt voivat saattaa järjestelyn periaatteiden noudattamatta jättämiseen liittyvät tapaukset käsiteltäväksi ottamalla suoraan yhteyttä tietosuojakehykseen osallistuviin organisaatioihin ⁽¹¹⁰⁾. Valitusten käsittelyn helpottamiseksi organisaation on otettava käyttöön tehokas oikeussuojamekanismi. Organisaation tietosuojaperiaatteissa on tätä varten ilmoitettava selvästi yhteyspiste, joka toimii joko organisaatiossa tai sen ulkopuolella ja joka käsittelee valitukset (mukaan lukien unionissa mahdollisesti sijaitsevat asiaankuuluvat elimet, jotka voivat vastata tiedusteluihin tai valituksiin), sekä nimetty riippumaton riitojenratkaisuelin (ks. johdanto-osan 70 kappale). Saatuaan valituksen joko suoraan kyseiseltä henkilöltä tai kauppaministeriöltä, kun tietosuojaviranomainen on siirtänyt asian käsittelyn sille, organisaation on toimitettava vastaus unionin rekisteröidylle 45 päivän kuluessa ⁽¹¹¹⁾. Samoin organisaatioiden on vastattava viipymättä järjestelyn periaatteiden noudattamista koskeviin tiedusteluihin ja muihin tietopyyntöihin, jotka on tehnyt kauppaministeriö tai tietosuojaviranomainen ⁽¹¹²⁾ (jos organisaatio on sitoutunut tekemään yhteistyötä tietosuojaviranomaisen kanssa).
- (70) Henkilöt voivat esittää valituksen myös suoraan (joko Yhdysvalloissa tai unionissa olevalle) riippumattomalle riitojenratkaisuelimelle, jonka organisaatio on nimittänyt tutkimaan ja ratkaisemaan yksittäiset valitukset (elleivät ne ole ilmeisen perusteettomia tai aiheettomia) ja tarjoamaan asianmukaisen ja ilmaisen muutoksenhakumennettelyn ⁽¹¹³⁾. Tällaisen elimen määrittämien seuraamusten ja oikeussuojakeinojen on oltava riittävän tiukkoja sen varmistamiseksi, että organisaatiot noudattavat järjestelyn periaatteita ja peruuttavat tai korjaavat periaatteiden noudattamatta jättämisestä aiheutuvat vaikutukset ja olosuhteista riippuen lopettavat henkilötietojen jatkokäsittelyn ja/tai poistavat ne. Lisäksi periaatteiden noudattamatta jättämistä koskevat havainnot on julkistettava ⁽¹¹⁴⁾. Organisaation nimeämien riippumattomien riitojenratkaisuelimien on sisällytettävä julkisille verkkosivuilleen asiaankuuluvat tiedot, jotka koskevat tietosuojakehystä ja niiden sen puitteissa tarjoamia palveluja ⁽¹¹⁵⁾. Niiden on julkaistava vuosittain kertomus, jossa esitetään näitä palveluja koskevat kootut tilastot ⁽¹¹⁶⁾.

⁽¹¹⁰⁾ Liite I, III jakson 11 kohdan d alakohdan i alakohta.

⁽¹¹¹⁾ Liite I, III jakson 11 kohdan d alakohdan i alakohta.

⁽¹¹²⁾ Tämän käsittelevän viranomaisen nimittämä tietosuojaviranomaisten paneeli tietosuojaviranomaisten roolia koskevan täydentävän periaatteen mukaisesti (liite I, III jakson 5 kohta).

⁽¹¹³⁾ Liite I, III jakson 11 kohdan d alakohta.

⁽¹¹⁴⁾ Liite I, II jakson 7 kohta ja III jakson 11 kohdan e alakohta.

⁽¹¹⁵⁾ Liite I, III jakson 11 kohdan d alakohdan ii alakohta.

⁽¹¹⁶⁾ Vuosikertomuksen on sisällettävä 1) kertomusvuoden aikana vastaanotettujen tietosuojakehykseen liittyvien valitusten yhteismäärä, 2) vastaanotettujen valitusten tyypit, 3) riitojenratkaisuun liittyvät laatutoimenpiteet, kuten valitusten käsittelyajan pituus, ja 4) valitusten tulokset, erityisesti määrättyjen oikeussuojakeinojen tai seuraamusten määrät ja tyypit.

- (71) Periaatteiden noudattamista koskevien tarkastelumenettelyjen osana kauppaministeriö varmistaa, että tietosuojakehykseen osallistuvat organisaatiot ovat todella rekisteröityneet niihin riippumattomiin muutoksenhakumekanismeihin, joihin ne väittävät rekisteröityneensä ⁽¹¹⁷⁾. Organisaatioiden ja vastuussa olevien riippumattomien muutoksenhakumekanismien on vastattava nopeasti tietosuojakehystä koskeviin kauppaministeriön tiedusteluihin ja tietopyyntöihin. Kauppaministeriö tekee yhteistyötä riippumattomien muutoksenhakumekanismien kanssa varmistaakseen, että niiden verkkosivustoilla on tietoja järjestelyn periaatteista ja niiden tietosuojakehyksen puitteissa tarjoamista palveluista ja että ne julkaisevat vuosikertomuksia ⁽¹¹⁸⁾.
- (72) Jos organisaatio ei noudata riitojenratkaisu- tai itsesääntelyelimen päätöstä, tämän on ilmoitettava sovellettavien periaatteiden noudattamatta jättämisestä kauppaministeriölle ja liittovaltion kauppakomissiolle (tai muulle Yhdysvaltojen viranomaiselle, jolla on toimivalta tutkia organisaatiossa tapahtuvaa noudattamatta jättämistä) tai toimivaltaiselle tuomioistuimelle ⁽¹¹⁹⁾. Jos organisaatio kieltäytyy noudattamasta jonkin yksityisyyden suojan itsesääntelystä vastaavan tahon, riippumattoman riitojenratkaisuelimen tai valtiollisen elimen lopullista päätöstä tai jos tällainen elin katsoo, että organisaatio jättää toistuvasti järjestelyn periaatteet noudattamatta, se voidaan katsoa periaatteiden jatkuvaksi noudattamatta jättämiseksi. Tämän seurauksena organisaatio poistetaan tietosuojakehyksen osallistujaluettelosta, kun kauppaministeriö on ilmoittanut tästä kyseiselle organisaatiolle 30 päivää etukäteen ja antanut periaatteita rikkoneelle organisaatiolle mahdollisuuden esittää vastineensa ⁽¹²⁰⁾. Jos organisaatio luettelosta poistamisen jälkeen väittää edelleen osallistuvansa tietosuojakehykseen, kauppaministeriö siirtää asian liittovaltion kauppakomission tai muun toimivaltaisen lainvalvontaviraston käsiteltäväksi ⁽¹²¹⁾.
- (73) Kolmanneksi yksityishenkilöt voivat tehdä valituksensa myös jollekin unionin kansalliselle tietosuojaviranomaiselle, joka voi käyttää asetuksen (EU) 2016/679 mukaisia tutkinta- ja ratkaisuvaltuuksiaan. Organisaatiot ovat velvollisia tekemään yhteistyötä, kun tietosuojaviranomaiset tutkivat valituksia ja tekevät niitä koskevia päätöksiä, joko silloin, kun valitus koskee työsuhteen yhteydessä kerättyjen henkilöstötietojen käsittelyä, tai kun asianomainen organisaatio on vapaaehtoisesti suostunut tietosuojaviranomaisten valvontaan ⁽¹²²⁾. Organisaatioiden on erityisesti vastattava tiedusteluihin, noudatettava tietosuojaviranomaisen antamia lausuntoja, mukaan lukien korjaavat tai korvaavat toimenpiteet, ja toimitettava tietosuojaviranomaiselle kirjallinen vahvistus siitä, että kyseiset toimenpiteet on toteutettu ⁽¹²³⁾. Jos tietosuojaviranomaisen antamia kehotuksia ei noudateta, tietosuojaviranomainen siirtää tapauksen kauppaministeriölle (joka voi poistaa organisaation tietosuojakehyksen osallistujaluettelosta) tai mahdollisten täytäntöönpanotoimien osalta liittovaltion kauppakomissiolle tai liikenneministeriölle (kieltäytyminen yhteistyöstä tietosuojaviranomaisen kanssa tai järjestelyn periaatteiden noudattamisesta voi Yhdysvaltain lainsäädännön mukaan johtaa seuraamuksiin) ⁽¹²⁴⁾.
- (74) Jotta yhteistyössä tapahtuva valitusten käsittely olisi tehokkaampaa, sekä kauppaministeriö että liittovaltion kauppakomissio ovat perustaneet erityisen yhteyspisteen, joka vastaa yhteydenpidosta suoraan tietosuojaviranomaisten kanssa ⁽¹²⁵⁾. Nämä yhteyspisteet auttavat tietosuojaviranomaisen tiedusteluissa, jotka koskevat järjestelyn periaatteiden noudattamista organisaatioissa.
- (75) Tietosuojaviranomainen ⁽¹²⁶⁾ antaa lausunnon, kun kiistan molemmilla osapuolilla on ollut asianmukainen tilaisuus esittää haluamansa huomiot ja todistusaineisto. Paneeli voi antaa lausunnon niin nopeasti kuin asianmukainen menettely sallii, yleensä 60 päivän kuluessa valituksen vastaanottamisesta ⁽¹²⁷⁾. Jos organisaatio ei noudata lausuntoa 25 päivän kuluessa sen antamisesta eikä anna mitään tyydyttävää selitystä viivästykselle, paneeli voi ilmoittaa aikomuksestaan joko saattaa asia kauppakomissiolle (tai muulle Yhdysvaltojen toimivaltaiselle täytäntöönpanoviranomaiselle) tai katsoa, että yhteistyötä koskevaa sitoumusta on rikottu vakavasti. Ensimmäisessä tapauksessa tämä voi johtaa liittovaltion kauppakomissiosta annetun lain 5 §:n (tai vastaavan säädöksen) mukaisiin täytäntöönpa-

⁽¹¹⁷⁾ Liite I, jakso "Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät".

⁽¹¹⁸⁾ Ks. liite III, jakso "Kauppaministeriö edistää yhteistyötä järjestelyn periaatteisiin liittyviä palveluja tarjoavien vaihtoehtoisten riitojenratkaisuelinten kanssa". Ks. myös liite I, III jakson 11 kohdan d alakohdan ii ja iii alakohta.

⁽¹¹⁹⁾ Ks. liite I, III jakson 11 kohdan e alakohta.

⁽¹²⁰⁾ Ks. liite I, III jakson 11 kohdan g alakohta, erityisesti ii ja iii alakohta.

⁽¹²¹⁾ Ks. liitteen III jakso "Tietosuojakehykseen osallistumista koskevien totuudenvastaisten väitteiden havaitseminen ja niihin puuttuminen".

⁽¹²²⁾ Liite I, II jakson 7 kohdan b alakohta.

⁽¹²³⁾ Liite I, III jakson 5 kohta.

⁽¹²⁴⁾ Liite I, III jakson 5 kohdan c alakohdan ii alakohta.

⁽¹²⁵⁾ Liite III (ks. jakso "Kauppaministeriö helpottaa yhteistyötä tietosuojaviranomaisten kanssa") ja liite IV (ks. jaksot "Etusijan antaminen valitusten käsittelemiselle ja tutkimukset" ja "Lainvalvontayhteistyö EU:n tietosuojaviranomaisten kanssa").

⁽¹²⁶⁾ Tietosuojaviranomaisen olisi laadittava tietosuojaviranomaisten epävirallisen paneelin työjärjestys työnsä ja keskinäisen yhteistyön organisointia koskevan toimivaltansa perusteella.

⁽¹²⁷⁾ Liite I, III jakson 5 kohdan c alakohdan i alakohta.

notoimiin ⁽¹²⁸⁾. Jälkimmäisessä tapauksessa paneeli ilmoittaa asiasta kauppaministeriölle, joka katsoo, että jos organisaatio kieltäytyy noudattamasta tietosuojaviranomaisten paneelin lausuntoa, kyseessä on periaatteiden jatkuva noudattamatta jättäminen. Tällöin organisaatio poistetaan tietosuojakehyksen osallistujaluettelosta.

- (76) Jos tietosuojaviranomainen, jolle valitus on osoitettu, ei ole toteuttanut toimenpiteitä tai ne ovat riittämättömiä valituksen käsittelemiseksi, valituksen tekijällä on mahdollisuus hakea muutosta toimenpiteiden tai niiden puuttumisen johdosta kyseisen EU:n jäsenvaltion kansallisissa tuomioistuimissa.
- (77) Henkilöt voivat tehdä valituksen tietosuojaviranomaiselle myös silloin, kun tietosuojaviranomaisten paneelia ei ole nimetty organisaation riitojenratkaisuelimeksi. Näissä tapauksissa tietosuojaviranomainen voi saattaa tällaiset valitukset joko Yhdysvaltojen kauppaministeriön tai liittovaltion kauppakomission käsiteltäväksi. Yhteistyön helpottamiseksi ja lisäämiseksi tapauksissa, joissa on kyse henkilöiden tekemistä valituksista tai joissa tietosuoja-kehukseen osallistuva organisaatio ei ole noudattanut periaatteita, kauppaministeriö perustaa erityisen yhteyspisteen pitämään yhteyttä tietosuojaviranomaisiin ja avustamaan niitä tutkimuksissa, jotka koskevat järjestelyn periaatteiden noudattamista organisaatiossa ⁽¹²⁹⁾. Lisäksi liittovaltion kauppakomissio on sitoutunut perustamaan erityisen yhteyspisteen ⁽¹³⁰⁾.
- (78) Kauppaministeriö on sitoutunut vastaanottamaan, tarkastamaan ja parhaansa mukaan käsittelemään valitukset organisaatioista, jotka eivät ole noudattaneet järjestelyn periaatteita ⁽¹³¹⁾. Tätä varten kauppaministeriö laatii tietosuojaviranomaisille erityismenettelyt, joiden puitteissa valitukset siirretään erityisen yhteyspisteen käsiteltäväksi ja joiden puitteissa niitä seurataan ja niiden johdosta toteutetaan lisätoimia organisaatioiden kanssa ratkaisun löytymisen helpottamiseksi ⁽¹³²⁾. Yksittäisten valitusten käsittelyn jouduttamiseksi kyseinen yhteyspiste toimii sovellettavien periaatteiden noudattamista koskevilla kysymyksissä suoraan asiaankuuluvan tietosuojaviranomaisen kanssa ja erityisesti ilmoittaa tälle valitusten käsittelyn etenemisestä viimeistään 90 päivän kuluttua siitä, kun asia on siirretty sen käsiteltäväksi ⁽¹³³⁾. Tämän ansiosta rekisteröidyillä on mahdollisuus tehdä valitus suoraan kansalliselle tietosuojaviranomaiselle, kun tietosuojakehykseen osallistuvat organisaatiot eivät noudata sovellettavia periaatteita, ja saada valitus siirrettyä kauppaministeriölle, joka on tietosuojakehystä hallinnoiva viranomainen.
- (79) Jos kauppaministeriö toteaa viran puolesta tehtyjen tarkastusten, valitusten tai muiden tietojen perusteella, että organisaatio on jatkuvasti jättänyt noudattamatta järjestelyn periaatteita, se poistaa tällaisen organisaation tietosuoja-kehysten osallistujaluettelosta ⁽¹³⁴⁾. Jos organisaatio kieltäytyy noudattamasta minkä tahansa yksityisyyden suojan itsesääntelystä vastaavan tahon, riippumattoman riitojenratkaisuelimen tai valtiollisen elimen, mukaan lukien tietosuojaviranomainen, lopullista päätöstä, tämä katsotaan periaatteiden jatkuvaksi noudattamatta jättämiseksi ⁽¹³⁵⁾.
- (80) Tietosuojakehykseen osallistuvien organisaatioiden on kuuluttava Yhdysvaltojen toimivaltaisten viranomaisten – erityisesti liittovaltion kauppakomission ⁽¹³⁶⁾ – toimivaltaan. Näillä viranomaisilla on tarvittavat tutkinta- ja täytäntöönpanovaltuudet, joiden ansiosta ne voivat tehokkaasti varmistaa järjestelyn periaatteiden noudattamisen. Liittovaltion kauppakomissio asettaa etusijalle sellaiset järjestelyn periaatteiden noudattamatta jättämistä koskevat tapaukset, jotka on saatu riippumattomilta riitojenratkaisu- tai itsesääntelyelimiltä, kauppaministeriöltä ja tietosuoja-viranomaisilta (jotka toimivat joko omasta aloitteestaan tai valitusten perusteella), sen määrittämiseksi, onko liittovaltion kauppakomissiosta annetun lain 5 §:ää rikottu ⁽¹³⁷⁾. Liittovaltion kauppakomissio on sitoutunut luomaan vakiomuotoisen siirtomenettelyn, nimeämään yhteyspisteen käsittelemään tietosuojaviranomaisten sille siirtämiä tapauksia ja vaihtamaan tietoja tällä tavoin siirretyistä tapauksista. Lisäksi se voi ottaa suoraan vastaan henkilöiden tekemiä valituksia ja toteuttaa tietosuojakehykseen liittyviä tutkimuksia omasta aloitteestaan, erityisesti osana yksityisyyden suojaa koskevia laajempia tutkimuksiaan.

⁽¹²⁸⁾ Liite I, III jakson 5 kohdan c alakohdan ii alakohta.

⁽¹²⁹⁾ Ks. liite III, jakso "Kauppaministeriö helpottaa yhteistyötä tietosuojaviranomaisten kanssa".

⁽¹³⁰⁾ Ks. liite IV, jaksot "Etusijan antaminen valitusten käsittelemiselle ja tutkimukset" ja "Lainvalvontayhteistyö EU:n tietosuojaviranomaisten kanssa".

⁽¹³¹⁾ Liite III, jakso "Kauppaministeriö helpottaa yhteistyötä tietosuojaviranomaisten kanssa".

⁽¹³²⁾ Liite I, II jakson 7 kohdan e alakohta, ja liite III, jakso "Kauppaministeriö helpottaa yhteistyötä tietosuojaviranomaisten kanssa".

⁽¹³³⁾ Ks. edellinen alaviite.

⁽¹³⁴⁾ Liite I, III jakson 11 kohdan g alakohta.

⁽¹³⁵⁾ Liite I, III jakson 11 kohdan g alakohta.

⁽¹³⁶⁾ Tietosuojakehykseen osallistuvan organisaation on ilmoitettava julkisesti, että se on sitoutunut noudattamaan järjestelyn periaatteita, julkistettava tietosuojaperiaatteensa järjestelyn periaatteiden mukaisesti ja pantava ne kaikilta osin täytäntöön. Jos organisaatio ei noudata periaatteita, siihen voidaan kohdistaa lainvalvontatoimia FTC-lain 5 §:n nojalla. Säännöksessä kielletään kaupankäynnissä toteutettavat tai kaupankäyntiin vaikuttavat sopimattomat ja vilpilliset toimet.

⁽¹³⁷⁾ Ks. myös kauppaministeriön vastaavat sitoumukset, liite V.

- (81) Jos valitusta ei ole ratkaistu tyydyttävästi minkään muun oikeussuojamekanismin avulla, unionin rekisteröity voi turvautua viimesijaisena muutoksenhakumekanismina toimivan EU:n ja Yhdysvaltojen tietosuojakehyksen paneelin, jäljempänä 'tietosuojakehyksen paneeli', sitovaan välimiesmenettelyyn⁽¹³⁸⁾. Organisaatioiden on ilmoitettava henkilöille, että nämä voivat pyytää sitovaa välimiesmenettelyä, ja niillä on velvollisuus esittää vastineensa, kun henkilö on turvautunut tähän mahdollisuuteen toimittamalla ilmoituksen asianomaiselle organisaatiolle⁽¹³⁹⁾.
- (82) Tietosuojakehyksen paneeli koostuu vähintään kymmenestä välimiehestä, jotka kauppaministeriö ja komissio nimittävät heidän riippumattomuutensa ja nuhteettomuutensa ja heidän yksityisyydensuojaa koskevaan Yhdysvaltojen lainsäädäntöön ja unionin tietosuojalainsäädäntöön liittyvän kokemuksensa perusteella. Osapuolet valitsevat kunkin yksittäisen riita-asian käsittelyä varten välimiehistä yhden tai kolmen välimiehen⁽¹⁴⁰⁾ paneelin.
- (83) Kauppaministeriö on valinnut välimiesmenettelyjen hallinnoijaksi International Centre for Dispute Resolution -keskuksen, jäljempänä 'ICDR', joka on American Arbitration Association -yhdistyksen, jäljempänä 'AAA', kansainvälinen osasto. Tietosuojakehyksen paneelin menettelyissä sovelletaan sovittuja välimiesmenettelysääntöjä ja nimettyjä välimiehiä koskevia käytäntösääntöjä. ICDR:n ja AAA:n verkkosivusto tarjoaa henkilöille tiivistetyssä muodossa tietoa välimiesmenettelystä ja välimiesmenettelyn vireillepanomenettelystä.
- (84) Kauppaministeriön ja komission välillä sovitut välimiesmenettelyä koskevat säännöt täydentävät tietosuojakehystä, joka sisältää useita ominaisuuksia, joiden ansiosta mekanismi on paremmin unionin rekisteröityjen käytettävissä: i) kansallinen tietosuojaviranomainen voi avustaa rekisteröityä tämän valmistellessa vaatimustaan paneelin käsiteltäväksi, ii) vaikka välimiesmenettely tapahtuu Yhdysvalloissa, unionin rekisteröidyt voivat osallistua menettelyyn video- tai puhelinneuvottelussa, joka on henkilöille maksuton, iii) vaikka välimiesmenettelyssä käytettävä kieli on tavallisesti englantia, istunto voidaan periaatteessa tulkata ja aineisto kääntää perustellusta pyynnöstä ilman, että tästä aiheutuu rekisteröidylle kustannuksia, ja iv) vaikka kunkin osapuolen on maksettava omat asianajopalkkionsa, kauppaministeriö hoitaa tietosuojakehykseen osallistuvien organisaatioiden vuotuisista rahoitusosuuksista koostuvaa rahastoa, josta katetaan välimiesmenettelyn tukikelpoiset kustannukset sellaiseen enimmäismäärään asti, jonka Yhdysvaltojen viranomaiset määrittävät komissiota kuultuaan⁽¹⁴¹⁾.
- (85) Tietosuojakehyksen paneelilla on valtuudet määrätä yksilökohtaisesta, ei-rahallisesta kompensatiosta⁽¹⁴²⁾, joka on tarpeen järjestelyn periaatteiden noudattamatta jättämisen korjaamiseksi. Vaikka paneeli ottaa päätöstä tehdessään huomioon muut tietosuojakehyksen mekanismien perusteella toteutetut korjaavat toimenpiteet, henkilöt voivat silti turvautua välimiesmenettelyyn, jos ne pitävät näitä muita toimenpiteitä riittämättöminä. Näin unionin rekisteröidyt voivat vedota välimiesmenettelyyn kaikissa tapauksissa, joissa tietosuojakehykseen osallistuvien organisaatioiden, riippumattomien muutoksenhakumekanismien tai Yhdysvaltojen toimivaltaisten viranomaisten (kuten liittovaltion kauppakomission) toiminnan tai toimimatta jättämisen vuoksi valituksia ei ole ratkaistu tyydyttävästi. Välimiesmenettelyyn ei voida vedota, jos tietosuojaviranomaisella on toimivalta ratkaista vaatimus tietosuojakehykseen osallistuvan organisaation osalta, toisin sanoen tapauksissa, joissa organisaatio joko on velvollinen tekemään yhteistyötä tietosuojaviranomaisten kanssa ja noudattamaan ohjeita työsuhteen yhteydessä kerättyjen henkilöstötietojen käsittelyn osalta tai on vapaaehtoisesti sitoutunut tekemään niin. Henkilöt voivat vaatia välimiesoikeuden päätöksen täytäntöönpanoa Yhdysvaltojen tuomioistuimissa liittovaltion välimiesmenettelystä annetun lain (Federal Arbitration Act) nojalla ja varmistaa siten, että heidän käytössään on oikeussuojakeinoja, jos organisaatio ei noudata päätöstä.

⁽¹³⁸⁾ Ks. liitteen I liite I "Välimiesmenettelyä koskeva malli".

⁽¹³⁹⁾ Ks. liite I, II jakson 1 kohdan a alakohdan xi alakohta ja II jakson 7 kohdan c alakohta.

⁽¹⁴⁰⁾ Osapuolet sopivat paneelin välimiesten määrästä.

⁽¹⁴¹⁾ Liitteen I liite I, G kohdan 6 alakohta.

⁽¹⁴²⁾ Henkilöt eivät voi vaatia välimiesmenettelyssä vahingonkorvausta, mutta välimiesmenettelyyn vetoaminen ei sulje pois mahdollisuutta hakea vahingonkorvausta Yhdysvaltojen yleisissä tuomioistuimissa.

- (86) Jos organisaatio ei kunnioita sitoumustaan noudattaa järjestelyn periaatteita ja julkaistuja tietosuojaperiaatteita, Yhdysvaltojen lainsäädännön nojalla voi olla käytettävissä muita oikeussuojakeinoja, esimerkiksi mahdollisuus vaatia vahingonkorvauksia. Henkilöt voivat esimerkiksi tietyissä olosuhteissa käyttää oikeussuojakeinoja (mukaan lukien vahingonkorvausvaatimukset) Yhdysvaltojen kuluttajalainsäädännön nojalla, kun kyse on harhaanjohtavista lausumista taikka sopimattomista tai vilpillisistä toimista tai käytännöistä ⁽¹⁴³⁾, sekä vahingonkorvauslainsäädännön nojalla (erityisesti yksityiselämän loukkaus ⁽¹⁴⁴⁾, identiteettivarkaus ⁽¹⁴⁵⁾ ja yksityiselämää koskevien tietojen julkaiseminen ⁽¹⁴⁶⁾).
- (87) Edellä kuvatut eri muutoksenhakukeinot varmistavat yhdessä, että jokainen valitus, joka koskee EU:n ja Yhdysvaltojen tietosuojakehyksen vastaista varmennettujen organisaatioiden toimintaa, voidaan tosiasiallisesti käsitellä ja ratkaista.

3. VIRANOMAISTEN PÄÄSY EUROOPAN UNIONISTA YHDYSVALTOIHIN SIIRRETTYIHIN HENKILÖTIETOIHIIN JA NÄIDEN TIETOJEN KÄYTTÖ

- (88) Komissio on arvioinut myös niitä rajoituksia ja suojatoimia, mukaan lukien Yhdysvaltojen lainsäädännön mukaiset valvonta- ja oikeussuojamekanismit, jotka koskevat sitä, kuinka viranomaiset voivat kerätä ja käyttää yhdysvaltalaisille rekisterinpitäjille ja käsittelijöille siirrettyjä henkilötietoja yleisen edun mukaisia tarkoituksia ja erityisesti lainvalvontatarkoituksia ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten, jäljempänä 'viranomaisten pääsy tietoihin' ⁽¹⁴⁷⁾. Komissio ottaa huomioon useita kriteerejä arvioidessaan, vastaavatko edellytykset, joiden nojalla viranomaiset käyttävät Yhdysvaltoihin tämän päätöksen nojalla siirrettyjä tietoja, "olennaisilta osin" asetuksen (EU) 2016/679 45 artiklan 1 kohdassa esitettyjä vaatimuksia, sellaisena kuin unionin tuomioistuin on niitä tulkinnut perusoikeuskirjan valossa.
- (89) Kaikista henkilötietojen suojaa koskevan oikeuden rajoituksista on säädettävä lailla, ja näiden rajoitusten laajuus on määritettävä jo siinä oikeusperustassa, joka mahdollistaa puuttumisen näihin oikeuksiin ⁽¹⁴⁸⁾. Lisäksi sen oikeasuhteisuutta koskevan vaatimuksen täyttämiseksi, jonka mukaan henkilötietojen suojaa koskevia poikkeuksia ja rajoituksia on sovellettava vain siltä osin kuin se on ehdottoman välttämätöntä demokraattisessa yhteiskunnassa, jotta voidaan saavuttaa yleisen edun mukaiset tavoitteet, jotka vastaavat unionin tunnustamia tavoitteita, tässä oikeusperustassa on vahvistettava selkeät ja täsmälliset säännöt, joilla säännellään kyseisten toimenpiteiden soveltamisalaa ja soveltamista ja vahvistetaan vähimmäistakeet, niin että henkilöillä, joiden tietoja on siirretty, on riittävät takeet, joiden nojalla heidän henkilötietojensa suojataan tehokkaasti väärinkäytön riskiltä ⁽¹⁴⁹⁾. Lisäksi näiden

⁽¹⁴³⁾ Ks. kuluttajansuojalainsäädäntö: Kalifornia (Cal. Civ. Code 1750–1785 § (West) Consumers Legal Remedies Act), Kolumbian piirikunta (D.C. Code 28-3901 §), Florida (Fla. Stat. 501.201–501.213 §, Deceptive and Unfair Trade Practices Act), Illinois (815 Ill. Comp. Stat. 505/1–505/12, Consumer Fraud and Deceptive Business Practices Act) ja Pennsylvania (73 Pa. Stat. Ann. 201-1–201-9.3 § (West) Unfair Trade Practices and Consumer Protection Law).

⁽¹⁴⁴⁾ Toisin sanoen jos kyseessä on tahallinen puuttuminen henkilön yksityisasioihin tavalla, joka olisi järkevälle ja huolelliselle henkilölle erittäin loukkaava (Restatement (2nd) of Torts, 652 §:n b momentti).

⁽¹⁴⁵⁾ Vahingonkorvauslainsäädäntöä sovelletaan yleisesti silloin, kun henkilön identiteetti on varastettu tai hänen nimeään tai kuvaansa käytetään yrityksen tai tuotteen mainostamiseen tai johonkin vastaavaan kaupalliseen tarkoitukseen (ks. Restatement (2nd) of Torts, 652C §).

⁽¹⁴⁶⁾ Toisin sanoen kun henkilön yksityiselämää koskevat tiedot julkaistaan tavalla, joka olisi järkevälle ja huolelliselle henkilölle erittäin loukkaava, eivätkä tiedot ole yleisen oikeutetun edun mukaisia (Restatement (2nd) of Torts, 652D §).

⁽¹⁴⁷⁾ Tällä on merkitystä myös liitteessä I olevan I jakson 5 kohdan näkökulmasta. Tämän jakson ja vastaavasti yleisen tietosuoja-asetuksen nojalla tietosuojavaatimusten noudattamista ja yksityisyyden suojaa koskeviin periaatteisiin kuuluva oikeuksia voidaan rajoittaa. Tällaiset rajoitukset eivät kuitenkaan ole absoluuttisia, vaan niihin voidaan vedota vain useiden edellytysten täytyessä, esimerkiksi siltä osin kuin se on tarpeen tuomioistuimen määräyksen noudattamiseksi tai yleisen edun, lainvalvonnan tai kansallisen turvallisuuden vaatimusten täyttämiseksi. Tässä yhteydessä ja selkeyden vuoksi tässä jaksossa viitataan myös toimeenpanoasetuksessa EO 14086 vahvistettuihin edellytyksiin, joita arvioidaan muun muassa johdanto-osan 127–141 kappaleessa.

⁽¹⁴⁸⁾ Ks. Schrems II, 174 ja 175 kohta oikeuskäytäntöviittauksineen. Ks. jäsenvaltioiden viranomaisten pääsyn osalta myös asia C-623/17, Privacy International, ECLI:EU:C:2020:790, 65 kohta, ja yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, La Quadrature du Net ym., ECLI:EU:C:2020:791, 175 kohta.

⁽¹⁴⁹⁾ Ks. Schrems II, 176 ja 181 kohta oikeuskäytäntöviittauksineen. Ks. jäsenvaltioiden viranomaisten pääsyn osalta myös Privacy International, 68 kohta, ja La Quadrature du Net and Others, 132 kohta.

sääntöjen ja takeiden on oltava oikeudellisesti sitovia, ja yksittäisten henkilöiden on voitava vedota niihin tuomioistuimissa ⁽¹⁵⁰⁾. Rekisteröidyillä on erityisesti oltava mahdollisuus nostaa kanne riippumattomassa ja puolueettomassa tuomioistuimessa, jotta he voivat saada pääsyn henkilötietoihinsa tai saada ne oikaistuiksi tai poistetuiksi ⁽¹⁵¹⁾.

3.1 Yhdysvaltojen viranomaisten pääsy tietoihin ja niiden käyttö lainvalvontatarkoituksia varten

- (90) Yhdysvaltojen lainsäädännössä rajoitetaan eri tavoin pääsyä henkilötietoihin, jotka on siirretty tietosuojakehyksen puitteissa lainvalvontatarkoituksessa. Rajoitukset koskevat henkilötietoihin pääsyn ja niiden käytön lisäksi asiaa koskevia valvonta- ja oikeussuojamekanismeja. Nämä säännökset vastaavat vaatimuksia, joihin viitataan tämän päätöksen johdanto-osan 89 kappaleessa. Seuraavassa arvioidaan yksityiskohtaisesti edellytyksiä, joiden täytyessä pääsy henkilötietoihin voi toteutua, ja näiden toimivaltuuksien käyttöön sovellettavia suojatoimia. Yhdysvaltojen hallitus on (oikeusministeriön kautta) antanut vakuutuksen sovellettavista rajoituksista ja suojatoimista (tämän päätöksen liite VI).

3.1.1 Oikeusperustat, rajoitukset ja suojatoimet

3.1.1.1 Rajoitukset ja suojatoimet, jotka koskevat henkilötietojen keräämistä lainvalvontatarkoituksia varten

- (91) Yhdysvaltojen liittovaltion syyttäjät ja liittovaltion tutkijat pääsevät tarkastelemaan varmennettujen yhdysvaltalaisen organisaatioiden käsittelemiä henkilötietoja, joita on tarkoitus siirtää unionista tietosuojakehyksen puitteissa lainvalvontatarkoituksia varten erilaisissa menettelyissä, kuten johdanto-osan 92–99 kappaleessa tarkemmin selitetään. Näitä menettelyjä sovelletaan samalla tavalla rekisteröidyn kansalaisuudesta tai asuinpaikasta riippumatta, kun tiedot saadaan miltä tahansa yhdysvaltalaiselta organisaatiolta ⁽¹⁵²⁾.
- (92) Ensinnäkin tuomari voi liittovaltion lainvalvontaviranomaisen tai liittovaltion syyttäjän pyynnöstä antaa etsintäluvan tai määrätä takavarikon (joka voi koskea myös sähköisesti tallennettuja tietoja) ⁽¹⁵³⁾. Tällainen määräys voidaan antaa vain, jos on ”perusteltu syy” ⁽¹⁵⁴⁾ siihen, että takavarikoitavia esineitä (rikokseen viittaavia todisteita, laittomasti hallussa pidettäviä esineitä tai omaisuutta, joka on suunniteltu tai aiottu käytettäväksi rikoksen tekemisessä) on todennäköisesti löydettävissä etsintäluvassa yksilöidystä paikasta. Määräyksessä on yksilöitävä takavarikoitava omaisuus tai tavara ja nimettävä tuomari, jolle päätös on palautettava. Henkilö, johon etsintä kohdistuu tai jonka

⁽¹⁵⁰⁾ Ks. Schrems II, 181 ja 182 kohta.

⁽¹⁵¹⁾ Ks. Schrems I, 95 kohta, ja Schrems II, 194 kohta. Euroopan unionin tuomioistuin on tältä osin erityisesti korostanut, että perusoikeuskirjan 47 artiklan (oikeus tehokkain oikeussuojakeinoihin riippumattomassa ja puolueettomassa tuomioistuimessa) noudattaminen liittyy unionissa vaadittavaan tietosuojan tasoon ja että komission on todettava sen noudattaminen ennen kuin se tekee tietosuojan riittävyyttä koskevan päätöksen asetuksen (EU) 2016/679 45 artiklan 1 kohdan nojalla (Schrems II, 186 kohta).

⁽¹⁵²⁾ Ks. liite VI. Ks. esimerkiksi lakien Wiretap Act, Stored Communications Act ja Pen Register Act (käsitellään tarkemmin johdanto-osan 95–98 kappaleessa) osalta asia *Suzlon Energy Ltd v. Microsoft Corp.*, 671 F.3d 726, 729 (9. Cir. 2011).

⁽¹⁵³⁾ Rikosprosessia koskevat liittovaltion säännöt (Federal Rules of Criminal Procedure), sääntö 41. Yhdysvaltojen korkein oikeus vahvisti vuonna 2018 antamassaan tuomiossa (*Timothy Ivory Carpenter v. Yhdysvallat*, nro 16-402, 585 U.S. (2018)), että etsintälupa tai etsintälupaa koskeva poikkeus tarvitaan myös siihen, että lainvalvontaviranomaiset voivat saada pääsyn puhelinmastoihin perustuviin matkapuhelinten historiallisiin sijaintitietoihin, jotka antavat kattavan yleiskuvan käyttäjän liikkeistä, ja että käyttäjällä voi olla kohtuullinen luottamus yksityisyyteen tällaisten tietojen osalta. Näin ollen tällaisia tietoja ei yleensä voida saada matkapuhelin-yhteyksiltä tuomioistuimen määräyksen perusteella, vaikka olisi olemassa perusteltu syy olettaa, että tiedot ovat merkityksellisiä ja olennaisia käynnissä olevan rikostutkinnan kannalta. Tietojen saaminen edellyttää, että perustellun syyn olemassaolo osoitetaan määräyksen käyttämisen yhteydessä.

⁽¹⁵⁴⁾ Korkeimman oikeuden mukaan ”perusteltu syy” on käytännöllinen, ei-tekninen standardi, joka edellyttää sellaista tosiasioihin perustuvaa käytännöllistä ajattelua, johon järkevä ja harkitsevainen ihminen perustaa toimintansa (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Etsintäluvan osalta perustellun syyn katsotaan olevan osoitettu, jos on olemassa kohtuullinen todennäköisyys sille, että etsinnässä löydetään todisteita rikoksesta (viite sama kuin edellä).

omaisuutta etsintä koskee, voi vaatia, että laittomalla etsinnällä saadut todisteet hylätään, jos nämä todisteet esitetään häntä vastaan rikosoikeudenkäynnissä ⁽¹⁵⁵⁾. Kun tietojen haltijaa (esimerkiksi yritystä) vaaditaan tällaisen oikeuden määräyksen nojalla antamaan tiedot, se voi riitauttaa vaatimuksen kohtuuttomana rasitteena ⁽¹⁵⁶⁾.

- (93) Toiseksi suuri valamiehistö (tuomarin tai avustavan tuomarin valitsema tuomioistuimen tutkintaelin) voi antaa – yleensä liittovaltion syyttäjän pyynnöstä – tiettyjen vakavien rikosten tutkinnan yhteydessä haasteen ⁽¹⁵⁷⁾, jossa henkilöä vaaditaan esittämään tai luovuttamaan liiketoimintatietoja, sähköisesti tallennettuja tietoja tai muita aineellisia esineitä. Lisäksi eri laeissa säädetään hallinnollisten haasteiden käyttämisestä tutkimuksissa, jotka koskevat terveydenhuoltoalan petoksia, lasten kaltoinkohtelua, salaisen palvelun turvatoimia tai valvottuja aineita, sekä valvontaviranomaisen tutkimuksissa. Tällaisissa tutkimuksissa voidaan vaatia luovuttamaan liiketoimintatietoja, sähköisesti tallennettuja tietoja tai muita aineellisia esineitä ⁽¹⁵⁸⁾. Molemmista tapauksista tietojen on oltava tutkimuksen kannalta merkityksellisiä eikä haaste saa olla kohtuuton eli liian laaja tai rasittava (haasteen vastaanottaja voi riitauttaa sen näillä perusteilla) ⁽¹⁵⁹⁾.
- (94) Hyvin samankaltaisia ehtoja sovelletaan hallinnollisiin haasteisiin, joita annetaan Yhdysvalloissa toimivien yritysten hallussa olevien tietojen saamiseksi siviilihallinnon tai sääntelyn tarkoituksiin ("yleinen etu"). Siviilihallintoon ja sääntelyyn liittyvien viranomaisten toimivalta esittää tällaisia hallinnollisia haasteita on vahvistettava lainsäädännössä. Hallinnollisen haasteen käyttöön sovelletaan "kohtuustestiä", joka edellyttää, että tutkinta suoritetaan laillisessa tarkoituksessa, haasteen yhteydessä pyydetyt tiedot ovat merkityksellisiä tämän tarkoituksen kannalta, kyseisellä omaisella ei vielä ole haasteessa pyytämien tietojen ja kaikki haasteen esittämiseen tarvittavat hallinnolliset vaiheet on käyty läpi ⁽¹⁶⁰⁾. Korkeimman oikeuden oikeuskäytännössä on myös selvennetty tarvetta löytää tasapaino pyydettyihin tietoihin kohdistuvan yleisen edun ja yksityisyyden suojaa koskevien henkilökohtaisten ja organisatoristen intressien välillä ⁽¹⁶¹⁾. Vaikka hallinnollisen haasteen käyttö ei edellytä tuomioistuimen ennakko hyväksyntää, siihen sovelletaan tuomioistuinvalvontaa, jos vastaanottaja riitauttaa haasteen edellä mainituilla perusteilla tai jos haasteen antanut viranomainen pyrkii panemaan haasteen täytäntöön tuomioistuinteitse ⁽¹⁶²⁾. Näiden yleisten rajoitusten lisäksi yksittäisistä lainsäädännöksistä voi seurata tarkempia (tiukempia) vaatimuksia ⁽¹⁶³⁾.

⁽¹⁵⁵⁾ Ks. *Mapp v. Ohio*, 367 U.S. 643 (1961).

⁽¹⁵⁶⁾ Ks. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir.1979) (sen mukaan asianmukainen menettely edellyttää kuulemisen pitämistä rasitteesta ennen kuin puhelinyhtiö veloitetaan tukemaan etsintää) ja *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

⁽¹⁵⁷⁾ Yhdysvaltojen perustuslain viides lisäys edellyttää ns. suuren valamiehistön haastetta (grand jury indictment), kun kyseessä on kuolemanrangaistukseen johtava tai muu törkeä rikos. Suuressa valamiehistössä on 16–23 jäsentä, ja sen tehtävänä on selvittää, onko olemassa perusteltu syy uskoa, että rikos on tapahtunut. Tätä tehtävää varten suurella valamiehistöllä on tutkintavaltuudet, joiden nojalla se voi antaa haasteita.

⁽¹⁵⁸⁾ Ks. liite VI.

⁽¹⁵⁹⁾ Rikosprosessia koskevat liittovaltion säännöt (Federal Rules of Criminal Procedure), sääntö 17.

⁽¹⁶⁰⁾ *United States v. Powell*, 379 U.S. 48 (1964).

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

⁽¹⁶²⁾ Korkein oikeus on tämentänyt, että riitautetun hallinnollisen haasteen yhteydessä tuomioistuimen on tarkasteltava, 1) onko tutkinnalla lain mukainen tarkoitus, 2) onko kyseessä oleva haasteasia kongressin toimivallassa ja 3) "ovatko pyydetyt asiakirjat merkityksellisiä tutkinnan kannalta". Korkein oikeus on myös todennut, että hallinnollisen haasteen on oltava "kohtuullinen", eli siinä on määriteltävä "ne ja vain ne vaadittavat asiakirjat, jotka ovat riittäviä kyseisen tutkinnan tarpeisiin", sekä "kuvattava seikkaperäisesti suoritettavan etsinnän sijaintipaikka ja kiinniotettavat henkilöt tai takavarikoitavat asiat".

⁽¹⁶³⁾ Esimerkiksi taloudellisen yksityisyyden suojasta annetussa laissa (Right to Financial Privacy Act) annetaan valtion viranomaiselle valtuudet saada rahoituslaitoksen hallussa olevia taloudellisia tietoja hallinnollisen haasteen nojalla vain, jos 1) on syytä olettaa, että pyydetyt tiedot ovat merkityksellisiä lainvalvontaan liittyvän lainmukaisen tutkinnan kannalta ja 2) asiakkaalle on toimitettu haasteesta kopio sekä ilmoitus, jossa esitetään riittävän tarkasti tutkinnan luonne (12 U.S.C. § 3405). Toinen esimerkki on luottokelpoisuusraportointia koskeva laki (Fair Credit Reporting Act), jonka mukaan luottokelpoisuusyritykset eivät saa luovuttaa kuluttajätietoja hallinnollisten haasteiden perusteella (vaan ainoastaan suuren valamiehistön haasteen tai tuomioistuimen määräyksen perusteella, 15 U.S.C. 1681 § ja sitä seuraavat pykälät). Viestintätietojen saatavuuden osalta sovelletaan tallennettua viestintää koskevan lain (Stored Communications Act) erityisvaatimuksia, esimerkiksi suhteessa mahdollisuuteen käyttää tähän hallinnollisia haasteita (ks. johdanto-osan 96–97 kappale).

- (95) Kolmanneksi lainvalvontaviranomaiset voivat saada käyttöönsä viestintätietoja usean oikeusperustan nojalla. Tuomioistuimien voi määrätä, että puhelinnumeroa tai sähköpostiosoitetta koskevia reaaliaikaisia, ei-sisällöllisiä numeronvalinta-, reititys-, osoitteenmuodostus- ja merkinantotietoja saa kerätä (käyttämällä lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmää), jos se katsoo viranomaisen osoittaneen, että todennäköisesti saatavat tiedot ovat merkityksellisiä vireillä olevan rikostutkinnan kannalta ⁽¹⁶⁴⁾. Määräyksessä on ilmoitettava muun muassa epäillyn henkilöllisyys, jos se on tiedossa, tiedot viestinnästä, johon määräystä sovelletaan, ja rikkominen, johon kerättävät tiedot liittyvät. Lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmän käyttö voidaan sallia enintään 60 päivän ajaksi, ja määräaika voidaan jatkaa ainoastaan uudella tuomioistuimen määräyksellä.
- (96) Lisäksi on mahdollista saada lainvalvontatarkoituksia varten pääsy internetpalveluntarjoajien, puhelinyhtiöiden ja viestintäpalvelujen tarjoajien kolmansien osapuolten hallussa oleviin tilaajatietoihin, liikennetietoihin ja tallennettuun sisältöön tallennettua viestintää koskevan lain (Stored Communications Act) perusteella ⁽¹⁶⁵⁾. Jotta lainvalvontaviranomaiset voivat saada pääsyn sähköisen viestinnän tallennettuun sisältöön, niiden on saatava tuomarilta määräys, jonka perusteena on perusteltu syy olettaa, että kyseisellä tilillä on todisteita rikoksesta ⁽¹⁶⁶⁾. Lainvalvontaviranomaiset voivat hankkia haasteen saadakseen tilausasiakkaiden rekisteröintitietoja, IP-osoitteita ja niihin liittyviä aikaleimoja tai laskutustietoja. Useimpien muiden tallennettujen, ei-sisällöllisten tietojen tapauksessa, kuten sellaisten sähköpostiotsikoiden osalta, joista viestin aihe ei ilmene, lainvalvontaviranomaisen on saatava oikeuden määräys, jonka tuomari antaa, jos hän katsoo, että on olemassa perusteltu syy olettaa, että pyydytetyt tiedot ovat merkityksellisiä ja olennaisia vireillä olevan rikostutkinnan kannalta.
- (97) Kun palveluntarjoajat vastaanottavat tallennettua viestintää koskevan lain mukaisia pyyntöjä, ne voivat vapaaehtoisesti ilmoittaa asiasta asiakkaalle tai tilaajalle, jonka tietoja pyydetään, paitsi jos asianomainen lainvalvontaviranomainen saa turvaamismääräyksen, jossa kielletään tällainen ilmoittaminen ⁽¹⁶⁷⁾. Tällainen turvaamismääräys on tuomioistuimen määräys, jossa edellytetään, että sähköisten viestintäpalvelujen tai etäkäyttöpalvelujen tarjoaja, jolle etsintälupa, haaste tai tuomioistuimen määräys on osoitettu, ei ilmoita kenellekään muulle henkilölle etsintäluvan, haasteen tai tuomioistuimen määräyksen olemassaolosta tuomioistuimen aiheelliseksi katsomana aikana. Turvaamismääräys annetaan, jos tuomioistuin toteaa olevan syytä uskoa, että ilmoittaminen vaarantaisi vakavasti tutkinnan tai viivästyttäisi perusteettomasti oikeudenkäyntiä esimerkiksi siksi, että se voisi vaarantaa henkilön hengen tai fyysisen turvallisuuden taikka johtaa syytteenpanon välttelyyn tai mahdollisten todistajien pelotteluun. Varaoikeusministerin muistion (joka sitoo kaikkia oikeusministeriön asianajajia ja edustajia) mukaan syyttäjien on määritettävä yksityiskohtaisesti, miksi turvaamismääräys tarvitaan, ja perusteltava tuomioistuimelle turvaamismääräyksen antamisen lakisääteisten perusteiden täyttyminen kyseisessä tapauksessa ⁽¹⁶⁸⁾. Muistio edellyttää myös, että turvaamismääräyksiä koskevilla hakemuksilla ei yleisesti ottaen saa pyrkiä viivyttämään ilmoittamista yli vuodella. Jos poikkeustapauksessa tarvitaan kestoalta pidempiä määräyksiä, niitä voidaan hakea vain Yhdysvaltojen oikeusministerin tai asiasta vastaavan apulaisoikeusministerin nimeämän valtuutetun kirjallisella suostumuksella. Lisäksi syyttäjän on tutkinnan päättyessä välittömästi arvioitava, onko olemassa perusteita voimassa olevien turvaamismääräysten jatkamiselle, ja jos näin ei ole, lopetettava turvaamismääräyksen voimassaolo ja varmistettava, että palveluntarjoajalle ilmoitetaan asiasta ⁽¹⁶⁹⁾.

⁽¹⁶⁴⁾ 18 U.S.C. 3123 §.

⁽¹⁶⁵⁾ 18 U.S.C. 2701–2713 §.

⁽¹⁶⁶⁾ 18 U.S.C. 2701 §(a)–(b)(1)(A). Jos asianomaiselle tilaajalle tai asiakkaalle ilmoitetaan asiasta (joko etukäteen tai tietyissä olosuhteissa viivästyneellä ilmoituksella), yli 180 päivän ajalta tallennetut sisältötiedot voidaan hankkia myös hallinnollisen haasteen tai suuren valamiehaston haasteen perusteella (18 U.S.C. 2701 §:n b momentin 1 kohdan B alakohta) tai tuomioistuimen määräyksellä (jos on perusteltua syy olettaa, että tiedot ovat merkityksellisiä ja olennaisia käynnissä olevan rikostutkinnan kannalta (18 U.S.C. 2701 §:n d momentti)). Liittovaltion muutoksenhakutuomioistuimen päätöksen mukaisesti valtion tutkijat kuitenkin yleensä saavat tuomareilta etsintäluvan yksityisen viestinnän tai tallennettujen tietojen keräämiseen kaupallisen viestintäpalvelun tarjoajalta. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁽¹⁶⁷⁾ 18 U.S.C. 2705 §:n b momentti.

⁽¹⁶⁸⁾ Ks. varaoikeusministeri Rod Rosensteinin 19.10.2017 antama muistio turvaamismääräyksiä (tai salassapitomääräyksiä) koskevien hakemusten rajoittamisesta osoitteessa <https://www.justice.gov/criminal-ccips/page/file/1005791/download>

⁽¹⁶⁹⁾ Varaoikeusministeri Lisa Moncaon 27.5.2022 antama muistio turvaamismääräysten hakemista 18 U.S.C. 2705 §:n b momentin mukaisesti koskevasta täydentävästä menettelystä.

- (98) Lainvalvontaviranomaiset voivat myös salakuunnella reaaliaikaisesti langallista, suullista tai sähköistä viestintää tuomioistuimen määräyksen perusteella, jos tuomari on esimerkiksi katsonut olevan todennäköistä, että langallisen tai sähköisen salakuuntelun avulla voidaan saada todisteita liittovaltion rikoksesta tai syytettä välttävän etsintäkuulutetun olinpaikasta ⁽¹⁷⁰⁾.
- (99) Muista turvaamistoimista säädetään useissa oikeusministeriön toimintaperiaatteissa ja suuntaviivoissa, kuten Yhdysvaltojen liittovaltion poliisin (FBI) Yhdysvaltojen sisäisiä operaatioita koskevissa oikeusministerin suuntaviivoissa (AGG-DOM), joissa vaaditaan muun muassa, että FBI käyttää mahdollisimman vähän häiritseviä tutkintamenetelmiä ja ottaa huomioon vaikutukset yksityisyyteen ja kansalaisvapauksiin ⁽¹⁷¹⁾.
- (100) Yhdysvaltojen hallituksen antamien lausumien mukaan edellä kuvatun kanssa samantasoista tai korkeampaa suojaa sovelletaan osavaltiotasolla toteutettaviin lainvalvontaviranomaisten tutkimuksiin (kun on kyse tutkimuksista, jotka suoritetaan osavaltion lakien mukaisesti) ⁽¹⁷²⁾. Lisäksi perustuslain säännöksissä sekä osavaltiotason laeissa ja oikeuskäytännössä vahvistetaan edellä mainittu suoja kohtuuttomilta etsinnöiltä ja takavarikoinneilta edellyttämällä etsintämääräyksen antamista ⁽¹⁷³⁾. Liittovaltiotasolla annettua suojaa vastaavasti etsintämääräys voidaan antaa vain osoitetun todennäköisen syyn perusteella, ja siinä on kuvailtava etsinnän sijaintikohde ja kiinniotettava henkilö tai takavarikoitava asia ⁽¹⁷⁴⁾.

⁽¹⁷⁰⁾ 18 U.S.C. 2510–2522 §.

⁽¹⁷¹⁾ Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (syyskuu 2008), ks. <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Muita sääntöjä ja toimintaperiaatteita, joilla rajoitetaan liittovaltion syyttäjien tutkimustoimia, on selostettu Yhdysvaltojen oikeusministeriön käsikirjassa, ks. <http://www.justice.gov/usam/united-states-attorneys-manual>. Näistä ohjeista poikkeamiseen on saatava etukäteen lupa FBI:n johtajalta, varajohtajalta tai johtajan nimeämältä apulaisjohtajalta, paitsi jos luvan hankkimiseen ei ole aikaa henkilöiden tai omaisuuden turvallisuuteen tai kansalliseen turvallisuuteen kohdistuvan uhan välittömyyden tai vakavuuden vuoksi (tällaisessa tapauksessa johtajalle tai muulle luvan myöntävälle henkilölle on ilmoitettava niin pian kuin mahdollista). Jos suuntaviivoja ei noudateta, FBI:n on ilmoitettava asiasta oikeusministeriölle, joka puolestaan ilmoittaa asiasta oikeusministerille ja varaoikeusministerille.

⁽¹⁷²⁾ Liite VI, alaviite 2. Ks. myös esim. asia *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("Yhdysvaltojen perustuslaki, siltä osin kuin sitä sovelletaan osavaltioihin, muodostaa yksilön oikeuksien ja kansalaisvapauksien alalla vähimmäistason, jota osavaltioiden tuomioistuinten päätöksillä ei voida alittaa"; asia *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Kantamme ei luonnollisestikaan vaikuta osavaltion toimivaltaan asettaa etsinnöille, kiinniottoille ja takavarikoille liittovaltion perustuslain vaatimuksia tiukempia edellytyksiä, jos se niin päättää.") *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Vaikka Arizonan perustuslaissa voidaan asettaa etsinnöille, kiinniottoille ja takavarikoille liittovaltion perustuslain tiukempia normeja, Arizonan tuomioistuimen eivät voi heikentää neljännen lisäyksen (Fourth Amendment) suoma suojaa.

⁽¹⁷³⁾ Enemmistö osavaltioista on toistanut neljännen lisäyksen tarjoaman suojan perustuslaissaan. See *Alabama Const. art. I, § 5*; *Alaska Const. art. I, § 14*; *1*; *Arkansas Const. art. II, § 15*; *California Const. art. I, § 13*; *Colorado Const. art. II, § 7*; *Connecticut Const. art. I, § 7*; *Delaware Const. art. I, § 6*; *Florida Const. art. I, § 12*; *Georgia Const. art. I, § I, para. XIII*; *Hawaii Const. art. I, § 7*; *Idaho Const. art. I, § 17*; *Illinois Const. art. I, § 6*; *Indiana Const. art. I, § 11*; *Iowa Const. art. I, § 8*; *Kansas Const. Bill of Rights, § 15*; *Kentucky Const. art. I, § 10*; *Louisiana Const. art. I, § 5*; *Maine Const. art. I, § 5*; *Massachusetts Const. Decl. of Rights art. 14*; *Michigan Const. art. I, § 11*; *Minnesota Const. art. I, § 10*; *Mississippi Const. art. III, § 23*; *Missouri Const. art. I, § 15*; *Montana Const. art. II, § 11*; *Nebraska Const. art. I, § 7*; *Nevada Const. art. I, § 18*; *New Hampshire Const. pt. 1, art. 19*; *N.J. Const. art. II, § 7*; *New Mexico Const. art. II, § 10*; *New York Const. art. I, § 12*; *North Dakota Const. art. I, § 8*; *Ohio Const. art. I, § 14*; *Oklahoma Const. art. II, § 30*; *Oregon Const. art. I, § 9*; *Pennsylvania Const. art. I, § 8*; *Rhode Island Const. art. I, § 6*; *South Carolina Const. art. I, § 10*; *South Dakota Const. art. VI, § 11*; *Tennessee Const. art. I, § 7*; *Texas Const. art. I, § 9*; *Utah Const. art. I, § 14*; *Vermont Const. ch. I, art. 11*; *West Virginia Const. art. III, § 6*; *Wisconsin Const. art. I, § 11*; *Wyoming Const. art. I, § 4*. Muut (esim. *Maryland*, *Pohjois-Carolina* ja *Virginia*) ovat vahvistaneet perustuslaissaan etsintämääräyksiä koskevia muotoiluja, joiden tuomioistuimet ovat tulkinneet tarjoavan samanlaisen tai korkeamman tasoisen suojan kuin neljäs lisäys (ks. *Maryland. Decl. of Rts. art. 26*; *North Carolina Const. art. I, § 20*; *Virginia Const. art. I, § 10*, ja asiaan liittyvä oikeuskäytäntö, esim. *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008); *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) ja *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Arizonalla ja Washingtonilla on perustuslaissaan kohtia, joilla suojellaan yksityisyyttä yleisemmällä tasolla (*Arizona Const. art. 2, § 8*; *Washington Const. art. I, § 7*), ja joiden tuomioistuimet ovat tulkinneet tarjoavan korkeamman tasoisen suojan kuin neljäs lisäys (ks. esim. *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

⁽¹⁷⁴⁾ Ks. esim. *California Penal Code § 1524,3(b)*; *Rule 3.6-3.13 Alabama Rules of Criminal Procedure*; *Section 10.79.035; Revised Code of Washington*; *Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia*.

3.1.1.2 Kerättyjen tietojen myöhempi käyttö

- (101) Eri säädöksissä, ohjeissa ja normeissa määrätään liittovaltion lainvalvontaviranomaisten keräämien tietojen myöhempiä käyttöä koskevista erityisistä suojatoimista. Lukuun ottamatta FBI:n toimintaan sovellettavia erityisjärjestelyjä (AGG-DOM ja ohje FBI:n kotimaisista tutkimuksista ja operaatioista (FBI Domestic Investigations and Operations Guide)) tässä jaksossa kuvattuja vaatimuksia sovelletaan yleisesti minkä tahansa liittovaltion viranomaisen suorittamaan tietojen myöhempään käyttöön, mukaan lukien tietojen käyttö siviilihallinnon ja sääntelyn tarkoituksiin. Tähän sisältyvät vaatimukset, jotka perustuvat hallinto- ja talousarvioviraston muistioihin/määräyksiin, tietoturvallisuuden nykyaikaistamista koskevan lakiin (Federal Information Security Management Modernization Act), sähköistä hallintoa koskevaan lakiin (E-Government Act) ja liittovaltion rekisterilakiin (Federal Records Act).
- (102) Säädösten Clinger-Cohen Act (P.L. 104–106, Division E) ja vuoden 1987 Computer Security Act (P.L. 100–235) valtuuttamana hallinto- ja talousarviovirasto, jäljempänä OMB, antoi yleiskirjeen nro A-130 yleisistä sitovista ohjeista, joita sovelletaan kaikkiin liittovaltion virastoihin (myös lainvalvontaviranomaisiin) niiden käsitellessä henkilöllisyyden määrittämistä koskevia tietoja (personally identifiable information) ⁽¹⁷⁵⁾. Yleiskirjeessä edellytetään erityisesti, että kaikki liittovaltion virastot rajaavat henkilöllisyyden määrittämistä koskevien tietojen luomisen, keräämisen, käytön, käsittelyn, säilyttämisen, ylläpidon, levittämisen ja luovuttamisen sellaiseen laajuuteen, joka on valtuutetun viraston tehtävien asianmukaisen suorittamisen kannalta lain mukaan sallittua, merkityksellistä ja kohtuudella tarpeen ⁽¹⁷⁶⁾. Lisäksi liittovaltion virastojen on varmistettava siinä määrin kuin se on kohtuudella mahdollista, että henkilöllisyyden määrittämistä koskevat tiedot ovat tarkkoja, olennaisia, ajantasaisia ja täydellisiä ja että ne on rajoitettu viraston tehtävien asianmukaisen suorittamisen kannalta välttämättömään vähimmäismäärään. Yleisellä tasolla liittovaltion virastojen on otettava käyttöön kattava tietosujoaohjelma, jolla varmistetaan sovellettavien tietosujoa vaatimusten noudattaminen, kehitetään ja arvioidaan tietosujoaperiaatteita ja hallitaan yksityisyysriskejä, ylläpidetään menettelyjä yksityisyyden suojan noudattamiseen liittyvien ongelmien havaitsemiseksi, dokumentoimiseksi ja raportoimiseksi, parannetaan työntekijöiden ja toimeksisaajien tietämystä yksityisyyden suojasta ja kehitetään sitä koskevaa koulutusta sekä otetaan käyttöön käytäntöjä ja menettelyjä sen varmistamiseksi, että henkilöstö on vastuussa tietosujoa vaatimusten ja -periaatteiden noudattamisesta ⁽¹⁷⁷⁾.
- (103) Lisäksi sähköistä hallintoa koskevassa E-Government Act -laissa ⁽¹⁷⁸⁾ edellytetään, että kaikki liittovaltion virastot (mukaan lukien lainvalvontaviranomaiset) ottavat käyttöön tietoturvatavoitteita, jotka ovat oikeasuhteisia luvattomasta pääsystä, käytöstä, luovuttamisesta, häiriöistä, muutoksista tai tuhoutumisesta aiheutuvan haitan riskiin ja laajuuteen nähden. Virastoilla on myös oltava tietohallintojohtaja, joka varmistaa, että tietoturva-vaatimuksia noudatetaan ja että vuosittain laaditaan tietoturvaohjelmaa ja -käytäntöjä koskeva riippumaton arviointi (esimerkiksi valvontaviranomaisen toimesta, ks. johdanto-osan 109 kappale) ⁽¹⁷⁹⁾. Vastaavasti liittovaltion asiakirjoja koskeva Federal Records Act -laki ⁽¹⁸⁰⁾ ja sitä täydentävät määräykset ⁽¹⁸¹⁾ edellyttävät, että liittovaltion virastojen hallussa oleviin tietoihin sovelletaan suojatoimia, joilla varmistetaan tietojen fyysinen eheys ja suojataan niitä luvattomalta käytöltä.
- (104) OMB ja Yhdysvaltojen kansallinen standardi- ja teknologiainstituutti (National Institute for Standards and Technology), jäljempänä 'NIST', ovat kehittäneet liittovaltion lainsäädännön mukaisen toimivallan, mukaan lukien vuoden 2014 tietoturvallisuuden nykyaikaistamista koskevan lain (Federal Information Security Modernisation Act), nojalla liittovaltion virastoja (myös lainvalvontaviranomaisia) sitovat normit, joissa täsmennetään käyttöön otettavat vähimmäistietoturva-vaatimukset, muun muassa pääsyn valvonta, tietoisuuden ja koulutuksen varmistaminen, valmiussuunnittelu, häiriötilanteisiin reagointi, tarkastus- ja vastuuvastuuvelvollisuusvälineet, järjestelmien ja tietojen eheystarkistukset sekä yksityisyyden suojan ja turvallisuusriskien arvioinnit ⁽¹⁸²⁾. Lisäksi kaikkien

⁽¹⁷⁵⁾ Toisin sanoen tiedot, joiden avulla yksilön henkilöllisyys voidaan selvittää tai jäljittää joko yksin tai yhdistettynä muihin tietoihin, jotka liittyvät tiettyyn henkilöön, ks. OMB Circular No. A-130, s. 33 ('henkilöllisyyden määrittämistä koskevien tietojen' määritelmä).

⁽¹⁷⁶⁾ OMB Circular No. A-130, Managing Information as a Strategic Resource, lisäys II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49 689 (28.7.2016), s. 17.

⁽¹⁷⁷⁾ Lisäys II, 5 §:n a–h momentti.

⁽¹⁷⁸⁾ 44 U.S.C. 36 luku.

⁽¹⁷⁹⁾ 44 U.S.C. 3544–3545 §.

⁽¹⁸⁰⁾ FAC, 44 U.S.C. 3105 §.

⁽¹⁸¹⁾ 36 C.F.R. 1228,150 § ja seuraavat pykälät, 1228,228 § ja lisäys A.

⁽¹⁸²⁾ Ks. esimerkiksi OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10.12.2020), ja NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

liittovaltion virastojen (myös lainvalvontaviranomaisten) on OMB:n ohjeiden mukaisesti ylläpidettävä ja sovellettava suunnitelmaa tietoturvaloukkausten käsittelemiseksi sekä niihin vastaamiseksi ja haittariskien arvioimiseksi ⁽¹⁸³⁾.

- (105) Tietojen säilyttämisen osalta liittovaltion virastojen (myös lainvalvontaviranomaisten) on Federal Records Act -lain ⁽¹⁸⁴⁾ mukaan vahvistettava rekisteritiedoille säilyttämisaika (jonka päätyttyä tiedot on hävitettävä), jolle on saatava kansallisista arkistoista vastaavan hallinnon (National Archives and Record Administration) hyväksyntä ⁽¹⁸⁵⁾. Säilytysaika määritetään eri tekijöiden perusteella, kuten tutkintatyyppin mukaan tai riippuen siitä, onko todistusaineisto edelleen tutkinnan kannalta merkityksellistä. Oikeusministerin AGG-DOM-suuntaviivoissa määrätään, että FBI:llä on oltava tällainen säilytysuunnitelma ja että sillä on oltava käytössään järjestelmä, josta se voi nopeasti hakea tutkinnan tilanteen ja perustan.
- (106) Myös OMB:n yleiskirje nro A-130 sisältää vaatimuksia, jotka koskevat henkilöllisyyden määrittämistä koskevien tietojen levittämistä. Henkilöön liitettävissä olevien tietojen levittäminen ja luovuttaminen on periaatteessa rajoitettava siihen, mikä on lain mukaan sallittua, olennaista ja kohtuudella tarpeen viraston tehtävien asianmukaisen hoitamisen kannalta ⁽¹⁸⁶⁾. Kun henkilöllisyyden määrittämistä koskevia tietoja jaetaan muiden valtion tahojen kanssa, liittovaltion virastojen on tarvittaessa asetettava ehdoksi (myös toteuttamalla erityisiä turvallisuus- ja yksityisyystarkastuksia), että tietojen käsittelyä hallinnoidaan kirjallisilla sopimuksilla (mukaan lukien tietojenkäyttösopimukset, tietojenvaihtosopimukset ja yhteisymmärryspöytäkirjat) ⁽¹⁸⁷⁾. Tietojen levittämisen perusteista voidaan todeta, että esimerkiksi AGG-DOM-ohjeistuksessa ja FBI:n ohjeessa kotimaisista tutkimuksista ja operaatioista (FBI Domestic Investigations and Operations Guide ⁽¹⁸⁸⁾) todetaan, että FBI:llä voi olla lakisäateinen velvoite tietojen levittämiseen (esim. kansainvälisen sopimuksen nojalla) tai se voi levittää tietoa tietyissä olosuhteissa, esimerkiksi muille yhdysvaltalaisille virastoille, jos luovuttaminen on yhteensopivaa sen tarkoituksen kanssa, jota varten tiedot on kerätty, ja se liittyy niiden velvollisuuksiin; kongressin komiteoille; ulkomaisille tahoille, jos tiedot liittyvät niiden velvollisuuksiin ja jos niiden levittäminen on Yhdysvaltojen etujen mukaista; tietojen levittäminen on erityisesti tarpeen henkilöiden tai omaisuuden turvallisuuden suojelemiseksi tai rikoksen tai kansalliseen turvallisuuteen kohdistuvan uhkan estämiseksi tai sellaiselta suojautumiseksi, ja tietojen luovuttaminen on yhteensopivaa sen tarkoituksen kanssa, jota varten tiedot on kerätty ⁽¹⁸⁹⁾.

3.1.2 Valvonta

- (107) Liittovaltion lainvalvontavirastoja valvovat useat elimet ⁽¹⁹⁰⁾. Kuten johdanto-osan 92–99 kappaleessa selitetään, tähän sisältyy useimmissa tapauksissa oikeuslaitoksen ennakkovalvonta, koska sen on annettava lupa yksittäisiin tiedonkeruutoimiin ennen kuin niihin voidaan ryhtyä. Lisäksi muut elimet valvovat rikosoikeudellisten lainvalvontaviranomaisten toiminnan eri vaiheita, kuten henkilötietojen keräämistä ja käsittelyä. Yhdessä nämä oikeudelliset ja muut elimet varmistavat, että lainvalvontaviranomaiset ovat riippumattoman valvonnan alaisia.

⁽¹⁸³⁾ Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information", ks. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, ja OMB Circular No. A-130. Esimerkiksi oikeusministeriön menettely tietoturvaloukkauksiin vastaamiseksi, ks. <https://www.justice.gov/file/4336/download>

⁽¹⁸⁴⁾ FRA, 44 U.S.C. 3101 § ja sitä seuraavat pykälät.

⁽¹⁸⁵⁾ Kansallisella arkistoviranomaisella (National Archives and Record Administration) on valtuudet arvioida virastojen asiakirjojen hallintakäytäntöjä, ja se voi määrittää, onko määrittäen tietojen säilyttäminen perusteltua (44 U.S.C.2904 § (c), 2906).

⁽¹⁸⁶⁾ OMB Circular No. A-130, Section 5.f.1.(d)

⁽¹⁸⁷⁾ OMB Circular No. A-130, Appendix I §3(d).

⁽¹⁸⁸⁾ Ks. myös FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

⁽¹⁸⁹⁾ AGG-DOM, Section VI, B and C; FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

⁽¹⁹⁰⁾ Tässä jaksossa mainittuja mekanismeja sovelletaan myös liittovaltion viranomaisten suorittamaan tietojen keruuseen ja käyttöön siviilihallinnon ja sääntelyn tarkoituksiin. Liittovaltion siviilihallinto- ja sääntelyvirastot ovat omien valvontaviranomaistensa ja kongressin valvonnassa. Tähän valvontaan osallistuu myös kongressin tarkastus- ja tutkintavirasto eli Government Accountability Office. Jos virastolla ei ole yksityisyyden suojaa ja kansalaisvapauksia käsittelevää nimettyä virkamiestä – tällainen tehtäväkuva löytyy tyypillisesti oikeusministeriön ja sisäisen turvallisuuden ministeriön kaltaisista virastoista, koska niillä on lainvalvontaan ja kansalliseen turvallisuuteen liittyviä vastuita – nämä tehtävät kuuluvat viraston tietosuojavastaavalle (Senior Agency Official for Privacy, SAOP). Kaikilla liittovaltion virastoilla on lakisäateinen velvollisuus nimetä SAOP, joka vastaa siitä, että virasto noudattaa yksityisyyden suojaa koskevia lakeja, sekä valvoo asiaan liittyvää toimintaa. Ks. esim. OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

- (108) Yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaavia virkamiehiä (Privacy and Civil Liberties Officers) on useissa lainvalvontatehtäviä suorittavissa ministeriöissä ⁽¹⁹¹⁾. Vaikka näiden viranomaisten toimivalta voi jonkin verran vaihdella perustana olevan lainsäädännön mukaan, se yleensä kattaa menettelyjen valvonnan sen varmistamiseksi, että kyseessä oleva ministeriö tai virasto ottaa asianmukaisesti huomioon yksityisyyden suojaan ja kansalaisvapauksiin liittyvät näkökohdat ja että se on ottanut käyttöön asianmukaiset menettelyt, jotta voidaan käsitellä sellaisten henkilöiden valitukset, jotka katsovat, että heidän yksityisyyttään tai kansalaisvapauksiaan on loukattu. Kunkin ministeriön tai viraston päälliköiden on varmistettava, että yksityisyyden suojasta ja kansalaisvapauksista vastaavilla virkamiehillä on tehtäviensä hoitamiseen tarvittavat materiaalit ja resurssit, että heillä on käytettävissään kaikki tehtäviensä hoitamiseen tarvittava aineisto ja henkilöstö ja että heille tiedotetaan ehdotetuista toimintapoliittisista muutoksista ja heitä kuullaan niistä ⁽¹⁹²⁾. Yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet raportoivat säännöllisesti kongressille muun muassa seuraavista: ministeriön tai viraston vastaanottamien valitusten lukumäärä ja tyyppi ja yhteenveto niihin annetuista päätöksistä, suoritettut arvioinnit ja tarkastelut sekä virkamiehen toteuttamien toimien vaikutus ⁽¹⁹³⁾.
- (109) Toiseksi oikeusministeriön, ja myös FBI:n, toimintaa valvoo riippumaton valvontaviranomainen (Inspector General) ⁽¹⁹⁴⁾. Valvontaviranomaiset ovat lakisääteisesti riippumattomia ⁽¹⁹⁵⁾, ja niiden tehtävänä on suorittaa riippumattomia tutkimuksia, arviointeja ja tarkastuksia ministeriön ohjelmista ja toimista. Niillä on pääsy kaikkiin tietoihin, raportteihin, tarkastusaineistoihin, arviointeihin, asiakirjoihin, työpapereihin, suosituksiin ja muuhun asianmukaiseen aineistoon, tarvittaessa haasteteitse, ja ne voivat ottaa todistajanlausuntoja ⁽¹⁹⁶⁾. Valvontaviranomaisten antamat suositukset korjaavia toimia varten eivät ole sitovia, mutta niiden tarkastuskertomukset, myös seurantakertomukset, (tai niiden puuttuminen) ⁽¹⁹⁷⁾ yleensä julkistetaan ja lähetetään kongressille, joka voi tältä pohjalta harjoittaa valvontatehtäväänsä (ks. johdanto-osan 111 kappale) ⁽¹⁹⁸⁾.

⁽¹⁹¹⁾ Ks. 42 U.S.C. 2000ee-1 §. Niitä ovat esimerkiksi oikeusministeriö, sisäisen turvallisuuden ministeriö ja FBI. Sisäisen turvallisuuden ministeriössä (Department of Homeland Security) on lisäksi tietosuojavastaava (Chief Privacy Officer), joka vastaa yksityisyyden suojan säilyttämisestä ja parantamisesta sekä läpinäkyvyyden edistämisestä ministeriössä (6 U.S.C. 142, Section 222. Kaikkia sisäisen turvallisuuden ministeriön järjestelmiä, tekniikkaa, lomakkeita ja ohjelmia, jotka keräävät henkilötietoja tai joilla on tietosuojavaihtokutuksia, valvoo tietosuojavastaava, jolla on – tarvittaessa haasteen perusteella – pääsy kaikkiin ministeriön tietoihin, raportteihin, tarkastuksiin, arviointeihin, asiakirjoihin, työpapereihin, suosituksiin ja muihin ministeriön käytössä oleviin aineistoihin. Tietosuojavastaava raportoi vuosittain kongressille sellaisesta ministeriön toiminnasta, jolla on vaikutuksia tietosuojaan, mukaan lukien yksityisyyden loukkauksia koskevat valitukset.

⁽¹⁹²⁾ 42 U.S.C. 2000ee-1 §:n d momentti.

⁽¹⁹³⁾ Ks. 42 U.S.C. 2000ee-1 §:n f momentin 1 ja 2 kohta. Esimerkiksi oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaavan johtavan virkamiehen ja yksityisyyden ja kansalaisvapauksien suojasta vastaavan toimiston raportin mukaan lokakuun 2020 ja maaliskuun 2021 välisenä aikana tehtiin 389 tietosuojatarkastusta, joiden kohteina olivat muun muassa tietojärjestelmät ja muut ohjelmat (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

⁽¹⁹⁴⁾ Vuonna 2002 annetulla sisäistä turvallisuutta koskevalla lailla (Homeland Security Act) sisäisen turvallisuuden ministeriöön perustettiin valvontaviranomaisen toimisto.

⁽¹⁹⁵⁾ Valvontaviranomaisilla on vakinainen virka, ja heidät voi erottaa ainoastaan presidentti, jonka on ilmoitettava kongressille kirjallisesti erottamisen syistä.

⁽¹⁹⁶⁾ Ks. Inspector General Act, 1978, 6 §.

⁽¹⁹⁷⁾ Esimerkiksi oikeusministeriön valvontaviranomaisen toimiston laatima yleiskatsaus sen antamista suosituksista ja siitä, missä määrin ne on pantu täytäntöön ministeriön ja virastojen seurantaomilla, ks. <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>

⁽¹⁹⁸⁾ Ks. Inspector General Act, 1978, 4 §:n 5 momentin 5 kohta. Esimerkiksi oikeusministeriön valvontaviranomaisen toimisto julkaisi hiljattain puolivuotiskertomuksensa kongressille (1.10.2021–31.3.2022, <https://oig.justice.gov/node/23596>). Se sisältää yleiskatsauksen oikeusministeriön ohjelmien ja toimien tarkastuksista, arvioinneista, erityisarvioinneista ja tutkimuksista. Näihin toimiin kuului entiseen toimeksisaajaan kohdistuva tutkinta, joka koski käynnissä olevan tutkimuksen puitteissa suoritettua sähköisen tarkkailun (henkilön salakuuntelun) lainvastaista paljastamista, mikä johti toimeksisaajan tuomitsemiseen. Valvontaviranomaisen toimisto suoritti myös tutkinnan oikeusministeriön virastojen tietoturvaohjelmista ja -käytännöistä. Siinä muun muassa testattiin tietoturvaliiketoiminnan, -menettelyjen ja -käytäntöjen toimivuutta edustavassa joukossa virastojen järjestelmiä.

- (110) Kolmanneksi, siltä osin kuin rikoslainsäädännön täytäntöönpanosta vastaavat ministeriöt toteuttavat terrorismin vastaisia toimia, niitä valvoo yksityisyyden ja kansalaisvapauksien valvontalautakunta (Privacy and Civil Liberties Oversight Board, PCLOB). Se on toimeenpanevaan osastoon kuuluva riippumaton toiminto, joka koostuu kaksipuoluisesta, viisijäsenisestä lautakunnasta, jonka presidentti nimittää kuuden vuoden toimikaudeksi senaatin hyväksynnällä ⁽¹⁹⁹⁾. PCLOB:n perustamissääntöjen mukaan sen vastuualaan kuuluu terrorismin vastainen politiikka ja sen täytäntöönpano yksityisyyden suojan ja kansalaisvapauksien suojelemiseksi. Tarkastelujaan varten se voi saada käyttöönsä kaikki asiaankuuluvat elinten tiedot, raportit, tarkastusaineistot, arvioinnit, asiakirjat, työpaperit ja suositukset, mukaan lukien turvallisuusluokitellut tiedot, suorittaa haastatteluja ja kuulla todistajia ⁽²⁰⁰⁾. Se saa raportteja useiden liittovaltion ministeriöiden ja virastojen ⁽²⁰¹⁾ kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavilta virkamiehiltä, ja se voi antaa suosituksia valtion viranomaisille ja lainvalvontaviranomaisille. Lisäksi se raportoi säännöllisesti kongressin valiokunnille ja presidentille ⁽²⁰²⁾. Lautakunnan raportit, myös kongressille toimitettavat raportit, julkistetaan mahdollisimman laajalti ⁽²⁰³⁾.
- (111) Lisäksi lainvalvontatoimia valvovat Yhdysvaltojen kongressin erityisvaliokunnat (edustajainhuoneen ja senaatin oikeusasioiden valiokunnat). Oikeusasioiden valiokunnat (Judiciary Committees) suorittavat säännöllistä valvontaa erityisesti toteuttamalla kuulemisia, tutkimuksia ja tarkasteluja ja laatimalla raportteja ⁽²⁰⁴⁾.

3.1.3 Oikeussuojakeinot

- (112) Kuten edellä todettiin, lainvalvontaviranomaisten on useimmissa tapauksissa saatava henkilötietojen keräämiseen etukäteen tuomioistuimen lupa. Vaikka lupaa ei vaadita hallinnollisten haasteiden tapauksessa, hallinnolliset haasteet on rajattu erityistapauksiin ja niihin voi hakea muutosta riippumattomassa tuomioistuimessa ainakin silloin, kun hallitus esittää täytäntöönpanoa tuomioistuimessa. Hallinnollisten haasteiden vastaanottajat voivat riitauttaa haasteet tuomioistuimessa sillä perusteella, että ne ovat kohtuuttomia, eli laajuudeltaan tai rasittavuudeltaan liiallisia ⁽²⁰⁵⁾.
- (113) Yksityishenkilöt voivat ensinnäkin esittää henkilötietojensa käsittelyä koskevia pyyntöjä tai valituksia lainvalvontaviranomaisille. Tähän sisältyy mahdollisuus pyytää pääsyä henkilötietoihin ja niiden oikaisemista ⁽²⁰⁶⁾. Terrorismin torjuntaan liittyvissä tapauksissa yksityishenkilöt voivat tehdä valituksen myös lainvalvontaviranomaisten puitteissa toimiville yksityisyyden suojasta ja kansalaisvapauksista vastaaville virkamiehille (tai muille vastaaville virkamiehille) ⁽²⁰⁷⁾.
- (114) Yhdysvaltojen lainsäädännössä säädetään lisäksi useista mahdollisuuksista käyttää oikeussuojakeinoja viranomaista tai sen virkamiestä vastaan, kun nämä viranomaiset käsittelevät henkilötietoja ⁽²⁰⁸⁾. Näihin oikeussuojakeinoihin kuuluvat erityisesti hallintomenettelylaki (Administrative Procedure Act, APA), tiedonvapautta koskeva laki (Freedom of Information Act, FOIA) ja sähköisen viestinnän tietosuojalaki (Electronic Communications Privacy Act, ECPA), ja niitä voivat käyttää kaikki henkilöt kansalaisuudesta riippumatta, jollei sovellettavista edellytyksistä muuta johdu.

⁽¹⁹⁹⁾ Lautakunnan jäsenet valitaan yksinomaan heidän ammatillisen pätevyytensä, saavutustensa, julkisen asemansa, kansalaisvapauksien ja yksityisyyden suojan alan asiantuntemuksensa ja kokemuksensa perusteella ottamatta huomioon heidän poliittista suuntautumistaan. Lautakunnassa voi olla enintään kolme samaan poliittiseen puolueeseen kuuluvaa jäsentä. Lautakuntaan nimitetty henkilö ei voi lautakunnassa toimiessaan olla vaaleilla valittu virkamies, virkamies tai liittovaltion hallituksen työntekijä muutoin kuin lautakunnan jäsenenä. Ks. 42 U.S.C. 2000ee §:n h momentti.

⁽²⁰⁰⁾ 42 U.S.C. 2000ee §:n g momentti.

⁽²⁰¹⁾ Ks. 42 U.S.C. 2000ee-1 §:n f momentin 1 kohdan A alakohdan iii alakohta. Näitä ovat ainakin oikeusministeriö, puolustusministeriö, sisäisen turvallisuuden ministeriö sekä mahdolliset muut PCLOB:n raporttien kannalta relevanteiksi katsomat ministeriöt, virastot tai toimeenpanovallan toimijat.

⁽²⁰²⁾ 42 U.S.C. 2000ee §:n e momentti.

⁽²⁰³⁾ 42 U.S.C. 2000ee §:n f momentti.

⁽²⁰⁴⁾ Valiokunnat järjestävät aihekohtaisia kuulemistilaisuuksia (ks. esimerkiksi edustajainhuoneen oikeusasioiden valiokunnan hiljattainen kuuleminen digitaalisista dragnet-verkoista, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>). Lisäksi FBI ja oikeusministeriö järjestävät säännöllisiä valvontakuulemisia, ks. <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⁾ Ks. liite VI.

⁽²⁰⁶⁾ OMB:n yleiskirje nro A-130, liite II, 3 kohdan a ja f alakohta, jossa edellytetään, että liittovaltion virastot varmistavat asianmukaisen pääsyn tietoihin ja mahdollisuuden oikaista tiedot yksityishenkilöiden pyynnöstä, ja vahvistavat menettelyt yksityisyyden suojaan liittyvien valitusten ja pyyntöjen vastaanottamista ja käsittelyä varten.

⁽²⁰⁷⁾ Ks. 42 U.S.C. 2000ee-1 § esimerkiksi oikeusministeriön ja sisäisen turvallisuuden ministeriön osalta. Ks. myös OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

⁽²⁰⁸⁾ Tässä jaksossa mainittuja oikeussuojamekanismeja sovelletaan myös liittovaltion viranomaisten suorittamaan tietojen keruuseen ja käyttöön siviilihallinnon ja sääntelyn tarkoituksiin.

- (115) Hallintomenettelylaissa olevien muutoksenhakua tuomioistuimessa koskevien säännösten ⁽²⁰⁹⁾ mukaan ”henkilöllä, jonka oikeuksia on loukattu viraston toiminnan seurauksena tai johon viraston toiminta vaikuttaa haitallisesti tai jonka etua on loukattu”, on oikeus hakea muutosta tuomioistuimessa ⁽²¹⁰⁾. Tähän sisältyy mahdollisuus pyytää tuomioistuinta ”toteamaan lainvastaiseksi ja kumoamaan viraston sellaiset toimet, havainnot ja päätelmät, joiden katsotaan olevan [...] mielivaltaisia, epämääräisiä, harkintavallan väärinkäyttöä tai muuten lainvastaisia” ⁽²¹¹⁾.
- (116) Erityisesti sähköisen viestinnän tietosuojalain (ECPA) II osastossa ⁽²¹²⁾ säädetään lakisääteisten yksityisyyden suojaa koskevien oikeuksien järjestelmästä, ja sitä sovelletaan lainvalvontatarkoituksessa tapahtuvaan pääsyyn viestintäpalveluja tarjoavien kolmansien osapuolten hallussa olevaan langallisen, suullisen tai sähköisen viestinnän sisältöön ⁽²¹³⁾. Siinä kriminalisoidaan laitton (eli ilman tuomioistuimen lupaa tapahtuva tai muuten ei-sallittu) pääsy tällaiseen viestintään ja säädetään kyseessä olevan henkilön mahdollisuudesta nostaa Yhdysvaltojen liittovaltion tuomioistuimessa siviilikanne sellaista hallituksen virkamiestä vastaan, joka on tahallisesti syylistynyt tällaisiin laittomiin tekoihin, tai Yhdysvaltoja vastaan, todelliseen vahinkoon perustuvan ja rangaistusluonteisen vahingonkorvauksen sekä kielto- tai vahvistustuomion saamiseksi.
- (117) Lisäksi useissa muissa säädöksissä (Wiretap Act ⁽²¹⁴⁾, Computer Fraud and Abuse Act ⁽²¹⁵⁾, Federal Torts Claim Act ⁽²¹⁶⁾, Right to Financial Privacy Act ⁽²¹⁷⁾ ja Fair Credit Reporting Act ⁽²¹⁸⁾) annetaan henkilöille oikeus nostaa kanne Yhdysvaltojen viranomaista tai virkamiestä vastaan henkilötietojensa käsittelyn vuoksi.

⁽²⁰⁹⁾ 5 U.S.C. 702 §.

⁽²¹⁰⁾ Yleensä vain ”lopullinen” viraston toimi – pikemmin kuin ”väliaikainen, menettelyllinen tai välillinen” viraston toimi – kuuluu tuomioistuinvalvonnan piiriin. Ks. 5 U.S.C. 704 §.

⁽²¹¹⁾ 5 U.S.C. 706 §:n 2 momentin A kohta.

⁽²¹²⁾ 18 U.S.C. 2701–2712 §.

⁽²¹³⁾ ECPA suojaa tietoja, jotka ovat kahdenlaisten verkkopalveluyritysten hallussa: i) sähköiset viestintäpalvelut, esimerkiksi puhelin tai sähköposti, sekä ii) etäkäyttöpalvelut, kuten tallenne- ja käsittelypalvelut.

⁽²¹⁴⁾ 18 U.S.C. 2510 § ja sitä seuraavat pykälät. Salakuuntelua koskevan lain (Wiretap Act, 18 U.S.C. 2520 §) mukaan henkilö, jonka langallista, suullista tai sähköistä viestintää salakuunnellaan, paljastetaan tai käytetään tahallisesti, voi nostaa siviilikanteen kyseisen lain rikkomisesta, tietyissä olosuhteissa myös yksittäistä virkamiestä tai Yhdysvaltoja vastaan. Muun kuin sisällöllisen tiedon (esimerkiksi IP-osoite, sähköpostin lähettäjän/vastaanottajan osoite) keräämisestä ks. myös lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiä koskeva 18 osaston luku (Pen Registers and Trap and Trace Devices) (18 U.S.C. 3121–3127 §, ja siviilikanteesta 2707 §).

⁽²¹⁵⁾ 18 U.S.C. 1030 §. Tietokonepetoksista ja -väärinkäytöksistä annetun lain (Computer Fraud and Abuse Act) mukaan henkilö voi nostaa kanteen toista henkilöä vastaan tahallisesti luvattomasta tietoihin pääsystä (tai luvallisen pääsyn rajojen ylittämisestä) tietojen saamiseksi jostakin finanssilaitoksesta, Yhdysvaltojen hallituksen tietokonejärjestelmästä tai muusta tietyistä tietokoneista, ja tietyissä olosuhteissa myös yksittäistä valtion virkamiestä vastaan.

⁽²¹⁶⁾ 28 U.S.C. 2671 § ja sitä seuraavat pykälät. Liittovaltion vahingonkorvauslain (Federal Tort Claims Act) mukaan henkilö voi nostaa tietyissä olosuhteissa kanteen Yhdysvaltoja vastaan sellaisen ”tuottamuksellisen tai laittoman teon tai laiminlyönnin vuoksi, johon hallituksen työntekijä on syylistynyt tehtävässään tai työssään”.

⁽²¹⁷⁾ 12 U.S.C. 3401 § ja sitä seuraavat pykälät. Taloudellisen yksityisyyden suojasta annetun lain (Right to Financial Privacy Act) mukaan henkilö voi tietyissä olosuhteissa nostaa kanteen Yhdysvaltoja vastaan, jos suojattuja taloudellisia tietoja on hankittu tai luovutettu säännösten vastaisesti. Viranomaisten pääsy suojattuihin taloudellisiin tietoihin on yleensä kielletty, ellei tietojen luovuttamista vaadita laillisen haasteen tai etsintäluvan tai (tietyin rajoituksin) virallisen kirjallisen pyynnön nojalla ja henkilö, jonka tietoja pyydetään, saa ilmoituksen tällaisesta pyynnöstä.

⁽²¹⁸⁾ 15 U.S.C. 1681–1681x §. Luottokelpoisuusraportointia koskevan lain (Fair Credit Reporting Act) nojalla henkilö voi nostaa kanteen sellaista henkilöä vastaan, joka ei noudata vaatimuksia (erityisesti vaatimusta laillisesta luvasta), jotka koskevat kuluttajien luottokelpoisuutta koskevien tietojen keruuta, levittämistä ja käyttöä, tai tietyin edellytyksin hallituksen virastoa vastaan.

- (118) Lisäksi tiedonvapautta koskevan lain (Freedom of Information Act, FOIA, 5 U.S.C. 552 §) ⁽²¹⁹⁾ mukaan jokaisella henkilöllä on oikeus saada pääsy liittovaltion virastojen rekistereihin, myös silloin, kun ne sisältävät yksityishenkilön henkilötietoja. Kun kaikki hallinnolliset muutoksenhakukeinot on käytetty, yksityishenkilö voi vedota tällaiseen tietoihinpääsyoikeuteen tuomioistuimessa, ellei kyseisiä tietoja ole suojattu julkisuudelta poikkeuksella tai erityisellä lainvalvontaviranomaisten päätöksellä ⁽²²⁰⁾. Tässä tapauksessa tuomioistuin arvioi, sovelletaanko poikkeusta ja onko kyseinen toimivaltainen viranomainen vedonnut siihen laillisesti.

3.2 Yhdysvaltojen viranomaisten pääsy tietoihin ja niiden käyttö kansalliseen turvallisuuteen liittyviä tarkoituksia varten

- (119) Yhdysvaltojen lainsäädäntöön sisältyy erilaisia rajoituksia ja suojatoimia, jotka koskevat henkilötietoihin pääsyä ja niiden käyttöä kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Siinä säädetään myös valvonta- ja oikeussuojamekanismeista, jotka vastaavat tämän päätöksen johdanto-osan 89 kappaleessa mainittuja vaatimuksia. Seuraavassa arvioidaan yksityiskohtaisesti edellytyksiä, joiden täytyessä pääsy henkilötietoihin voi toteutua, ja näiden toimivaltuuksien käyttöön liittyvien suojatoimien soveltamista.

3.2.1 Oikeusperustat, rajoitukset ja suojatoimet

3.2.1.1 Sovellettava oikeudellinen kehys

- (120) Yhdysvaltojen viranomaiset voivat kerätä unionista tietosuojakehykseen osallistuville organisaatioille siirrettäviä tietoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten erilaisten oikeudellisten välineiden nojalla ja noudattaen asiaa koskevia edellytyksiä ja suojatoimia.
- (121) Sen jälkeen kun Yhdysvalloissa sijaitsevat organisaatiot ovat vastaanottaneet henkilötietoja, Yhdysvaltojen tiedusteluelimet voivat hakea pääsyä tällaisiin tietoihin kansalliseen turvallisuuteen liittyviä tarkoituksia varten ainoastaan lakisääteisen luvan nojalla, erityisesti ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act), jäljempänä 'FISA-laki', nojalla tai sellaisten säännösten nojalla, joissa sallitaan pääsy kansallista turvallisuutta koskevien kirjeiden (National Security Letters, NSL) perusteella ⁽²²¹⁾. FISA-laki sisältää useita oikeusperustoja, joita voidaan käyttää kerätessä (ja käsiteltäessä) tietosuojakehyksen (FISA 105 § ⁽²²²⁾, FISA 302 § ⁽²²³⁾, FISA 402 § ⁽²²⁴⁾, FISA 501 § ⁽²²⁵⁾ ja FISA 702 § ⁽²²⁶⁾) puitteissa siirrettyjä, EU:n rekisteröityjä koskevia henkilötietoja, kuten johdanto-osan 142–152 kappaleessa tarkennetaan.

⁽²¹⁹⁾ 5 U.S.C. 552 §.

⁽²²⁰⁾ Nämä poikkeukset ovat kuitenkin rajoitettuja. Esimerkiksi 5 U.S.C. 552 §:n b momentin 7 kohdan mukaan FOIA-oikeudet on suljettu pois, kun on kyse "tiedoista tai tiedoista, jotka on koottu lainvalvontaa varten, mutta vain siinä määrin, että tällaisten lainvalvontaan liittyvien tiedostojen tai tietojen luovuttaminen A) johtaisi siihen, että sen voitaisiin kohtuudella olettaa haittaavan täytäntöönpanomenettelyjä, B) riistäisi henkilöltä oikeuden oikeudenmukaiseen oikeudenkäyntiin tai puolueettomaan käsittelyyn tuomioistuimessa, C) johtaisi siihen, että sen voitaisiin kohtuudella odottaa muodostavan luvatun puuttumisen henkilön yksityisyyden suojaan, D) johtaisi siihen, että sen voitaisiin kohtuudella olettaa paljastavan luottamuksellisen lähteen henkilöllisyyden, mukaan lukien valtiollinen, paikallinen tai ulkomainen virasto tai viranomainen tai mikä tahansa yksityinen instituutio, joka on antanut tiedot luottamuksellisesti, ja jos on kyse tiedoista tai tiedoista, jotka on koottu lainvalvontaviranomainen rikostutkinnan yhteydessä tai virasto, joka suorittaa laillista kansalliseen turvallisuuteen liittyvää tiedustelua koskevaa tutkimusta, luottamuksellisen lähteen toimittamat tiedot, E) johtaisi lainvalvontaan liittyvässä tutkimuksessa tai syytteen nostamisessa käytettyjen tekniikoiden ja menettelyjen paljastumiseen tai lainvalvontaan liittyvässä tutkimuksessa tai syytteen nostamisessa käytettyjen ohjeiden paljastumiseen, jos kyseisen paljastumisen voitaisiin kohtuudella odottaa johtavan lain kiertämisen riskiin, tai F) johtaisi siihen, että sen voitaisiin kohtuudella odottaa vaarantavan henkilön hengen tai fyysisen turvallisuuden". Myös "aina silloin, kun tehdään pyyntö, johon liittyy pääsy tiedostoihin [joiden luovuttaminen voitaisiin kohtuudella odottaa haittaavan lainvalvontamenettelyjä] ja A) tutkimuksessa tai menettelyssä on kyse mahdollisesta rikosoikeuden rikkomisesta ja B) on syytä uskoa, että i) tutkimuksen tai menettelyn kohde ei ole tietoinen sen vireilläolosta ja että ii) tiedostojen olemassaolon paljastamisen voidaan kohtuudella odottaa voivan vaikuttaa lainvalvontamenettelyyn, virasto voi ainoastaan niin kauan kuin kyseinen tilanne jatkuu, katsoa, että tiedostoihin ei sovelleta tämän kohdan vaatimuksia". (5 U.S.C. 552 §:n 1 momentin c kohdan 1 alakohhta).

⁽²²¹⁾ 12 U.S.C. 3414 §; 15 U.S.C. 1681u–1681v §; ja 18 U.S.C. 2709 §. Ks. johdanto-osan 153 kappale.

⁽²²²⁾ 50 U.S.C. 1804 §, joka koskee perinteistä yksilöllistä sähköistä valvontaa.

⁽²²³⁾ 50 U.S.C. 1822 §, joka koskee fyysistä etsintää ulkomaantiedustelutarkoituksessa.

⁽²²⁴⁾ 50 U.S.C. 1842 § luettuna yhdessä 1841 §:n 2 momentin kanssa ja 18 osaston 3127 §, joka koskee lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien asentamista.

⁽²²⁵⁾ 50 U.S.C. 1861 §, jonka mukaan FBI voi "hakea määräystä, jonka nojalla yleinen liikenteenharjoittaja, julkinen majoituspalvelu, fyysinen varastotila tai ajoneuvojen vuokrauspalvelu saa luovuttaa hallussaan olevia tietoja ulkomaisten tiedustelutietojen keräämistä tai kansainvälistä terrorismia koskevaa tutkimusta varten".

⁽²²⁶⁾ 50 U.S.C. 1881a §, jonka nojalla Yhdysvaltojen tiedustelu-yhteisön toimijat voivat pyytää yhdysvaltalaisilta yrityksiltä pääsyä tietoihin, myös internetviestinnän sisältöön, niin, että kohteena ovat tietyt muut kuin yhdysvaltalaiset henkilöt Yhdysvaltojen ulkopuolella ja että sähköisiä viestintäpalveluja tarjoavat yritykset voidaan lain nojalla pakottaa avustamaan asiassa.

- (122) Yhdysvaltojen tiedusteluelimillä on myös mahdollisuus kerätä henkilötietoja Yhdysvaltojen ulkopuolella, mukaan lukien unionin ja Yhdysvaltojen välillä kulkevat henkilötiedot. Kerääminen Yhdysvaltojen ulkopuolella perustuu presidentin toimeenpanoasetukseen 12333 ⁽²²⁷⁾ ⁽²²⁸⁾.
- (123) Tietojen kerääminen signaalitiedustelun avulla on tämänhetkisen tietosuojan riittävyyden toteamisen kannalta merkityksellisin tiedustelutiedon keräämisen muoto, koska se koskee sähköisen viestinnän ja tietojen keräämistä tietojärjestelmistä. Yhdysvaltojen tiedusteluelimet voivat kerätä tietoja signaalitiedustelun avulla sekä Yhdysvalloissa (FISA-lain perusteella) että siinä yhteydessä, kun tietoja ollaan siirtämässä Yhdysvaltoihin (toimeenpanoasetuksen 12333 perusteella).
- (124) Yhdysvaltojen presidentti antoi 7 päivänä lokakuuta 2022 toimeenpanoasetuksen 14086 "Enhancing Safeguards for United States Signals Intelligence", jossa asetetaan rajoitukset ja suojatoimet kaikelle Yhdysvaltojen signaalitiedustelutoiminnalle. Toimeenpanoasetuksella korvataan suurelta osin presidentin määräys PPD 28 ⁽²²⁹⁾ ja vahvistetaan niitä edellytyksiä, rajoituksia ja suojatoimia, joita sovelletaan kaikkeen signaalitiedustelutoimintaan (eli FISA-lain ja toimeenpanoasetuksen 12333 perusteella) riippumatta siitä, missä se toteutetaan ⁽²³⁰⁾. Lisäksi sillä perustetaan uusi oikeussuojamekanismi, jonka avulla yksityishenkilöt ⁽²³¹⁾ voivat vedota näihin suojatoimiin ja vaatia niiden täytäntöönpanoa (ks. tarkemmin johdanto-osan 176–194 kappale). Näin toimeenpanoasetuksella on pantu täytäntöön Yhdysvaltojen lainsäädännössä EU:n ja Yhdysvaltojen välillä käytyjen neuvottelujen tulokset sen jälkeen, kun unionin tuomioistuin oli mitätöinyt tietosuojan tason riittävyyttä koskevan komission päätöksen (ks. johdanto-osan 6 kappale). Näin ollen kyseinen toimeenpanoasetus on erityisen tärkeä osa tässä päätöksessä arvioitua oikeudellista kehystä.
- (125) Toimeenpanoasetuksella 14086 käyttöön otetut rajoitukset ja suojatoimet täydentävät FISA-lain 702 §:ssä ja toimeenpanoasetuksessa 12333 säädettyjä rajoituksia ja suojatoimia. Tiedustelupalvelujen on sovellettava jäljempänä kuvattuja vaatimuksia (3.2.1.2 ja 3.2.1.3 jakso) FISA-lain 702 §:n ja toimeenpanoasetuksen 12333 mukaiseen signaalitiedustelutoimintaan esimerkiksi valitessaan/määritellessään FISA-lain 702 §:n nojalla hankittavien ulkomaantiedustelutietojen luokkia, kerätessään ulkomaantiedustelu- tai vastatiedustelutietoa toimeenpanoasetuksen 12333 nojalla ja tehdessään yksittäisiä kohdentamispäätöksiä FISA-lain 702 §:n ja toimeenpanoasetuksen 12333 nojalla.
- (126) Tässä presidentin antamassa toimeenpanoasetuksessa asetetut vaatimukset sitovat koko tiedusteluyhteisöä. Nämä vaatimukset on pantava täytäntöön virastojen toimintaperiaatteilla ja menettelyillä, joilla ne muunnetaan konkreettisiksi ohjeiksi päivittäistä toimintaa varten. Tältä osin toimeenpanoasetuksessa 14086 annetaan Yhdysvaltojen tiedusteluelimille enintään yksi vuosi aikaa päivittää nykyiset toimintaperiaatteensa ja menettelynsä (eli 7 päivään lokakuuta 2023 mennessä), jotta ne vastaisivat toimeenpanoasetuksen vaatimuksia. Tällaisia ajantasaistettuja toimintaperiaatteita ja menettelytapoja on kehitettävä ja asetettava yleisesti saataville yhteistyössä oikeusministerin, kansallisen tiedustelupalvelun johtajan toimiston kansalaisvapauksien suojelusta vastaavan virkamiehen (Civil Liberties Protection Officer of the Director of National Intelligence), jäljempänä 'ODNI CLPO', ja yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan (PCLOB), kanssa. PCLOB on riippumaton valvontaelin, jolla on lupa tarkistaa toimeenpanoavallan toimintapolitiikkoja ja niiden toteuttamista yksityisyyden ja kansalaisvapauksien suojelemiseksi (ks. johdanto-osan 110 kappale, joka koskee PCLOB:n tehtäviä ja asemaa) ⁽²³²⁾. Kun päivitetty toimintaperiaatteet ja menettelytavat on otettu käyttöön, PCLOB arvioi ne

⁽²²⁷⁾ EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981, sellaisena kuin se on muutettuna 30.7.2008). Toimeenpanoasetuksessa 12333 määritellään Yhdysvaltojen tiedustelutoiminnan tavoitteet, tarkoitus, tehtävät ja vastuut (mukaan lukien tiedusteluyhteisön eri toimijoiden roolit) ja vahvistetaan tiedustelutoiminnassa noudatettavat yleisperiaatteet.

⁽²²⁸⁾ Yhdysvaltojen perustuslain II artiklan mukaan vastuu kansallisen turvallisuuden varmistamisesta ja erityisesti ulkomaantiedustelutiedon keräämisestä kuuluu asevoimien ylipäällikkönä toimivan presidentin toimivaltaan.

⁽²²⁹⁾ Toimeenpanoasetus 14086 korvaa aikaisemman presidentin määräyksen 28 (PPD 28) lukuun ottamatta sen 3 §:ää ja täydentävää liitettä (jossa edellytetään, että tiedusteluelimet tarkistavat vuosittain signaalitiedustelun painopisteet ja vaatimukset ottaen huomioon signaalitiedustelutoiminnan hyödyt Yhdysvaltojen kansallisen edun kannalta sekä toiminnan aiheuttamat riskit) sekä 6 §:ää (joka sisältää yleisiä määräyksiä), ks. National Security Memorandum on Partial Revocation of Presidential Policy Directive 28: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>

⁽²³⁰⁾ Ks. toimeenpanoasetuksen 14086 5 §:n f momentti, jossa selitetään, että toimeenpanoasetuksella on sama soveltamisala kuin PPD 28:lla. PPD 28:aa sovellettiin sen alaviitteen 3 mukaan signaalitiedustelutoimintaan, jossa kerättiin viestintää tai viestintää koskevia tietoja, lukuun ottamatta signaalitiedustelutoimintaa, jonka tarkoituksena on testata ja kehittää signaalitiedusteluvalmiuksia.

⁽²³¹⁾ Ks. tältä osin esimerkiksi toimeenpanoasetuksen 14086 5 §:n h momentti, jossa selvennetään, että toimeenpanoasetuksen suojatoimet luovat lain mukaisen oikeutuksen ja että yksityishenkilöt voivat käyttää niitä oikeussuojamekanismin avulla.

⁽²³²⁾ Ks. EO 14086 2 §:n c momentin iv kohdan C alakohta.

varmistaa, että ne ovat yhdenmukaisia toimeenpanoasetuksen kanssa. Kunkin tiedusteluviraston on 180 päivän kuluessa siitä, kun PCLOB on saattanut tällaisen arvioinnin päätökseen, harkittava huolellisesti kaikkia PCLOB:n suosituksia ja pantava ne täytäntöön tai muutoin käsiteltävä niitä. Yhdysvaltojen hallitus julkaisi tällaiset päivitetty toimintaperiaatteet ja menettelyt 3. heinäkuuta 2023 ⁽²³³⁾.

3.2.1.2 Rajoitukset ja suojatoimet, jotka koskevat henkilötietojen keräämistä kansalliseen turvallisuuteen liittyviä tarkoituksia varten

- (127) Toimeenpanoasetuksessa 14086 on useita yleisiä vaatimuksia, jotka koskevat kaikkea signaalitiedustelutoimintaa (muun muassa henkilötietojen kerääminen, käyttö ja levittäminen).
- (128) Tällaisen toiminnan on perustuttava lakiin tai presidentin valtuutukseen, ja se on toteutettava Yhdysvaltain lainsäädännön, myös perustuslain, mukaisesti ⁽²³⁴⁾.
- (129) Käytössä on oltava asianmukaiset suojatoimet sen varmistamiseksi, että yksityisyyden suoja ja kansalaisvapaudet otetaan tällaisen toiminnan suunnittelussa huomioon olennaisina näkökohtina ⁽²³⁵⁾.
- (130) Varsinkin signaalitiedustelutoimintaa voidaan harjoittaa vasta sitten, kun on todettu, että toiminta on tarpeen validoitua tiedustelun painopistettä varten (ks. 'validoitu tiedustelun painopiste', johdanto-osan 135 kappale) ⁽²³⁶⁾.
- (131) Lisäksi tällaisia toimia voidaan toteuttaa vain siinä laajuudessa ja tavalla, joka on oikeassa suhteessa siihen validoituihin tiedustelun painopisteeseen, jota varten ne on hyväksytty ⁽²³⁷⁾. Toisin sanoen on saavutettava asianmukainen tasapaino kyseisen tiedustelun painopisteen merkittävyyden ja asianomaisten henkilöiden yksityisyyteen ja kansalaisvapauksiin kohdistuvien vaikutusten välillä heidän kansalaisuudestaan tai asuinpaikastaan riippumatta ⁽²³⁸⁾.
- (132) Signaalitiedustelutoimintaa valvotaan, jotta voidaan varmistaa näiden yleisten vaatimusten noudattaminen, jotka perustuvat lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteisiin (tarkempaa tietoa 3.2.2 kohdassa) ⁽²³⁹⁾.
- (133) Näitä yleisiä vaatimuksia perustellaan signaalitiedustelutietojen keräämisen osalta sillä, että käytössä on lukuisia ehtoja ja rajoituksia, joilla varmistetaan, että yksilöiden oikeuksiin puuttuminen rajoittuu siihen, mikä on tarpeen ja oikeasuhteista legitimiin tavoitteen saavuttamiseksi.
- (134) Toimeenpanoasetuksella rajoitetaan kahdella tavalla syitä, joiden perusteella tietoja voidaan kerätä osana signaalitiedustelutoimintaa. Toimeenpanoasetuksessa määritetään legitiimit tavoitteet, joihin signaalitiedustelutietojen keräämisellä voidaan pyrkiä. Niitä ovat esimerkiksi pyrkimys ymmärtää tai arvioida Yhdysvaltojen kansallista turvallisuutta uhkaavien tai mahdollisesti uhkaavien ulkomaisten organisaatioiden, esimerkiksi kansainvälisten terroristijärjestöjen, valmiuksia, pyrkimyksiä tai toimintaa, suojautua ulkomaisilta sotilaallisilta valmiuksilta ja toiminnalta ja ymmärtää tai arvioida maailmanlaajuisen turvallisuuteen vaikuttavia kansainvälisiä uhkia, kuten ilmastonmuutosta ja muita ekologisia muutoksia, kansanterveysriskejä ja humanitaarisia uhkia ⁽²⁴⁰⁾. Toisaalta toimeenpanoasetuksessa luetellaan tiettyjä tavoitteita, joita ei koskaan saa edistää signaalitiedustelutoiminnalla. Niitä

⁽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⁾ EO 14086 2 §:n a momentin i kohta.

⁽²³⁵⁾ EO 14086 2 §:n a momentin ii kohta.

⁽²³⁶⁾ EO 14086 2 §:n a momentin ii kohdan A alakohta. Tämä ei aina edellytä, että signaalitiedustelu olisi ainoa keino tutkia validoituihin tiedustelun painopisteeseen liittyviä näkökohtia. Signaalitiedustelutietojen keräämistä voidaan käyttää vaihtoehtoisten validointitapojen varmistamiseen (esimerkiksi muista tiedustelulähteistä saatujen tietojen vahvistamiseen) tai samojen tietojen luotettavan saatavuuden ylläpitämiseen (EO 14086 2 §:n c momentin i kohdan A alakohta).

⁽²³⁷⁾ EO 14086 2 §:n a momentin ii kohdan B alakohta.

⁽²³⁸⁾ EO 14086 2 §:n a momentin ii kohdan B alakohta.

⁽²³⁹⁾ EO 14086 2 §:n a momentin iii kohta luettuna yhdessä 2 §:n d momentin kanssa.

⁽²⁴⁰⁾ EO 14086 2 §:n b momentin i kohta. Koska toimeenpanoasetuksessa on rajattu oikeutettujen tavoitteiden luettelo, joka ei kata mahdollisia tulevia uhkia, toimeenpanoasetus antaa presidentille mahdollisuuden päivittää luetteloa, jos ilmenee uusia kansalliseen turvallisuuteen liittyviä välttämättömiä tarpeita, kuten kansalliseen turvallisuuteen kohdistuvia uusia uhkia. Tällaiset päivitykset on yleensä julkistettava, ellei presidentti päättää, että julkistaminen vaarantaisi Yhdysvaltojen kansallisen turvallisuuden (EO 14086, 2 §:n b momentin i kohdan B alakohta).

ovat esimerkiksi pyrkimykset vaikeuttaa yksilöiden tai tiedotusvälineiden harjoittamaa arvostelua, eriävien mielipiteiden ilmaisemista, ilmaisunvapautta tai poliittisten mielipiteiden ilmaisemista, saattaa ihmisiä huonompaan asemaan näiden etnisen alkuperän, rodun, sukupuolen, sukupuoli-identiteetin, seksuaalisen suuntautumisen tai uskonnon perusteella taikka antaa kilpailuetu yhdysvaltalaisille yrityksille ⁽²⁴¹⁾.

- (135) Tiedusteluelimet eivät voi vedota toimeenpanoasetuksessa 14086 määritettyihin legitiimeihin tavoitteisiin sellaisinaan perustellakseen signaalitiedustelutietojen keräämistä, vaan niiden pohjalta on osoitettava operatiivisia tarkoituksia varten konkreettisempia painopisteitä, joita varten signaalitiedustelutietoja voidaan kerätä. Toisin sanoen varsinainen kerääminen on mahdollista ainoastaan jonkin yksityiskohtaisemman painopisteen puitteissa. Tällaiset painopisteet vahvistetaan erityisessä prosessissa, jonka tarkoituksena on varmistaa sovellettavien lakisääteisten vaatimusten noudattaminen, mukaan lukien yksityisyyden suojaan ja kansalaisvapauksiin liittyvät vaatimukset. Tiedustelun painopisteet laatii kansallisen tiedusteluviraston johtaja (ns. kansallisia tiedustelun painopisteitä koskevassa kehityksessä), minkä jälkeen ne toimitetaan presidentin hyväksyttäväksi ⁽²⁴²⁾. Ennen kuin johtaja ehdottaa presidentille tiedustelun painopisteitä, hänen on toimeenpanoasetuksen 14086 mukaisesti hankittava kunkin painopisteen osalta ODNI CLPO:n arvio seuraavista: 1) edistääkö painopiste yhtä tai useampaa toimeenpanoasetuksessa lueteltua legitiimiä tavoitetta, 2) onko painopiste sellainen, että sitä ei ole suunniteltu eikä sen odoteta johtavan signaalitiedustelutietojen keräämiseen toimeenpanoasetuksessa kiellettyä tavoitetta varten ja 3) onko painopiste vahvistettu sen jälkeen, kun on otettu asianmukaisesti huomioon kaikkien henkilöiden yksityisyyden suoja ja kansalaisvapaudet heidän kansalaisuudestaan tai asuinpaikastaan riippumatta ⁽²⁴³⁾. Jos johtaja on eri mieltä CLPO:n arviosta, presidentille on esitettävä molemmat näkemykset ⁽²⁴⁴⁾.
- (136) Näin ollen tällä prosessilla varmistetaan erityisesti, että yksityisyyden suoja koskevat näkökohdat otetaan huomioon jo tiedustelun painopisteitä laadittaessa.
- (137) Kun tiedustelun painopiste on vahvistettu, on lisäksi otettava huomioon useita vaatimuksia päätettäessä, voidaanko tällaisen painopisteen puitteissa kerätä tietoja signaalitiedustelulla ja missä määrin. Näillä vaatimuksilla pannaan täytäntöön toimeenpanoasetuksen 2 §:n a momentissa vahvistetut yleiset tarpeellisuus- ja oikeasuhteisuusvaatimukset.
- (138) Signaalitiedustelutoimintaa voidaan harjoittaa ainoastaan, ”kun kaikkien asiaankuuluvien tekijöiden perustellun arvioinnin jälkeen on todettu, että tietojen kerääminen on tarpeen tiettyä tiedustelun painopistettä varten” ⁽²⁴⁵⁾. Kun Yhdysvaltojen tiedusteluelimet määrittävät, onko määritettyjä tietoja tarpeen kerätä validoitua tiedustelun painopistettä varten signaalitiedustelun avulla, niiden on otettava huomioon muiden, vähemmän yksityisyyteen puuttuvien lähteiden ja menetelmien, myös diplomaattisten ja julkisten lähteiden, saatavuus, käytettävyyys ja asianmukaisuus ⁽²⁴⁶⁾. Tällaiset vaihtoehtoiset, vähemmän yksityisyyteen puuttuvat lähteet ja menetelmät on asetettava etusijalle, jos niitä on saatavilla ⁽²⁴⁷⁾.
- (139) Kun tällaisia kriteerejä sovellettaessa katsotaan, että on tarpeen kerätä tietoja signaalitiedustelulla, keruun on oltava niin räätälöityä kuin mahdollista eikä sillä saa olla kohtuuttomia vaikutuksia yksityisyyden suojaan ja kansalaisvapauksiin ⁽²⁴⁸⁾. Jotta voidaan varmistaa, että yksityisyyden suojalle ja kansalaisvapaudelle ei aiheudu kohtuuttomia vaikutuksia – eli voidaan löytää tasapaino kansallisen turvallisuuden tarpeiden ja yksityisyyden ja kansalaisvapauksien suojelun välille –, on otettava asianmukaisesti huomioon kaikki asiaankuuluvat tekijät, esimerkiksi asetetun tavoitteen luonne, keräystoiminnan vaikutus yksityisyyteen ja sen kesto, keräyksen odotettavissa oleva vaikutus asetettuun tavoitteeseen, kohtuudella ennakoitavissa olevat seuraukset yksilöille sekä kerättävien tietojen luonne ja arkaluonteisuus ⁽²⁴⁹⁾.

⁽²⁴¹⁾ EO 14086 2 §:n b momentin ii kohta.

⁽²⁴²⁾ National Security Act, 102A §, ja EO 14086, 2 §:n b momentin iii kohta.

⁽²⁴³⁾ Poikkeustapauksissa (erityisesti silloin, kun tällaista prosessia ei voida toteuttaa, koska on vastattava uuteen tai kehitymässä olevaan tiedustelutarpeeseen) tällaiset painopisteet voi määrittää suoraan presidentti tai jonkin tiedusteluyhteisön toimijan johtaja, joiden on periaatteessa sovellettava samoja perusteita kuin ne esitetään toimeenpanoasetuksen 14086 2 §:n b momentin iii kohdan A alakohdan 1–3 alakohdassa, ks. myös saman toimeenpanoasetuksen 4 §:n momentti.

⁽²⁴⁴⁾ EO 14086 2 §:n b momentin iii kohdan C alakohta.

⁽²⁴⁵⁾ EO 14086 2 §:n b momentti ja c momentin i kohdan A alakohta.

⁽²⁴⁶⁾ EO 14086 2 §:n c momentin i kohdan A alakohta.

⁽²⁴⁷⁾ EO 14086 2 §:n c momentin i kohdan A alakohta.

⁽²⁴⁸⁾ EO 14086 2 §:n c momentin i kohdan B alakohta.

⁽²⁴⁹⁾ EO 14086 2 §:n c momentin i kohdan B alakohta.

(140) Koska tämä päätös tietosuojan riittävyydestä koskee Yhdysvalloissa sijaitseville organisaatioille siirrettäviä tietoja, sen kannalta on eniten merkitystä sillä, miten tietoja kerätään signaalitiedustelun avulla Yhdysvalloissa. Tällaisen tietojenkeruun on aina oltava kohdennettua, kuten johdanto-osan 142–153 kappaleessa tarkemmin selitetään.

(141) 'Valikoimatonta keruuta' ⁽²⁵⁰⁾ voidaan suorittaa ainoastaan Yhdysvaltojen ulkopuolella toimeenpanoasetuksen 12333 perusteella. Myös tässä tapauksessa on toimeenpanoasetuksen 14086 mukaan asetettava etusijalle kohdennettu keruu ⁽²⁵¹⁾. Toisin sanoen valikoimaton keruu on sallittua vain, jos validoitua tiedustelun painopistettä tukevia tietoja ei voida kohtuudella saada kohdennetulla keruulla ⁽²⁵²⁾. Jos tietojen valikoimaton keruu on tarpeen Yhdysvaltojen ulkopuolella, siihen sovelletaan toimeenpanoasetuksen 14086 mukaisia erityisiä suoja-toimia ⁽²⁵³⁾. Ensinnäkin on käytettävä erilaisia menetelmiä ja teknisiä toimenpiteitä kerättävien tietojen rajaamiseksi vain siihen, mikä on tarpeen validoitua tiedustelun painopistettä varten, ja minimoitava merkityksettömien tietojen kerääminen ⁽²⁵⁴⁾. Lisäksi toimeenpanoasetuksessa rajataan valikoimattomasti kerättyjen tietojen käyttö (myös kyselyt) kuuteen tavoitteeseen, joihin kuuluvat terrorismin torjunta, panttivankitilanteet ja henkilöiden pitäminen vankina ulkomaisen hallituksen, järjestön tai henkilön toimesta tai puolesta, suojautuminen ulkomaiselta vakoilulta, sabotaasilta tai salamurhilta sekä suojautuminen joukkotuhouksien kehittämisestä, hallussapidosta tai levittämisestä taikka niihin liittyvistä teknologioista aiheutuvilta uhkilta ⁽²⁵⁵⁾. Kaikenlainen kyselyjen tekeminen tiedoista, jotka on koottu valikoimattomasti signaalitiedustelun avulla, on sallittu vain, jos se on tarpeen validoitua tiedustelun painopistettä varten ja näiden kuuden tavoitteen saavuttamiseksi ja jos siinä noudatetaan sellaisia toimintaperiaatteita ja menettelytapoja, joissa otetaan asianmukaisesti huomioon kyselyjen vaikutus kaikkien henkilöiden yksityisyyteen ja kansalaisvapauksiin riippumatta heidän kansalaisuudestaan tai siitä, missä he asuvat ⁽²⁵⁶⁾.

(142) Toimeenpanoasetuksen 14086 vaatimusten lisäksi Yhdysvalloissa sijaitsevalle organisaatiolle siirrettyjen tietojen keräämiseen signaalitiedustelulla sovelletaan FISA-lain 702 §:n mukaisia erityisiä rajoituksia ja suoja-toimia ⁽²⁵⁷⁾. FISA-lain 702 § mahdollistaa ulkomaisten tiedustelutietojen keräämisen kohdistamalla tiedustelutoimintaa muihin kuin yhdysvaltalaisiin henkilöihin, joiden voidaan kohtuudella olettaa oleskelevan Yhdysvaltojen ulkopuolella, siten, että yhdysvaltalaisia sähköisten viestintäpalvelujen tarjoajia veloitetaan avustamaan tässä ⁽²⁵⁸⁾. Ulkomaisten tiedustelutietojen keräämiseksi FISA-lain 702 §:n nojalla oikeusministeri ja kansallisen tiedustelupalvelun johtaja

⁽²⁵⁰⁾ Toisin sanoen sellaisten suurten signaalitiedustelussa saatujen tietomäärien kerääminen, jotka teknisistä tai toiminnallisista syistä hankitaan ilman erottelutekijöitä (esimerkiksi ilman erityisiä tunnisteita tai valintakriteerejä), ks. EO 14086, 4 §:n b momentti. Toimeenpanoasetuksen 14086 mukaan, ja kuten johdanto-osan 141 kappaleessa tarkemmin selitetään, toimeenpanoasetuksen 12333 mukainen valikoimaton keruu suoritetaan ainoastaan, kun se on tarpeen tiettyjen validoitujen tiedustelun painopisteiden puitteissa, ja siihen sovelletaan useita rajoituksia ja suoja-toimia, joiden tarkoituksena on estää tietojen summittainen käyttö. Valikoimatonta keruuta on siksi tarkasteltava suhteessa yleisluonteiseen ja summittaiseen keruuseen ("joukkovalvonta"), johon ei sovelleta mitään rajoituksia tai suoja-toimia.

⁽²⁵¹⁾ EO 14086 2 §:n c momentin ii kohdan A alakohta.

⁽²⁵²⁾ EO 14086 2 §:n c momentin ii kohdan A alakohta.

⁽²⁵³⁾ Toimeenpanoasetuksen 14086 valikoimatonta keruuta koskevia erityissääntöjä sovelletaan myös kohdennettuun signaalitiedustelussa tapahtuvaan tiedonkeruuseen, jossa tilapäisesti käytetään rajaamattomasti (esim. ilman erityisiä valintatermejä tai tunnisteita) hankittuja tietoja eli valikoimatonta keruuta (joka on mahdollista vain Yhdysvaltojen alueen ulkopuolella). Näin ei ole silloin, kun tällaisia tietoja käytetään ainoastaan kohdennetun signaalitiedustelutoiminnan teknisen alkuvaiheen tukena, säilytetään vain lyhyen ajan tämän vaiheen loppuun saattamiseksi ja poistetaan välittömästi sen jälkeen (toimeenpanoasetuksen 14086 2 §:n c momentin ii kohdan D alakohta). Tässä tapauksessa alkuvaiheen valikoimattoman keruun ainoa tarkoitus on mahdollistaa kohdennettu tietojen keruu tiettyä tunnisteiden tai valintatermien avulla. Tällaisessa tilanteessa hallituksen tietokantoihin lisätään vain tietyn erottelutekijän avulla löytyvät tiedot, ja loput tiedot tuhotaan. Tällaista kohdennettua keruuta säännellään siksi edelleen signaalitiedustelulaisten keruuseen sovellettavilla yleisillä säännöillä, ja myös toimeenpanoasetuksen 14086 2 §:n a–b momentilla ja 2 §:n c momentin i kohdalla.

⁽²⁵⁴⁾ EO 14086 2 §:n c momentin ii kohdan A alakohta.

⁽²⁵⁵⁾ EO 14086 2 §:n c momentin ii kohdan B alakohta. Presidentti voi päivittää tätä luetteloa, jos ilmenee uusia kansallista turvallisuutta koskevia vaatimuksia, kuten kansalliseen turvallisuuteen kohdistuvia uusia uhkia. Tällaiset päivitykset on yleensä julkistettava, ellei presidentti päättää, että julkistaminen vaarantaisi Yhdysvaltojen kansallisen turvallisuuden (EO 14086, 2 §:n c momentin ii kohdan C alakohta). Valikoimattomasti kerättyjen tietojen kyselyt, ks. EO 14086 2 §:n c momentin iii kohdan D alakohta.

⁽²⁵⁶⁾ EO 14086 2 §:n a momentin ii kohdan A alakohta luettuna yhdessä 2 §:n c momentin iii kohdan D alakohdan kanssa. Ks. myös liite VII.

⁽²⁵⁷⁾ 50 U.S.C. 1881 §.

⁽²⁵⁸⁾ 50 U.S.C. 1881a §:n a momentti. Kuten PCLOB on huomauttanut, 702 §:ssä tarkoitettua valvonnan "kohteena ovat tietyt [ei-yhdysvaltalaiset] henkilöt, jotka on määritetty yksilöllisesti" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2.7.2014, Section 702 Report, s. 111). Ks. myös NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. 'Sähköisten viestintäpalvelujen tarjoaja' määritellään 50 U.S.C. 1881 §:n a momentin 4 kohdassa.

toimittavat ulkomaantiedustelun valvonnasta vastaavalle tuomioistuimelle (Foreign Intelligence Surveillance Court), jäljempänä 'FISC-tuomioistuin', vuotuiset sertifiointit, joissa yksilöidään hankittavien ulkomaisten tiedustelutietojen luokat ⁽²⁵⁹⁾. Sertifiointeihin on liitettävä kohdentamis-, minimointi- ja kyselymenettelyt, jotka myös tuomioistuin on hyväksynyt ja jotka sitovat oikeudellisesti yhdysvaltalaisia tiedustelupalveluja.

- (143) FISC on liittovaltion lainsäädännön nojalla perustettu riippumaton tuomioistuin ⁽²⁶⁰⁾, jonka päätöksiin voidaan hakea muutosta ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimelta (Foreign Intelligence Surveillance Court of Review), jäljempänä 'FISCR-tuomioistuin' ⁽²⁶¹⁾, ja viime kädessä Yhdysvaltojen korkeimmalta oikeudelta ⁽²⁶²⁾. FISC-tuomioistuimen (ja FISCR-tuomioistuimen) tukena on viidestä lakimiehestä ja viidestä teknisestä asiantuntijasta koostuva pysyvä paneeli. Sen jäsenillä on kokemusta kansalliseen turvallisuuteen ja kansalaisvapauksiin liittyvistä kysymyksistä ⁽²⁶³⁾. Tuomioistuin nimittää ryhmästä yhden toimimaan *amicus curiae* -ominaisuudessa tehtäväänään avustaa määräystä tai muutoksenhakua koskeissa hakemuksissa, joissa tuomioistuimen mukaan on kyse uudesta tai merkittävästä lainsäädännön tulkinnasta, paitsi jos tuomioistuin katsoo, että kyseinen nimitys ei ole asianmukainen ⁽²⁶⁴⁾. Tällä varmistetaan erityisesti, että yksityisyyden suojaan liittyvät näkökohdat otetaan asianmukaisesti huomioon tuomioistuimen tekemässä arvioinnissa. Tuomioistuin voi myös nimittää yksittäisen henkilön tai organisaation toimimaan *amicus curiae*na, esimerkiksi toimimaan teknisenä asiantuntijana, kun se katsoo sen tarpeelliseksi, tai antaa yksittäiselle henkilölle tai organisaatiolle tämän hakemuksesta luvan saada esittää *amicus curiae* -kirjelmä ⁽²⁶⁵⁾.
- (144) FISC-tuomioistuin käy läpi sertifiointit ja niihin liittyvät menettelyt (erityisesti kohdentamis- ja minimointimenettelyt) FISA-lain vaatimusten noudattamiseksi. Jos se katsoo, että vaatimukset eivät täyty, se voi evätä sertifiointin kokonaan tai osittain ja vaatia menettelyjen muuttamista ⁽²⁶⁶⁾. FISC-tuomioistuin on vahvistanut tältä osin toistuvasti, että sen 702 §:n mukaisten kohdentamis- ja minimointimenettelyjen tarkastelu ei rajoitu kirjallisiin menettelyihin vaan sisältää myös sen, miten hallitus panee menettelyt täytäntöön ⁽²⁶⁷⁾.
- (145) Kansallinen turvallisuusvirasto NSA (FISA-lain 702 §:n nojalla kohdentamisesta vastaava tiedusteluelin) tekee yksittäiset kohdentamismääritykset FISC-tuomioistuimen hyväksymien kohdentamisenmenettelyjen mukaisesti. Menettelyissä edellytetään, että kansallinen turvallisuusvirasto arvioi kaikkien olosuhteiden perusteella, että tiettyyn henkilöön tehtävällä kohdentamisella saadaan todennäköisesti sertifiointissa yksilöityä tietyn luokan ulkomaantiedustelutietoa ⁽²⁶⁸⁾. Tämä arviointi on täsmennettävä, ja sen on perustuttava tosiseikkoihin, analyttiseen arviointiin,
- ⁽²⁵⁹⁾ 50 U.S.C. 1881a §:n g momentti.
- ⁽²⁶⁰⁾ FISC-tuomioistuin koostuu Yhdysvaltojen korkeimman oikeuden presidentin nimittämistä tuomareista. Tuomarit valitaan Yhdysvaltojen presidentin nimittämistä piirituomareista, joiden nimityksen senaatti on vahvistanut. Tuomarit nimitetään eliniäkseen, ja nimitys voidaan peruuttaa ainoastaan hyvän synn vuoksi. Toimikaudet FISC-tuomioistuimessa on porrastettu, ja toimikauden pituus on seitsemän vuotta. FISA-lain mukaan tuomarit on valittava vähintään seitsemästä Yhdysvaltojen tuomiopiiristä. Ks. 50 U.S.C. 1803 §:n a momentti. Tuomareiden tukena on kokeneita juristiavustajia, jotka muodostavat tuomioistuimen oikeudellisen henkilöstön ja valmistelevat tietojen keruupyynnöiden oikeudellisen analyysin. Ks. ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen puheenjohtajan Reggie B. Waltonin kirje senaatin oikeusasioiden valiokunnan puheenjohtajalle Patrick J. Leahylle, jäljempänä 'Waltonin kirje', 29.7.2013, s. 2, saatavilla osoitteessa <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>
- ⁽²⁶¹⁾ FISCR-tuomioistuin koostuu Yhdysvaltojen korkeimman oikeuden presidentin nimittämistä tuomareista, jotka valitaan Yhdysvaltojen liittovaltion piirituomioistuimista tai muutoksenhakutuomioistuimista. Tuomarien toimikaudet on porrastettu, ja yhden toimikauden pituus on seitsemän vuotta. Ks. 50 U.S.C. 1803 §:n b momentti.
- ⁽²⁶²⁾ Ks. 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h) ja 1881 a (i)(4).
- ⁽²⁶³⁾ 50 U.S.C. 1803 §:n i momentin 1 kohta ja 3 kohdan A alakohta.
- ⁽²⁶⁴⁾ 50 U.S.C. 1803 §:n i momentin 2 kohdan A alakohta.
- ⁽²⁶⁵⁾ 50 U.S.C. 1803 §:n i momentin 2 kohdan B alakohta.
- ⁽²⁶⁶⁾ Ks. esim. FISC:n lausunto 18. lokakuuta 2018 (saatavilla osoitteessa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf), minkä ulkomaantiedustelun muutoksenhakutuomioistuin vahvisti 12. heinäkuuta 2019 antamallaan lausunnolla (saatavilla osoitteessa: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf).
- ⁽²⁶⁷⁾ Ks. esimerkiksi FISC, Memorandum Opinion and Order, s. 35 (18.11.2020) (hyväksytty julkaistavaksi 26.4.2021) (liite D).
- ⁽²⁶⁸⁾ 50 U.S.C. 1881a §:n a momentti, kansallisen turvallisuusviraston käyttämät menettelyt ei-yhdysvaltalaisen henkilön, joiden voidaan kohtuudella uskoa olevan Yhdysvaltojen ulkopuolella, kohdentamiseksi ulkomaantiedustelutiedon hankintaa varten ulkomaantiedustelun valvontaa koskevan vuoden 1978 lain (Foreign Intelligence Surveillance Act of 1978), sellaisena kuin se on muutettuna maaliskuussa 2018, 702 §:n mukaisesti (kansallisen turvallisuusviraston kohdentamisenmenettelyt) (saatavilla osoitteessa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf), s. 1–4, selitetty tarkemmin PCLOB:n raportissa, s. 41 ja 42.

analyytikon erityiskoulutukseen ja kokemukseen sekä hankittavan ulkomaantiedustelutiedon luonteeseen ⁽²⁶⁹⁾. Kohdentaminen toteutetaan yksilöimällä niin kutsutut valintakriteerit, joilla määritetään tietyt viestintävälineet, kuten kohteen sähköpostiosoite tai puhelinnumero, mutta ei koskaan avainkäsitteitä tai henkilöiden nimiä ⁽²⁷⁰⁾.

- (146) Ensinnä kansallisen turvallisuusviraston analyttikot yksilöivät ne ulkomailla olevat ei-yhdysvaltalaiset henkilöt, joiden valvonta analyttikkojen arvion mukaan johtaa sertifiointipäätöksessä määriteltyyn ulkomaantiedustelutietoon ⁽²⁷¹⁾. Kuten kansallisen turvallisuusviraston kohdentamismenettelyissä todetaan, kansallinen turvallisuusvirasto voi kohdistaa valvontaa kohteeseen vain, jos se on jo saanut kohteesta jotakin tietoa ⁽²⁷²⁾. Tämä voi perustua eri lähteistä, esimerkiksi henkilötiedustelusta, saatuihin tietoihin. Analyttikon on saatava näistä muista lähteistä tietoa myös mahdollisen kohteen käyttämästä erityisestä valintakriteeristä (eli viestintävälineestä). Sen jälkeen, kun henkilöt on yksilöity ja heidän kohdentamisensa on hyväksytty kansallisen turvallisuusviraston kattavassa arviointijärjestelmässä ⁽²⁷³⁾, laaditaan valintakriteerit ja sovelletaan niitä ("tasked selectors"). Näiden kriteerien avulla määritetään kohteiden käyttämät viestintävälineet (esimerkiksi sähköpostiosoitteet) ⁽²⁷⁴⁾.

- (147) Kansallisen turvallisuusviraston on dokumentoitava tosiasialliset syyt, joiden vuoksi henkilö on valittu tiedustelun kohteeksi ⁽²⁷⁵⁾, ja vahvistettava säännöllisin väliajoin alkuperäisen kohdentamisen jälkeen, että kohdentamisperuste täyttyy edelleen ⁽²⁷⁶⁾. Kun kohdentamisperuste ei enää täyty, tietojen keruu on lopetettava ⁽²⁷⁷⁾. Kansallisen turvallisuusviraston suorittaman kohteen valinnan ja kirjatun kohdentamisarviointin tulosten ja perustelujen tarkastelusta kohdentamismenettelyjen noudattamisen osalta vastaavat kahden kuukauden välein oikeusministeriön tiedusteluvälikomitean toimivat virkamiehet, joiden velvollisuutena on ilmoittaa mahdollisista rikkomisista FISC-tuomioistuimelle ja kongressille ⁽²⁷⁸⁾. Kansallisen turvallisuusviraston kirjalliset asiakirjat helpottavat FISC-tuomioistuimen suorittamaa valvontaa sen suhteen, onko tietyt henkilöt kohdennettu asianmukaisesti FISA-lain 702 §:n nojalla, johdanto-osan 173 ja 174 kappaleessa kuvattujen valvontavaltuuksien mukaisesti ⁽²⁷⁹⁾. Kansallisen tiedusteluviraston (DNI) johtajan on myös raportoitava FISA-lain 702 §:n mukaisten kohteiden kokonaismäärä vuosittain julkaistavissa tilastollisissa avoimuusraporteissa. Yritykset, jotka saavat FISA-lain 702 §:n mukaisia määräyksiä, voivat julkaista saamiaan pyyntöjä koskevat tiedot yhteen koottuina (avoimuusraporteissa) ⁽²⁸⁰⁾.

⁽²⁶⁹⁾ Kansallisen turvallisuusviraston kohdentamismenettelyt, s. 4.

⁽²⁷⁰⁾ Ks. PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 32, 33 ja 45 sekä muut viitteet. Ks. myös oikeusministerin ja kansallisen tiedusteluviraston johtajan puolivuositilauksen laatima arvio FISA-lain 702 §:n noudattamisesta (Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence), raportointikausi 1.12.2016–31.5.2017, s. 41 (lokakuu 2018) (saatavilla osoitteessa https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf).

⁽²⁷¹⁾ PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 42 ja 43.

⁽²⁷²⁾ Kansallisen turvallisuusviraston kohdentamismenettelyt, s. 2.

⁽²⁷³⁾ PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 46. Kansallisen turvallisuusviraston on esimerkiksi varmistettava, että kohteen ja valintakriteerin välillä on yhteys, ja dokumentoitava ulkomaantiedustelutiedot, jotka on tarkoitus hankkia. Kahden kansallisen turvallisuusviraston vanhemman analyttikon on tarkastettava ja hyväksyttävä kyseiset tiedot, ja koko prosessia seurataan, jotta ODNI ja oikeusministeriö voivat myöhemmin suorittaa periaatteiden noudattamista koskevan tarkastelun. Ks. NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.4.2014.

⁽²⁷⁴⁾ 50 U.S.C. 1881a §:n h momentti.

⁽²⁷⁵⁾ Kansallisen turvallisuusviraston kohdentamismenettelyt, s. 8. Ks. myös PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 46. Kirjallisten perustelujen toimittamatta jättäminen on dokumentaatioon liittyvä rikkominen, josta on ilmoitettava FISC-tuomioistuimelle ja kongressille. Ks. oikeusministerin ja kansallisen tiedusteluviraston johtajan puolivuositilauksen laatima arvio FISA-lain 702 §:n noudattamisesta (Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence), raportointijakso 1.12.2016–31.5.2017, s. 41 (lokakuu 2018), oikeusministeriön/ODNI:n vaatimustenmukaisuusraportti FISC-tuomioistuimelle, joulukuu 2016 – toukokuu 2017 (DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017), s. A-6 (saatavilla osoitteessa https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf).

⁽²⁷⁶⁾ Ks. Yhdysvaltojen hallituksen ilmoitus FISC-tuomioistuimelle (U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements), s. 2 ja 3 (15.7.2015) ja liitteessä VII annetut tiedot.

⁽²⁷⁷⁾ Ks. Yhdysvaltojen hallituksen ilmoitus FISC-tuomioistuimelle (U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements), s. 2 ja 3 (15.7.2015); ilmoituksessa todetaan, että jos hallitus myöhemmin arvioi, että kohteen valintakriteerin käytön jatkamisen ei odoteta johtavan ulkomaantiedustelutiedon saamiseen, tehtävä on lopetettava pikaisesti, ja tämän viivästyminen voi johtaa raportoitavaan säännösten rikkomiseen. Ks. myös liitteessä VII esitetyt tiedot.

⁽²⁷⁸⁾ PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 70–72; Yhdysvaltojen FISC-tuomioistuimen työjärjestyksen säännön 13 kohdan b alakohta (saatavilla osoitteessa <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>).

⁽²⁷⁹⁾ Ks. myös oikeusministeriön/ODNI:n vaatimustenmukaisuusraportti FISC-tuomioistuimelle, joulukuu 2016 – toukokuu 2017 (DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017), s. A-6.

⁽²⁸⁰⁾ 50 U.S.C. 1874 §.

- (148) Muihin oikeusperustoihin, jotka koskevat organisaatioille siirrettyjen henkilötietojen keräämistä Yhdysvalloissa, sovelletaan erilaisia rajoituksia ja suoja-toimia. Yleisesti ottaen tietojen valikoimaton keruu on nimenomaisesti kielletty FISA-lain 402 §:n (lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmät (pen registers, trap and trace authority)) nojalla ja NSL:ää käyttäen, ja sen sijaan vaaditaan erityisten "valintakriteerien" käyttöä ⁽²⁸¹⁾.
- (149) Perinteisen yksilöllisen sähköisen valvonnan toteuttamiseksi (FISA-lain 105 §:n mukaisesti) tiedusteluelinten on toimitettava FISC-tuomioistuimelle hakemus, jossa esitetään tosiseikat ja olosuhteet, joihin vedotaan sen perustelemiseksi, että on todennäköisiä syitä uskoa, että vieras valta tai sen asiamies ⁽²⁸²⁾ käyttää tai aikoo käyttää tiettyä välinettä. FISC-tuomioistuin arvioi muun muassa sen, onko esitettyjen tosiseikkojen perusteella todennäköistä, että näin todella on ⁽²⁸³⁾.
- (150) FISC-tuomioistuimen antamaa määräystä on haettava, jotta voidaan tehdä tilojen tai omaisuuden etsintä, jonka tarkoituksena on tietojen, aineiston tai omaisuuden (esimerkiksi tietokonelaitteen) tutkinta, takavarikointi tms. FISA-lain 301 §:n perusteella ⁽²⁸⁴⁾. Tällaisella hakemuksella on muun muassa osoitettava, että on olemassa todennäköinen syy siihen, että etsinnän kohteena on vieras valta tai sen asiamies, että etsittävässä tilassa on tai etsittävään omaisuuteen sisältyy ulkomaantiedustelutietoa ja että etsittävä tila on vieraan vallan (asiamiehen) omistuksessa, käytössä tai hallussa tai siirrettävänä sille tai siltä ⁽²⁸⁵⁾.
- (151) Samoin lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien (pen registers, trap and trace devices) asentaminen (FISA-lain 402 §:n mukaisesti) edellyttää hakemuksen tekemistä FISC-tuomioistuimen (tai yhdysvaltalaisen alemman oikeusasteen tuomarin) määräyksen saamiseksi ja erityisen valintakriteerin käyttöä, eli kriteerin, joka nimenomaisesti yksilöi henkilön, tilin tms. ja jota käytetään niin suuressa määrin kuin on kohtuullista haluttujen tietojen laajuuden rajoittamiseksi ⁽²⁸⁶⁾. Tämä oikeusperusta ei koske viestinnän sisältöä, vaan tavoitteena on saada tietoa palvelua käyttävästä asiakkaasta tai tilaajasta (kuten nimi, osoite, tilaajanumero, vastaanotetun palvelun pituus ja tyyppi, maksun alkuperä ja mekanismi).
- (152) FISA-lain 501 §:ssä ⁽²⁸⁷⁾ sallitaan liiketoimintatietojen kerääminen yleisestä kuljetusliikkeestä (eli henkilöstä tai oikeushenkilöstä, joka kuljettaa ihmisiä tai omaisuutta maitse, rautateitse, vesiteitse tai ilmateitse korvausta vastaan), julkisista majoituspalveluista (esimerkiksi hotellista, motellista tai matkustajakodista), ajoneuvojen vuokrauspalvelusta tai fyysisestä varastotilasta (eli tilasta tavaroiden ja aineiden varastointiin tai siihen liittyvistä palveluista) ⁽²⁸⁸⁾. Kyseisen pykälän mukaan myös tämä edellyttää hakemusta FISC-tuomioistuimelle tai alemman oikeusasteen tuomarille. Hakemuksessa on eriteltävä halutut tiedot sekä erityiset ja ymmärrettävät tosiseikat, joiden perusteella on syytä uskoa, että tietoihin liittyvä henkilö on vieras valta tai vieraan vallan asiamies ⁽²⁸⁹⁾.
- (153) Lisäksi eri säädöksissä sallitaan kansallista turvallisuutta koskevat kirjeet (NSL), ja tutkinnasta vastaavat virastot voivat hankkia niiden avulla tietyiltä tahoilta (esimerkiksi rahoituslaitoksilta, luottotietoselvitystoimistoilta, sähköisen viestinnän tarjoajilta) määrättyjä tietoja (viestinnän sisältöä lukuun ottamatta), jotka sisältyvät luottoraportteihin, kirjanpitoon sekä sähköisissä tilausasiakas- ja liiketapahtumarekistereissä oleviin tietoihin ⁽²⁹⁰⁾. Sähköiseen viestintään pääsyn sallimisesta annettua NSL:ää koskevaa säädöstä voi hyödyntää ainoastaan FBI, ja edellytyksenä on sellaisen kriteerin käyttö, jolla nimenomaisesti yksilöidään henkilö, oikeushenkilö, puhelinnumero tai tili ja jolla todistetaan, että tiedoilla on merkitystä hyväksytylle kansallista turvallisuutta koskevalle tutkimukselle kansainväliseltä terrorismilta tai salaiselta tiedustelutoiminnalta suojautumiseksi ⁽²⁹¹⁾. NSL:n vastaanottaja voi vastustaa kirjeessä esitettyjä vaatimuksia viemällä asian tuomioistuimen käsiteltäväksi ⁽²⁹²⁾.

⁽²⁸¹⁾ 50 U.S. Code 1842 §:n c momentin 3 kohta ja NSL:n osalta 12 U.S.C. 3414 §:n a momentin 2 kohta, 15 U.S.C. 1681u §; 15 U.S.C. 1681v §; ja 18 U.S.C. 2709 §:n a momentti.

⁽²⁸²⁾ "Vieraan vallan asiamiehellä" voidaan tarkoittaa myös ei-yhdysvaltalaisia henkilöitä, jotka harjoittavat kansainvälistä terrorismia tai joukkotuhoaseiden kansainvälistä levittämistä (mukaan luettuna valmistelevat toimet) (50 U.S.C. 1801 §:n b momentin 1 kohta).

⁽²⁸³⁾ 50 U.S.C. 1804 §. Ks. myös 1841 §:n 4 momentti valintakriteerien valinnan osalta.

⁽²⁸⁴⁾ 50 U.S.C. 1821 §:n 5 momentti.

⁽²⁸⁵⁾ 50 U.S.C. 1823 §:n a momentti.

⁽²⁸⁶⁾ 50 U.S.C. 1842 § ja 1841 §:n 2 momentti sekä 18 osaston 3127 §.

⁽²⁸⁷⁾ 50 U.S.C. 1862 §.

⁽²⁸⁸⁾ 50 U.S.C. 1861 ja 1862 §.

⁽²⁸⁹⁾ 50 U.S.C. 1862 §:n b momentti.

⁽²⁹⁰⁾ 12 U.S.C. 3414 §; 15 U.S.C. 1681u-1681v §; ja 18 U.S.C. 2709 §.

⁽²⁹¹⁾ 18 U.S.C. 2709 §:n b momentti.

⁽²⁹²⁾ Esimerkiksi 18 U.S.C. 2709 §:n d momentti.

3.2.1.3 Kerättyjen tietojen myöhempi käyttö

- (154) Yhdysvaltojen tiedusteluelinten signaalitiedustelun avulla keräämien henkilötietojen käsittelyyn sovelletaan useita suojatoimia.
- (155) Ensinnäkin kunkin tiedusteluelimen on varmistettava asianmukainen tietoturva ja estettävä asiattomien pääsy signaalitiedustelun avulla kerättyihin henkilötietoihin. Eri välineissä, kuten laeissa, ohjeissa ja standardeissa, täsmennetään tätä varten käyttöön otettavat tietoturvan vähimmäisvaatimukset (esimerkiksi monivaiheinen tunnistus ja salaus) ⁽²⁹³⁾. Pääsy kerättyihin tietoihin on annettava vain valtuutetulle ja koulutetulle henkilöstölle, joka tarvitsee tietoja tehtäviensä suorittamiseksi ⁽²⁹⁴⁾. Yleisesti ottaen tiedusteluelinten on tarjottava työntekijöilleen asianmukaista koulutusta myös menettelyistä, joilla ilmoitetaan lainsäädännön (mukaan lukien EO 14086) rikkomisesta ja puututaan siihen ⁽²⁹⁵⁾.
- (156) Toiseksi tiedusteluelinten on noudatettava tarkkuutta ja puolueettomuutta koskevia tiedusteluyhteisön normeja, jotka koskevat erityisesti tietojen laadun ja luotettavuuden varmistamista, vaihtoehtoisten tietolähteiden huomioon ottamista ja puolueettomuutta analyyseja tehtäessä ⁽²⁹⁶⁾.
- (157) Kolmanneksi toimeenpanoasetuksessa 14086 selvennetään tietojen säilyttämisen osalta, että ei-yhdysvaltalaisen henkilöiden henkilötietoihin sovelletaan samoja säilytysaikoja kuin yhdysvaltalaisen henkilöiden tietoihin ⁽²⁹⁷⁾. Tiedustelupalvelujen on määriteltävä tarkasti säilytysajat ja/tai tekijät, jotka on otettava huomioon määritettäessä sovellettavien säilytysaikojen pituutta (esim. ovatko tiedot todisteena rikoksesta; ovatko tiedot ulkomaantiedustelutietoja; tarvitaanko tietoja yksityishenkilöiden tai organisaatioiden turvallisuuden suojelemiseksi, mukaan lukien kansainvälisen terrorismin uhrin tai kohteet. Tekijöistä säädetään eri säädöksissä ⁽²⁹⁸⁾.
- (158) Neljänneksi signaalitiedustelun avulla kerättyjen henkilötietojen levittämiseen sovelletaan erityisiä sääntöjä. Yleisenä vaatimuksena on, että ei-yhdysvaltalaisen henkilöiden henkilötietoja voidaan levittää vain, jos ne sisältävät samantyyppistä tietoa kuin mitä voidaan levittää yhdysvaltalaisista henkilöistä, esimerkiksi tietoja, joita tarvitaan henkilön tai organisaation turvallisuuden suojelemiseksi (kuten kansainvälisten terroristijärjestöjen kohteet, uhrin tai panttivangit) ⁽²⁹⁹⁾. Henkilötietoja ei myöskään saa levittää pelkästään henkilön kansalaisuuden tai asuinmaan perusteella tai toimeenpanoasetuksen 14086 vaatimusten kiertämiseksi ⁽³⁰⁰⁾. Tietoja voidaan levittää Yhdysvaltojen hallinnon sisällä vain, jos valtuutetulla ja koulutetulla henkilöllä on perusteltu syy uskoa, että vastaanottajalla on

⁽²⁹³⁾ EO 14086, 2 §:n c momentin iii kohdan B alakohdan 1 alakohta. Ks. myös kansallisesta turvallisuudesta annetun lain (National Security Act) VIII osasto (turvallisuusluokiteltuihin tietoihin pääsyä koskevat vaatimukset), EO 12333 1.5 § (tiedusteluyhteisön elinten johtajille asetettu vaatimus tietojen jakamista ja turvallisuutta sekä yksityisyyttä koskevien ohjeiden ja muiden oikeudellisten vaatimusten noudattamisesta), televiestintä- ja tietojärjestelmien turvallisuutta koskevasta kansallisesta käytännöstä annettu kansallista turvallisuutta koskeva ohje 42 (National Policy for the Security of National Security Telecommunications and Information Systems) (kansallisia turvallisuusjärjestelmiä käsittelevän komitean ohjeistaminen antamaan kansallisten turvallisuusjärjestelmien turvallisuutta koskevia ohjeita toimeenpanoyksiköille ja -virastoille) ja kyberturvallisuuden parantamiseen liittyvä kansallista turvallisuutta koskeva muistio 8 (Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems) (aikataulut ja ohjeet siitä, miten kyberturvallisuusvaatimukset pannaan täytäntöön kansallisissa turvallisuusjärjestelmissä, mukaan lukien monivaiheinen tunnistus, salaus, pilvipalvelut ja päätepisteiden havaitsemispalvelut).

⁽²⁹⁴⁾ EO 14086 2 §:n c momentin iii kohdan B alakohdan 2 alakohta. Lisäksi henkilötietoihin, joiden säilyttämisestä ei ole tehty lopullista päätöstä, saa tutustua ainoastaan tällaisen päätöksen tekemiseksi tai tueksi tai hyväksyttyä hallinnollisia, testaukseen, kehittämiseen, turvallisuuteen tai valvontaan liittyviä tehtäviä varten (EO 14086 2 §:n c momentin iii kohdan B alakohdan 3 alakohta).

⁽²⁹⁵⁾ EO 14086 2 §:n d momentin ii kohta.

⁽²⁹⁶⁾ EO 14086 2 §:n c momentin iii kohdan C alakohta.

⁽²⁹⁷⁾ EO 14086 2 §:n c momentin iii kohdan A alakohdan 2 alakohdan a–c alakohta. Yleisesti ottaen kunkin elimen on otettava käyttöön käytäntöjä ja menettelyjä, joiden tarkoituksena on minimoida signaalitiedustelun avulla kerättyjen henkilötietojen levittämistä ja säilyttämistä (EO 14086 2 §:n c momentin iii kohdan A alakohta).

⁽²⁹⁸⁾ Ks. esim. tiedustelutoiminnan talousarviota koskevan vuoden 2015 lain (Intelligence Authorization Act for Fiscal Year 2015) 309 §. yksittäisten tiedustelupalvelujen FISA-lain 702 §:n nojalla hyväksymät ja FISC:n hyväksymät minimointimenettelyt; oikeusministerin ja FRA:n hyväksymät menettelyt (jotka edellyttävät, että Yhdysvaltojen liittovaltion virastot, myös kansallisen turvallisuuden virastot, vahvistavat rekistereilleen säilytysajat, jotka kansallisen arkisto- ja rekisterihallinnon on hyväksyttävä).

⁽²⁹⁹⁾ EO 14086 2 §:n c momentin iii kohdan A alakohdan 1 alakohdan a alakohta ja 5 alakohdan d alakohta luettuna yhdessä EO 12333 2.3 §:n kanssa.

⁽³⁰⁰⁾ EO 14086 2 §:n c momentin iii kohdan A alakohdan 1 alakohdan b ja e alakohta.

tarve saada tiedot ⁽³⁰¹⁾ ja että vastaanottaja suojaa tiedot asianmukaisesti ⁽³⁰²⁾. Kun halutaan määrittää, voidaanko henkilötietoja levittää Yhdysvaltojen hallinnon ulkopuolisille vastaanottajille (mukaan lukien vieraan vallan hallitus tai kansainvälinen järjestö), on otettava huomioon levittämisen tarkoitus, levitettävien tietojen luonne ja laajuus sekä mahdolliset haitalliset vaikutukset asianomaisiin henkilöihin ⁽³⁰³⁾.

- (159) Kunkin tiedusteluelimen on toimeenpanoasetuksen 14086 nojalla säilytettävä asianmukaiset asiakirjat signaalitiedustelun avulla saatujen tietojen keruusta myös sovellettavien lakisäätelien vaatimusten noudattamisen valvonnan ja tehokkaiden oikeussuojakeinojen helpottamiseksi. Asiakirjavaatimukset koskevat esimerkiksi tosiseikkoja, joiden perusteella arvioidaan, että tietty tiedonkeruutoimi on tarpeen validoitua tiedustelun painopistettä varten ⁽³⁰⁴⁾.
- (160) Edellä mainittujen toimeenpanoasetuksen 14086 suojatoimien lisäksi signaalitiedustelun avulla kerättyjen tietojen käytön suhteen kaikkiin Yhdysvaltojen tiedusteluviranomaisiin sovelletaan yleisempiä vaatimuksia, jotka koskevat käyttötarkoituksen rajoittamista, tietojen minimointia, tarkkuutta, tietoturva, säilyttämistä ja levittämistä. Yleisemmät vaatimukset perustuvat erityisesti OMB:n kiertokirjeeseen nro A-130, sähköistä hallintoa koskevaan lakiin, liittovaltion rekisterilakiin (ks. johdanto-osan 101–106 kappale) ja kansallisten turvallisuusjärjestelmien komitean (CNSS) ohjeisiin ⁽³⁰⁵⁾.

3.2.2 **Valvonta**

- (161) Yhdysvaltojen tiedusteluelinten toimintaa valvovat eri elimet.
- (162) Ensinnäkin toimeenpanoasetuksessa 14086 edellytetään, että kullakin tiedusteluelimellä on oikeusala, valvonnasta ja vaatimustenmukaisuudesta vastaavia korkean tason virkamiehiä sovellettavan Yhdysvaltojen lainsäädännön noudattamisen varmistamiseksi ⁽³⁰⁶⁾. Näiden on valvottava säännöllisesti signaalitiedustelutoimintaa ja varmistettava, että vaatimustenvastaisuudet korjataan. Tiedusteluelinten on annettava kyseisille virkamiehille pääsy kaikkiin merkityksellisiin tietoihin valvontatehtävien suorittamiseksi, eivätkä elimet saa ryhtyä toimiin estääkseen valvontatoimia tai vaikuttaakseen niihin epäasianmukaisesti ⁽³⁰⁷⁾. Lisäksi kaikista merkittävistä vaatimustenvastaisuuksista ⁽³⁰⁸⁾, jotka valvonnasta vastaava virkamies tai muu työntekijä on havainnut, on ilmoitettava viipymättä tiedusteluelimen johtajalle ja kansallisen tiedusteluviraston johtajalle, jonka on varmistettava, että kaikki tarvittavat toimet toteutetaan merkittävän vaatimustenvastaisuuden korjaamiseksi ja toistumisen estämiseksi ⁽³⁰⁹⁾.
- (163) Valvontatehtävää hoitavat virkamiehet, jotka on nimetty sääntöjenmukaisuuden valvomisen tehtävään, sekä yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet ja valvontaviranomaiset ⁽³¹⁰⁾.

⁽³⁰¹⁾ Esim. AGG-DOM:n mukaan FBI voi levittää tietoa vain, jos vastaanottajalla on tarve saada tieto täyttääkseen tehtävänsä tai suojellakseen kansalaisia.

⁽³⁰²⁾ EO 14086 2 §:n c momentin iii kohdan A alakohdan 1 alakohdan c alakohta. Tiedustelupalvelut voivat esimerkiksi levittää tietoja rikostutinnan kannalta merkityksellisissä olosuhteissa tai rikokseen liittyvissä olosuhteissa, esimerkiksi antamalla varoituksia tappamisen, vakavan ruumiinvamman tai sieppauksen uhasta; levittämällä tietoa kyberuhkista, tietoturvapoiikkeamista tai järjestelmiin tunkeutumisen vastatoimista; sekä varoittamalla kohteita tai mahdollisia rikosten uhreja.

⁽³⁰³⁾ EO 14086 2 §:n c momentin iii kohdan A alakohdan 1 alakohdan d alakohta.

⁽³⁰⁴⁾ EO 14086 2 §:n c momentin iii kohdan E alakohta.

⁽³⁰⁵⁾ Ks. CNSS Policy No. 22, Cybersecurity Risk Management Policy ja CNSS:n ohje 1253, jossa annetaan yksityiskohtaisia ohjeita kansallisia turvallisuusjärjestelmiä varten käyttöön otettavista tietoturva-toimista.

⁽³⁰⁶⁾ EO 14086 2 §:n d momentin i kohdan A ja B alakohta.

⁽³⁰⁷⁾ EO 14086 2 §:n d momentin i kohdan B ja C alakohta.

⁽³⁰⁸⁾ Tällä tarkoitetaan sovellettavan Yhdysvaltojen lainsäädännön järjestelmällistä tai tahallista noudattamatta jättämistä, joka voisi vaarantaa tiedusteluyhteisön jonkin toimijan maineen tai koskemattomuuden tai muulla tavoin kyseenalaistaa tiedusteluyhteisön toiminnan asianmukaisuuden, myös kun otetaan huomioon mahdollinen merkittävä vaikutus asianomaisten henkilöiden yksityisyyteen ja kansalaisvapauksiin liittyviin etuihin, ks. EO 14086 5 §:n l momentti.

⁽³⁰⁹⁾ EO 14086 2 §:n d momentin iii kohta.

⁽³¹⁰⁾ EO 14086 2 §:n d momentin i kohdan B alakohta.

(164) Lainvalvontaviranomaisten tavoin kaikissa tiedusteluelimissä on yksityisyyden suojasta ja kansalaisvapauksista vastaavia virkamiehiä⁽³¹¹⁾. Näiden virkamiesten toimivalta kattaa yleensä menettelyjen valvonnan sen varmistamiseksi, että kyseessä oleva ministeriö tai elin ottaa asianmukaisesti huomioon yksityisyyden suojaan ja kansalaisvapauksiin liittyvät huolenaiheet ja on ottanut käyttöön asianmukaiset menettelyt, jotta voidaan käsitellä sellaisten henkilöiden valitukset, jotka katsovat, että heidän yksityisyyttään tai kansalaisvapauksiaan on loukattu (ja joissakin tapauksissa niillä voi olla, esimerkiksi kansallisen turvallisuusviraston johtajan toimiston ODN:n tapaan, toimivalta tutkia valituksia⁽³¹²⁾). Tiedusteluelinten johtajien on varmistettava, että yksityisyyden suojasta ja kansalaisvapauksista vastaavilla virkamiehillä on tehtäviensä hoitamiseen tarvittavat resurssit, että heillä on käytettävissään kaikki tehtäviensä hoitamiseen tarvittava aineisto ja henkilöstö ja että heille tiedotetaan ehdotetuista toimintapoliittisista muutoksista ja heitä kuullaan niistä⁽³¹³⁾. Yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet raportoivat säännöllisesti kongressille ja PCLOB:lle muun muassa seuraavista: ministeriön tai elimen vastaanottamien valitusten lukumäärä ja luonne sekä yhteenveto valituksiin annetuista päätöksistä, suoritettut arvioinnit ja tarkastelut sekä virkamiehen toteuttamien toimien vaikutus⁽³¹⁴⁾.

(165) Toiseksi kullakin tiedusteluelimellä on riippumaton valvontaviranomainen, jonka vastuulla on muun muassa valvoa ulkomaantiedustelutoimintaa. Tähän sisältyy ODN:n yhteydessä oleva tiedusteluyhteisön valvontaviranomaisen toimisto, jolla on kattava toimivalta koko tiedusteluyhteisön suhteen ja valtuudet tutkia valituksia tai tietoja, jotka koskevat väitteitä lainvastaisesta menettelystä tai toimivallan väärinkäytöstä ODN:n ja/tai tiedusteluyhteisön ohjelmien ja toimien yhteydessä⁽³¹⁵⁾. Lainvalvontaviranomaisten tapaan (ks. johdanto-osan 109 kappale) tällaiset valvontaviranomaiset ovat lakisääteisesti riippumattomia⁽³¹⁶⁾ ja vastuussa tarkastuksista ja tutkimuksista, jotka koskevat kansalliseen tiedusteluun liittyviä, kyseessä olevan viraston ohjelmia ja toimia, mukaan lukien valtaoikeuksien väärinkäyttö tai lain rikkominen⁽³¹⁷⁾. Niillä on pääsy kaikkiin tietoihin, raportteihin, tarkastusai-

⁽³¹¹⁾ Ks. 42 U.S.C. 2000ee-1 §. Näitä ovat esimerkiksi Yhdysvaltojen ulkoasiainministeriö, oikeusministeriö, sisäisen turvallisuuden ministeriö, puolustusministeriö, NSA, keskustiedustelupalvelu CIA, FBI ja ODNI.

⁽³¹²⁾ Ks. EO 14086 3 §:n c momentti.

⁽³¹³⁾ 42 U.S.C. 2000ee-1 §:n d momentti.

⁽³¹⁴⁾ Ks. 42 U.S.C. 2000ee-1 §:n f momentin 1 ja 2 kohta. Esimerkiksi kansallisen turvallisuusviraston kansalaisvapauksien sekä yksityisyyden suojaan ja avoimuutta käsittelevän viraston raportista (tammikuu–kesäkuu 2021) käy ilmi, että virasto teki 591 arviointia kansalaisvapauksiin ja yksityisyyden suojaan liittyvistä vaikutuksista eri yhteyksissä, esimerkiksi tiedonkeruutoimien, tiedonjakojärjestelyjen ja -päättösten, tietojen säilyttämistä koskevien päätösten ynnä muiden yhteydessä, ottaen huomioon eri tekijät, kuten toimintaan liittyvien tietojen määrän ja tyyppin, asianomaiset henkilöt, tietojen käyttötarkoituksen ja ennakoitun käytön sekä käytössä olevat suojatoimet yksityisyyteen kohdistuvien mahdollisten riskien lieventämiseksi (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Vastaavasti CIA:n yksityisyyden suojasta ja kansalaisvapauksista vastaavan toimiston laatimissa raporteissa (tammikuu–kesäkuu 2019) annetaan tietoa toimiston valvontatoimista, esimerkiksi toimeenpanoasetuksen 12333 mukaisten oikeusministerin suuntaviivojen noudattamisesta tietojen säilyttämisen ja levittämisen osalta, sekä ohjeita PPD 28 -määräyksen täytäntöönpanosta, tietoturvaloukkausten tunnistamista ja niihin puuttumista koskevista vaatimuksista ja henkilötietojen käytön ja käsittelyn arvioinneista (<https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).

⁽³¹⁵⁾ Tämän valvontaviranomaisen nimittää presidentti, ja nimityksen vahvistaa senaatti. Valvontaviranomaisen voi erottaa ainoastaan presidentti.

⁽³¹⁶⁾ Valvontaviranomaisilla on vakinainen virka, ja heidät voi erottaa ainoastaan presidentti, jonka on ilmoitettava kongressille kirjallisesti erottamisen syistä. Tämä ei välttämättä tarkoita sitä, että heidän ei tarvitse noudattaa mitään ohjeita. Joissakin tapauksissa ministeriön tai viraston päällikkö voi kieltää valvontaviranomaista aloittamasta, suorittamasta tai saattamasta päätökseen tarkastusta tai tutkintaa, jos se on tarpeen tärkeiden kansallisten (turvallisuus)etujen suojelemiseksi. Kongressille on kuitenkin ilmoitettava tämän toimivallan käytöstä, ja tämän perusteella kyseessä oleva päällikkö voidaan asettaa vastuuseen. Ks. esimerkiksi valvontaviranomaisesta vuonna 1978 annetun lain (Inspector General Act of 1978) 8 § (puolustusministeriön osalta), 8E § (oikeusministeriön osalta) ja 8G §:n d momentin 2 kohdan A ja B alakohta (kansallisen turvallisuusviraston osalta), 50. U.S.C. § 403q (b) (CIA:n osalta); Intelligence Authorization Act For Fiscal Year 2010 -asiakirjan 405 §:n f momentti (tiedusteluyhteisön osalta).

⁽³¹⁷⁾ Inspector General Act of 1978, sellaisena kuin se on muutettuna, Pub. L. 117-108, 8.4.2022. Kuten esimerkiksi kongressille osoitetuissa puolivuositiedotuksissa (ajanjaksolta 1.4.2021–31.3.2022) selostettiin, kansallisen turvallisuusviraston valvontaviranomainen teki arviointia toimeenpanoasetuksen 12333 nojalla kerättyjen yhdysvaltalaisen henkilöiden tietojen käsittelystä, signaalitiedustelutietojen poistamismenettelystä, kansallisen turvallisuusviraston käyttämästä automatisoidusta kohdentamisvälineestä sekä FISA-lain 702 §:n mukaisen tiedonkeruun dokumentaatio- ja kyselysääntöjen noudattamisesta ja antoi tässä yhteydessä useita suosituksia (ks. <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>, s. 5–8 ja <https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrj00HJ9qDXGHqHLw%3d%3d×tamp=1657810395907>, s. 10–13). Ks. myös tiedusteluyhteisön valvontaviranomaisen viimeaikaiset tarkastukset ja tutkimukset, jotka koskevat tietoturva- ja kansalliseen turvallisuuteen liittyvien turvallisuusluokiteltujen tietojen luvaton luovuttamista (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, s. 8 ja 11, sekä https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, s. 19 ja 20).

neistoihin, arviointeihin, asiakirjoihin, työpapereihin, suosituksiin ja muuhun asianmukaiseen aineistoon, tarvittaessa haasteteitse, ja ne voivat ottaa todistajanlausuntoja⁽³¹⁸⁾. Valvontaviranomaiset saattavat epäiltyjä rikoksia koskevat asiat tuomioistuinten käsiteltäviksi ja antavat elinten johtajille suosituksia korjaavista toimista⁽³¹⁹⁾. Vaikka niiden suositukset eivät ole sitovia, niiden raportit, myös seurantaraportit, (tai niiden puuttuminen)⁽³²⁰⁾ julkistetaan usein ja lähetetään kongressille, joka voi tältä pohjalta harjoittaa valvontatehtävänsä (ks. johdanto-osan 168–169 kappale)⁽³²¹⁾.

- (166) Kolmanneksi presidentin tiedustelutoimintaa käsittelevän neuvoa-antavan lautakunnan (President's Intelligence Advisory Board, PIAB) osaksi perustettu tiedustelutoiminnan valvonnasta vastaava lautakunta (Intelligence Oversight Board, IOB) valvoo, että Yhdysvaltojen tiedusteluviranomaiset noudattavat perustuslakia ja kaikkia sovellettavia sääntöjä⁽³²²⁾. PIAB on presidentin toimeenpanovirastoon kuuluva neuvoa-antava elin, jossa on 16 jäsentä, jotka presidentti nimittää Yhdysvaltojen hallituksen ulkopuolelta. IOB koostuu enintään viidestä jäsenestä, jotka presidentti nimittää PIAB:n jäsenten keskuudesta. Toimeenpanoasetuksen 12333⁽³²³⁾ mukaan kaikkien tiedusteluelinten johtajien on ilmoitettava tiedustelutoiminnasta, josta on syytä uskoa, että se voi olla laitonta tai vastoin toimeenpanoasetusta tai presidentin määräystä IOB:lle. Jotta voidaan varmistaa, että IOB:llä on pääsy tehtäviensä suorittamiseen tarvittaviin tietoihin, toimeenpanoasetuksessa 13462 ohjeistetaan kansallisen tiedusteluviraston johtajaa ja tiedusteluelinten johtajia antamaan tietoja ja apua, joita IOB katsoo tarvitsevänsä tehtäviensä hoitamiseksi, lain sallimissa rajoissa⁽³²⁴⁾. IOB:n on puolestaan ilmoitettava presidentille tiedustelutoiminnasta, jonka se katsoo rikkovan Yhdysvaltojen lainsäädäntöä (mukaan lukien täytäntöönpanoasetukset) ja johon oikeusministeri, kansallisen tiedusteluviraston johtaja tai tiedusteluelimen johtaja ei ole puuttunut asianmukaisesti⁽³²⁵⁾. Lisäksi IOB:n on ilmoitettava oikeusministerille mahdollisista rikoslain rikkomisista.

- (167) Neljänneksi tiedustelupalvelut ovat PCLOB:n valvonnan alaisia. PCLOB:n perustamissääntöjen mukaan sen vastuualaan kuuluu terrorismin vastainen politiikka ja sen täytäntöönpano yksityisyyden suojan ja kansalaisvapauksien suojelemiseksi. Tarkastellessaan tiedusteluelinten toimintaa se voi saada käyttöönsä kaikki asiaankuuluvat elinten tiedot, raportit, tarkastusaineistot, arvioinnit, asiakirjat, työpaperit ja suositukset, mukaan lukien turvallisuusluokitellut tiedot, suorittaa haastatteluja ja kuulla todistajia⁽³²⁶⁾. Se saa raportteja useiden liittovaltion ministeriöiden ja virastojen⁽³²⁷⁾ kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavilta virkamiehiltä, ja se voi antaa suosituksia valtion viranomaisille ja tiedustelupalveluille. Lisäksi se raportoi säännöllisesti kongressin valiokunnille ja presidentille⁽³²⁸⁾. Lautakunnan raportit, myös kongressille toimitettavat raportit, julkistetaan mahdollisimman laajalti⁽³²⁹⁾. PCLOB on laatinut useita valvonta- ja seurantaraportteja, muun muassa analyysin FISA-lain 702 §:n perusteella toteutetuista ohjelmista ja yksityisyyden suojasta tässä yhteydessä sekä presidentin määräyksen PPD 28 ja toimeenpanoasetuksen 12333 täytäntöönpanosta⁽³³⁰⁾. PCLOB:n tehtävänä on myös

⁽³¹⁸⁾ Ks. Inspector General Act, 1978, 6 §.

⁽³¹⁹⁾ Ks. saman lain 4 §:n 6-5 momentti.

⁽³²⁰⁾ Ks. valvontaviranomaisten raporttien ja suositusten seurannasta esimerkiksi oikeusministeriön valvontaviranomaisen raporttiin annettu vastaus, jossa todettiin, että FBI ei ollut riittävän avoin FISC-tuomioistuimelle vuosina 2014–2019 tehdyissä hakemuksissa. Tämä johti uudistuksiin, joilla parannettiin sääntöjen noudattamista, valvontaa ja vastuuvuorollisuutta FBI:ssä (esimerkiksi FBI:n johtaja määräsi yli 40 korjaavaa toimea, joista 12 koski erityisesti FISA-menettelyä dokumentoinnin, valvonnan, rekisterien ylläpidon, koulutuksen ja tarkastusten osalta) (ks. <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>). Ks. esimerkiksi oikeusministeriön valvontaviranomaisen tarkastus, joka koskee FBI:n pääneuvonantajan toimiston (Office of the General Counsel) tehtäviä ja vastuualueita kansalliseen turvallisuuteen liittyviin FBI:n toimiin sovellettavien lakien, käytäntöjen ja menettelyjen noudattamisen valvonnassa, sekä liite 2, johon sisältyy FBI:n kirje kaikkien suositusten hyväksymisestä. Tältä osin liitteessä 3 esitetään yleiskatsaus jatkotoimista ja tiedoista, joita valvontaviranomainen tarvitsee FBI:ltä voidakseen saattaa suosituksensa päätökseen (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

⁽³²¹⁾ Ks. Inspector General Act, 1978, 4 §:n 5 momentin 5 kohta.

⁽³²²⁾ Ks. EO 13462.

⁽³²³⁾ EO 12333 1.6 §:n c momentti.

⁽³²⁴⁾ EO 13462 8 §:n a momentti.

⁽³²⁵⁾ EO 13462 6 §:n b momentti.

⁽³²⁶⁾ 42 U.S.C. 2000ee §:n g momentti.

⁽³²⁷⁾ Ks. 42 U.S.C. 2000ee-1 §:n f momentin 1 kohdan A alakohdan iii alakohhta. Näitä ovat ainakin oikeusministeriö, puolustusministeriö, sisäisen turvallisuuden ministeriö, kansallisen tiedusteluviraston johtaja ja keskustiedustelupalvelu (CIA), sekä mahdolliset muut PCLOB:n raporttien kannalta relevanteiksi katsomat ministeriöt, virastot tai toimeenpanovallan toimijat.

⁽³²⁸⁾ 42 U.S.C. 2000ee §:n e momentti.

⁽³²⁹⁾ 42 U.S.C. 2000ee §:n f momentti.

⁽³³⁰⁾ Saatavilla osoitteessa <https://www.pclob.gov/Oversight>

suorittaa erityisiä valvontatehtäviä toimeenpanoasetuksen 14086 täytäntöönpanon osalta erityisesti tarkastelemalla, ovatko elimen menettelyt yhdenmukaisia asetuksen kanssa (ks. johdanto-osan 126 kappale), ja arvioimalla oikeussuojakeinojen toimintaa (ks. johdanto-osan 194 kappale).

- (168) Viidenneksi toimeenpanovallan valvontamekanismien lisäksi myös tietyillä Yhdysvaltojen kongressin valiokunnilla (edustajainhuoneen ja senaatin tiedustelu- ja oikeusasioden valiokunnilla) on valvontavelvoitteita, jotka liittyvät kaikkeen Yhdysvaltojen harjoittamaan ulkomaantiedusteluun. Näiden valiokuntien jäsenillä on pääsy sekä turvallisuusluokiteltuihin tietoihin että tiedustelumenetelmiin ja -ohjelmiin ⁽³³¹⁾. Valiokunnat harjoittavat valvontatehtäviään eri tavoin, erityisesti kuulemisten, tutkimusten, tarkastelujen ja raporttien avulla ⁽³³²⁾.
- (169) Kongressin valiokunnat saavat säännöllisesti raportteja tiedustelutoiminnasta, myös oikeusministeriltä, kansallisen tiedusteluviraston johtajalta, tiedusteluelimiltä ja muilta valvontaelimiltä (esimerkiksi valvontaviranomaiset), ks. johdanto-osan 164 ja 165 kappale. Erityisesti kansallista turvallisuutta koskevan lain (National Security Act) mukaan "presidentti varmistaa, että kongressin tiedusteluvaliokunnille tiedotetaan kaikilta osin ja viipymättä Yhdysvaltojen tiedustelutoiminnasta, mukaan lukien tässä alaluvussa edellytetty merkittävä ennakoitu tiedustelu-toiminta" ⁽³³³⁾. Lisäksi "presidentti varmistaa, että kaikesta laittomasta tiedustelutoiminnasta ilmoitetaan viipymättä kongressin tiedusteluvaliokunnille samoin kuin mahdollisista korjaavista toimita, jotka on toteutettu tai jotka aiotaan toteuttaa laittoman toiminnan johdosta" ⁽³³⁴⁾.
- (170) Lisäksi erityisestä lainsäädännöstä seuraa muita raportointivaatimuksia. FISA-laissa edellytetään erityisesti, että oikeusministeri tiedottaa "kaikilta osin" tiettyjen kyseisen lain pykälien mukaisesti senaatille ja edustajainhuoneen tiedustelu- ja oikeusasioden valiokunnalle hallituksen toimista ⁽³³⁵⁾. Siinä edellytetään myös, että hallitus antaa kongressin valiokunnille jäljennökset kaikista FISC-tuomioistuimen tai FISCR-muutoksenhakutuomioistuimen päätöksistä, määräyksistä tai lausunnoista, joihin sisältyy FISA-lain säännösten "merkittävää tulkintaa". Mitä tulee FISA-lain 702 §:n mukaiseen valvontaan, parlamentaarista valvontaa harjoitetaan toimittamalla vaaditut raportit tiedustelu- ja oikeusasioden valiokunnille sekä toteuttamalla säännöllisiä katsauksia ja kuulemisia. Näihin kuuluvat oikeusministerin puolivuotiskertomus, jossa esitellään FISA-lain 702 §:n soveltamista ja jossa ovat liitteinä muun muassa oikeusministeriön ja ODN:n selvitykset sääntöjen noudattamisesta ja kuvaus mahdollisista tapauksista, joissa sääntöjä ei ole noudatettu ⁽³³⁶⁾, sekä oikeusministerin ja DNI:n erillinen puolivuositainen arvio, jossa selvitetään kohdentamiseen ja minimointiin liittyvien menettelyjen noudattamista ⁽³³⁷⁾.

⁽³³¹⁾ 50 U.S.C. 3091 §.

⁽³³²⁾ Valiokunnat järjestävät esimerkiksi temaattisia kuulemisia (ks. esimerkiksi edustajainhuoneen oikeusasioden valiokunnan äskettäin järjestämä kuuleminen digitaalisista dragnet-verkoista ("digital dragnets"), <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, ja edustajainhuoneen tiedusteluasioiden valiokunnan kuuleminen tekoälyn käytöstä tiedusteluyhteisössä, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>, sekä säännölliset valvontaa koskevat kuulemiset esimerkiksi FBI:stä ja oikeusministeriön kansallisesta turvallisuudesta vastaavasta jaostosta, <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>. Esimerkkinä tutkimuksesta ks. senaatin tiedusteluasioiden valiokunnan tutkimus Venäjän puuttumisesta Yhdysvaltojen vuoden 2016 vaaleihin, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. Raportoinnin osalta ks. esimerkiksi katsaus valiokunnan (valvontaan liittyvästä) toiminnasta senaatin tiedusteluasioiden valiokunnan raportissa (ajanjakso 4.1.2019–3.1.2021) senaatille, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>

⁽³³³⁾ Ks. 50 U.S.C. 3091 §:n a momentin 1 kohta. Tässä säännöksessä vahvistetaan yleiset vaatimukset, jotka koskevat kongressin toteuttamaa kansallisen turvallisuuden alan valvontaa.

⁽³³⁴⁾ Ks. 50 U.S.C. 3091 §:n b momentti.

⁽³³⁵⁾ Ks. 50 U.S.C. 1808 §, 1846 §, 1862 §, 1871 § ja 1881f §.

⁽³³⁶⁾ Ks. 50 U.S.C. 1881f §.

⁽³³⁷⁾ Ks. 50 U.S.C. 1881a §:n l momentin 1 kohta.

- (171) Lisäksi FISA-laissa edellytetään, että Yhdysvaltojen hallitus ilmoittaa vuosittain kongressille (ja yleisölle) muun muassa haettujen ja myönnettyjen FISA-määräysten (FISA Orders) lukumäärän sekä arviot valvonnan kohteena olevien yhdysvaltalaisien ja ei-yhdysvaltalaisien henkilöiden määrästä ⁽³³⁸⁾. Laissa edellytetään myös, että kansallista turvallisuutta koskevien kirjeiden (NSL) määrästä annetaan julkinen raportti sekä yhdysvaltalaisien että ei-yhdysvaltalaisien henkilöiden osalta (samalla FISA-määräysten ja -sertifiointipäätösten sekä NSL-pyyntöjen vastaanottajat voivat antaa avoimuusraportin tietyin edellytyksin) ⁽³³⁹⁾.
- (172) Yleisesti ottaen Yhdysvaltojen tiedusteluyhteisö pyrkii lisäämään monin tavoin (ulkomaan)tiedustelunsa avoimuutta. Esimerkiksi vuonna 2015 ODNI hyväksyi tiedustelun avoimuutta koskevat periaatteet ja avoimuutta koskevan täytäntöönpanosuunnitelman ja määräsi kunkin tiedusteluelimen nimeämään tiedustelun avoimuudesta vastaavan virkamiehen edistämään avoimuutta ja johtamaan avoimuusaloitteita ⁽³⁴⁰⁾. Näiden toimien osana tiedusteluyhteisö on julkistanut ja julkistaa edelleen muun muassa ODNI:n hallinnoimalla erityisellä IC on the Record -verkkosivustolla sellaisia osia toimintaperiaatteista, menettelytavoista, valvontaraporteista, FISA-lain 702 §:n ja toimeenpanoasetuksen 12333 mukaisia toimia koskevista raporteista, FISC-tuomioistuimen päätöksistä ja muusta aineistosta, joiden turvallisuusluokitus on poistettu ⁽³⁴¹⁾.
- (173) Lisäksi FISA-lain 702 §:n mukainen henkilötietojen kerääminen kuuluu johdanto-osan 162–168 kappaleessa mainittujen valvontaelinten harjoittaman valvonnan ohella myös FISC-tuomioistuimen valvonnan alaisuuteen ⁽³⁴²⁾. FISC-tuomioistuimen työjärjestyksen säännön 13 mukaan Yhdysvaltojen tiedusteluelinten sääntöjen noudattamista valvovien virkamiesten on ilmoitettava kaikista FISA-lain 702 §:n kohdentamis-, minimointi- ja kyselymenettelyjen rikkomisista oikeusministeriölle ja ODNI:lle, jotka puolestaan ilmoittavat niistä FISC-tuomioistuimelle. Lisäksi oikeusministeriö ja ODNI toimittavat FISC-tuomioistuimelle puolivuositteittaiset yhteistä valvontaa koskevat arviointiraportit, joissa yksilöidään kohdentamismenettelyjen noudattamisen suuntaukset, annetaan tilastotietoja, kuvataan säännösten rikkomisten luokat, esitetään yksityiskohtaisesti, miksi tietyt kohdentamissäännösten rikkomiset ovat tapahtuneet, ja esitellään toimenpiteet, joita tiedusteluelimet ovat toteuttaneet välttääkseen rikkomisen toistumisen ⁽³⁴³⁾.
- (174) Tarvittaessa (esimerkiksi jos havaitaan, että kohdentamismenettelyjä on rikottu) tuomioistuin voi määrätä asianomaisen tiedusteluelimen ryhtymään korjaaviin toimiin ⁽³⁴⁴⁾. Nämä korjaavat toimet voivat vaihdella yksittäisistä toimenpiteistä rakenteellisiin toimenpiteisiin, esimerkiksi tiedonhankinnan lopettamisesta ja laittomasti hankittujen tietojen poistamisesta keruumenettelyn muuttamiseen, myös henkilöstön ohjeistuksen ja koulutuksen osalta ⁽³⁴⁵⁾. Lisäksi FISC-tuomioistuin käsittelee vaatimustenvastaisuustapauksia 702 §:n mukaisia sertifiointeja

⁽³³⁸⁾ 50 U.S.C. 1873 §:n b momentti. Lisäksi 402 §:n mukaan ”kansallisen tiedusteluviraston johtaja toteuttaa oikeusministeriä kuultuaan ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen tai ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimen antaman sellaisen päätöksen, määräyksen tai lausunnon turvallisuusluokituksen poistamista koskevan tarkastelun (601 §:n e momentin mukaisesti), johon sisältyy jonkin lain säännöksen merkittävä tulkinta, mukaan lukien uusi tai merkittävä tulkinta käsitteestä ”erityinen valintakriteeri”, ja kyseisen tarkastelun mukaisesti saattaa julkisesti saataville mahdollisimman suuressa määrin kyseisen päätöksen, määräyksen tai lausunnon”.

⁽³³⁹⁾ 50 U.S.C. 1873 §:n b momentin 7 kohta ja 1874 §.

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

⁽³⁴¹⁾ Ks. IC on the Record, saatavilla osoitteessa <https://icontherecord.tumblr.com/>

⁽³⁴²⁾ FISC-tuomioistuin on todennut aiemmin, että ”tuomioistuimelle on ilmeistä, että täytäntöönpanosta vastaavat virastot sekä [ODNI] ja [oikeusministeriön kansallisesta turvallisuudesta vastaava jaosto] osoittavat huomattavia resursseja 702 §:n mukaisten vaatimusten noudattamista ja valvontaa koskeviin velvollisuuksiinsa. Vaatimustenvastaisuudet havaitaan pääsääntöisesti viipymättä ja asianmukaisia korjaavia toimia toteutetaan; toimiin kuuluu sellaisten tietojen poistaminen, jotka on saatu epäasianmukaisesti tai joihin sovelletaan muuten sovellettavien menettelyjen mukaisia hävittämisvaatimuksia.” FISA Court, Memorandum Opinion and Order (2014) [lainaus muokattu] (saatavilla osoitteessa <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>).

⁽³⁴³⁾ Ks. esimerkiksi oikeusministeriön/ODNI:n 702 §:ää koskeva vaatimustenmukaisuusraportti FISC-tuomioistuimelle ajanjaksolta kesäkuu 2018 – marraskuu 2018 (DO/ODNI FISA 702 Compliance Report to FISC for June 2018 – Nov 2018), s. 21–65.

⁽³⁴⁴⁾ 50 U.S.C. 1803 §:n h momentti. Ks. myös PCLOB, 702 §:ää koskeva raportti (Section 702 Report), s. 76. Ks. myös FISC Memorandum Opinion and Order, 3.10.2011, esimerkiksi puutteita koskevasta määräyksestä, jossa hallitus määräittiin korjaamaan havaitut puutteet 30 päivän kuluessa. Saatavilla osoitteessa <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>. Ks. Waltonin kirje, 4 §, s. 10 ja 11. Ks. myös FISC-tuomioistuimen lausunto, 18.10.2018 (FISC Opinion), saatavilla osoitteessa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, sellaisena kuin ulkomaantiedustelun valvonnan muutoksenhakutuomioistuin on sen vahvistanut 12.7.2019 antamassaan lausunnossa, saatavilla osoitteessa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_12_Jul_19.pdf, jossa FISC-tuomioistuin muun muassa määräsi hallituksen noudattamaan tiettyjä FISC-tuomioistuinta koskevia ilmoitus-, dokumentointi- ja raportointivaatimuksia.

⁽³⁴⁵⁾ Ks. esimerkiksi FISC, Memorandum Opinion and Order, s. 76 (6.12.2019) (julkaistavaksi 4.9.2020), jossa FISC-tuomioistuin määräsi hallituksen toimittamaan 28.2.2020 mennessä kirjallisen raportin toimista, joita se oli toteuttanut parantaakseen menettelyjä FISA-lain 702 §:n tietoihin perustuvien, säännösrikkomusten takia poisvedettävien raporttien tunnistamiseksi ja poistamiseksi, sekä muista seikoista. Ks. myös liite VII.

koskevassa vuotuisessa tarkastelussaan määrittääkseen, ovatko toimitetut sertifiointit FISA-lain vaatimusten mukaisia. Vastaavasti, jos FISC-tuomioistuimien katsoo, että hallituksen antamat sertifiointit eivät olleet riittäviä, esimerkiksi erityisten säännösten rikkomisen vuoksi, se voi antaa ns. puutteita koskevan määräyksen (deficiency order), jossa hallitusta vaaditaan korjaamaan rikkominen 30 päivän kuluessa tai lopettamaan 702 §:n mukainen sertifiointi tai olemaan panematta sitä täytäntöön. Lopuksi FISC-tuomioistuin arvioi rikkomistapauksissa havaitsemaan suuntauksia ja saattaa edellyttää niihin puuttumiseksi menettelyjen muuttamista tai lisävalvontaa ja -raportointia ⁽³⁴⁶⁾.

3.2.3 Oikeussuojakeinot

- (175) Kuten tässä kohdassa tarkemmin kerrotaan, unionin rekisteröidyillä on Yhdysvalloissa useita keinoja nostaa kanne riippumattomassa ja puolueettomassa tuomioistuimessa, jolla on valtuudet antaa sitovia päätöksiä. Yhdessä nämä keinot antavat yksilölle mahdollisuuden tutustua omiin henkilötietoihinsa, saattaa tarkasteltavaksi sen, onko hallituksen pääsy hänen tietoihinsa lainmukaista, ja, jos rikkominen todetaan, saada se korjattua, myös oikaisemalla tai poistamalla yksilön henkilötiedot.
- (176) Ensinnäkin toimeenpanoasetuksen 14086 nojalla on perustettu erityinen oikeussuojamekanismi, jota täydennetään tietosuojaa käsittelevän muutoksenhakutuomioistuimen perustamisesta annetulla AG-asetuksella, jotta voidaan käsitellä ja ratkaista henkilöiden tekemät valitukset, jotka koskevat Yhdysvaltojen signaalitiedustelutoimintaa. Jokaisella EU:ssa olevalla henkilöllä on oikeus tehdä oikeussuojamekanismin kautta valitus signaalitiedustelutoimintaa koskevan Yhdysvaltojen lainsäädännön (esimerkiksi EO 14086, FISA-lain 702 §, EO 12333) väitetystä rikkomisesta, joka vaikuttaa kielteisesti henkilön yksityisyyteen ja kansalaisvapauksiin liittyviin etuihin ⁽³⁴⁷⁾. Tämä oikeussuojamekanismi on sellaisista valtioista tai alueellisista taloudellisen yhdentymisen järjestöistä peräisin olevien henkilöiden käytettävissä, jotka Yhdysvaltojen oikeusministeri on nimennyt "vaatimukset täyttäväksi valtioiksi" ⁽³⁴⁸⁾. Yhdysvaltojen oikeusministeri nimesi 30. kesäkuuta 2023 Euroopan unionin ja kolme Euroopan vapaakauppaliiton maata, jotka yhdessä muodostavat Euroopan talousalueen, EO 14086:n 3 §:n f momentin nojalla "vaatimukset täyttäväksi valtioiksi" ⁽³⁴⁹⁾. Tämä nimeäminen ei vaikuta Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan soveltamiseen.
- (177) Euroopan unionin rekisteröidyn, joka haluaa tehdä tällaisen valituksen, on toimitettava se EU:n jäsenvaltion valvontaviranomaiselle, jolla on toimivalta valvoa viranomaisten suorittamaa henkilötietojen käsittelyä (tietosuojaviranomaiselle) ⁽³⁵⁰⁾. Näin varmistetaan, että oikeussuojamekanismi on helposti käytettävissä, kun henkilöille annetaan mahdollisuus ottaa yhteyttä "kodin lähellä" olevaan viranomaiseen ja asioida sen kanssa omalla kielellään. Kun johdanto-osan 178 kappaleessa tarkoitettujen valituksen tekemisen edellytykset on tarkastettu, toimivaltainen tietosuojaviranomainen kanavoi valituksen Euroopan tietosuojaneuvoston sihteeristön kautta oikeussuojamekanismiin.
- (178) Valituksen tekemiselle oikeussuojamekanismin kautta on asetettu vain vähän edellytyksiä, sillä henkilöiden ei tarvitse osoittaa, että heidän tietoihinsa on tosiasiallisesti kohdistettu Yhdysvaltojen signaalitiedustelutoimintaa ⁽³⁵¹⁾. Jotta oikeussuojamekanismissa voidaan aloittaa tarkastelu, on kuitenkin annettava tietyt perustiedot, jotka koskevat esimerkiksi henkilötietoja, joiden voidaan kohtuudella olettaa tulleen siirretyksi Yhdysvaltoihin, sekä keinoja, joilla tietojen siirron uskotaan tapahtuneen, niitä Yhdysvaltojen hallituksen yksiköitä, joiden uskotaan osallistuvan väitettyyn rikkomiseen (jos ne ovat on tiedossa), perusteita, joiden nojalla väitetään, että Yhdysvaltojen lainsäädäntöä on rikottu (vaikka tämäkään ei edellytä sen osoittamista, että Yhdysvaltojen tiedusteluviranomaiset olisivat tosiasiallisesti keränneet henkilötietoja), ja haetun oikaisutoimen luonnetta.

⁽³⁴⁶⁾ Ks. liite VII.

⁽³⁴⁷⁾ Ks. EO 14086 4 §:n k momentin iv kohta, jossa säädetään, että valituksen tekijä voi tehdä valituksen oikeussuojamekanismiin vain omasta puolestaan (ei siis hallituksen, valtiosta riippumattoman tai hallitustenvälisen järjestön edustajana). Käsite "vaikuttaa haitallisesti" ei edellytä, että valituksen tekijä täyttää tietyn kynnysvaatimuksen voidakseen käyttää oikeussuojamekanismia (ks. johdanto-osan 178 kappale). Sen sijaan siinä selvennetään, että ODNI CLPO:lla ja DPRC:llä on valtuudet korjata signaalitiedustelutoimintaa koskevan Yhdysvaltojen lainsäädännön rikkomiset, jotka vaikuttavat haitallisesti valituksen tekijän yksityisyyteen ja kansalaisvapauksiin. Sitä vastoin sovellettavan Yhdysvaltojen lainsäädännön sellaisten vaatimusten rikkominen, joiden tarkoituksena ei ole yksilöiden suojele (esim. talousarviovaatimukset), jäisi ODNI CLPO:n ja DPRC:n toimivallan ulkopuolelle.

⁽³⁴⁸⁾ EO 14086 3 §:n f momentti.

⁽³⁴⁹⁾ <https://www.justice.gov/opcl/executive-order-14086>.

⁽³⁵⁰⁾ EO 14086 4 §:n d momentin v kohta.

⁽³⁵¹⁾ Ks. EO 14086 4 §:n k momentin i-iv kohta.

- (179) Tähän oikeussuojamekanismiin toimitettujen valitusten alustavan tutkinnan suorittaa ODNI CLPO, jonka nykyistä lakisääteistä asemaa ja toimivaltaa on laajennettu koskemaan toimeenpanoasetuksen 14086 nojalla toteutettuja erityisiä toimia ⁽³⁵²⁾. Tiedusteluyhteisössä CLPO on muun muassa vastuussa sen varmistamisesta, että kansalaisvapauksien ja yksityisyyden suojele sisällytetään asianmukaisesti ODNI:n ja tiedusteluelinten toimintalinjoihin ja menettelyihin, sen valvomista, että ODNI noudattaa sovellettavia kansalaisvapauksia ja yksityisyyttä koskevia vaatimuksia, ja yksityisyyden suojaa koskevien vaikutustenarviointien tekemisestä ⁽³⁵³⁾. Ainoastaan kansallisen tiedusteluviraston johtaja voi erottaa ODNI CLPO:n syyistä eli virheen, väärinkäytöksen, tietoturvaloukkauksen, velvollisuuksien laiminlyönnin tai toimintakyvyttömyyden vuoksi ⁽³⁵⁴⁾.
- (180) ODNI CLPO:lla on tarkastelua tehdessään käytettävissään tiedot arvioinnin laatimista varten, ja hän voi tukeutua eri tiedusteluelimissä toimivien yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaavien virkamiesten apuun, jota näillä on velvollisuus antaa ⁽³⁵⁵⁾. Tiedusteluelimet eivät saa estää ODNI CLPO:ta tekemästä tarkasteluja tai vaikuttaa niihin epäasianmukaisesti. Tämä koskee myös kansallisen tiedusteluviraston johtajaa, joka ei saa puuttua tarkasteluun ⁽³⁵⁶⁾. Tarkastellessaan valitusta ODNI CLPO:n on sovellettava lainsäädäntöä "puolueettomasti" ottaen huomioon sekä kansalliset turvallisuusedut signaalitiedustelutoiminnassa että yksityisyyden suojan ⁽³⁵⁷⁾.
- (181) ODNI CLPO määrittää tarkastelun osana, onko sovellettavaa Yhdysvaltojen lainsäädäntöä rikottu, ja jos näin on, päättää asianmukaisista korjaustoimista ⁽³⁵⁸⁾. Tällä tarkoitetaan toimenpiteitä, joilla korjataan havaittu rikkomisen kokonaisuudessaan, kuten tietojen laittoman hankinnan lopettaminen, laittomasti kerättyjen tietojen poistaminen, laillisesti kerättyjä tietoja koskevien mutta epäasianmukaisesti tehtyjen kyselyjen tulosten poistaminen, laillisesti kerättyjen tietojen käyttöoikeuden rajaaminen asianmukaisesti koulutettuun henkilöstöön tai ilman laillista lupaa hankittuja tai laittomasti levitettyjä tietoja sisältävien tiedusteluraporttien peruuttaminen ⁽³⁵⁹⁾. ODNI CLPO:n päätökset yksittäisistä valituksista (sekä korjaustoimista) sitovat asianomaisia tiedusteluelimiä ⁽³⁶⁰⁾.
- (182) ODNI CLPO:n on säilytettävä tekemäänsä tarkastelua koskevat asiakirjat ja esitettävä turvallisuusluokiteltu päätös, jossa selitetään ODNI CLPO:n tekemien toiseikkoja koskevien havaintojen perusteet ja määritetään, onko tarkastelun kohteena ollut rikkomisen tapahtunut ja mikä on asianmukainen korjaustoimi ⁽³⁶¹⁾. Jos ODNI CLPO:n tarkastelussa paljastuu jonkin FISC-tuomioistuimen valvonnan alaisen viranomaisen tekemä rikkominen, CLPO:n on lisäksi toimitettava turvallisuusluokiteltu raportti kansallisesta turvallisuudesta vastaavalle apulaisoikeusministerille, joka puolestaan on velvollinen ilmoittamaan säännösten noudattamatta jättämisestä FISC-tuomioistuimelle, joka voi toteuttaa lisätoimenpiteitä (johdanto-osan 173 ja 174 kappaleessa kuvatun menettelyn mukaisesti) ⁽³⁶²⁾.
- (183) Kun tarkastelu on saatu päätökseen, ODNI CLPO ilmoittaa valituksen tekijälle kansallisen viranomaisen välityksellä, että "tarkastelussa ei havaittu soveltamisalaan kuuluvia rikkomisia" tai että "ODNI CLPO on antanut päätöksen, jossa vaaditaan asianmukaista korjausta" ⁽³⁶³⁾. Näin voidaan suojata kansallisen turvallisuuden suojaamiseksi toteutettujen toimien luottamuksellisuutta samalla, kun henkilöille annetaan päätös, jossa vahvistetaan, että heidän valituksensa on tutkittu ja käsitelty asianmukaisesti. Henkilö voi lisäksi riitauttaa tämän päätöksen. Tätä varten hänelle ilmoitetaan mahdollisuudesta hakea muutosta DPRC-tuomioistuimessa CLPO:n päätösten uudelleentarkastelua varten (ks. johdanto-osan 184 kappale ja sitä seuraavat kappaleet). Lisäksi hänelle ilmoitetaan, että jos asiasta nostetaan kanne tuomioistuimessa, valitaan erityinen asianajaja, joka ajaa valituksen esittäjän etua ⁽³⁶⁴⁾.

⁽³⁵²⁾ EO 14086 3 §: c momentin iv kohta. Ks. myös National Security Act 1947, 50 U.S.C. 403-3d §:n 103 momentin D kohta CLPO:n asemasta ODNI:ssä.

⁽³⁵³⁾ 50 U.S.C 3029 §:n b momentti.

⁽³⁵⁴⁾ EO 14086 3 §: c momentin iv kohta.

⁽³⁵⁵⁾ EO 14086 3 §:n c momentin iii kohta.

⁽³⁵⁶⁾ EO 14086 3 §: c momentin iv kohta.

⁽³⁵⁷⁾ EO 14086 3 §:n c momentin i kohdan B alakohdan i ja iii alakohta.

⁽³⁵⁸⁾ EO 14086 3 §:n c momentin i kohta.

⁽³⁵⁹⁾ EO 14086 4 §:n a momentti.

⁽³⁶⁰⁾ EO 14086 3 §:n c ja d momentti.

⁽³⁶¹⁾ EO 14086 3 §:n c momentin i kohdan F ja G alakohta.

⁽³⁶²⁾ Ks. myös EO 14086 3 §:n c momentin i kohdan D alakohta.

⁽³⁶³⁾ EO 14086 3 §:n c momentin i kohdan E alakohdan 1 alakohta.

⁽³⁶⁴⁾ EO 14086 3 §:n c momentin i kohdan E alakohdan 2 ja 3 alakohta.

- (184) Jokainen valituksen tekijä ja jokainen tiedusteluyhteisön toimija voi hakea ODNI CLPO:n päätöksen uudelleentarkastelua tietosuojaä käsittelevässä muutoksenhakutuomioistuimessa (DPRC). Tällaiset uudelleentarkastelua koskevat hakemukset on toimitettava 60 päivän kuluessa siitä, kun ODNI CLPO:lta on saatu ilmoitus siitä, että ODNI CLPO:n tarkastelu on valmis. Hakemuksessa on esitettävä kaikki tiedot, jotka henkilö haluaa toimittaa DPRC-tuomioistuimelle (esimerkiksi oikeudellisia seikkoja koskevat perustelut tai tiedot lainsäädännön soveltamisesta asian tosiseikkoihin) ⁽³⁶⁵⁾. Unionin rekisteröidyt voivat edelleen jättää hakemuksensa toimivaltaiselle tietosuojaviranomaiselle (ks. johdanto-osan 177 kappale).
- (185) DPRC on riippumaton tuomioistuin, jonka oikeusministeri on perustanut toimeenpanoasetuksella 14086 ⁽³⁶⁶⁾. Siihen kuuluu vähintään kuusi tuomaria, jotka oikeusministeri nimittää kuultuaan PCLOB:tä, kauppaministeriä ja kansallisen tiedusteluviraston johtajaa, neljän vuoden toimikaudeksi, joka voidaan uusia ⁽³⁶⁷⁾. Oikeusministeri ottaa tuomareiden nimittämisessä huomioon perusteet, joita toimeenpanovalta käyttää arvioidessaan liittovaltion oikeuslaitokseen ehdolla olevia henkilöitä, aiempaa tuomioistuinkokemusta korostaen ⁽³⁶⁸⁾. Tuomarien on lisäksi oltava oikeusalan ammattilaisia (eli asianajajayhdistyksen päteviä aktiivisia jäseniä, joilla on asianmukainen lupa juristin ammatin harjoittamiseen), ja heillä on oltava asianmukaista kokemusta yksityisyyttä ja kansallista turvallisuutta koskevasta lainsäädännöstä. Oikeusministerin on pyrittävä varmistamaan, että aina vähintään puolella tuomareista on aiempaa tuomioistuinkokemusta ja että kaikista tuomareista on tehty turvallisuusselvitys, jotta he voivat saada pääsyn kansallista turvallisuutta koskeviin turvallisuusluokiteltuihin tietoihin ⁽³⁶⁹⁾.
- (186) DPRC-tuomioistuimeen voidaan nimittää ainoastaan henkilöitä, jotka täyttävät johdanto-osan 185 kappaleessa mainitut pätevyysvaatimukset ja jotka eivät ole toimeenpanovalan työntekijöitä nimittämishetkellä tai olleet sitä kahtena edeltävänä vuotena. Vastaavasti tuomareilla ei saa DPRC-tuomioistuimen toimikautensa aikana olla muita virkatehtäviä eivätkä he saa toimia Yhdysvaltojen hallinnossa (muutoin kuin DPRC-tuomioistuimen tuomareina) ⁽³⁷⁰⁾.
- (187) Tuomioistuinmenettelyn riippumattomuus saavutetaan useilla takeilla. Varsinkaan toimeenpanovalta (oikeusministeri ja tiedusteluelimet) ei saa puuttua DPRC-tuomioistuimen tarkasteluun tai vaikuttaa siihen epäasianmukaisesti ⁽³⁷¹⁾. DPRC-tuomioistuimen on itse ratkaistava asiat puolueettomasti ⁽³⁷²⁾, ja se toimii oman (äänten enemmistöllä hyväksytyn) työjärjestyksensä mukaisesti. Lisäksi ainoastaan oikeusministeri voi erottaa DPRC-tuomioistuimen tuomareita ja ainoastaan syystä (eli virheen, väärinkäytöksen, tietoturvaloukkauksen, velvollisuuksien laiminlyönnin tai toimintakyvyttömyyden vuoksi) otettuaan asianmukaisesti huomioon liittovaltion tuomareihin sovellettavat vaatimukset, jotka on vahvistettu oikeudellista menettelyä ja esteellisyyttä koskevilla säännöillä ⁽³⁷³⁾.

⁽³⁶⁵⁾ AG-asetuksen 201.6 §:n a ja b momentti.

⁽³⁶⁶⁾ 3 §:n d momentin i kohta ja AG-asetus. Yhdysvaltojen korkein oikeus (Supreme Court of the United States) on hyväksynyt, että oikeusministeri voi perustaa riippumattomia elimiä, joilla on päätösvaltaa käsitellä myös yksittäisiä asioita, ks. erityisesti *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) ja *United States v. Nixon*, 418 U.S. 683, 695 (1974). EO 14086:n eri vaatimusten, kuten DPRC:n tuomareiden nimittämistä ja erottamista koskevien kriteerien ja menettelyn, noudattamista valvoo erityisesti oikeusministeriön ylitarkastaja (ks. myös johdanto-osan 109 kappale, joka koskee valvontaviranomaisten lakisäätöstä valtaa).

⁽³⁶⁷⁾ EO 14086 3 §:n d momentin i kohdan A alakohta ja AG-asetuksen 201.3 §:n a momentti.

⁽³⁶⁸⁾ AG-asetuksen 201.3 §:n b momentti.

⁽³⁶⁹⁾ EO 14086 3 §:n d momentin i kohdan B alakohta.

⁽³⁷⁰⁾ EO 14086 3 §:n d momentin i kohdan A alakohta ja AG-asetuksen 201.3 §:n a ja c momentti. DPRC-tuomioistuimeen nimetyt henkilöt voivat osallistua tuomioistuimen ulkopuoliseen toimintaan, mukaan lukien liiketoiminta, rahoitustoiminta, voittoa tavoittelematon varainhankinta, luottamustoimet ja juristin ammatin harjoittaminen, jos tällainen toiminta ei haittaa heidän tehtäviensä puolueetonta hoitamista eikä DPRC-tuomioistuimen tehokkuutta tai riippumattomuutta (AG-asetuksen 201.7 §:n c momentti).

⁽³⁷¹⁾ EO 14086 3 §:n d momentin iii ja iv kohta ja AG-asetuksen 201.7 §:n d momentti.

⁽³⁷²⁾ EO 14086 3 §:n d momentin i kohdan D alakohta ja AG-asetuksen 201.9 §.

⁽³⁷³⁾ EO 14086 3 §:n d momentin iv kohta ja AG-asetuksen 201.7 §:n d momentti. Ks. myös *Bumap v. Yhdysvallat*, 252 U.S. 512, 515 (1920), jossa vahvistettiin Yhdysvaltojen oikeusjärjestyksessä pitkään voimassa ollut periaate, jonka mukaan erottamisvalta on seurausta nimittämisvallasta (kuten myös oikeusministeriön oikeudellisen neuvonantajan toimisto (Office of Legal Counsel of the DoJ) totesi lausunnossa *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 166 (1996)).

- (188) DPRC-tuomioistuimelle tehtyt hakemukset käsitellään kolmen tuomarin kokoonpanossa, johon kuuluu puheenjohtajana toimiva tuomari, jonka on toimittava Yhdysvaltojen tuomareita koskevien käytännönsäätöjen mukaisesti ⁽³⁷⁴⁾. Kutakin kokoonpanoa avustaa erityisasiamies (Special Advocate) ⁽³⁷⁵⁾, jolla on pääsy kaikkiin tapausta koskeviin tietoihin, myös turvallisuusluokiteltuihin tietoihin ⁽³⁷⁶⁾. Erityisasiamiehen tehtävänä on varmistaa, että valituksen esittäjän edut ovat edustettuina ja että DPRC-tuomioistuimen tuomarikokoonpano on hyvin perillä kaikista merkityksellisistä oikeudellisista ja tosiseikoista ⁽³⁷⁷⁾. Erityisasiamies voi lisäksi pyytää kirjallisilla kysymyksillä valituksen esittäjältä tietoja muodostaakseen kantansa yksityishenkilön DPRC-tuomioistuimelle esittämästä uudelleentarkastelua koskevasta hakemuksesta ⁽³⁷⁸⁾.
- (189) DPRC tarkastelee ODNI CLPO:n tekemiä päätöksiä (päätökset siitä, onko sovellettavaa Yhdysvaltojen lainsäädäntöä rikottu, ja päätökset asianmukaisesta korjauksesta) vähintään ODNI CLPO:n tutkimuksen asiakirjojen sekä valituksen esittäjän, erityisasiamiehen tai tiedusteluelimen toimittamien tietojen ja huomautusten perusteella ⁽³⁷⁹⁾. DPRC-tuomioistuimen tuomarikokoonpanolla on pääsy kaikkiin tarkastelun suorittamiseksi tarvittaviin tietoihin, jotka se voi saada ODNI CLPO:lta (kokoonpano voi esimerkiksi pyytää CLPO:ta täydentämään tietoja lisätiedoilla tai tosiasiallisilla havainnoilla, jos se on tarpeen tarkastelun suorittamiseksi) ⁽³⁸⁰⁾.
- (190) Tarkastelunsa päätteeksi DPRC-tuomioistuin voi 1) päättää, ettei ole näyttöä siitä, että valituksen tekijän henkilötietoihin olisi kohdistettu signaalitiedustelutoimintaa, 2) päättää, että ODNI CLPO:n päätökset olivat oikeudellisesti asianmukaisia ja että niiden tueksi on esitetty riittävä näyttö, tai 3) jos DPRC-tuomioistuin on eri mieltä ODNI CLPO:n päätöksistä (jotka koskevat sitä, onko sovellettavaa Yhdysvaltojen lainsäädäntöä rikottu, tai sitä, mikä on asianmukainen korjaus), antaa omat päätöksensä ⁽³⁸¹⁾.

⁽³⁷⁴⁾ EO 14086 3 §:n d momentin i kohdan B alakohta ja AG-asetuksen 201.7 §:n a–c momentti. Oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaava toimisto (OPCL), joka tarjoaa hallinnollista tukea DPRC-tuomioistuimelle ja erityisasiamiehille (ks. AG-asetuksen 201.5 §), valitsee kolmihenkeisen kokoonpanon rotaatioperiaatteella sen varmistamiseksi, että kussakin kokoonpanossa on vähintään yksi tuomari, jolla on aiempaa tuomioistuinkokemusta (jos yhdelläkään kokoonpanon tuomareista ei ole tällaista kokemusta, puheenjohtajana toimii OPCL:n ensimmäiseksi valitsema tuomari).

⁽³⁷⁵⁾ AG-asetuksen 201.4 §. Oikeusministeri nimittää vähintään kaksi erityisasiamiestä kahden vuoden toimikaudeksi, joka voidaan uusia, kuultuaan kauppaministeriä, kansallisen tiedusteluviraston johtajaa ja PCLOB:tä. Erityisasiamiehillä on oltava asianmukaista kokemusta yksityisyyttä ja kansallista turvallisuutta koskevasta lainsäädännöstä. Heidän on oltava kokeneita asianajajia ja asianajajayhdistyksen päteviä aktiivisia jäseniä, joilla on asianmukainen lupa juristin ammatin harjoittamiseen. Lisäksi he eivät saa olla ensimmäisen nimityksensä yhteydessä työskennelleet toimeenpanovallan palveluksessa kahden edellisen vuoden aikana. Puheenjohtajana toimiva tuomari valitsee kunkin hakemuksen tarkastelua varten erityisasiamiehen avustamaan tuomarikokoonpanoa, ks. AG-asetuksen 201.8 §:n a momentti.

⁽³⁷⁶⁾ AG-asetuksen 201.8 §:n c momentti ja 201.11 §.

⁽³⁷⁷⁾ EO 14086 3 §:n d momentin i kohdan C alakohta ja AG-asetuksen 201.8 §:n e momentti. Erityisasiamies ei edusta valituksen esittäjää eikä hänellä ole tähän asianajaja-asiakassuhdetta.

⁽³⁷⁸⁾ Ks. AG-asetuksen 201.8 §:n d ja e momentti. OPCL tarkastelee näitä kysymyksiä ensin asianomaista tiedusteluyhteisön toimijaa kuullen, jotta turvallisuusluokitellut tai luottamukselliset tai suojatut tiedot voidaan määrittää ja poistaa ne valituksen esittäjälle toimitettavista tiedoista. Erityisasiamiehen tällaisten kysymysten perusteella saamat lisätiedot lisätään erityisasiamiehen DPRC-tuomioistuimelle toimittamiin tietoihin.

⁽³⁷⁹⁾ EO 14086 3 §:n d momentin i kohdan D alakohta.

⁽³⁸⁰⁾ EO 14086 3 §:n d momentin iii kohta ja AG-asetuksen 201.9 §:n b momentti.

⁽³⁸¹⁾ EO 14086 3 §:n d momentin i kohdan E alakohta ja AG-asetuksen 201.9 §:n c–e momentti. EO 14086:n 4 §:n a momentin mukaisen 'asianmukaisen korjauksen' määritelmän mukaan DPRC-tuomioistuimen on otettava huomioon "tavat, joilla todetun kaltaiseen rikkomiseen on tavallisesti puututtu", kun se päättää rikkomisen johdosta toteutettavasta korjaavasta toimenpiteestä, eli DPRC tarkastelee muiden tekijöiden ohella, miten vastaavat rikkomiset on aiemmin korjattu, varmistaakseen, että korjaava toimenpide on tuloksellinen ja asianmukainen.

- (191) DPCR-tuomioistuimien tekee kaikissa tapauksissa kirjallisen päätöksen äänten enemmistöllä. Jos tarkastelussa paljastuu sovellettavien sääntöjen rikkominen, päätöksessä täsmennetään kaikki asianmukaiset korjaukset, joihin kuuluvat laittomasti kerättyjen tietojen poistaminen, epäasianmukaisesti tehtyjen kyselyjen tulosten poistaminen, laillisesti kerättyjen tietojen saatavuuden rajaaminen asianmukaisesti koulutettuun henkilöstöön sekä ilman laillista lupaa hankittuja tai laittomasti levitettyjä tietoja sisältävien tiedusteluraporttien peruuttaminen⁽³⁸²⁾. DPCR-tuomioistuimen päätös on sille tehdyn valituksen osalta sitova ja lopullinen⁽³⁸³⁾. Jos tarkastelussa paljastuu jonkin FISC-tuomioistuimen valvonnan alaisen viranomaisen tekemä rikkominen, DPCR-tuomioistuimen on myös toimitettavaturvallisuuksuokiteltu raportti kansallisesta turvallisuudesta vastaavalle apulaisoikeusministerille, joka on puolestaan velvollinen ilmoittamaan säännösten noudattamatta jättämisestä FISC-tuomioistuimelle, joka voi toteuttaa lisätoimenpiteitä (johdanto-osan 173 ja 174 kappaleessa kuvatus menettelyn mukaisesti)⁽³⁸⁴⁾.
- (192) Jokainen DPCR-tuomioistuimen päätös toimitetaan ODNI CLPO:lle⁽³⁸⁵⁾. Tapauksissa, joissa DPCR:n tarkastelu on käynnistetty valituksen tekijän hakemuksesta, valituksen tekijälle ilmoitetaan kansallisen viranomaisen välityksellä, että DPCR on saattanut tarkastelunsa päätökseen ja että ”tarkastelussa ei joko havaittu soveltamisalaan kuuluvia rikkomisia tai DPCR on määrännyt ratkaisun, joka edellyttää asianmukaista korjaavia toimenpiteitä”⁽³⁸⁶⁾. Oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaava toimisto (OPCL) pitää kirjaa kaikista DPCR:n tarkastelemista tiedoista ja tehdyistä päätöksistä. Kirjatut päätökset asetetaan saataville ei-sitovina ennakkotapauksina tuleville DPCR-tuomioistuimille⁽³⁸⁷⁾.
- (193) Kauppaministeriön on myös pidettävä kirjaa jokaisesta valituksen tekijästä⁽³⁸⁸⁾. Avoimuuden lisäämiseksi kauppaministeriön on vähintään joka viides vuosi otettava yhteyttä asianomaisiin tiedusteluviranomaisiin tarkistaakseen, onko DPCR:n tarkasteluun liittyvien tietojen turvaluokitus poistettu⁽³⁸⁹⁾. Jos näin on, henkilölle ilmoitetaan, että kyseiset tiedot ovat saatavilla sovellettavan lainsäädännön nojalla (eli henkilö voi pyytää pääsyä tietoihin FOIA-lain nojalla, ks. johdanto-osan 199 kappale).
- (194) Lisäksi tämän oikeussuojamekanismin moitteetonta toimintaa arvioidaan säännöllisesti ja riippumattomasti. Tarkemmin sanottuna toimeenpanoasetuksen 14086 mukaan PCLOB, joka on riippumaton elin, tarkastelee oikeussuojamekanismin toimintaa vuosittain (ks. johdanto-osan 110 kappale)⁽³⁹⁰⁾. Osana tätä tarkastelua PCLOB muun muassa arvioi, ovatko ODNI CLPO ja DPCR-tuomioistuin käsitelleet valitukset oikea-aikaisesti, ovatko ne saaneet käyttöönsä kaikki tarvittavat tiedot, onko EO 14086 -asetuksen aineelliset suojatoimet otettu asianmukaisesti huomioon tarkastelumenettelyssä ja onko tiedusteluyhteisö noudattanut täysin ODNI CLPO:n ja DPCR:n päätöksiä. PCLOB laatii tarkastelunsa tuloksista raportin presidentille, oikeusministerille, kansallisen tiedusteluviraston johtajalle, tiedusteluelinten johtajille, ODNI CLPO:lle ja kongressin tiedusteluvaliokunnille. Raportti julkaistaan myös turvallisuusluokittelemattomana versiona. Raportti otetaan lisäksi huomioon tämän päätöksen toimivuutta koskevassa komission suorittamassa määräaikaistarkastelussa. Oikeusministerin, kansallisen tiedusteluviraston johtajan, ODNI CLPO:n ja tiedusteluelinten johtajien on toteutettava tai muutoin otettava huomioon kaikki tällaisiin raportteihin sisältyvät suositukset. Lisäksi PCLOB antaa vuosittain julkisen vahvistuksen siitä, että valitukset käsitellään oikeussuojamekanismissa EO 14086:n vaatimusten mukaisesti.

⁽³⁸²⁾ EO 14086 4 §:n a momentti.

⁽³⁸³⁾ EO 14086 3 §:n d momentin ii kohta ja AG-asetuksen 201.9 §:n g momentti. Koska DPCR:n päätös on lopullinen ja sitova, mikään muu toimeenpano- tai hallintoelin (Yhdysvaltojen presidentti mukaan luettuna) ei voi kumota DPCR:n päätöstä. Tämä on vahvistettu myös korkeimman oikeuden oikeuskäytännössä, jossa on selvennetty, että delegoimalla riippumattomalle elimelle toimeenpanoon sisältyvän yksinomaisen toimivaltansa antaa sitovia päätöksiä oikeusministeri poistaa itseltään mahdollisuuden puuttua millään tavoin kyseisen elimen päätöksiin (ks. *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)).

⁽³⁸⁴⁾ EO 14086 3 §:n d momentin i kohdan F alakohta ja AG-asetuksen 201.9 §:n i momentti.

⁽³⁸⁵⁾ AG-asetuksen 201.9 §:n h momentti.

⁽³⁸⁶⁾ EO 14086 3 §:n d momentin i kohdan H alakohta ja AG-asetuksen 201.9 §:n h momentti. Ilmoituksen luonteesta ks. AG-asetuksen 201.9 §:n h momentin 3 kohta.

⁽³⁸⁷⁾ AG-asetuksen 201.9 §:n j momentti.

⁽³⁸⁸⁾ EO 14086 3 §:n d momentin v kohdan A alakohta.

⁽³⁸⁹⁾ EO 14086 3 §:n d momentin v kohta.

⁽³⁹⁰⁾ EO 14086 3 §:n e momentti. Ks. myös [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

- (195) EO 14086:n nojalla perustetun erityisen oikeussuojamekanismin lisäksi kaikki yksityishenkilöt (kansalaisuudesta tai asuinpaikasta riippumatta) voivat käyttää oikeussuojakeinoja Yhdysvaltojen yleisissä tuomioistuimissa ⁽³⁹¹⁾.
- (196) Erityisesti FISA-laissa ja siihen liittyvässä lainsäädännössä säädetään henkilöiden mahdollisuudesta nostaa Yhdysvaltoja vastaan siviilikanne rahamääräisen vahingonkorvauksen saamiseksi, kun heitä koskevia tietoja on käytetty tai luovutettu laittomasti ja tahallisesti ⁽³⁹²⁾, nostaa Yhdysvaltojen hallituksen virkamiehiä vastaan kanne näiden toimiessa henkilökohtaisessa ominaisuudessa rahamääräisen vahingonkorvauksen saamiseksi ⁽³⁹³⁾; sekä riitauttaa valvonnan laillisuus (ja vaatia tietojen hävittämistä) siinä tapauksessa, että Yhdysvaltojen hallitus aikoo käyttää tai luovuttaa mitä tahansa sähköisessä valvonnassa hankittuja tai siitä johdettuja tietoja kyseistä henkilöä vastaan oikeudellisessa tai hallinnollisessa menettelyssä Yhdysvalloissa ⁽³⁹⁴⁾. Yleisemmällä tasolla on niin, että jos hallitus aikoo käyttää tiedustelutoimien aikana saatuja tietoja epäiltyä vastaan rikosasiassa, perustuslaissa ja muussa oikeudessa ⁽³⁹⁵⁾ asetetaan velvollisuus luovuttaa tietyt tiedot, jotta vastaaja voi riitauttaa hallituksen toteuttaman todisteiden keruun ja käytön laillisuuden.
- (197) Lisäksi on olemassa useita oikeussuojakeinoja, joilla voidaan ryhtyä oikeudellisiin toimenpiteisiin hallituksen virkamiehiä vastaan, kun nämä ovat lainvastaisesti päässeet henkilötietoihin tai käyttäneet niitä laittomasti, myös väitettyihin kansalliseen turvallisuuteen liittyviin tarkoituksiin (eli Computer Fraud and Abuse Act ⁽³⁹⁶⁾; Electronic Communications Privacy Act ⁽³⁹⁷⁾; ja Right to Financial Privacy Act ⁽³⁹⁸⁾). Kaikki nämä lait koskevat tiettyjä tietoja, kohteita ja/tai pääsylajeja (esim. tietokoneen etäyhteys internetin kautta) ja tietyin edellytyksin (esim. tarkoitussellinen/tahallinen toiminta, virkatehtävien ulkopuolinen toiminta, aiheutunut vahinko).
- (198) Hallintomenettelylaki (Administrative Procedure Act, APA ⁽³⁹⁹⁾) tarjoaa yleisemmän oikeussuojakeinon, jonka mukaan ”henkilöllä, jonka oikeuksia on loukattu viraston toiminnan seurauksena tai johon viraston toiminta vaikuttaa haitallisesti tai jonka etua on loukattu” on oikeus hakea muutosta tuomioistuimesta ⁽⁴⁰⁰⁾. Tähän sisältyy mahdollisuus pyytää tuomioistuinta ”toteamaan lainvastaiseksi ja kumoamaan viraston sellaiset toimet, havainnot ja päätelmät, joiden katsotaan olevan [...] mielivaltaisia, epämääräisiä, harkintavallan väärinkäyttöä tai muuten lainvastaisia” ⁽⁴⁰¹⁾. Esimerkiksi liittovaltion muutoksenhakutuomioistuin antoi vuonna 2015 APA-lakia koskevassa asiassa päätöksen ⁽⁴⁰²⁾, jonka mukaan Yhdysvaltojen hallituksen suorittama puhelujen metatietojen joukkokeruu ei ollut FISA-lain 501 §:n nojalla luvallista.
-
- ⁽³⁹¹⁾ Näiden keinojen saatavuus edellyttää ”kanne-oikeuden” osoittamista. Tämä normi, jota sovelletaan kaikkiin henkilöihin kansalaisuudesta riippumatta, on peräisin Yhdysvaltojen perustuslain III artiklan riitaisuusvaatimuksesta (‘case or controversy’ requirement). Korkeimman oikeuden mukaan tämä edellyttää, että 1) henkilölle on aiheutunut todellista vahinkoa (eli hänen oikeudellisesti suojattuja etujaan on loukattu tavalla, joka on yhtäältä konkreettinen ja erottuva ja toisaalta tosiasiallinen tai välittömästi uhkaava), 2) vahingon ja tuomioistuimessa riitautetun toiminnan välillä on syy-yhteys ja 3) on todennäköistä pikemminkin kuin mahdollista, että tuomioistuimen myönteinen päätös korvaisi haitan (ks. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).
- ⁽³⁹²⁾ 18 U.S.C. 2712 §.
- ⁽³⁹³⁾ 50 U.S.C. 1810 §.
- ⁽³⁹⁴⁾ 50 U.S.C. 1806 §.
- ⁽³⁹⁵⁾ Ks. *Brady v. Maryland*, 373 U.S. 83 (1963), ja *Jencks Act*, 18 U.S.C. 3500 §.
- ⁽³⁹⁶⁾ 18 U.S.C. 1030 §.
- ⁽³⁹⁷⁾ 18 U.S.C. 2701–2712 §.
- ⁽³⁹⁸⁾ 12 U.S.C. 3417 §.
- ⁽³⁹⁹⁾ 5 U.S.C. 702 §.
- ⁽⁴⁰⁰⁾ Yleensä vain ”lopullinen” viraston toimi – pikemmin kuin ”väliaikainen, menettelyllinen tai välillinen” viraston toimi – kuuluu tuomioistuinvalvonnan piiriin. Ks. 5 U.S.C. 704 §.
- ⁽⁴⁰¹⁾ 5 U.S.C. 706 §:n 2 momentin A kohta.
- ⁽⁴⁰²⁾ *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); näissä asioissa riitautettu puhelinliikennedatan valikoimattoman keräämisen ohjelma lakkautettiin USA FREEDOM Act -lailla vuonna 2015.

- (199) Johdanto-osan 176–198 kappaleessa mainittujen oikeussuojakeinojen lisäksi jokaisella henkilöllä on oikeus pyytää käyttöönsä liittovaltion virastoissa olevia asiakirjoja FOIA-lain nojalla, myös silloin, kun niihin sisältyy kyseisen henkilön henkilötietoja ⁽⁴⁰³⁾. Tällaisen tietoihin pääsyn saaminen voi helpottaa menettelyn käynnistämistä yleisissä tuomioistuimissa, myös kanneoikeuden osoittamisen tueksi. Virastot voivat pidättäytyä antamasta tietoja, jotka kuuluvat tiettyjen luetteloitujen poikkeusten piiriin, mihin kuuluu muun muassa pääsy turvallisuusluokiteltuihin kansallista turvallisuutta koskeviin tietoihin ja lainvalvontaan kuuluvaa tutkintaa koskeviin tietoihin ⁽⁴⁰⁴⁾, mutta tieto pyytäneillä, jotka eivät ole tyytyväisiä vastaukseen, on mahdollisuus riittauttaa vastaus hallinnollisessa menettelyssä ja myöhemmin tuomioistuinkäsittelyssä (liittovaltion tuomioistuimissa ⁽⁴⁰⁵⁾).
- (200) Edellä esitetystä seuraa, että kun Yhdysvaltojen lainvalvontaviranomaiset ja kansallisesta turvallisuudesta vastaavat viranomaiset saavat pääsyn tämän päätöksen soveltamisalaan kuuluviin henkilötietoihin, tätä pääsyä säännellään oikeudellisella kehyksellä, jossa asetetaan edellytykset tietoihin pääsulle ja varmistetaan, että pääsy tietoihin ja tietojen myöhempi käyttö rajoittuvat siihen, mikä on tarpeen ja oikeasuhteista yleiseen etuun liittyvän tavoitteen saavuttamiseksi. Henkilöt voivat vedota näihin suojatoimiin tehokkaiden oikeussuojakeinojen nojalla.

4. PÄÄTELMÄT

- (201) Komissio katsoo, että Yhdysvallat varmistaa – Yhdysvaltojen kauppaministeriön vahvistamien periaatteiden avulla – henkilötietojen suojan tason, joka vastaa olennaisilta osin asetuksella (EU) 2016/679 taattua tasoa, kun henkilötietoja siirretään unionista Yhdysvalloissa sijaitseville varmennetuille organisaatioille EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisesti.
- (202) Lisäksi komissio katsoo, että kyseisten periaatteiden tosiasiallinen noudattaminen taataan läpinäkyvyysvelvoitteilla ja tietosuojakehyksen hallinnolla, josta huolehtii kauppaministeriö. Lisäksi Yhdysvaltain lainsäädäntöön sisältyvät valvontamekanismit ja oikeussuojakeinot kokonaisuutena mahdollistavat sen, että tietosuojasääntöjen rikkomiset voidaan tunnistaa ja niistä voidaan rankaista käytännössä, ja että ne myös tarjoavat rekisteröidylle oikeussuojakeinoja, joiden avulla rekisteröity voi saada pääsyn itseään koskeviin henkilötietoihin ja tarvittaessa oikaista tai poistaa ne.
- (203) Yhdysvaltojen oikeusjärjestystä koskevien käytettävissä olevien tietojen perusteella, mukaan lukien liitteissä VI ja VII esitetyt tiedot, komissio katsoo, että Yhdysvaltojen viranomaisten yleisen edun nimissä toteuttama puuttuminen erityisesti rikoslain valvontaan ja kansalliseen turvallisuuteen liittyvissä tarkoituksissa niiden yksilöiden perusoikeuksiin, joiden henkilötietoja siirretään unionista Yhdysvaltoihin EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisesti, tulee rajatuksi siihen, mikä on ehdottoman välttämätöntä kyseessä olevan lainmukaisen tavoitteen saavuttamiseksi, ja että tällaista puuttumista vastaan on olemassa tehokas oikeussuoja. Edellä esitetyn perusteella on näin ollen päätettävä, että Yhdysvallat takaa asetuksen (EU) 2016/679 45 artiklassa, kun sitä tulkitaan ottaen huomioon Euroopan unionin perusoikeuskirja, tarkoitettun riittävän suojan henkilötiedoille, jotka siirretään Euroopan unionista EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisesti varmennetuille organisaatioille.
- (204) Koska toimeenpanoasetuksella 14086 käyttöön otetut rajoitukset, suojatoimet ja oikeussuojamekanismit ovat olennaisia osia Yhdysvaltojen oikeudellisessa kehyksessä, johon komission arviointi perustuu, tämän päätöksen hyväksyminen perustuu varsinkin siihen, että kaikki Yhdysvaltojen tiedusteluelimet hyväksyvät ajantasaistetut käytännöt ja menettelyt toimeenpanoasetuksen 14086 täytäntöönpanemiseksi, mikä on tapahtunut 3. heinäkuuta 2023 (ks. johdanto-osan 176 kappale), ja että unioni nimetään vaatimukset täyttäväksi organisaatioksi oikeussuojamekanismia varten, mikä on tapahtunut 30. kesäkuuta 2023 (ks. johdanto-osan 176 kappale).

⁽⁴⁰³⁾ 5 U.S.C. 552 §. Samanlaisia säännöksiä on olemassa osavaltiotasolla.

⁽⁴⁰⁴⁾ Jos näin on, asianomainen henkilö saa yleensä vain vakiovastauksen, jossa virasto kieltäytyy joko vahvistamasta tai kiistämästä asiakirjojen olemassaoloa. Ks. *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014). Turvallisuusluokituksen perusteet ja kesto vahvistetaan toimeenpanoasetuksessa 13526, jossa säädetään yleissäännöksi, että turvallisuusluokituksen poistumisen tietty ajankohta tai siihen johtava tapahtuma on määrittävä sen mukaan, miten kauan tiedot ovat kansallisen turvallisuuden kannalta arkaluonteisia, ja turvallisuusluokitus on poistettava automaattisesti kyseisenä ajankohtana (ks. EO 13526 kohta 1.5).

⁽⁴⁰⁵⁾ Tuomioistuin käsittelee asian kokonaan uudestaan päättäessään, oliko tietojen antamatta jättäminen asianmukaista, ja voi velvoittaa hallituksen antamaan tiedot (5 U.S.C. 552 §:n a momentin 4 kohdan B alakohta).

5. TÄMÄN PÄÄTÖKSEN VAIKUTUKSET JA TIETOSUOJAVIRANOMAISTEN TOIMET

- (205) Jäsenvaltioiden ja niiden elinten on toteutettava tarvittavat toimenpiteet unionin toimielinten antamien säädösten noudattamiseksi, sillä niiden oletetaan olevan lainmukaisia ja aiheuttavan siten oikeusvaikutuksia siihen asti, että ne perutaan, kumotaan kumoamiskanteen johdosta tai julistetaan pätemättömiksi ennakkoratkaisupyynnön tai lainvastaisuusväitteen perusteella.
- (206) Näin ollen asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukainen tietosuojan riittävyttä koskeva komission päätös sitoo kaikkia elimiä jäsenvaltioissa, joille se on osoitettu, mukaan lukien niiden riippumattomat valvontaviranomaiset. Erityisesti siirtoja unionissa olevalta rekisterinpitäjältä tai henkilötietojen käsittelijältä Yhdysvalloissa sijaitseville varmennetuille organisaatioille voidaan toteuttaa ilman muuta lupaa.
- (207) Olisi kuitenkin muistettava, kuten asetuksen (EU) 2016/679 58 artiklan 5 kohdassa ja unionin tuomioistuimen asiassa Schrems antamassa tuomiossa todetaan ⁽⁴⁰⁶⁾, että jos kansallinen tietosuojaviranomainen esimerkiksi valituksen käsittelyn yhteydessä asettaa kyseenalaiseksi sen, onko tietosuojan riittävyttä koskeva komission päätös yksityisyydensuojaa ja tietosuojaa koskevan perusoikeuden mukainen, kansallisessa lainsäädännössä on säädettävä oikeussuojakeinoista, joiden avulla viranomainen voi esittää väitteensä kansallisessa tuomioistuimessa, jonka on tarvittaessa pyydettävä unionin tuomioistuimelta ennakkoratkaisua ⁽⁴⁰⁷⁾.

6. TÄMÄN PÄÄTÖKSEN SEURANTA JA TARKASTELU

- (208) Tuomioistuimen oikeuskäytännön ⁽⁴⁰⁸⁾ mukaisesti ja kuten asetuksen (EU) 2016/679 45 artiklan 4 kohdassa todetaan, komission olisi tietosuojan tason riittävyttä koskevan päätöksen hyväksymisen jälkeen jatkuvasti seurattava asiaa koskevaa kehitystä kolmannessa maassa. Näin komissio voi arvioida sitä, takaako kyseinen kolmas maa edelleen olennaisilta osin vastaavan suojan tason. Tällainen tarkastelu on joka tapauksessa tehtävä, kun komissio saa tietoja, jotka aiheuttavat perusteltuja epäilyksiä tältä osin.
- (209) Komission olisi sen vuoksi seurattava jatkuvasti Yhdysvaltojen tilannetta tässä päätöksessä arvioidun henkilötietojen käsittelyä koskevan oikeudellisen kehyksen ja käytännön osalta. Prosessin helpottamiseksi Yhdysvaltojen viranomaisten olisi viipymättä ilmoitettava komissiolle Yhdysvaltojen oikeusjärjestyksen olennaisesta kehityksestä, joka vaikuttaa tämän päätöksen kohteena olevaan oikeudelliseen kehykseen, sekä tässä päätöksessä arvioitujen, henkilötietojen käsittelyyn liittyvien käytäntöjen kehityksestä Yhdysvalloissa toimivien varmennettujen organisaatioiden suorittaman henkilötietojen käsittelyn ja viranomaisten pääsyä henkilötietoihin koskevien rajoitusten ja suojatoimien osalta.
- (210) Jotta komissio voisi harjoittaa tehokkaasti valvontatehtäväänsä, jäsenvaltioiden olisi lisäksi ilmoitettava komissiolle kaikista kansallisten tietosuojaviranomaisten toteuttamista asiaankuuluvista toimista, varsinkin siinä tapauksessa, että ne liittyvät unionin rekisteröityjen esittämiin kysymyksiin tai valituksiin, jotka koskevat henkilötietojen siirtoa unionista varmennetuille organisaatioille Yhdysvaltoihin. Komissiolle olisi myös ilmoitettava mahdollisista havainnoista, joiden mukaan rikosten ehkäisemisestä, tutkimisesta, paljastamisesta tai syytetoimista tai kansallisesta turvallisuudesta vastaavien Yhdysvaltojen viranomaisten, mukaan lukien valvontaelimet, toimet eivät takaa vaadittavaa suojatasoa.

⁽⁴⁰⁶⁾ Schrems, 65 kohta.

⁽⁴⁰⁷⁾ Schrems, 65 kohta. "Tässä yhteydessä kansallisen lainsäätäjän asiana on säätää oikeussuojakeinoista, joiden avulla asianomainen kansallinen valvontaviranomainen voi esittää perusteltuina pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne kyseisen viranomaisen tavoin epäilevät komission päätöksen pätevyyttä, pyytää ennakkoratkaisua päätöksen pätevyyden tutkimiseksi."

⁽⁴⁰⁸⁾ Schrems, 76 kohta.

- (211) Asetuksen (EU) 2016/679 ⁽⁴⁰⁹⁾ 45 artiklan 3 kohdan mukaisesti komission olisi tämän päätöksen hyväksymisen jälkeen tarkasteltava säännöllisesti, ovatko Yhdysvaltojen EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa takaaman tietosuojan tason riittävyyttä koskevat päätelmät edelleen tosiasiallisesti ja oikeudellisesti perusteltuja. Koska erityisesti toimeenpanoasetus 14086 ja AG-asetus edellyttävät uusien mekanismien luomista ja uusien suojatoimien täytäntöönpanoa, tätä päätöstä olisi tarkasteltava ensimmäisen kerran vuoden kuluessa sen voimaantulosta sen tarkistamiseksi, onko kaikki asiaankuuluvat osatekijät pantu kaikilta osin täytäntöön ja toimivatko ne tehokkaasti käytännössä. Tämän ensimmäisen tarkastelun jälkeen ja sen tuloksista riippuen komissio päättää tiiviissä yhteistyössä asetuksen (EU) 2016/679 93 artiklan 1 kohdalla perustetun komitean ja Euroopan tietosuojaneuvoston kanssa tulevien tarkastelujen ajankohdista ⁽⁴¹⁰⁾.
- (212) Tarkastelujen suorittamiseksi komission olisi tavattava kauppaministeriö, liittovaltion kauppakomissio ja liikenneministeriö sekä tarvittaessa muita EU:n ja Yhdysvaltojen tietosuojakehyksen täytäntöönpanoon osallistuvia ministeriöitä ja virastoja sekä asioissa, jotka koskevat hallituksen pääsyä tietoihin, oikeusministeriön, ODNIn (mukaan lukien CLPO), tiedusteluyhteisön muiden toimijoiden, DPRC-tuomioistuimen ja erityisasiamiesten edustajia. Euroopan tietosuojaneuvoston jäsenten edustajien olisi voitava osallistua kokoukseen.
- (213) Tarkastelujen olisi katettava kaikki tämän päätöksen toimintaan liittyvät näkökohdat, jotka koskevat henkilötietojen käsittelyä Yhdysvalloissa ja erityisesti kyseisten periaatteiden noudattamista ja toteutumista, kiinnittäen erityistä huomiota tietojen edelleen siirtämisen yhteydessä annettavaan suojaan, asiaa koskevan oikeuskäytännön kehitykseen, yksilön oikeuksien käytön tehokkuuteen, järjestelyn periaatteiden noudattamisen seurantaan ja täytäntöönpanoon sekä hallituksen pääsyä tietoihin koskeviin rajoituksiin ja suojatoimiin, erityisesti EO 14086:n mukaisten suojatoimien täytäntöönpanoon ja soveltamiseen, myös tiedusteluelinten kehittämien toimintaperiaatteiden ja menettelyjen kautta, EO 14086:n sekä FISA-lain 702 §:n ja EO 12333:n väliseen vuorovaikutukseen ja valvontamekanismien ja oikeussuojakeinojen toimivuuteen (mukaan lukien EO 14086:n nojalla perustetun uuden oikeussuojamekanismin toiminta). Tällaisten tarkastelujen yhteydessä kiinnitetään huomiota myös tietosuojaviranomaisten ja Yhdysvaltojen toimivaltaisten viranomaisten väliseen yhteistyöhön, mukaan lukien ohjeiden ja muiden tulkintavälineiden kehittäminen periaatteiden soveltamista ja muita kehyksen toimintaan liittyviä näkökohtia varten.
- (214) Komission olisi laadittava tarkastelun perusteella julkinen kertomus, joka toimitetaan Euroopan parlamentille ja neuvostolle.

7. TÄMÄN PÄÄTÖKSEN SOVELTAMISEN KESKEYTTÄMINEN TAI PÄÄTÖKSEN KUMOAMINEN TAI MUUTTAMINEN

- (215) Jos käytettävissä olevat tiedot, erityisesti tämän päätöksen seurannasta saatavat tiedot tai Yhdysvaltojen tai jäsenvaltioiden viranomaisten toimittamat tiedot, osoittavat, että tämän päätöksen nojalla siirretyille tiedoille taattu tietosuojan taso ei mahdollisesti ole enää riittävä, komission olisi ilmoitettava viipymättä asiasta Yhdysvaltojen toimivaltaisille viranomaisille ja vaadittava asianmukaisten toimenpiteiden toteuttamista tietyn kohtuullisen ajan kuluessa.
- (216) Jos Yhdysvaltojen toimivaltaiset viranomaiset eivät kyseisen määräajan päättyessä ole toteuttaneet näitä toimenpiteitä tai muutoin osoittaneet tyydyttävästi, että tämän päätöksen perustana on edelleen riittävä suojan taso, komissio aloittaa asetuksen (EU) 2016/679 93 artiklan 2 kohdassa tarkoitetun menettelyn tämän päätöksen soveltamisen keskeyttämiseksi tai päätöksen kumoamiseksi osittain tai kokonaan.
- (217) Vaihtoehtoisesti komissio aloittaa kyseisen menettelyn tämän päätöksen muuttamiseksi erityisesti soveltamalla tiedonsiirtoihin lisäehtoja tai rajoittamalla tietosuojan riittävyyttä koskevan päätelmän soveltamisalan vain sellaisiin tiedonsiirtoihin, joiden osalta riittävän tietosuojan jatkuvuus on varmistettu.

⁽⁴⁰⁹⁾ Asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukaisesti "täytäntöönpanosäädöksessä on säädettävä [...] määräaikaistarkastelusta, jossa on otettava huomioon kaikki asiaan liittyvä kehitys kyseisessä kolmannessa maassa tai kansainvälisessä järjestössä."

⁽⁴¹⁰⁾ Asetuksen (EU) 2016/679 45 artiklan 3 kohdassa säädetään, että määräaikaistarkastelu on suoritettava vähintään joka neljäs vuosi. Ks. myös Euroopan tietosuojaneuvosto: Tietosuojan riittävyyden viitearvot, WP 254 rev. 01.

- (218) Komission olisi aloitettava keskeyttämis- tai kumoamismenettely erityisesti, jos
- a) on viitteitä siitä, että tämän päätöksen nojalla henkilötietoja EU:sta vastaanottaneet organisaatiot eivät noudata järjestelyn periaatteita ja että toimivaltaiset valvonta- ja täytäntöönpanoelimet eivät puutu tällaiseen vaatimusten- vastaisuuteen tehokkaasti;
 - b) on viitteitä siitä, että Yhdysvaltojen viranomaiset eivät noudata sovellettavia ehtoja ja rajoituksia, jotka koskevat Yhdysvaltojen viranomaisten pääsyä EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa siirrettyihin henkilötietoihin lainvalvontaan ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten; tai
 - c) Euroopan unionin rekisteröityjen valitukset jätetään todellisuudessa käsittelemättä, myös ODNI CLPO:n ja/tai DPRC-tuomioistuimen toimesta.
- (219) Komission olisi myös harkittava menettelyn aloittamista tämän päätöksen muuttamiseksi, sen soveltamisen keskeyttämiseksi tai sen kumoamiseksi, jos Yhdysvaltojen toimivaltaiset viranomaiset eivät toimita tietoja tai selvityksiä, joita tarvitaan arvioitaessa Euroopan unionista Yhdysvaltoihin siirrettyjen henkilötietojen suojan tasoa tai tämän päätöksen noudattamista. Tässä suhteessa komission olisi otettava huomioon se, missä määrin asiaa koskevia tietoja voidaan saada muista lähteistä.
- (220) Asianmukaisesti perustelluissa kiireellisissä tapauksissa, esimerkiksi jos toimeenpanoasetusta 14086 tai AG-asetusta muutetaan tavalla, joka heikentää tässä päätöksessä kuvattua suojelun tasoa, tai jos Yhdysvaltojen oikeusministerin suorittama unionin nimeäminen oikeussuojamekanismia varten vaatimukset täyttäväksi organisaatioksi peruutetaan, komissio käyttää mahdollisuutta hyväksyä asetuksen (EU) 2016/679 93 artiklan 3 kohdassa tarkoitettua menettelyä noudattaen välittömästi sovellettavia täytäntöönpanosäädöksiä tämän päätöksen soveltamisen keskeyttämiseksi tai päätöksen kumoamiseksi tai sen muuttamiseksi.

8. LOPPUPÄÄTELMÄT

- (221) Euroopan tietosuojaneuvosto on julkaissut lausuntonsa ⁽⁴¹¹⁾, joka on otettu huomioon tätä päätöstä valmisteltaessa.
- (222) Euroopan parlamentti on antanut päätöslauselman EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman suojan riittävydestä ⁽⁴¹²⁾.
- (223) Tässä päätöksessä säädetyt toimenpiteet ovat direktiivin (EU) 2016/679 93 artiklan 1 kohdan nojalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Yhdysvallat varmistaa asetuksen (EU) 2016/679 45 artiklan tarkoituksiin sellaisten henkilötietojen riittävän suojan tason, joita siirretään unionista sellaisille Yhdysvalloissa sijaitseville organisaatioille, jotka sisältyvät Yhdysvaltojen kauppaministeriön ylläpitämään ja julkisesti saataville asettamaan tietosuojakehysluetteloon (Data Privacy Framework List) liitteessä I olevan I jakson 3 kohdan mukaisesti.

2 artikla

Aina kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät asetuksen (EU) 2016/679 58 artiklan mukaisia toimivaltuuksiaan suojellakseen yksilöiden henkilötietoja tämän päätöksen 1 artiklassa tarkoitettujen tiedonsiirtojen osalta, asianomaisten jäsenvaltioiden on ilmoitettava siitä komissiolle viipymättä.

⁽⁴¹¹⁾ Lausunto 5/2023 Euroopan komission luonnoksesta täytäntöönpanopäätökseksi EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisen henkilötietojen suojan riittävästä tasosta, 28.2.2023.

⁽⁴¹²⁾ Euroopan parlamentin päätöslauselma 11. toukokuuta 2023 EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman suojan riittävydestä.

3 artikla

1. Komissio seuraa jatkuvasti tämän päätöksen kohteena olevan oikeudellisen kehyksen soveltamista, mukaan lukien ne edellytykset, joiden mukaisesti tietoja siirretään edelleen, yksilön oikeuksia käytetään ja Yhdysvaltojen viranomaisilla on pääsy tämän päätöksen nojalla siirrettyihin tietoihin, sen arvioimiseksi, takaako Yhdysvallat edelleen suojan riittävän tason 1 artiklassa tarkoitetulla tavalla.
2. Jäsenvaltiot ja komissio ilmoittavat toisilleen tapauksista, joissa näyttää siltä, että Yhdysvaltojen elimet, joilla on lakisääteiset valtuudet toteuttaa täytäntöönpanotoimia liitteessä I vahvistettujen järjestelyn periaatteiden noudattamiseksi, eivät ota käyttöön tehokkaita havainto- ja valvontamekanismeja, joiden avulla voidaan havaita liitteessä I vahvistettujen järjestelyn periaatteiden rikkomistapaukset ja rangaista niistä käytännössä.
3. Jäsenvaltiot ja komissio ilmoittavat toisilleen mahdollisista havainnoista, joiden mukaan kansallisesta turvallisuudesta, lainvalvonnasta tai muusta yleisestä edusta vastaavat Yhdysvaltojen viranomaiset puuttuisivat henkilötietojen suojaa koskevaan oikeuteen enemmän kuin on välttämätöntä ja oikeasuhteista ja/tai tällaista oikeuteen puuttumista vastaan ei ole tehokasta oikeussuojaa.
4. Vuoden kuluttua siitä päivästä, jona tämä päätös annetaan tiedoksi jäsenvaltioille, ja sen jälkeen tiiviissä yhteistyössä asetuksen (EU) 2016/679 93 artiklan 1 kohdalla perustetun komitean ja Euroopan tietosuojaneuvoston kanssa päätetyin välein komissio arvioi 1 artiklan 1 kohdassa tarkoitetun päätelmän kaikkien saatavilla olevien tietojen perusteella, mukaan lukien tiedot, jotka on saatu osana Yhdysvaltojen toimivaltaisten viranomaisten kanssa tehtyä tarkastelua.
5. Jos komissio saa viitteitä siitä, että tietosuojan taso ei ole enää riittävä, komissio ilmoittaa asiasta Yhdysvaltojen toimivaltaisille viranomaisille. Se päättää tarvittaessa tämän päätöksen soveltamisen keskeyttämisestä tai päätöksen muuttamisesta tai kumoamisesta tai sen soveltamisalan rajoittamisesta asetuksen (EU) 2016/679 45 artiklan 5 kohdan mukaisesti. Komissio voi myös hyväksyä tällaisen päätöksen, jos Yhdysvaltain hallituksen yhteistyöhaluttomuus estää komissiota arvioimasta, takaako Yhdysvallat edelleen suojan riittävän tason.

4 artikla

Tämä päätös on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä 10 päivänä heinäkuuta 2023.

Komission puolesta
Didier REYNDERS
Komission jäsen

LIITE I

YHDYSVALTOJEN KAUPPAMINISTERIÖN HYVÄKSYMÄT EU:N JA YHDYSVALTOJEN
TIETOSUOJAKEHYKSEN PERIAATTEET

I. YLEISKATSAUS

1. Yhdysvallat ja Euroopan unioni, jäljempänä 'EU', ovat molemmat sitoutuneet edistämään yksityisyyden suojaa ja oikeusvaltioperiaatetta ja tunnustavat transatlanttisten tietovirtojen merkityksen kansalaisilleen, talouksilleen ja yhteiskunnilleen. Yhdysvallat suhtautuu kuitenkin yksityisyyden suojaan eri tavalla kuin EU. Yhdysvalloissa käytetään alakohtaista lähestymistapaa, jossa yhdistyvät lainsäädäntö, sääntely ja itsesääntely. Yhdysvaltojen kauppaministeriö, jäljempänä 'ministeriö', hyväksyy tietosuojakehyksen periaatteet, jotka sisältävät myös täydentävät periaatteet, jäljempänä yhdessä 'järjestelyn periaatteet', ja periaatteiden liitteen I, jäljempänä 'liite I'. Kauppaministeriö hyväksyy periaatteet sen toimivallan nojalla, joka sille on annettu laissa kansainvälisen kaupan kasvattamista, edistämistä ja kehittämistä varten (15 U.S.C. 1512 §). Järjestelyn periaatteet on laadittu yhdessä Euroopan komission, jäljempänä 'komissio', elinkeinoelämän ja muiden sidosryhmien kanssa Yhdysvaltojen ja EU:n välisen kaupankäynnin helpottamiseksi. Järjestelyn periaatteet, jotka ovat keskeinen osa EU:n ja Yhdysvaltojen tietosuojakehystä, jäljempänä 'tietosuojakehyks', tarjoavat Yhdysvalloissa toimiville organisaatioille luotettavan mekanismin henkilötietojen siirtämiseksi EU:sta Yhdysvaltoihin siten, että samalla varmistetaan, että EU:n rekisteröidyt edelleenkin hyötyvät tehokkaista turvatoimista ja suojatoimista, joihin heillä EU:n lainsäädännön mukaan on oikeus silloin, kun heidän EU:n ulkopuolisiin maihin siirrettyjä henkilötietojaan käsitellään. Järjestelyn periaatteet on tarkoitettu yksinomaan sellaisten Yhdysvalloissa toimivien organisaatioiden käyttöön, jotka vastaanottavat henkilötietoja EU:sta voidakseen hyödyntää EU:n ja Yhdysvaltojen tietosuojakehystä ja siten tietosuojan riittävyyttä koskevaa komission päätöstä⁽¹⁾. Järjestelyn periaatteet eivät vaikuta henkilötietojen käsittelyyn EU:n jäsenvaltioissa sovellettavan asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus',⁽²⁾ soveltamiseen. Järjestelyn periaatteilla ei myöskään rajoiteta yksityisyyttä koskevia velvoitteita, joita muutoin sovelletaan Yhdysvaltojen lainsäädännön mukaisesti.
2. Jotta organisaatio voi tukeutua EU:n ja Yhdysvaltojen tietosuojakehykseen tehdessään henkilötietojen siirtoja EU:sta, sen on annettava oma varmennus kauppaministeriölle (tai ministeriön nimeämälle taholle). Vaikka organisaatiot näin ollen liittyvät tietosuojakehykseen täysin vapaaehtoisesti, järjestelyn periaatteiden noudattaminen on pakollista: organisaatioiden, jotka antavat oman varmennuksen kauppaministeriölle ja julkisesti ilmoittavat sitoutuvansa noudattamaan järjestelyn periaatteita, on noudatettava periaatteita kaikilta osin. Jotta organisaatio voi liittyä EU:n ja Yhdysvaltojen tietosuojakehykseen, sen on täytettävä seuraavat vaatimukset: a) sen on oltava liittovaltion kauppakomission, liikenneministeriön tai muun periaatteiden noudattamista valvovan lakisääteisen elimen tutkinta- ja täytäntöönpanovallan alainen (*muuta yhdysvaltalaisia lakisääteisiä elimiä, jotka EU tunnustaa, voidaan lisätä myöhemmin liitteessä*); b) sen on julkisesti sitouduttava noudattamaan järjestelyn periaatteita, c) sen on julkistettava tietosuojaperiaatteensa järjestelyn periaatteiden mukaisesti ja d) sen on pantava ne kaikilta osin täytäntöön.⁽³⁾ Jos organisaatio rikkoo järjestelyn periaatteita, liittovaltion kauppakomissio voi kohdistaa siihen lainvalvontatoimia kauppakomissiosta annetun lain (Federal Trade Commission Act) 5 §:n nojalla (ks. 15 U.S.C. 45 §, jossa kielletään sopimattomat ja vilpilliset toimet) tai liikenneministeriö voi kohdistaa siihen lainvalvontatoimia liittovaltion kauppakomissiosta annetun lain nojalla (ks. 49 U.S.C. 41712 §, jossa kielletään liikenteenharjoittajaa tai lipunvälittäjää harjoittamasta sopimatonta tai vilpillistä menettelyä lentoliikenteessä tai lentokuljetusten myynnissä). Lainvalvontatoimiin voidaan ryhtyä myös muiden sellaisten lakien tai säädösten nojalla, joissa kielletään tuollaiset toimet.

⁽¹⁾ Jos komission päätöstä, joka koskee EU:n ja Yhdysvaltojen välisen tietosuojakehyksen tarjoaman tsuojan riittävyyttä, sovelletaan myös Islantiin, Liechtensteiniin ja Norjaan, tietosuojakehyks kattaa paitsi Euroopan unionin jäsenvaltiot myös nämä kolme maata. Sen vuoksi viittaukset EU:hun ja sen jäsenvaltioihin tarkoittavat myös Islantia, Liechtensteiniä ja Norjaa.

⁽²⁾ Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

⁽³⁾ EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn periaatteet on muutettu 'EU:n ja Yhdysvaltojen tietosuojakehyksen periaateiksi'. (Ks. omaa varmennusta koskeva täydentävä periaate.)

3. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa, jäljempänä 'tietosuojakehyksen osallistujaluettelo', yhdysvaltalaisista organisaatioista, jotka ovat toimittaneet oman varmennuksensa kauppaministeriölle ja vahvistaneet sitoutuvansa noudattamaan järjestelyn periaatteita. Organisaatio voi hyödyntää EU:n ja Yhdysvaltojen EU:n ja Yhdysvaltojen tietosuojakehyksen etuja siitä päivästä lähtien, jona kauppaministeriö merkitsee organisaation tietosuojakehyksen osallistujaluetteloon. Kauppaministeriö poistaa organisaation tietosuojakehyksen osallistujaluettelosta, jos organisaatio vetäytyy EU:n ja Yhdysvaltojen tietosuojakehyksestä vapaaehtoisesti tai jos se jättää toimittamatta kauppaministeriölle vuotuisen uudelleenvarmennuksensa. Organisaation on jatkettava järjestelyn periaatteiden soveltamista henkilötietoihin, jotka se on saanut EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa, ja sen on annettava kauppaministeriölle tästä sitoumus vuosittain niin kauan kuin se säilyttää kyseisiä tietoja tai annettava tiedoille "riittävä" suoja muiden hyväksytyjen keinojen avulla (esimerkiksi käyttämällä sopimusta, joka vastaa täysin komission hyväksymissä vakiosopimuslauselusekkeissa olevia ehtoja). Muussa tapauksessa sen on palautettava tai hävitettävä tiedot. Kauppaministeriö poistaa tietosuojakehyksen osallistujaluettelosta myös organisaatiot, jotka ovat jatkuvasti jättäneet noudattamatta järjestelyn periaatteita. Niiden on palautettava tai hävitettävä henkilötiedot, jotka ne saivat EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa. Kun organisaatio poistetaan tietosuojakehyksen osallistujaluettelosta, sillä ei enää ole oikeutta hyödyntää komission tietosuojan riittävyttä koskevaa päätöstä vastaanottaakseen henkilötietoja EU:sta.
4. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa myös sellaisista yhdysvaltalaisista organisaatioista, jotka ovat aiemmin antaneet oman varmennuksensa kauppaministeriölle mutta jotka on myöhemmin poistettu tietosuojakehyksen osallistujaluettelosta. Kauppaministeriö esittää näiden organisaatioiden osalta selkeän varoitustekstin siitä, että nämä organisaatiot eivät osallistu EU:n ja Yhdysvaltojen tietosuojakehykseen. Tietosuojakehyksen osallistujaluettelosta poistaminen merkitsee, että kyseiset organisaatiot eivät voi väittää noudattavansa EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita ja että niiden on vältettävä kaikkia lausuntoja tai harhaanjohtavia käytäntöjä, joista voisi saada sen käsityksen, että ne osallistuvat EU:n ja Yhdysvaltojen Tällaisilla organisaatioilla ei ole enää oikeutta hyödyntää tietosuojan riittävyttä koskevaa Euroopan komission päätöstä, jonka nojalla nämä järjestöt voisivat vastaanottaa henkilötietoja EU:sta. Liittovaltion kauppakomissio, liikenneministeriö tai jokin muu lainvalvontaviranomainen voi kohdistaa lainvalvontatoimenpiteitä organisaatioon, joka edelleen väittää osallistuvansa EU:n ja Yhdysvaltojen tietosuojakehykseen tai antaa muita kehykseen liittyviä vääriä tietoja sen jälkeen, kun se on poistettu tietosuojakehyksen osallistujaluettelosta.
5. Järjestelyn periaatteiden noudattamista voidaan rajoittaa seuraavasti: a) siinä määrin kuin on tarpeellista tuomioistuimen määräyksen noudattamiseksi tai julkisen edun, lainvalvonnan tai kansallisen turvallisuuden vaatimusten vuoksi, myös silloin, kun lain tai hallituksen antaman asetuksen seurauksena syntyy ristiriitaisia velvoitteita, b) lailla, tuomioistuimen määräyksellä tai hallituksen antamalla asetuksella, jossa annetaan nimenomainen lupa tiettyyn toimintaan, jos organisaatio voi tällaista lupaa käyttäessään osoittaa, että se poikkeaa järjestelyn periaatteista vain siinä määrin kuin on tarpeellista, jotta lupaan liittyvä ensisijainen ja perusteltu intressi voi toteutua, tai c) jos yleisessä tietosuojasetuksessa sallitaan poikkeus, asetuksessa asetetuista edellytyksistä, ja tällaisia poikkeuksia sovelletaan vertailukelpoisissa olosuhteissa. Tässä yhteydessä Yhdysvaltojen laissa säädettyihin suojatoimiin yksityisyyden ja kansalaisvapauksien suojaamiseksi sisältyvät myös toimeenpanoasetuksessa 14086 (*) vaaditut suojatoimet siinä esitetyin edellytyksin (mukaan lukien sen tarpeellisuutta ja oikeasuhteisuutta koskevat vaatimukset). Organisaatioiden tulisi toimia tämän tavoitteen kanssa yhdenmukaisesti ja pyrkiä panemaan nämä periaatteet täytäntöön kaikilta osin ja läpinäkyvästi. Niiden tulisi muun muassa pyrkiä antamaan tietosuojaperiaatteissaan selvitys siitä, että periaatteista poiketaan edellä b kohdassa mainitulla perusteella. Jos organisaatiolla on järjestelyn periaatteiden ja/tai Yhdysvaltojen lainsäädännön nojalla vaihtoehtoja, joiden välillä se voi valita, organisaatioiden odotetaan samasta syystä – eli yksityisyyden suojan parantamiseksi – valitsevan mahdollisuuksien mukaan korkeatasoisemman suojan.
6. Organisaatioiden on sovellettava järjestelyn periaatteita kaikkiin EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa siirrettyihin henkilötietoihin sen jälkeen, kun organisaatiot ovat liittyneet tietosuojakehykseen. Jos organisaatio on päättänyt hyödyntää tietosuojakehyksen etuja sellaisten henkilöstötietojen osalta, jotka siirretään EU:sta käytettäväksi työsuhteiden hoitamisessa, sen on ilmoitettava tästä antaessaan oman varmennuksensa kauppaministeriölle ja noudatettava vaatimuksia, jotka on vahvistettu omaa varmennusta koskevassa täydentävässä periaatteessa.

(*) Toimeenpanomääräys 7. lokakuuta 2022, Enhancing Safeguards for United States Signals Intelligence Activities (Yhdysvaltojen signaalitiedustelua koskevien suojatoimien tehostaminen).

7. Yhdysvaltojen lainsäädäntöä sovelletaan kysymyksiin, jotka liittyvät EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden ja järjestelyyn kuuluvien organisaatioiden tietosuojaperiaatteiden tulkintaan ja noudattamiseen. Poikkeuksena ovat organisaatiot, jotka ovat sitoutuneet yhteistyöhön EU:n tietosuojaviranomaisten kanssa. Ellei toisin mainita, sovelletaan kaikkia periaatteisiin kuuluvia asianmukaisia sääntöjä.
8. Määritelmät:
- a. 'Henkilötiedoilla' tarkoitetaan missä tahansa muodossa rekisteröityä tunnistetun tai tunnistettavan henkilön tietoja, joihin sovelletaan yleistä tietosuoja-asetusta ja jotka yhdysvaltalainen organisaatio on vastaanottanut EU:sta.
 - b. 'Henkilötietojen käsittelyllä' tarkoitetaan kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen tai levittäminen sekä poistaminen tai tuhoaminen.
 - c. 'Rekisterinpitäjällä' tarkoitetaan henkilöä tai organisaatiota, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot.
9. Järjestelyn periaatteiden ja periaatteiden liitteen I voimaantulopäivä on päivä, jona tietosuojan riittävyttä koskeva Euroopan komission päätös tulee voimaan.

II. JÄRJESTELYN PERIAATTEET

1. ILMOITUSPERIAATE

- a. Organisaation on ilmoitettava henkilöille
 - i. osallistumisestaan EU:n ja Yhdysvaltojen tietosuojakehykseen ja annettava heille linkki tietosuoja-kehyksen osallistujaluetteloon tai kyseisen luettelon verkko-osoite,
 - ii. siitä, minkä tyyppisiä henkilötietoja on kerätty, sekä tarvittaessa organisaatioon kuuluvat Yhdysvalloissa toimivat yksiköt tai tytäryhtiöt, jotka niin ikään noudattavat järjestelyn periaatteita,
 - iii. sitoumuksestaan soveltaa järjestelyn periaatteita kaikkiin henkilötietoihin, jotka organisaatio vastaanottaa EU:sta EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa,
 - iv. tarkoitukset, joihin se kerää ja käyttää henkilötietoja,
 - v. organisaation yhteystiedot ja kuinka sille voi esittää tiedusteluja tai valituksia, samoin kuin tieto kaikista asiaankuuluvista EU:ssa sijaitsevista elimistä, jotka voivat vastata tällaisiin tiedusteluihin tai valituksiin,
 - vi. minkä tyyppisille kolmansille osapuolille se luovuttaa henkilötietoja ja keitä nämä kolmannet osapuolet ovat, sekä tarkoitukset, joita varten se luovuttaa tietoja niille,
 - vii. heidän oikeudestaan tutustua henkilötietoihinsa,
 - viii. valinnanmahdollisuuksista ja välineistä, jotka organisaatio tarjoaa henkilöille, jotta nämä voivat rajoittaa henkilötietojensa käyttöä ja julkistamista,
 - ix. riippumattomasta riitojenratkaisuelimestä, joka on nimetty valitusten käsittelyä varten ja johon henkilöt voivat asianmukaisesti turvautua maksutta, ja siitä, onko kyseessä 1) tietosuojaviranomaisten perustama paneeli, 2) EU:hun sijoittautunut vaihtoehtoinen riitojenratkaisuelin vai 3) Yhdysvaltoihin sijoittautunut vaihtoehtoinen riitojenratkaisuelin,
 - x. siitä, että organisaatio on liittovaltion kauppakomission, liikenneministeriön tai jonkin muun Yhdysvalloissa toimivaltaisen lakisääteisen elimen tutkinta- ja täytäntöönpanovallan alainen,
 - xi. mahdollisuudesta saada asia tietyin edellytyksin sitovan väliesmenettelyn käsiteltäväksi, ⁽⁹⁾
 - xii. vaatimuksesta, jonka mukaan henkilötietoja on luovutettava julkisen viranomaisen esittämän lainmukaisen pyynnön nojalla muun muassa kansalliseen turvallisuuteen tai lainvalvontaan liittyvien vaatimusten täyttämiseksi, ja
 - xiii. organisaation vastuusta tapauksissa, joissa tietoja on siirretty edelleen kolmansille osapuolille.

⁽⁹⁾ Ks. esimerkiksi muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen c kohta.

- b. Edellä mainittu ilmoitus on annettava siten, että käytetty kieli on selkeää ja että ilmoitus on henkilön helposti havaittavissa, silloin kun henkilöä pyydetään ensimmäistä kertaa antamaan henkilötietoja organisaatiolle, tai niin pian kuin ilmoituksen antaminen on käytännössä mahdollista. Ilmoitus on annettava joka tapauksessa ennen kuin organisaatio käyttää henkilötietoja muuhun tarkoitukseen kuin siihen, jota varten henkilötiedot siirtävä organisaatio on henkilötiedot alun perin kerännyt tai jota varten se on niitä käsitellyt, tai ennen kuin organisaatio luovuttaa henkilötiedot ensimmäisen kerran kolmannelle osapuolelle.

2. VALINTAPERIAATE

- a. Organisaation on tarjottava henkilöille mahdollisuus valita, voiko heidän henkilötietojaan i) luovuttaa kolmannelle osapuolelle tai ii) käyttää olennaisesti erilaiseen tarkoitukseen kuin siihen, johon ne oli alun perin kerätty tai johon henkilöt ovat myöhemmin antaneet suostumuksensa. Henkilöille on tarjottava valinnanvapauden käyttämistä varten mekanismeja, jotka ovat selkeitä ja henkilöiden helposti havaittavissa ja käytettävissä.
- b. Edellisestä kohdasta poiketen valintamahdollisuutta ei tarvitse tarjota, kun tiedot annetaan kolmannelle osapuolelle, joka toimii kyseisen organisaation edustajana suorittaen tiettyjä tehtäviä organisaation puolesta ja sen ohjeiden mukaisesti. Organisaation on kuitenkin aina tehtävä sopimus edustajan kanssa.
- c. Arkaluonteisten tietojen osalta (esimerkiksi henkilötiedot, jotka koskevat henkilön terveydentilaa, rotua tai etnistä alkuperää, poliittista kantaa, uskonnollista tai eettistä vakaumusta, kuulumista ammattiliittoon tai sukupuolielämää) henkilöiden on annettava organisaatiolle nimenomainen suostumuksensa, jos kyseisiä tietoja aiotaan i) luovuttaa kolmannelle osapuolelle tai ii) käyttää muuhun tarkoitukseen kuin siihen, johon ne oli alun perin kerätty tai johon henkilöt ovat myöhemmin antaneet suostumuksensa valintamahdollisuutta käyttäessään. Organisaation on lisäksi pidettävä arkaluonteisina kaikkia kolmannelta osapuolelta saatuja henkilötietoja, jos kyseinen kolmas osapuoli ilmoittaa tiedot arkaluonteisiksi ja käsittelee niitä sellaisina.

3. HENKILÖTIETOJEN EDELLEEN SIIRTÄMISEEN LIITTYVÄ VASTUUVELVOLLISUUSPERIAATE

- a. Jotta organisaatio voi siirtää henkilötietoja rekisterinpitäjänä toimivalle kolmannelle osapuolelle, sen on noudatettava ilmoitus- ja valintaperiaatteita. Sopimuksessa on määrättävä, että kyseisiä tietoja voidaan käsitellä vain tiettyä rajoitettua tarkoitusta varten siten, että tarkoitus vastaa henkilön asiassa antamaa suostumusta. Sopimuksessa tietojen vastaanottajan on sitouduttava järjestämään tietosuojaa, jonka taso vastaa järjestelyn periaatteita, ja ilmoittamaan organisaatiolle, jos se toteaa, ettei se enää kykene noudattamaan tätä velvoitetta. Sopimuksessa on määrättävä, että jos rekisterinpitäjänä toimiva kolmas osapuoli päättyy tällaiseen toteamukseen, se lakkaa käsittelemästä tietoja tai ryhtyy muihin kohtuullisiin ja asianmukaisiin toimiin tilanteen korjaamiseksi.
- b. Jotta organisaatio voi siirtää henkilötietoja edustajana toimivalle kolmannelle osapuolelle, sen on toimittava seuraavasti: i) sen on siirrettävä henkilötietoja vain tiettyä, rajoitettua tarkoitusta varten, ii) sen on varmistettava, että edustajalla on velvollisuus järjestää vähintään samantasoinen tietosuojaa kuin järjestelyn periaatteet edellyttävät, iii) sen on varmistettava kohtuullisin ja asianmukaisin toimin, että edustaja käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa järjestelyn periaatteiden mukaisia organisaation velvoitteita, iv) sen on vaadittava edustajaa ilmoittamaan organisaatiolle, jos edustaja toteaa, ettei se enää kykene tarjoamaan tietosuojaa, joka vastaa järjestelyn periaatteita, v) havaitessaan luvaton tiedonkäsitelyä, mukaan lukien iv kohdassa mainittu tilanne, sen on ryhdyttävä kohtuullisiin ja asianmukaisiin toimiin kyseisen tiedonkäsitelyn lopettamiseksi ja tilanteen korjaamiseksi ja vi) sen on pyynnöstä annettava kauppaministeriölle yhteenveto tai olennaiset osat sisältävä jäljennös yksityisyyden suojaa koskevista määräyksistä, jotka sisältyvät edustajan kanssa tehtyyn sopimukseen.

4. TURVALLISUUSPERIAATE

- a. Organisaatioiden, jotka keräävät, säilyttävät, käyttävät tai levittävät henkilötietoja, on toteutettava kohtuullisia ja asianmukaisia toimenpiteitä, joilla henkilötietoja suojataan katoamiselta, väärinkäytöltä, luvattomalta pääsylvä, luovuttamiselta, muuttamiselta tai tuhoamiselta. Organisaation on tällöin otettava asianmukaisesti huomioon tietojenkäsittelyn riskit ja henkilötietojen luonne.

5. TIETOJEN EHEYDEN JA KÄYTTÖTARKOITUKSEN RAJOITTAMISEN PERIAATE

- a. Järjestelyn periaatteiden mukaisesti henkilötietojen laajuus on rajoitettava tietoihin, jotka ovat merkityksellisiä tietojenkäsittelyn tarkoituksen kannalta.⁽⁶⁾ Tapa, jolla organisaatio käsittelee henkilötietoja, ei saa olla yhteensopimaton sen käyttötarkoituksen kanssa, johon tiedot on kerätty tai johon henkilö on myöhemmin antanut suostumuksensa. Organisaation on toteutettava tarvittavat kohtuulliset toimet sen varmistamiseksi, että henkilötiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia. Organisaation on noudatettava järjestelyn periaatteita niin kauan kuin se säilyttää henkilötietoja.
- b. Tietoja saa säilyttää muodossa, josta henkilöllisyys käy ilmi tai josta henkilöllisyys on selvitetävissä⁽⁷⁾, ainoastaan niin kauan kuin se on tarpeen tietojenkäsittelyn 5 a kohdan mukaisen tarkoituksen kannalta. Tämä velvoite ei estä organisaatioita käsittelemästä henkilötietoja pitempiäkin aikoja, jos käsittelyn kesto ja laajuus palvelevat kohtuullisella tavalla seuraavia tarkoituksia: yleisen edun mukainen tietojen arkistointi, journalismi, kirjallisuus ja taide, tieteellinen tutkimus tai historiantutkimus ja tilastollinen analyysi. Näissä tapauksissa tietojenkäsittelyyn sovelletaan EU:n ja Yhdysvaltojen tietosuojakehyksen muita periaatteita ja sääntöjä. Organisaatioiden olisi toteutettava kohtuulliset ja asianmukaiset toimenpiteet tämän säännöksen noudattamiseksi.

6. TIETOIHIN PÄÄSYÄ KOSKEVA PERIAATE

- a. Henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja heidän on voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä tai joita on käsitelty järjestelyn periaatteiden vastaisesti. Tätä ei kuitenkaan sovelleta, jos tiedonsaannista aiheutuva rasitus tai siihen liittyvät kustannukset olisivat suhteettoman suuria verrattuina henkilön tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa tai jos tietojen luovuttaminen loukkaisi muun kuin kyseisen henkilön oikeuksia.

7. MUUTOKSENHAKU-, TÄYTÄNTÖÖNPANO- JA VASTUUPERIAATE

- a. Tehokkaaseen tietosuojaan on sisällyttävä vankat mekanismit, joilla varmistetaan järjestelyn periaatteiden noudattaminen, se, että henkilö voi hakea muutosta silloin, kun häntä koskevien tietojen osalta on rikottu järjestelyn periaatteita, ja se, että organisaatiolle koituu seuraamuksia järjestelyn periaatteiden noudattamatta jättämisestä. Mekanismeihin on kuuluttava vähintään seuraavaa:
 - i. helposti käytettävissä olevat riippumattomat muutoksenhakumekanismit, joissa jokaisen henkilön valitukset ja häntä koskevat riidat tutkitaan ja ratkaistaan ripeästi järjestelyn periaatteita noudattaen ilman, että henkilölle aiheutuu kuluja, ja joissa määrätään maksettavaksi vahingonkorvauksia, jos tästä on säädetty sovellettavassa laissa tai yksityissektorin luomissa normeissa,
 - ii. seurantamenettelyt, joilla – erityisesti silloin, kun järjestelyn periaatteita oli rikottu – varmistetaan, että organisaatioiden antamat vakuutukset niiden noudattamasta yksityisyyden suojasta pitävät paikkansa ja että yksityisyyden suoja on toteutettu esitetyllä tavalla, ja
 - iii. organisaatioille asetettava velvollisuus korjata puutteet, jotka johtuvat siitä, että ne eivät ole noudattaneet järjestelyn periaatteita vaikka ovat ilmoittaneet tekevänsä niin, ja tällaisille organisaatioille koituvat seuraamukset. Seuraamusten on oltava riittävän tiukkoja sen varmistamiseksi, että organisaatiot noudattavat järjestelyn periaatteita.
- b. Organisaatioiden ja niiden valitsemien riippumattomien muutoksenhakumekanismien on vastattava nopeasti EU:n ja Yhdysvaltojen tietosuojakehystä koskeviin ministeriön tiedusteluihin ja pyyntöihin. Kaikkien organisaatioiden on vastattava viipymättä valituksiin, jotka EU:n jäsenvaltioiden viranomaiset ovat toimittaneet kauppaministeriön kautta ja jotka koskevat järjestelyn periaatteiden noudattamista. Organisaatioiden, jotka ovat päättäneet tehdä yhteistyötä tietosuojaviranomaisten kanssa, mukaan lukien organisaatiot, jotka käsittelevät henkilöstötietoja, on vastattava suoraan näille viranomaisille asioissa, jotka koskevat valituksien käsittelyä ja niihin annettavia ratkaisuja.

⁽⁶⁾ Olosuhteista riippuen tiedonkäsittelyn tarkoitukset saattavat olla hyväksyttäviä, jos ne palvelevat esimerkiksi seuraavia pyrkimyksiä: asiakassuhteiden hoitamista, säännösten noudattamiseen liittyviä ja oikeudellisia näkökohtia, tarkastusta, turvallisuutta ja petosten torjuntaa, organisaation laillisten oikeuksien säilyttämistä tai puolustamista tai muita sellaisia tarkoituksia, jotka vastaavat sitä mitä järkevä ja huolellinen henkilö voi odottaa tiedonkeruulta ko. tilanteessa.

⁽⁷⁾ Jos organisaatio tai kolmas osapuoli, jolla on pääsy tietoihin, kykenisi kohtuudella tunnistamaan henkilön, kun otetaan huomioon tunnistamisessa kohtuullisen todennäköisesti käytettävät välineet (ja kun otetaan muun muassa huomioon tunnistamiseen tarvittava aika ja kustannukset ja tietojenkäsittelyhetkellä käytettävissä oleva teknologia), henkilöllisyys on tässä yhteydessä "selvitettävissä".

- c. Organisaatioiden on osallistuttava välimiesmenettelyyn ja noudatettava liitteessä I asetettuja ehtoja, jos henkilö on pyytänyt sitovaa välimiesmenettelyä lähettämällä asiaa koskevan ilmoituksen kyseessä olevalle organisaatiolle ja jos hän on tällöin noudattanut liitteessä I selostettuja menettelytapoja ja täyttänyt siinä asetetut edellytykset.
- d. Kun henkilötietoja siirretään edelleen, tietosuojakehykseen osallistuva organisaatio on vastuussa sellaisten henkilötietojen käsittelystä, jotka se on vastaanottanut EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa ja myöhemmin siirtänyt sen edustajana toimivalle kolmannelle osapuolelle. Järjestelyyn osallistuva organisaatio on järjestelyn periaatteiden mukaan korvausvelvollinen, jos sen edustaja käsittelee henkilötietoja tavalla, joka ei ole järjestelyn periaatteiden mukainen, ellei organisaatio osoita, että se ei ole vastuussa tapahtumasta, joka johti syntyneeseen vahinkoon.
- e. Jos järjestelyyn osallistuvalla organisaatiolle annetaan sääntöjen rikkomiseen perustuva tuomioistuimen tai järjestelyn periaatteissa tai periaatteiden tulevassa liitteessä luetellun Yhdysvalloissa toimivan lakisääteisen elimen (esimerkiksi liittovaltion kauppakomission tai liikenneministeriön) määräys, organisaation on luottamuksellisuusvaatimusten rajoissa julkistettava kaikki EU:n ja Yhdysvaltojen tietosuojakehystä koskevat osat sellaisista sääntöjen noudattamista koskevista kertomuksista tai arviointikertomuksista, jotka on toimitettu kyseiselle tuomioistuimelle tai Yhdysvalloissa toimivalle lakisääteiselle elimelle. Tietosuojaviranomaiset voivat sen kautta tuoda esiin järjestelyyn osallistuviin organisaatioihin liittyviä ongelmia, jotka koskevat järjestelyn periaatteiden noudattamista. Liittovaltion kauppakomissio ja liikenneministeriö tarkastelevat etusijaisina sellaiset järjestelyn periaatteiden noudattamatta jättämistä koskevat asiat, jotka kauppaministeriö ja EU:n jäsenvaltioiden viranomaiset ovat siirtäneet sen käsiteltäväksi. Liittovaltion kauppakomissio ja liikenneministeriö antavat asianmukaisessa aikataulussa tietoja näistä asioista sen jäsenvaltion viranomaiselle, joka on siirtänyt kyseisen asian liittovaltion kauppakomission käsiteltäväksi, noudattaen voimassa olevia luottamuksellisuutta koskevia rajoituksia.

III. TÄYDENTÄVÄT PERIAATTEET

1. Arkaluonteiset tiedot

- a. Organisaation ei tarvitse saada nimenomaista suostumusta arkaluonteisten tietojen käsittelyyn, jos tietojenkäsittely
 - i. on rekisteröidyn tai muun henkilön elintärkeiden etujen mukaista,
 - ii. on tarpeen oikeudellisen vaatimuksen laatimiseksi tai siihen vastaamiseksi,
 - iii. on tarpeen lääketieteellisen hoidon antamiseksi tai diagnoosin tekemiseksi,
 - iv. suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiyhdistystoimintaan liittyvän säätöön, yhdistyksen tai minkä tahansa muun voittoa tavoittelemattoman elimen laillisen toiminnan yhteydessä ja sillä edellytyksellä, että käsittely koskee ainoastaan näiden elinten jäseniä tai henkilöitä, joilla on niihin säännölliset elinten tarkoituksiin liittyvät yhteydet, ja että tietoja ei luovuteta kolmansille osapuolille ilman rekisteröityjen suostumusta,
 - v. on tarpeen organisaation velvoitteiden täyttämiseksi työoikeuden alalla tai
 - vi. koskee tietoja, jotka henkilö on nimenomaisesti saattanut julkisiksi.

2. Journalistiset poikkeukset

- a. Kun otetaan huomioon perustuslain suoja, jonka Yhdysvallat antaa lehdistönvapaudelle, noudatetaan seuraavaa sääntöä: jos Yhdysvaltojen perustuslain ensimmäisessä lisäyksessä ilmaistut vapaan lehdistön oikeudet ovat ristiriidassa yksityisyyden suojaan liittyvien etujen kanssa, perustuslain ensimmäisen lisäyksen on ohjattava näiden etujen tasapainottamista yhdysvaltalaisen henkilöiden ja organisaatioiden toimien osalta.
- b. Järjestelyn periaatteiden vaatimukset eivät koske henkilötietoja, jotka on kerätty julkaisemista, radio- ja tv-lähetystoimintaa tai muuta journalistisen aineiston julkista viestintää varten siitä riippumatta, käytetäänkö tietoja vai ei, eivätkä tietoja, jotka löytyvät aikaisemmin julkaistusta tiedotusvälineiden arkistoista levitetystä aineistosta.

3. Toissijainen vastuu

- a. Internetpalveluntarjoajat, televiestinnän harjoittajat tai muut organisaatiot eivät ole järjestelyn periaatteiden mukaan vastuussa, jos ne toisen organisaation puolesta pelkästään siirtävät, reitittävät, välittävät tai varastoivat tietoja. EU:n ja Yhdysvaltojen tietosuojakehyksessä ei luoda toissijaista vastuuta. Jos organisaatio toimii pelkästään kolmansien osapuolien siirtämän tiedon kanavana eikä itse määrittele henkilötietojen käsittelyn tarkoitusta ja tapaa, se ei ole vastuussa tältä osin.

4. Due diligence -tarkastusten ja muiden tarkastusten tekeminen

- a. Tilintarkastajien ja investointipankkien toimintaan saattaa sisältyä henkilötietojen käsittelyä ilman, että asianomainen henkilö on antanut siihen suostumuksensa tai tietää siitä. Tämä on sallittua jäljempänä kuvatuissa olosuhteissa ilmoitus-, valinta- ja tiedonsaantiperiaatteiden mukaisesti.
- b. Julkisissa osakeyhtiöissä ja harvainyhtiöissä, myös järjestelyyn osallistuvissa organisaatioissa, tehdään säännöllisesti tarkastuksia. Tällaisten tarkastusten tavoite, erityisesti silloin, kun niissä tutkitaan mahdollisia väärinkäytöksiä, saattaa vaarantua, jos tarkastuksista annetaan tieto ennen aikaisesti. Vastaavasti järjestelyyn osallistuvassa organisaatiossa, joka on mukana mahdollisessa sulautumisessa tai yritysostossa, voidaan tehdä due diligence -tarkastuksia. Näissä tarkastuksissa kerätään ja käsitellään usein henkilötietoja, esimerkiksi johtavassa asemassa olevasta ja muusta keskeisiä tehtäviä hoitavasta henkilöstöstä. Liiketoimen ennen aikainen julkistaminen voisi haitata liiketoimen toteutumista ja olla jopa sovellettavan arvopaperilainsäädännön vastaista. Investointipankit ja asianajajat, jotka osallistuvat due diligence -tarkastukseen, ja tilintarkastajat tarkastuksia tehdessään voivat käsitellä tietoja asianomaisen tietämättä ainoastaan siinä määrin ja niin kauan kuin on tarpeen lakisääteiden tai yleisen edun mukaisten vaatimusten täyttämiseksi, sekä lisäksi olosuhteissa, joissa järjestelyn periaatteiden soveltaminen vaikuttaisi haitallisesti organisaation oikeutettuihin etuihin. Oikeutettuja etuja ovat muun muassa sen valvominen, että organisaatiot noudattavat lainmukaisia velvoitteitaan ja että niiden tilinpäätökset on laadittu sääntöjen mukaisesti, samoin kuin luottamuksellisuus, kun on kyse mahdollisista yritysostoista, sulautumisista, yhteisyrityksistä tai muista vastaavista investointipankkien tai tilintarkastajien toteuttamista toimista.

5. Tietosuojaviranomaisten tehtävä

- a. Organisaatiot toteuttavat sitoumuksensa, jonka mukaan ne tekevät yhteistyötä tietosuojaviranomaisten kanssa, jäljempänä kuvatulla tavalla. EU:sta henkilötietoja vastaanottavien yhdysvaltalaisien organisaatioiden on EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa sitouduttava käyttämään tehokkaita menettelyjä varmistaakseen järjestelyn periaatteiden noudattamisen. Muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti järjestelyyn osallistuvilla organisaatioilla on oltava a) i) muutoksenhakuväylä henkilöille, joita tiedot koskevat, a) ii) seurantamenettelyt sen tarkastamiseksi, että organisaatioiden antamat vakuutukset niiden noudattamasta yksityisyyden suojasta pitävät paikkansa, ja a) iii) velvollisuus korjata puutteet, jotka johtuvat periaatteiden noudattamatta jättämisestä, samoin kuin velvollisuus ylläpitää seuraamusjärjestelmää. Organisaatio voi täyttää muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen a kohdan i ja iii alakohdan vaatimukset noudattamalla tässä esitettyjä vaatimuksia yhteistyöstä tietosuojaviranomaisten kanssa.
- b. Organisaatio sitoutuu yhteistyöhön tietosuojaviranomaisten kanssa ilmoittamalla kauppatietosuojaviranomaisille antamassaan EU:n ja Yhdysvaltojen tietosuojakehyksen omassa varmennuksessa (ks. omaa varmennusta koskeva täydentävä periaate), että se
 - i. on päättänyt täyttää muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen a kohdan i ja iii alakohdan vaatimukset sitoutumalla yhteistyöhön tietosuojaviranomaisten kanssa
 - ii. tekee tietosuojaviranomaisten kanssa yhteistyötä tutkittaessa ja ratkaistaessa järjestelyn periaatteiden mukaisesti tehtyjä valituksia ja
 - iii. noudattaa kaikkia tietosuojaviranomaisten antamia ohjeita, joissa todetaan, että organisaation on järjestelyn periaatteiden noudattamiseksi toteutettava erityistoimia. Näihin kuuluvat korjaavat toimet ja korvaukset niiden henkilöiden hyväksi, joihin periaatteiden noudattamatta jättäminen on vaikuttanut.
- c. Tietosuojaviranomaisten paneelien toiminta
 - i. Tiedotuksesta ja neuvonnasta muodostuva tietosuojaviranomaisten yhteistyö järjestetään seuraavasti:
 1. Neuvonnasta vastaa EU:n tasolla perustettava epävirallinen tietosuojaviranomaisten paneeli, joka muun muassa auttaa yhtenäisen ja johdonmukaisen lähestymistavan varmistamisessa.
 2. Paneeli antaa yhdysvaltalaisille organisaatioille ohjeita yksityishenkilöiden tekemistä, ratkaistavina olevista valituksista, jotka koskevat EU:sta EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa siirrettyjen tietojen käsittelyä. Ohjeiden tarkoituksena on varmistaa, että järjestelyn periaatteita sovelletaan asianmukaisesti. Ohjeissa selostetaan myös asianosaisten hyväksi tehtävät korjaavat toimet, joita tietosuojaviranomaiset pitävät asianmukaisina.

3. Paneeli antaa tällaisia ohjeita tapauksista, joita organisaatiot ovat siirtäneet sen käsiteltäväksi, ja/tai valituksista, jotka koskevat tietosuojaviranomaisten kanssa EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa yhteistyöhön sitoutuneita organisaatioita ja jotka paneeli on saanut suoraan yksityishenkilöiltä. Samalla se kannustaa ja tarvittaessa auttaa valituksen tekijöitä turvautumaan ensin organisaation sisäisiin muutoksenhakumenettelyihin.
 4. Ohjeet annetaan vasta, kun kiistan molemmilla osapuolilla on ollut asianmukainen tilaisuus esittää haluamansa huomiot ja toimittaa haluamansa todistusaineisto. Paneeli pyrkii antamaan ohjeet niin nopeasti kuin asianmukainen menettely sallii. Yleissääntönä on, että paneeli antaa ohjeet 60 päivän kuluessa valituksen tai sille siirretyn tapauksen vastaanottamisesta, mahdollisuuksien mukaan lyhyemmässä ajassa.
 5. Paneeli julkistaa vastaanottamiensa valitusten käsittelyn tulokset, jos sen katsoo sen tarpeelliseksi.
 6. Ohjeiden antaminen paneelin kautta ei aseta paneelia tai yksittäisiä tietosuojaviranomaisia minkäänlaiseen vastuuseen.
- ii. Kuten edellä todettiin, tämän riitojenratkaisumenettelyn valitsevien organisaatioiden on sitouduttava noudattamaan tietosuojaviranomaisten ohjeita. Jos organisaatio ei noudata ohjeita 25 päivän kuluessa niiden antamisesta eikä ole antanut tyydyttävää selitystä viivästykselle, paneeli ilmoittaa, että se siirtää asian liittovaltion kauppakomissiolle, liikenneministeriölle tai muulle Yhdysvaltojen liitto- tai osavaltion elimelle, jolla on lakisääteiset valtuudet ryhtyä lainvalvontatoimenpiteisiin vilpillistä tai harhauttavaa menettelyä koskevissa asioissa, tai että se pitää yhteistyösopimusta vakavan sopimusrikkomuksen vuoksi mitättömänä. Jälkimmäisessä tapauksessa paneeli ilmoittaa mitättömyydestä kauppaministeriölle, jotta tietosuojakehyksen osallistujaluetteloa voidaan muuttaa tarvittavalla tavalla. Jos sitoumusta tietosuojaviranomaisten kanssa tehtävästä yhteistyöstä tai järjestelyn periaatteita ei noudateta, liittovaltion kauppakomissiosta annetun lain 5 §:n (15 U.S.C. 45 §), 49 U.S.C. 41712 §:n tai muun vastaavan säännöksen nojalla voidaan nostaa vilpillistä menettelyä koskeva kanne.
- d. Jos organisaatio haluaa, että sen EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvät edut kattavat myös henkilöstötiedot, jotka on siirretty EU:sta käytettäväksi työsuhteiden hoitamisen yhteydessä, organisaation on sitouduttava tekemään yhteistyötä tietosuojaviranomaisten kanssa näiden tietojen osalta (ks. henkilöstötietoja koskeva täydentävä periaate).
- e. Tämän vaihtoehdon valitsevilta organisaatioilta veloitetaan vuosimaksu, jolla on tarkoitus kattaa paneelin toimintakulut. Niiltä voidaan tämän lisäksi veloittaa tarpeelliset käännöskulut, joita aiheutuu, kun paneeli käsittelee sille siirrettyjä asioita ja organisaatiota vastaan tehtyjä valituksia. Maksun määrän määrittää kauppaministeriö komissiota kuultuaan. Maksun voi periä kolmas osapuoli, jonka kauppaministeriö valitsee tätä tarkoitusta varten kerättyjen varojen säilyttäjäksi. Kauppaministeriö tekee tiivistä yhteistyötä komission ja tietosuojaviranomaisten kanssa asianmukaisten menettelyjen saamiseksi käyttöön maksun kautta kerättyjen varojen jakamista varten sekä muissa paneeliin liittyvissä menettelyllisissä ja hallinnollisissa kysymyksissä. Kauppaministeriö ja komissio voivat yhteisestä sopimuksesta muuttaa sitä, kuinka usein maksu peritään.

6. Oma varmennus

- a. Organisaatio voi hyödyntää EU:n ja Yhdysvaltojen tietosuojakehyksen etuja siitä päivästä lähtien, jona kauppaministeriö merkitsee organisaation tietosuojakehyksen osallistujaluetteloon. Kauppaministeriö merkitsee organisaation tietosuojakehyksen osallistujaluetteloon vasta todettuaan, että organisaation ensimmäinen oma varmennus on saatettu päätökseen. Vastaavasti se poistaa organisaation kyseisestä luettelosta, jos organisaatio vetäytyy järjestelystä vapaaehtoisesti, jättää toimittamatta vuotuisen uudelleenvarmennuksensa tai jättää jatkuvasti noudattamatta järjestelyn periaatteita (ks. riitojenratkaisua ja täytäntöönpanoa koskeva täydentävä periaate).
- b. Antaakseen ensimmäisen oman varmennuksensa tai uudelleenvarmennuksensa EU:n ja Yhdysvaltojen tietosuojakehyksessä organisaation on toimitettava kauppaministeriölle asiakirja, jonka on allekirjoittanut sen organisaation toimihenkilö, joka antaa (tilanteen mukaan) oman varmennuksen tai uudelleenvarmennuksen järjestelyn periaatteiden noudattamisesta. ⁽⁸⁾ Asiakirja sisältää vähintään seuraavat tiedot:

⁽⁸⁾ Organisaatiossa toimivan henkilön, jolla on oikeus edustaa organisaatiota ja sen kaikkia kehyksen soveltamisalaan kuuluvia yksiköjä järjestelyn periaatteiden noudattamisen osalta, on annettava varmennus kauppaministeriön tietosuojakehystä käsittelevän verkkosivuston kautta.

- i. oman varmennuksen tai uudelleenvarmennuksen antavan yhdysvaltalaisen organisaation nimi sekä niiden siihen kuuluvien Yhdysvalloissa toimivien yksiköiden tai tytäryhtiöiden nimet, jotka myös noudattavat järjestelyn periaatteita ja jotka organisaatio haluaa järjestelyn kattavan
 - ii. kuvaus organisaation toiminnoista, jotka liittyvät henkilötietoihin, joita sen on määrä vastaanottaa EU:sta EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa
 - iii. kuvaus tällaisia henkilötietoja koskevista organisaation tietosuojaperiaatteista. Kuvauksessa annetaan muun muassa seuraavat tiedot:
 1. jos organisaatiolla on julkiset verkkosivut, verkko-osoite, jossa sen tietosuojaperiaatteet ovat saatavilla, tai jos julkisia verkkosivuja ei ole, tieto siitä, missä yleisö voi tutustua kyseisiin periaatteisiin, ja
 2. milloin tietosuojaperiaatteet on pantu täytäntöön
 - iv. mikä on organisaation yhteyspiste asioissa, jotka koskevat valitusten käsittelyä, tietoihin tutustumista koskevia pyyntöjä sekä kaikkia muita järjestelyn periaatteisiin liittyviä kysymyksiä ⁽⁹⁾. Ilmoitettavia tietoja ovat muun muassa seuraavat:
 1. organisaation asianomaisten henkilöiden tai yhteyspisteiden nimet, tehtävänimikkeet (soveltuvin osin), sähköpostiosoitteet ja puhelinnumerot ja
 2. organisaation asianomainen yhdysvaltalainen postiosoite
 - v. millä erityisellä lakisääteisellä elimellä (joka mainitaan järjestelyn periaatteissa tai niiden tulevassa liitteessä) on toimivalta käsitellä organisaatiosta tehtyt valitukset, jotka koskevat mahdollisia sopimattomia tai vilpillisiä käytäntöjä ja yksityisyyttä koskevien lakien ja asetusten rikkomista
 - vi. kaikkien sellaisten yksityisyydensuojaohjelmien nimet, joihin organisaatio osallistuu
 - vii. tarkastamismenetelmä (eli oma varmennus tai ulkopuolisen tahon suorittamat arvioinnit, mukaan lukien tällaiset arvioinnit suorittava kolmas osapuoli) ⁽¹⁰⁾ ja
 - viii. asiaankuuluvat saatavilla olevat riippumattomat muutoksenhakumekanismit periaatteisiin liittyvien ratkaisemattomien valitusten tutkimiseksi ⁽¹¹⁾.
- c. Jos organisaatio haluaa, että sen EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvät edut kattavat myös henkilöstötiedot, jotka on siirretty EU:sta käytettäväksi työsuhteiden yhteydessä, tämä on mahdollista, jos lakisääteisellä elimellä, joka mainitaan järjestelyn periaatteissa tai niiden tulevassa liitteessä, on toimivalta käsitellä organisaatiota vastaan esitetyt vaateet, jotka koskevat henkilöstötietojen käsittelyä. Lisäksi organisaation on mainittava tämä ensimmäisessä omassa varmennuksessaan ja mahdollisissa uudelleenvarmennuksissa sekä ilmoitettava, että se sitoutuu tekemään yhteistyötä EU:n toimivaltaisten viranomaisten kanssa henkilöstötietoja ja tietosuojaviranomaisten tehtäviä koskevien täydentävien periaatteiden mukaisesti (tapauksen mukaan) ja että se noudattaa näiden viranomaisten antamia ohjeita. Organisaation on myös toimitettava kauppaministeriölle jäljennös sen henkilöstöä koskevista tietosuojaperiaatteista sekä ilmoitettava, missä henkilöstö, jota asia koskee, voi tutustua organisaation tietosuojaperiaatteisiin.

⁽⁹⁾ Ensimmäinen 'organisaation yhteyspiste' tai 'organisaation toimihenkilö' ei voi olla organisaation ulkopuolella (esimerkiksi ulkopuolinen asiamies tai ulkopuolinen konsultti).

⁽¹⁰⁾ Ks. tarkastusta koskeva täydentävä periaate.

⁽¹¹⁾ Ks. riitojenratkaisua ja täytäntöönpanoa koskeva täydentävä periaate.

- d. Kauppaministeriö pitää yllä tietosuojakehyksen osallistujaluetteloa organisaatioista, jotka ovat toimittaneet täydellisen ensimmäisen oman varmennuksen, ja saattaa sen julkisesti saataville. Kauppaministeriö päivittää luettelon vuosittain annettavilla omilla uudelleenvarmennuksilla sekä ilmoituksilla, jotka on saatu riitojenratkaisua ja täytäntöönpanoa koskevan täydentävän periaatteen mukaisesti. Uudelleenvarmennus on annettava uudelleen vähintään kerran vuodessa. Jos organisaatio ei uusi omaa varmennustaan, se poistetaan tietosuojakehyksen osallistujaluettelosta eikä sille enää myönnetä EU:n ja Yhdysvaltojen tietosuojakehyksen etuja. Kaikilla organisaatioilla, jotka kauppaministeriö on merkinnyt tietosuojakehyksen osallistujaluetteloon, on oltava ilmoitusperiaatteen mukaiset tietosuojaperiaatteet, joissa mainitaan, että organisaatiot noudattavat järjestelyn periaatteita. ⁽¹²⁾ Jos organisaation tietosuojaperiaatteet ovat saatavilla verkossa, niissä on oltava linkki kauppaministeriön tietosuojakehystä käsittelevälle verkkosivustolle sekä linkki sellaisen riippumattoman muutoksenhakumekanismiin verkkosivustolle tai valituslomakkeeseen, joka voi tutkia järjestelyn periaatteisiin liittyvät ratkaisemattomat valitukset ilman, että henkilölle aiheutuu siitä kustannuksia.
- e. Järjestelyn periaatteita sovelletaan välittömästi oman varmennuksen jälkeen. Järjestelyyn osallistuvien organisaatioiden, jotka ovat aiemmin antaneet oman varmennuksen EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatteiden noudattamisesta, on päivitettävä tietosuojaperiaatteensa siten, että niissä viitataan nyt "EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteisiin". Tällaisten organisaatioiden on sisällytettävä tämä viittaus periaatteisiinsa mahdollisimman pian, joka tapauksessa viimeistään kolmen kuukauden kuluttua EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden voimaantulopäivästä.
- f. Organisaation on sovellettava järjestelyn periaatteita kaikkiin henkilötietoihin, jotka organisaatio vastaanottaa EU:sta EU:n ja Yhdysvaltojen tietosuojakehyksen perusteella. Sitoutumista järjestelyn periaatteiden noudattamiseen ei rajoiteta ajallisesti niiden henkilötietojen osalta, jotka organisaatio on vastaanottanut ollessaan oikeutettu EU:n ja Yhdysvaltojen tietosuojakehyksen etuihin. Sitoutuminen merkitsee sitä, että organisaatio soveltaa järjestelyn periaatteita tällaisiin tietoihin niin kauan kuin se tallentaa, käyttää tai luovuttaa tietoja, vaikka se myöhemmin mistä tahansa syystä jättäytyisi EU:n ja Yhdysvaltojen tietosuojakehyksen ulkopuolelle. Jos organisaatio haluaa vetäytyä EU:n ja Yhdysvaltojen tietosuojakehyksestä, sen on ilmoitettava tästä kauppaministeriölle etukäteen. Ilmoituksesta on käytävä ilmi myös, mitä organisaatio tekee henkilötiedoille, jotka se on saanut EU:n ja Yhdysvaltojen tietosuojakehyksen perusteella (eli säilyttääkö, palauttaako vai hävittääkö se tiedot, ja jos se säilyttää tiedot, mitä hyväksyttyä keinoa se käyttää tietojen suojaamiseksi). Jos organisaatio vetäytyy EU:n ja Yhdysvaltojen tietosuojakehyksestä mutta haluaa säilyttää tällaiset tiedot, sen on joko vahvistettava kauppaministeriölle vuosittain sitoumuksensa, jonka mukaan se jatkaa periaatteiden soveltamista tietoihin, tai annettava tiedoille "riittävä" suoja muiden hyväksyttyjen keinojen avulla (esimerkiksi käyttämällä sopimusta, joka vastaa täysin komission hyväksymissä vakiosopimuslausekkeissa olevia ehtoja). Muussa tapauksessa sen on palautettava tai hävitettävä tiedot. ⁽¹³⁾ Organisaation, joka vetäytyy EU:n ja Yhdysvaltojen tietosuojakehyksestä, on poistettava kaikista tietosuojaperiaatteistaan kaikki EU:n ja Yhdysvaltojen tietosuojakehystä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuisi edelleen EU:n ja Yhdysvaltojen tietosuojakehykseen ja että se olisi oikeutettu järjestelyn etuihin.

⁽¹²⁾ Ensimmäistä kertaa oman varmennuksen antava organisaatio ei voi lopullisissa tietosuojaperiaatteissaan ilmaista osallistuvansa EU:n ja Yhdysvaltojen tietosuojakehykseen ennen kuin kauppaministeriö ilmoittaa organisaatiolle, että se voi näin tehdä. Organisaation on toimitettava kauppaministeriölle luonnos järjestelyn periaatteiden mukaisista tietosuojaperiaatteista, kun se antaa ensimmäisen oman varmennuksen. Kun kauppaministeriö on todennut, että organisaation ensimmäinen oma varmennus on muuten saatettu päätökseen, kauppaministeriö ilmoittaa organisaatiolle, että sen olisi viimeisteltävä (esimerkiksi tarvittaessa julkaistava) EU:n ja Yhdysvaltojen tietosuojakehyksen mukaiset tietosuojaperiaatteensa. Organisaation on ilmoitettava kauppaministeriölle viipymättä, kun tietosuojaperiaatteet on viimeistely, jolloin kauppaministeriö merkitsee organisaation tietosuojakehyksen osallistujaluetteloon.

⁽¹³⁾ Jos organisaatio päättää vetäytymishetkellä säilyttää EU:n ja Yhdysvaltojen tietosuojakehyksen perusteella saamansa henkilötiedot ja vahvistaa kauppaministeriölle vuosittain sitoumuksensa, jonka mukaan se jatkaa periaatteiden soveltamista tietoihin, organisaation on varmennettava kauppaministeriölle kerran vuodessa vetäytymisensä jälkeen (eli paitsi jos ja siihen asti, että organisaatio antaa tiedoille "riittävän" suojan muiden hyväksyttyjen keinojen avulla tai palauttaa ja hävittää kaikki tällaiset tiedot ja ilmoittaa kauppaministeriölle tästä toimesta), mitä se on tehnyt näille henkilötiedoille, mitä se tekee kaikille näille henkilötiedoille, joita se edelleen säilyttää, ja kuka toimii jatkossa yhteyspisteenä järjestelyn periaatteisiin liittyvissä kysymyksissä.

- g. Organisaation, joka lakkaa olemasta erillinen oikeussubjekti yhtiömuotoon liittyvän muutoksen, kuten sulautumisen, yritystoston, konkurssin tai purkamisen seurauksena, on ilmoitettava tästä kauppaministeriölle etukäteen. Ilmoitukseen on sisällyttävä tieto myös siitä, aikooko yhtiömuodon muutoksen yhteydessä muodostuva yksikkö i) osallistua edelleen EU:n ja Yhdysvaltojen tietosuojakehykseen aiemmin annetun oman varmennuksen kautta, ii) antaa oman varmennuksen EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvana uutena yksikkönä (esimerkiksi kun uudella yksiköllä tai jäljelle jääneellä yksiköllä ei vielä ole omaa varmennusta, jonka perusteella se voisi osallistua tietosuojakehykseen), vai iii) ottaa käyttöön muita suojatoimia, kuten kirjallisen sopimuksen, jolla varmistetaan järjestelyn periaatteiden jatkuva soveltaminen kaikkiin henkilötietoihin, jotka organisaatio on saanut tietosuojakehyksen perusteella ja jotka säilytetään. Jos i, ii tai iii alakohtaa ei sovelleta, kaikki EU:n ja Yhdysvaltojen tietosuojakehyksen perusteella saadut henkilötiedot on palautettava tai hävitettävä viipymättä.
- h. Kun organisaatio vetäytyy EU:n ja Yhdysvaltojen tietosuojakehyksestä mistä tahansa syystä, sen on poistettava kaikki maininnat, joista voisi päätellä, että se osallistuu edelleen EU:n ja Yhdysvaltojen tietosuojakehykseen tai että se on oikeutettu tietosuojakehyksen etuihin. Jos EU:n ja Yhdysvaltojen tietosuojakehyksen varmennusmerkki on käytössä, myös se on poistettava. Jos organisaatio antaa yleisölle vääriä tietoja järjestelyn periaatteiden noudattamisesta, liittovaltion kauppakomissio, liikenneministeriö tai muu asiaankuuluva valtiollinen elin voi nostaa organisaatiota vastaan kanteen. Kauppaministeriölle annetut väärät tiedot ovat kanneperuste vääriä lausuntoja koskevan Yhdysvaltojen lain nojalla (False Statements Act, 18 U.S.C. § 1001).

7. Tarkastus

- a. Organisaatioiden on otettava käyttöön seurantamenettely, jonka avulla tarkastetaan, että organisaation antamat vakuutukset EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisista yksityisyydensuojakäytännöistä pitävät paikkansa ja että yksityisyyden suoja on toteutettu organisaation esittämällä tavalla ja järjestelyn periaatteiden mukaisesti.
- b. Täyttääkseen muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaiset tarkastamisvaatimukset organisaation on tarkastettava annettujen vakuutusten paikkansapitävyys arvioinnilla, jonka suorittaa organisaatio itse tai jokin ulkopuolinen taho.
- c. Jos organisaatio on valinnut itsearvioinnin, tarkastuksen on osoitettava, että sen EU:sta saamia henkilötietoja koskevat tietosuojaperiaatteet ovat täsmällisiä, kattavia, helposti saatavilla, periaatteiden mukaisia ja kaikilta osin täytäntöönpanut (eli niitä noudatetaan). Tarkastuksessa on myös käytävä ilmi, että henkilöille annetaan tieto kaikista organisaation sisäisistä valitusten käsittelymekanismeista ja riippumattomista muutoksenhakumechanismeista, joille henkilöt voivat tehdä valituksia, organisaatio on ottanut käyttöön menettelyt, joiden avulla työntekijöitä koulutetaan tietosuojaperiaatteiden noudattamisessa ja joiden mukaisesti työntekijöille määrätään seuraamuksia tietosuojaperiaatteiden noudattamatta jättämisestä, ja organisaatiolla on käytössään sisäisiä menettelyjä, joiden mukaisesti tarkastellaan säännöllisin väliajoin objektiivisesti, onko edellä selostettua noudatettu. Organisaation toimihenkilön tai muun valtuutetun edustajan on vähintään kerran vuodessa allekirjoitettava lausunto, jossa todennetaan, että itsearviointi on suoritettu. Lausunto on pyynnöstä asetettava henkilöiden saataville, tai sen on oltava käytettävissä periaatteiden noudattamista koskevan tutkinnan tai valitusmenettelyn yhteydessä.
- d. Jos organisaatio on valinnut arvioinnin, jossa ulkopuolinen taho tarkastelee periaatteiden noudattamista, tarkastuksen on osoitettava, että organisaation EU:sta saamia henkilötietoja koskevat tietosuojaperiaatteet ovat täsmällisiä, kattavia, helposti saatavilla, periaatteiden mukaisia ja kaikilta osin täytäntöönpanut (eli niitä noudatetaan). Tarkastuksessa on myös käytävä ilmi, että henkilöille annetaan tieto mekanismeista, joiden kautta he voivat tehdä valituksia. Arvioinnissa voidaan hyödyntää tarpeen mukaan muun muassa tarkastusta, satunnaisotantaan perustuvia tarkistuksia, "houkutuslintuja" tai teknisiä apuvälineitä. Arvioinnin tekijän, organisaation toimihenkilön tai muun valtuutetun edustajan on vähintään kerran vuodessa allekirjoitettava lausunto, jossa todennetaan, että ulkopuolisen tekemä periaatteiden noudattamista koskeva arviointi on saatettu menestyksellisesti päätökseen. Lausunnon on pyynnöstä oltava henkilöiden saatavilla, tai sen on oltava käytettävissä periaatteiden noudattamista koskevan tutkinnan tai valitusmenettelyn yhteydessä.
- e. Organisaatioiden on dokumentoitava EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisten yksityisyydensuojakäytäntöjen täytäntöönpano ja toimitettava pyynnöstä asiaa koskeva dokumentaatio – periaatteiden noudattamista koskevan tutkinnan tai valitusmenettelyn yhteydessä – valituksia käsittelevälle riippumattomalle elimelle tai sopimattomia ja vilpillisiä käytäntöjä tutkivalle elimelle. Organisaatioiden on myös vastattava nopeasti kauppaministeriön tekemiin tiedusteluihin ja tietopyyntöihin, joilla pyritään selvittämään, noudattaako organisaatio järjestelyn periaatteita.

8. Tiedonsaanti

a. Tiedonsaantiperiaate käytännössä

- i. Järjestelyn periaatteiden mukaan tiedonsaanti on keskeistä yksityisyyden suojassa. Henkilö voi sen perusteella erityisesti tarkistaa häntä itseään koskevan tiedon paikkansapitävyyden. Tiedonsaantiperiaatteella tarkoitetaan, että henkilöillä on oikeus
 1. saada organisaatiolta vahvistus siitä, käsittelee se heitä koskevia henkilötietoja, ⁽¹⁴⁾
 2. saada kyseiset tiedot nähtäväkseen, jotta he voivat tarkastaa niiden paikkansapitävyyden ja niiden käsittelyn laillisuuden, ja
 3. saada tiedot korjatuiksi, muutetuiksi tai hävitetyiksi, jos ne ovat virheellisiä tai niitä on käsitelty järjestelyn periaatteiden vastaisesti.
- ii. Henkilön ei tarvitse perustella pyyntöään saada itseään koskevat tiedot. Vastatessaan henkilön tiedonsaantipyynnön organisaation on ensiksi kiinnitettävä huomiota siihen, miksi tietoja pyydetään. Jos tiedonsaantipyynnö on esimerkiksi epämääräinen tai kattaa laajan alan, organisaatio voi keskustella kyseisen henkilön kanssa, jotta pyynnön syy ymmärrettäisiin paremmin ja halutut tiedot löytyisivät helpommin. Organisaatio saattaa tiedustella, minkä organisaation osan tai osien kanssa henkilö on ollut tekemisissä, minkä luonteista tietoa pyyntö koskee tai mikä on tiedon käyttötarkoitus.
- iii. Tiedonsaantiperiaatteen perimmäisen luonteen mukaisesti organisaatioiden olisi aina vilpittömästi pyrittävä antamaan tiedot. Jos esimerkiksi määrätty tiedot on suojattava ja ne voidaan helposti erottaa muista pyynnön kohteena olevista henkilötiedoista, organisaation on erotettava suojattu tieto ja annettava muu tieto henkilön saataville. Jos organisaatio päättää, että pääsyä tietoihin on jossakin tapauksessa rajoitettava, päätös on perusteltava tietoja pyytävälle henkilölle ja hänelle on ilmoitettava, mistä tai keneltä hän voi saada asiasta lisätietoja.

b. Tiedonsaantioikeudesta johtuva rasitus ja sen aiheuttamat kulut

- i. Henkilötietoja koskevaa tiedonsaantioikeutta voidaan rajoittaa poikkeuksellisissa olosuhteissa, jos muun kuin tietoja pyytäneen henkilön laillisia oikeuksia loukattaisiin tai jos tiedonsaannista aiheutuva rasitus tai siihen liittyvät kustannukset olisivat suhteettoman suuria verrattuina henkilön tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa. Kustannukset ja tietojen antamisesta aiheutuvat rasitukset ovat tärkeitä tekijöitä, ja ne olisi otettava huomioon, mutta niiden perusteella ei päätetä, onko tiedon antaminen kohtuullista.
- ii. Jos henkilötietoa esimerkiksi käytetään yksityishenkilöä koskevan tärkeän päätöksen tekemiseen (esimerkiksi jos on kyse jonkin merkittävän etuuden, kuten vakuutuksen, lainan tai työpaikan, myöntämisestä tai epämisestä), organisaation on annettava tiedot, vaikka tietojen hankkiminen olisi suhteellisen vaikeaa tai kallista. Tämä on myös muiden näissä täydentävissä periaatteissa olevien sääntöjen mukaista. Vaikka pyydetty henkilötiedot eivät olisi arkaluonteisia ja vaikka niiden perusteella ei tehtäisi päätöksiä, joilla on merkittävä vaikutus henkilöön, mutta tiedot ovat helposti saatavilla ja niiden toimittaminen on halpaa, organisaation on myönnettävä pääsy kyseisiin tietoihin.

c. Luottamukselliset kaupalliset tiedot

- i. Luottamuksellinen kaupallinen tieto on organisaation suojelemaa tietoa, jonka julkaiseminen edistäisi kilpailijan toimintaa markkinoilla. Organisaatiot voivat kieltää tiedonsaannin tai rajoittaa sitä, jos antamalla täysi pääsy tietoihin paljastettaisiin sen omaa luottamuksellista kaupallista tietoa, esimerkiksi kyseisen organisaation markkinapäätelmiä tai luokituksia, taikka toisen organisaation luottamuksellista kaupallista tietoa, jos tällaista tietoa koskee sopimukseen perustuva luottamuksellisuusvelvoite.

⁽¹⁴⁾ Organisaation olisi vastattava henkilön kysymyksiin, jotka koskevat tiedonkäsittelyn tarkoitusta, käsiteltyjen henkilötietojen luokkia sekä henkilötietojen vastaanottajia tai vastaanottajien luokkia.

- ii. Jos luottamuksellinen kaupallinen tieto on erotettavissa muista tiedonsaantipyynnön kohteena olevista henkilötiedoista, organisaation on erotettava luottamuksellinen tieto ja asetettava ei-luottamuksellinen tieto henkilön saataville.
- d. Tietokantojen hallinnointi
- i. Organisaatio voi järjestää tiedonsaannin luovuttamalla henkilölle halutut henkilötiedot, eikä tiedonsaanti edellytä mahdollisuutta käyttää organisaation tietokantoja.
 - ii. Pääsy koskee vain organisaation säilyttämiä henkilötietoja. Tiedonsaantiperiaate ei sinänsä velvoita säilyttämään tai ylläpitämään henkilötietoja, järjestämään niitä uudelleen tai muuttamaan tietokantojen rakennetta.
- e. Milloin tietojensaantia voidaan rajoittaa?
- i. Koska organisaatioiden olisi aina vilpittömästi pyrittävä antamaan henkilölle pääsy tämän henkilötietoihin, olosuhteita, joissa organisaatiot voivat rajoittaa tätä pääsyä, on vähän, ja tietoihin pääsy voidaan rajoittaa vain erityisistä syistä. Kuten myös yleisessä tietosuojasetuksessa säädetään, organisaatio voi kieltäytyä luovuttamasta tietoja, jos niiden luovuttaminen todennäköisesti vaarantaisi vastakkaisen tärkeän yleisen edun. Tällaisia yleisiä etuja ovat esimerkiksi kansallinen turvallisuus, maanpuolustus tai yleinen turvallisuus. Lisäksi pääsy voidaan kieltää, kun tietoja käsitellään pelkästään tutkimus- tai tilastotarkoituksiin. Muita syitä tiedonsaannin estämiseen tai rajoittamiseen ovat seuraavat:
 - 1. tietojen luovuttaminen haittaa lakien täytäntöönpanoa ja lainvalvontaa, mukaan luettuina rikosten ehkäisy, tutkinta ja havaitseminen, tai rikosperusteisen vahingonkorvausvaateen toteuttamista tai oikeutta puolueettomaan oikeudenkäyntiin,
 - 2. tietojen luovuttamisella loukataan muiden henkilöiden laillisia oikeuksia tai tärkeitä etuja,
 - 3. tietojen luovuttaminen rikkoo asianajosalaisuutta tai muuta vastaavaa ammatillista etuoikeutta tai velvoitetta,
 - 4. tietojen luovuttaminen vaikeuttaa työntekijää koskevan turvallisuusselvityksen tekemistä, työntekijän tekemän valituksen käsittelyä tai työntekijän seuraajan valintaa koskevaa suunnittelua ja yritysten uudelleenorganisointia, tai
 - 5. tietojen luovuttaminen vaarantaa luottamuksellisuuden, joka on tarpeen hoidettaessa moitteettomaan hallintoon liittyviä valvonta-, tarkastus- ja sääntelytehtäviä tai käytäessä nyt tai tulevaisuudessa organisaatiota koskevia neuvotteluja.
 - ii. Organisaation, joka vetoaa luovuttamisvelvollisuutta koskevaan poikkeukseen, on osoitettava, että poikkeus on tarpeellinen.
- f. Oikeus saada vahvistus henkilötietojen hallussapidosta. Maksu, joka voidaan periä tietojen luovuttamisesta aiheutuvien kustannusten kattamiseksi.
- i. Henkilöllä on oikeus saada vahvistus siitä, onko organisaatiolla häntä koskevia henkilötietoja. Henkilöllä on myös oikeus saada henkilötietonsa nähtäväkseen. Organisaatio voi periä maksun, joka ei saa olla liiallinen.
 - ii. Maksun periminen saattaa olla perusteltua esimerkiksi silloin, kun tietopyynnot ovat ilmeisen kohtuuttomia erityisesti toistuvuutensa takia.
 - iii. Tiedonsaantia ei voida estää kustannussyihin vetoamalla, jos rekisteröity tarjoutuu maksamaan kustannukset.
- g. Toistuvat tai tarpeettomat tietopyynnot
- i. Organisaatio voi asettaa kohtuulliset rajat sille, kuinka usein tietyn ajan kuluessa henkilölle voidaan luovuttaa hänen henkilötietonsa. Rajoja asettaessaan organisaation olisi otettava huomioon esimerkiksi se, kuinka usein henkilötietoja päivitetään, mihin tarkoitukseen tietoja käytetään ja mikä tietojen luonne on.

h. Petolliset tietopyynnöt

- i. Organisaation ei tarvitse luovuttaa tietoja, ellei se saa tarpeeksi tietoa voidakseen varmistua tiedonsaantipyynnön esittäjän henkilöllisyydestä.

i. Vastaamisaika

- i. Organisaatioiden olisi vastattava tietopyyntöihin kohtuullisessa ajassa, kohtuullisella tavalla ja sellaisessa muodossa, jonka henkilö voi helposti ymmärtää. Jos organisaatio toimittaa rekisteröidyille tietoja säännöllisin väliajoin, se voi vastata yksittäiseen tietopyyntöön säännöllisen toimituksen yhteydessä, jos tästä ei aiheudu kohtuutonta viivästystä.

9. **Henkilöstötiedot**

a. EU:n ja Yhdysvaltojen tietosuojakehyksen kattavuus

- i. Kun EU:ssa toimiva organisaatio siirtää (entistä tai nykyistä) henkilöstöään koskevia, työsuhteen yhteydessä kerättyjä henkilötietoja emoyhtiölle, organisaatioon sidoksissa olevalle yhtiölle tai riippumattomalle palvelujen tarjoajalle, joka sijaitsee Yhdysvalloissa ja osallistuu EU:n ja Yhdysvaltojen tietosuojakehykseen, tiedon siirtoon sovelletaan kyseinen tietojen siirto nauttii EU:n ja Yhdysvaltojen tietosuojakehyksen eduista. Näissä tapauksissa tietojen keräämiseen ja niiden käsittelyyn ennen siirtoa sovelletaan kyseisen EU:n jäsenvaltion kansallista lainsäädäntöä, ja kaikkia kyseisen lainsäädännön mukaisia ehtoja ja rajoituksia, jotka koskevat tietojen siirtoa, on noudatettava.
- ii. Järjestelyn periaatteita sovelletaan vain silloin, kun siirretään tai annetaan käyttöön yksittäinen henkilötieto, jonka perusteella henkilö tunnustetaan tai on tunnistettavissa. Yhdistettyihin työntekijätietoihin perustuvat tilastot, joissa ei ole henkilötietoja, tai tiedot, joista nimet on poistettu, eivät ole ongelmallisia yksityisyyden suojan kannalta.

b. Ilmoitus- ja valintaperiaatteiden soveltaminen

- i. Yhdysvaltalainen organisaatio, joka on vastaanottanut EU:sta henkilöstötietoja EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa, voi luovuttaa tiedot kolmannelle osapuolelle tai käyttää niitä muuhun kuin alkuperäiseen käyttötarkoitukseen ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Jos organisaatio aikoo esimerkiksi käyttää työsuhteessa kerättyjä henkilötietoja muuhun kuin työsuhteeseen liittyvään tarkoitukseen, kuten markkinointiin, kyseisen yhdysvaltalaisen organisaation on tarjottava työntekijöille asianmukainen valintamahdollisuus ennen tietojen käyttämistä, elleivät työntekijät ole jo aiemmin antaneet lupaa tietojen käyttöön tällaisiin tarkoituksiin. Tällainen käyttö ei saa olla ristiriidassa niiden tarkoitusten kanssa, joita varten henkilötiedot on kerätty tai joihin henkilö on myöhemmin antanut luvan. Jos työntekijät kieltävät tietojen käyttämisen, heidän tekemänsä valinta ei myöskään saa rajoittaa heidän uramahdollisuuksiaan eikä heitä saa rangaista sen vuoksi.
- ii. On huomattava, että joistakin EU:n jäsenvaltioista tehtäviin tiedonsiirtoihin sovelletaan tiettyjä yleisiä ehtoja, jotka voivat rajoittaa tällaisten tietojen muuta käyttöä myös sen jälkeen, kun tiedot on siirretty EU:n ulkopuolelle, ja näitä ehtoja on noudatettava.
- iii. Lisäksi työnantajien on kohtuullisin pyrkimyksin pidettävä huolta siitä, että henkilötietojen käyttöä koskevia henkilöstön valintoja noudatetaan. Tällöin voi olla kyse esimerkiksi siitä, että rajoitetaan pääsyä tällaisiin henkilötietoihin, esitetään määrätty tiedot anonyymeinä tai käytetään nimien sijasta koodeja tai salanimiä, jos oikeiden nimien käyttö ei liikkeenjohdollisista syistä ole välttämätöntä.
- iv. Organisaatio voi olla antamatta ilmoitusta tai myöntämättä valintamahdollisuutta siinä määrin ja sellaisena ajanjaksona kuin on tarpeellista, jotta organisaation mahdollisuudet nimittää tai ylentää työntekijöitä tai tehdä muita henkilöstöön liittyviä päätöksiä eivät vaarantu.

c. Tiedonsaantiperiaatteen soveltaminen

- i. Täydentävässä tiedonsaantiperiaatteessa selostetaan syitä, joiden perusteella voidaan kieltäytyä luovuttamasta pyydettyjä henkilötietoja tai rajoittaa niiden saantia. EU:n työnantajien on luonnollisesti noudatettava paikallisia säädöksiä ja varmistettava, että EU:hun sijoittautuneet työntekijät saavat tietoja kotimaansa lainsäädännön mukaisesti huolimatta siitä, missä tietoja käsitellään ja säilytetään. EU:n ja Yhdysvaltojen tietosuojakehys edellyttää, että tällaista tietoa Yhdysvalloissa käsittelevä organisaatio tekee asiassa yhteistyötä ja luovuttaa tiedot joko suoraan tai eurooppalaisen työnantajan välityksellä.

d. Täytäntöönpano

- i. Jos henkilötietoa käytetään ainoastaan työsuhteen yhteydessä, työntekijään nähden tiedoista on ensisijaisesti vastuussa EU:ssa toimiva organisaatio. Tästä seuraa, että jos eurooppalaiset työntekijät valittavat tietosuojaoikeuksiensa rikkomisesta eivätkä ole tyytyväisiä sisäisen selvityksen tai valitus- ja muutoksenhakumenettelyn tulokseen (tai jonkin sellaisen valitusmenettelyn tulokseen, joka on toteutettu ammattiliiton kanssa tehdyn sopimuksen mukaisesti), heidän on käännätyävä työskentelymaansa kansallisen tietosuojaviranomaisen tai työvoimaviranomaisen puoleen. Tätä sovelletaan myös tapauksiin, joissa väitetyn työntekijöiden henkilötietojen virheellisen käsittelyn on toteuttanut yhdysvaltalainen organisaatio, joka on saanut tiedot työnantajalta ja on niin ollen osallinen väitettyyn järjestelyn periaatteiden rikkomiseen. Tämä on tehokkain tapa soveltaa usein päällekkäisiä oikeuksia ja velvollisuuksia, jotka johtuvat paikallisista työlaeista, työsopimuksista ja tietosuojasäädöksistä.
- ii. EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvan yhdysvaltalaisen organisaation, joka käyttää EU:sta toimitettua henkilötietoa ja haluaa kyseisten tiedonsiirtojen kuuluvan EU:n ja Yhdysvaltojen tietosuojakehyksen piiriin, olisi tämän vuoksi sitouduttava tekemään yhteistyötä toimivaltaisten EU:n viranomaisten kanssa näiden tekemissä tutkimuksissa ja noudattamaan kyseisten viranomaisten näissä tapauksissa antamia ohjeita.

e. Tietojen edelleen siirtämiseen liittyvää vastuuvuolisuutta koskeva periaate

- i. Vähäistä työntekijämäärää koskeva, EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa toteutettava henkilötietojen siirto rekisterinpitäjälle voidaan toteuttaa tiedonsaantiperiaatetta soveltamatta ja ilman, että rekisterinpitäjänä toimivan kolmannen osapuolen kanssa tehdään sopimusta, vaikka tätä muutoin vaadittaisiin edelleen siirtämiseen liittyvää vastuuvuolisuutta koskevan periaatteen mukaan, kun on kyse EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvan organisaation satunnaisesta henkilöstöön liittyvästä operatiivisesta toimesta, jossa tietoja käytetään esimerkiksi lentolipun tai hotellihuoneen varaamiseen tai vakuutusuojan järjestämiseen, ja kun järjestelyyn osallistuva organisaatio on noudattanut ilmoitus- ja valintaperiaatteita.

10. Tietojen edelleen siirtämistä koskevat pakolliset sopimukset

a. Tietojenkäsittelyä koskevat sopimukset

- i. Kun henkilötietoja siirretään EU:sta Yhdysvaltoihin ainoastaan tietojen käsittelyä varten, tästä on laadittava sopimus riippumatta siitä, osallistuuko tietojen käsittelijä EU:n ja Yhdysvaltojen tietosuojakehykseen.
- ii. Eurooppalaisen rekisterinpitäjän on tehtävä sopimus aina, kun tietoja siirretään pelkästään käsittelytarcoituksessa riippumatta siitä, käsitelläänkö tiedot EU:ssa vai sen ulkopuolella, ja siitä, osallistuuko tietojen käsittelijä EU:n ja Yhdysvaltojen tietosuojakehykseen. Sopimuksen tarkoituksena on varmistaa, että henkilötietojen käsittelijä
1. toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti,
 2. toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta katoamiselta, muuttamiselta, luvattomalta luovuttamiselta tai pääsyn antamiselta tietoihin, ymmärtää, onko edelleen siirtäminen sallittua, ja
 3. ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää antamaan vastauksia henkilöille, jotka toteuttavat järjestelyn periaatteiden mukaisia oikeuksiaan.

- iii. Koska järjestelyyn osallistuvat organisaatiot tarjoavat riittävän tietosuojan, siihen kuuluvien organisaatioiden kanssa tehtävät, pelkkää tietojenkäsittelyä koskevat sopimukset eivät edellytä ennakkolupaa.
- b. Siirrot samaan ryhmään kuuluvien yritysten tai yksiköiden välillä
- i. Kun henkilötietoja siirretään kahden sellaisen rekisterinpitäjän välillä, jotka kuuluvat samaan yritysryhmään, tietojen edelleen siirtämiseen liittyvää vastuuvuorollisuutta koskevan periaatteen mukaan sopimusta ei aina vaadita. Samaa ryhmään kuuluvien yritysten ja yksiköiden rekisterinpitäjät voivat tehdä siirrot muiden instrumenttien nojalla. Tällaisia ovat muun muassa EU:n yrityksiä koskevat sitovat säännöt ja muut ryhmän sisäiset instrumentit (esimerkiksi vaatimustenmukaisuus- ja valvontaohjelmat). Näillä rekisterinpitäjät varmistavat, että henkilötietojen suoja säilyy järjestelyn periaatteiden mukaisena. Kun tällaisia siirtoja tehdään, järjestelyyn osallistuva organisaatio on edelleen vastuussa järjestelyn periaatteiden noudattamisesta.
- c. Siirrot rekisterinpitäjien välillä
- i. Kun siirtoja tehdään rekisterinpitäjien välillä, vastaanottavan rekisterinpitäjän ei tarvitse olla järjestelyyn osallistuva organisaatio eikä sillä tarvitse olla riippumatonta muutoksenhakumekanismia. Järjestelyyn osallistuvan organisaation on tehtävä sopimus tietojen vastaanottavan, rekisterinpitäjänä toimivan kolmannen osapuolen kanssa. Sopimuksessa on määrittävä, että tietosuojan taso vastaa EU:n ja Yhdysvaltojen tietosuojakehyksen tasoa, mutta siinä ei tarvitse määrätä, että kolmas osapuoli osallistuu järjestelyyn tai että sillä on riippumaton muutoksenhakumekanismi. Kolmannen osapuolen on kuitenkin asetettava käyttöön vastaava mekanismi.

11. Riitojenratkaisu ja täytäntöönpano

- a. Muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteessa määrätään vaatimuksista, jotka koskevat EU:n ja Yhdysvaltojen tietosuojakehyksen täytäntöönpanoa. Sitä, miten muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen a kohdan ii alakohdan vaatimukset täytetään, selostetaan tarkastusta koskevassa täydentävässä periaatteessa. Tässä täydentävässä periaatteessa käsitellään muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen a kohdan i ja iii alakohtaa, jotka molemmat edellyttävät riippumattomia muutoksenhakumekanismeja. Nämä mekanismit voivat olla muodoiltaan erilaisia, mutta niiden on oltava muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen vaatimusten mukaisia. Organisaatiot täyttävät vaatimukset, jos ne i) noudattavat yksityis sektorilla laadittuja yksityisyydensuojaohjelmia, joissa järjestelyn periaatteet on otettu osaksi sääntöjä ja joihin on sisällytetty samantyyppiset tehokkaat täytäntöönpanomekanismit kuin muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteessa on kuvattu, ii) noudattavat sellaisten valvontaviranomaisten päätöksiä, jotka ovat lakien ja asetusten mukaan toimivaltaisia käsittelemään yksittäisiä valituksia ja riita-asioita, tai iii) sitoutuvat tekemään yhteistyötä EU:n tietosuojaviranomaisten tai niiden valtuuttamien edustajien kanssa.
- b. Tarkoitus on, että tämä luettelo on esimerkinomainen eikä rajoittava. Yksityisellä sektorilla voidaan kehittää muita täytäntöönpanomekanismeja, kunhan ne täyttävät muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen ja täydentävien periaatteiden vaatimukset. On huomattava, että muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen vaatimukset täydentävät vaatimusta, jonka mukaan itsesääntelytoimien on oltava täytäntöönpanokelpoisia liittovaltion kauppakomissiossa annetun lain 5 §:n (15 U.S.C. 45 §), jossa kielletään sopimattomat ja vilpilliset toimet, 49 U.S.C. 41712 §:n, jossa kielletään liikenteenharjoittajaa tai lipunvälittäjää harjoittamasta sopimatonta tai vilpillistä menettelyä lentoliikenteessä tai lentokuljetusten myynnissä, tai muun tällaiset toimet kieltävän lain tai asetuksen nojalla.
- c. Jotta varmistettaisiin, että organisaatiot noudattavat EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa antamia sitoumuksia, ja jotta tuettaisiin ohjelman hallinnointia, organisaatioiden ja riippumattomia muutoksenhakumekanismeja hallinnoivien elinten on kauppaministeriön pyynnöstä annettava tietoja, jotka liittyvät EU:n ja Yhdysvaltojen tietosuojakehykseen. Lisäksi organisaatioiden on vastattava viivytystä valituksiin, jotka tietosuojaviranomaiset ovat toimittaneet kauppaministeriön välityksellä ja joilla pyritään selvittämään, ovatko organisaatiot noudattaneet järjestelyn periaatteita. Vastauksessa olisi käsiteltävä valituksen aiheellisuutta ja – jos valitus todetaan aiheelliseksi – sitä, miten organisaatio aikoo korjata ongelman. Kauppaministeriö huolehtii saamiensa tietojen luottamuksellisuudesta Yhdysvaltojen lainsäädännön mukaisesti.

d. Muutoksenhakumenettelyt

- i. Henkilöitä olisi kannustettava esittämään mahdolliset valituksensa ensiksi asianomaisille organisaatioille ennen asioiden viemistä riippumattomien muutoksenhakumekanismien käsiteltäväksi. Organisaatioiden on vastattava 45 päivän kuluessa valituksen vastaanottamisesta. Se, onko muutoksenhakumekanismi riippumaton, on tosiasiakysymys, joka voidaan osoittaa erityisesti puolueettomuudella, kokoonpanon ja rahoituksen läpinäkyvyydellä sekä aiemmilla hyvillä tuloksilla. Kuten muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteissa edellytetään, muutoksenhaun on oltava henkilöiden helposti käytettävissä ja maksutonta. Riippumattomien riitojenratkaisuelinten olisi tutkittava kaikki valitukset paitsi ne, jotka ovat ilmeisen perusteettomia. Tämä ei estä sitä, että riippumaton riitojenratkaisuelin, joka on vastuussa muutoksenhakumekanismista, asettaa ehtoja valitusten tutkimiselle, mutta näiden ehtojen on oltava läpinäkyviä ja perusteltuja. Siten on esimerkiksi mahdollista jättää tutkimatta valitus, joka ei kuulu ohjelman soveltamisalaan tai jonka tutkiminen kuuluu jollekin toiselle foorumille. Ehdoilla ei kuitenkaan pitäisi heikentää organisaation sitoumusta tutkia asianmukaiset valitukset. Lisäksi muutoksenhakumekanismi hallinnoivien elinten olisi annettava henkilöille täydelliset ja helposti saatavilla olevat tiedot siitä, miten riitojenratkaisumenettely etenee sen jälkeen, kun valitus on tehty. Näiden tietojen tulisi sisältää ilmoitus mekanismin yksityisyydensuojakäytännöistä järjestelyn periaatteiden mukaisesti. Jotta valitusten käsittelyyn sovellettavaa menettelyä voitaisiin helpottaa, muutoksenhakumekanismi hallinnoivien elinten olisi tehtävä yhteistyötä välineiden, kuten vakioomutoisten valituslomakkeiden, laatimiseksi.
- ii. Riippumattomia muutoksenhakumekanismi hallinnoivien elinten on sisällytettävä julkisille verkkosivuilleen tietoja EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteista sekä palveluista, joita ne sen puitteissa tuottavat. Näiden tietojen tulee sisältää 1) tiedot järjestelyn vaatimuksista, joiden mukaan on järjestettävä riippumaton muutoksenhakumekanismi, tai linkki tällaisiin vaatimuksiin, 2) linkki kauppaministeriön tietosuojakehystä käsittelevälle verkkosivulle, 3) tieto siitä, että elimen EU:n ja Yhdysvaltojen tietosuojakehyksen yhteydessä tuottamat riitojenratkaisupalvelut ovat henkilöille maksuttomia, 4) kuvaus siitä, kuinka järjestelyn periaatteisiin liittyvä valitus voidaan jättää käsiteltäväksi, 5) aikataulu, jonka mukaisesti järjestelyn periaatteisiin liittyvä valitus käsitellään, ja 6) kuvaus siitä, millaiset korjaavat toimet ovat mahdollisia.
- iii. Riippumattomia muutoksenhakumekanismi hallinnoivien elinten on julkaistava vuosittain kertomus, jossa esitetään niiden riitojenratkaisupalveluja koskevat tilastot yhdistettyjen lukujen avulla. Vuosikertomuksen tulee sisältää 1) kertomusvuoden aikana saatujen järjestelyn periaatteisiin liittyvien valitusten yhteismäärä, 2) saatujen valitusten lajit, 3) riitojenratkaisuun liittyvät laatutoumenpiteet, kuten valitusten käsittelyajan pituus, ja 4) valitusten tulokset, erityisesti määräytyjen oikeussuojakeinojen tai seuraamusten määrät ja lajit.
- iv. Kuten liitteessä I esitetään, henkilöiden käytettävissä on välimiesmenettely sellaisten vaateiden osalta, jotka ovat jääneet vaille ratkaisua. Välimiesmenettelyn avulla voidaan saada vastaus kysymykseen, onko järjestelyyn osallistuva organisaatio rikkonut järjestelyyn perustuvia velvoitteitaan kyseisen henkilön osalta ja onko kyseinen rikkominen edelleen täysin tai osittain korjaamatta. Välimiesmenettelyä voidaan käyttää ainoastaan tähän tarkoitukseen. Välimiesmenettelyä ei voida käyttää esimerkiksi asioissa, jotka liittyvät järjestelyn periaatteista⁽¹⁵⁾ myönnettäviin poikkeuksiin tai EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman suojan riittävyttä koskeviin väitteisiin. Välimiesmenettelyssä EU:n ja Yhdysvaltojen tietosuojakehyksen paneelilla, joka koostuu yhdestä tai kolmesta välimiehestä sen mukaan kuin osapuolet sopivat, on toimivalta määrätä yksilökohtaisesta, ei-rahallisesta kompensatiosta, joka on tarpeen järjestelyn periaatteiden noudattamatta jättämisen korjaamiseksi ja joka koskee ainoastaan kyseistä henkilöä. Tällaisia kompensatioita ovat henkilön mahdollisuus tutustua tietoihinsa sekä hänen tietojensa korjaaminen, poistaminen tai palauttaminen. Henkilöt ja järjestelyyn osallistuvat organisaatiot voivat hakea Yhdysvaltojen lainsäädännön nojalla annettuun välimiespaneelin päätökseen muutosta tuomioistuimessa ja vaatia sen täytäntöönpanoa tuomioistuimessa välimiesmenettelystä annetun liittovaltion lain (Federal Arbitration Act) nojalla.

e. Korjaavat toimenpiteet ja seuraamukset

- i. Riippumattoman riitojenratkaisuelimen määräämillä korjaavilla toimenpiteillä olisi saatava aikaan seuraavaa: organisaatio peruuttaa tai korjaa järjestelyn periaatteiden noudattamatta jättämisen vaikutukset siinä määrin kuin mahdollista, organisaation tietojenkäsittely on vastaisuudessa periaatteiden mukaista ja valituksen esittänyt henkilöä koskevien tietojen käsittely lakkaa soveltuvin osin. Seuraamusten on oltava riittävän ankaria sen varmistamiseksi, että organisaatio noudattaa järjestelyn periaatteita. Kun mahdollisia seuraamuksia on useampia ja niiden ankaruus vaihtelee, riitojenratkaisuelin voi määrätä sopivan seuraamuksen, jonka ankaruus vastaa rikkomisen vakavuutta. Seuraamukseksi olisi tietyissä olosuhteissa

⁽¹⁵⁾ Periaatteet, yleiskatsaus, 5 kohta.

määrättävä sekä se, että järjestelyn periaatteiden noudattamatta jättäminen julkaistaan, että se, että tiedot hävitetään.⁽¹⁶⁾ Muita seuraamuksia voivat olla merkin käyttöoikeuden keskeyttäminen tai peruuttaminen, järjestelyn periaatteiden noudattamatta jättämisestä henkilölle aiheutuneen vahingon korvaaminen ja kielto määräys. Yksityisellä sektorilla toimivien, riitojenratkaisusta tai itsesääntelystä vastaavien riippumattomien elinten on ilmoitettava tapauksen mukaan tuomioistuimelle tai asiassa toimivaltaiselle valtiolliselle elimelle sekä kauppaministeriölle sellaiset tapaukset, joissa osallistuva organisaatio ei noudata niiden päätöksiä.

f. Liittovaltion kauppakomission toiminta

- i. Liittovaltion kauppakomissio on sitoutunut asettamaan tarkastelussaan etusijalle tapaukset, jotka se on vastaanottanut i) yksityisyyden suojan itsesääntelystä vastaavilta elimiltä ja muilta riippumattomilta riitojenratkaisuelimiltä, ii) EU:n jäsenvaltioilta ja iii) kauppaministeriöltä. Tällöin tarkoituksena on selvittää, onko rikottu liittovaltion kauppakomissiosta annetun lain 5 §:ää, jossa kielletään sopimattomat ja vilpilliset toimet tai käytännöt kaupankäynnissä. Jos liittovaltion kauppakomissiolla on johtopäätöksensä mukaan aiheutta uskoa, että 5 §:ää on rikottu, se voi ratkaista asian hakemalla hallinnollista kielto määräystä (*cease and desist order*), jolla estetään kyseiset toimet, tai nostamalla kanteen liittovaltion piirioikeudessa (*federal district court*). Jos piirioikeus hyväksyy kanteen, sillä on vastaava vaikutus kuin kielto määräyksellä. Lain rikkomisessa on kyse totuudenvastaisista väitteistä, joiden mukaan organisaatiot noudattavat järjestelyn periaatteita tai osallistuvat EU:n ja Yhdysvaltojen tietosuojakehykseen, vaikka ne eivät enää ole tietosuojakehyksen osallistujaluettelossa tai eivät ole koskaan toimittaneet omaa varmennustaan kauppaministeriölle. Liittovaltion kauppakomissio voi hakea siviilioikeudellista seuraamusta hallinnollisen kielto määräyksen rikkomisesta sekä nostaa siviili- tai rikoskanteen liittovaltion tuomioistuimen päätöksen noudattamatta jättämisen vuoksi. Liittovaltion kauppakomissio ilmoittaa kauppaministeriölle kaikista tällaisista toimistaan. Kauppaministeriö kehottaa muita valtiollisia elimiä ilmoittamaan sille, mitkä ovat lopulliset johtopäätökset oikeudenkäynneissä tai muissa menettelyissä, jotka koskevat järjestelyn periaatteiden noudattamista.

g. Järjestelyn periaatteiden jatkuva noudattamatta jättäminen

- i. Jos organisaatio jättää jatkuvasti noudattamatta järjestelyn periaatteita, se menettää oikeutensa EU:n ja Yhdysvaltojen tietosuojakehyksen etuihin. Kauppaministeriö poistaa tietosuojakehyksen osallistujaluettelosta organisaatiot, jotka ovat jatkuvasti jättäneet noudattamatta järjestelyn periaatteita, ja niiden on palautettava tai hävitettävä henkilötiedot, jotka ne ovat vastaanottaneet EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa.
- ii. Periaatteiden noudattamatta jättäminen on jatkuva, jos organisaatio, joka on toimittanut kauppaministeriölle oman varmennuksen, kieltäytyy noudattamasta yksityisyyden suojan itsesääntelystä vastaavan elimen, riippumattoman riitojenratkaisuelimen tai valtiollisen elimen lopullista päätöstä tai jos tällainen elin, kauppaministeriö mukaan lukien, on todennut organisaation toistuvasti rikkoneen järjestelmän periaatteita siinä määrin, että sen oma ilmoitus periaatteiden noudattamisesta ei enää ole uskottava. Tapauksissa, joissa rikkomisen toteaa muu elin kuin kauppaministeriö, organisaation on viivytyksettä ilmoitettava asiasta kauppaministeriölle. Ilmoitusvelvoitteen laiminlyöminen on kanneperuste väärää lausuntoja koskevan Yhdysvaltojen lain nojalla (*False Statements Act*, 18 U.S.C. § 1001). Se, että organisaatio poistetaan yksityissektorilla toimivasta yksityisyyden suojan itsesääntelyä koskevasta ohjelmasta tai riippumattomasta riitojenratkaisumekanismista, ei merkitse sitä, että organisaatio vapautuu velvollisuudesta noudattaa järjestelyn periaatteita, mutta se merkitsee sitä, että organisaation katsotaan jatkuvasti jättävän noudattamatta järjestelyn periaatteita.
- iii. Kauppaministeriö poistaa organisaation tietosuojakehyksen osallistujaluettelosta sellaisen ilmoituksen seurauksena, jonka mukaan organisaatio jättää jatkuvasti noudattamatta järjestelyn periaatteita, tulipa ilmoitus organisaatiolta itseltään, yksityisyyden suojan itsesääntelyä harjoittavalta elimeltä tai muulta riippumattomalta riitojenratkaisuelimeltä tai valtiolliselta elimeltä. Organisaatiolle annetaan kuitenkin 30 päivän määräaika, jonka aikana sillä on tilaisuus antaa vastaus.⁽¹⁷⁾ Kauppaministeriön ylläpitämästä tietosuojakehyksen osallistujaluettelosta käyvät näin ollen selvästi ilmi organisaatiot, jotka ovat oikeutettuja EU:n ja Yhdysvaltojen tietosuojakehyksen etuihin, ja organisaatiot, jotka eivät enää ole oikeutettuja kyseisiin etuihin.
- iv. Jos organisaatio hakee osallistumisoikeutta itsesääntelyelimessä voidakseen uudestaan osallistua EU:n ja Yhdysvaltojen tietosuojakehykseen, sen on toimitettava kyseiselle elimelle täydelliset tiedot aiemmasta osallistumisestaan EU:n ja Yhdysvaltojen tietosuojakehykseen.

⁽¹⁶⁾ Riippumattomat riitojenratkaisuelimet voivat harkita, missä tapauksissa seuraamuksia käytetään. Asianomaisten tietojen arkaluonteisuus on yksi niistä tekijöistä, jotka on otettava huomioon päätettäessä, vaaditaanko tietojen hävittämistä. Huomioon on otettava myös se, onko organisaatio kerätessään, käyttäessään tai luovuttaessaan tietoja rikkonut järjestelyn periaatteita räikeästi.

⁽¹⁷⁾ Kauppaministeriö ilmoittaa ilmoituksessa määräajan, joka on joka tapauksessa alle 30 päivää ja jonka kuluessa organisaation on vastattava ilmoitukseen.

12. Valintaperiaate – tietojen poistamisen ajoitus

- a. Valintaperiaatteen tarkoituksena on yleisesti ottaen varmistaa, että henkilötietoja käytetään ja luovutetaan tavalla, joka vastaa rekisteröidyn odotuksia ja valintoja. Sen mukaan rekisteröidyn on voitava milloin tahansa kieltää häntä itseään koskevien tietojen käyttäminen suoramarkkinointiin. Tällöin on kuitenkin noudatettava organisaation asettamia kohtuullisia aikarajoja, jotka antavat organisaatiolle riittävästi aikaa kiellon täytäntöönpanoon. Organisaatio voi myös vaatia saada riittävästi tietoja voidakseen varmistua tietojenkäsittelyn kieltämistä vaativan henkilöllisyydestä. Yhdysvalloissa tämän vaihtoehdon voi valita käyttämällä keskitettyä kielto-ohjelmaa. Joka tapauksessa henkilölle on tarjottava helposti käytettävissä oleva ja kohtuuhintainen menettely, jonka avulla hän voi käyttää tätä oikeuttaan.
- b. Organisaatio saa vastaavasti käyttää tietoa tiettyihin suoramarkkinointitarkoituksiin sellaisissa tapauksissa, joissa on käytännössä mahdotonta antaa henkilölle etukäteen mahdollisuutta kieltää tietojen käyttö, jos organisaatio tarjoaa hänelle samassa yhteydessä (ja pyynnöstä milloin tahansa) mahdollisuuden kieltää (ilman henkilölle koituvia kuluja) suoramarkkinoinnin kyseisestä hetkestä eteenpäin ja jos organisaatio noudattaa henkilön toivomusta.

13. Matkustustiedot

- a. Lentomatkustajien varaus- ja muita matkustustietoja, kuten kanta-asiakas- ja hotellivaraustietoja, sekä erityistarpeita, esimerkiksi uskonnon mukaisia aterioita tai fyysistä apua, koskevia tietoja voi siirtää EU:n ulkopuolella sijaitseville organisaatioille monissa eri olosuhteissa. Yleisen tietosuojasetuksen mukaan henkilötietoja voidaan tietosuojan tason riittävyttä koskevan päätöksen puuttuessa siirtää kolmanteen maahan, jos yleisen tietosuojasetuksen 46 artiklan mukainen riittävä tietosuojan taso taataan, tai erityistilanteissa, jos jokin yleisen tietosuojasetuksen 49 artiklassa säädetyistä edellytyksistä täyttyy (esimerkiksi jos rekisteröity on antanut nimenomaisen suostumuksensa siirtoon). EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvat yhdysvaltalaiset organisaatiot antavat riittävän henkilötietojen suojan ja saavat siten ottaa vastaan EU:sta siirrettyjä tietoja yleisen tietosuojasetuksen 45 artiklan nojalla ilman, että niiden täytyy ottaa käyttöön yleisen tietosuojasetuksen 46 artiklan mukaista siirtovälinettä tai täyttää asetuksen 49 artiklassa säädetyjä edellytyksiä. Koska EU:n ja Yhdysvaltojen tietosuojakehyksessä on arkaluonteista tietoa koskevia erityissääntöjä, tällaisia tietoja (joita on kerättävä esimerkiksi asiakkaan tarvitessa fyysistä apua) saa sisältyä järjestelyyn osallistuville organisaatioille siirrettäviin tietoihin. Tietoja siirtävän organisaation on kaikissa tapauksissa kuitenkin noudatettava sen EU:n jäsenvaltion lakia, jossa se toimii. Kyseisen valtion lainsäädännössä saattaa olla muun muassa arkaluonteisten tietojen käsittelyä koskevia erityissääntöjä.

14. Farmaseuttiset tuotteet ja lääkevalmisteet

- a. EU:n jäsenvaltioiden lainsäädännön ja järjestelyn periaatteiden soveltaminen
 - i. EU:n jäsenvaltioiden lainsäädäntöä sovelletaan henkilötietojen keruuseen ja kaikkeen tietojenkäsittelyyn, joka toteutetaan ennen tietojen siirtämistä Yhdysvaltoihin. Järjestelyn periaatteita sovelletaan, kun tiedot on siirretty Yhdysvaltoihin. Farmaseuttiseen tutkimukseen ja muihin tarkoituksiin käytettävien tietojen henkilöviittaukset olisi tarvittaessa anonymisoitava.
- b. Tulevaisuudessa tehtävä tieteellinen tutkimus
 - i. Farmaseuttisissa ja lääkeaineita koskevissa tutkimuksissa saadut henkilötiedot ovat usein arvokkaita tulevaisuudessa tehtävälle tieteelliselle tutkimukselle. Jos tiettyä tutkimusta varten kerättyjä henkilötietoja siirretään yhdysvaltalaiselle organisaatiolle, joka osallistuu EU:n ja Yhdysvaltojen tietosuojakehykseen, organisaatio voi käyttää tietoja toisessa, uudessa tutkimuksessa, jos ilmoitus- ja valintaperiaatetta on noudatettu ensimmäisen tutkimuksen yhteydessä. Annettavassa ilmoituksessa on kerrottava kaikista tiedon tulevista käyttötarkoituksista, esimerkiksi toistuvasta seurannasta, kyseistä tutkimusta sivuavista tutkimuksista ja markkinoinnista.

- ii. Ymmärrettävästi tiedon kaikkia tulevia käyttötarkoituksia ei pystytä täsmentämään, koska uusi tutkimus voi saada alkunsa uudesta näkökulmasta alkuperäiseen tietoon, lääketieteellisistä löydöistä ja edistysaskeleista tai kehityksestä kansanterveyden tai sääntelyn alalla. Tarvittaessa ilmoitukseen olisi siksi sisällytettävä maininta siitä, että henkilötietoja saatetaan käyttää farmaseuttisissa ja lääkeaineita koskeissa tutkimuksissa, joista ei tällä hetkellä vielä tiedetä. Jos tällainen käyttötarkoitus ei ole yhteensopiva sen tutkimuksen yleistarkoituksen kanssa, jonka vuoksi henkilötiedot on alun perin kerätty tai johon kyseinen henkilö on myöhemmin antanut suostumuksensa, häneltä on saatava uusi suostumus.
- c. Vetäytyminen kliinisestä kokeesta
- i. Koehenkilö voi milloin tahansa vetäytyä kliinisestä kokeesta, tai häntä voidaan pyytää tekemään näin. Kaikkia tätä ennen kerättyjä henkilötietoja saadaan silti käsitellä muiden kliinisessä kokeessa kerättyjen tietojen ohella, jos tästä on selkeästi ilmoitettu kyseiselle henkilölle siinä vaiheessa, kun hän on suostunut osallistumaan kokeeseen.
- d. Tietojen siirtäminen sääntelyä ja valvontaa varten
- i. Lääkkeitä ja lääkintälaitteita valmistavat yritykset saavat toimittaa EU:ssa tehdyissä kliinisissä kokeissa saatuja henkilötietoja yhdysvaltalaisille valvontaviranomaisille sääntely- ja valvontatarkoituksiin. Samanlaisia siirtoja saa tehdä muille tahoille kuin sääntelyviranomaisille, kuten yrityksen muille toimipaikoille ja muille tutkijoille, ilmoitus- ja valintaperiaatteen mukaisesti.
- e. Sokkotutkimukset
- i. Objektiivisuuden takaamiseksi osallistujat ja usein tutkijatkaan eivät monissa kliinisissä kokeissa saa tietää, mitä hoitoa kullekin henkilölle annetaan. Hoitotiedon antaminen vaarantaisi tutkimuksen ja sen tulosten validiteetin. Tällaisten kliinisten kokeiden eli sokkotutkimusten aikana osallistujille ei tarvitse antaa tietoja heidän hoidostaan, jos rajoituksesta on ilmoitettu siinä vaiheessa, kun kyseinen henkilö on päättänyt osallistua tutkimukseen, ja jos tietojen antaminen vaarantaisi tutkimuksen luotettavuuden.
 - ii. Osallistuminen tutkimukseen näillä edellytyksillä on riittävä osoitus siitä, että kyseinen henkilö luopuu oikeudestaan tiedonsaantiin. Kun tutkimus on saatettu päätökseen ja tulokset on analysoitu, siihen osallistuneilla on oltava oikeus halutessaan saada itseään koskevat tiedot. Tietoja olisi pyydettävä ensisijaisesti lääkäriltä tai muulta terveydenhoitohenkilökuntaan kuululta, joka on hoitanut kyseistä henkilöä tutkimuksen aikana, taikka tutkimuksen teettäneeltä organisaatiolta.
- f. Tuotteen turvallisuuden ja tehon seuranta
- i. Lääkkeitä ja lääkintälaitteita valmistavan yrityksen ei tarvitse soveltaa ilmoitusvelvollisuuteen, valintamahdollisuuteen, tietojen edelleen siirtoa koskevaan vastuuvollisuuteen eikä tiedonsaantiin liittyviä järjestelyn periaatteita toteuttaessaan seurantaa, joka koskee tuotteiden turvallisuutta ja tehokkuutta, jos periaatteiden noudattaminen estää noudattamasta viranomaisvaatimuksia. Tämä koskee myös haittatapahtumia koskevia ilmoituksia ja tiettyjä lääkkeitä tai lääkinnällisiä laitteita käyttävien potilaiden/henkilöiden jäljittämistä. Tämä koskee raportteja, joita esimerkiksi terveydenhoitopalvelujen tarjoajat antavat lääkkeitä ja lääkintälaitteita valmistaville yrityksille, samoin kuin raportteja, joita lääkkeitä ja lääkintälaitteita valmistavat yritykset antavat viranomaisille, kuten elintarvike- ja lääkevirastolle (Food and Drug Administration).
- g. Avainkoodatut tiedot
- i. Tutkimuksen johtaja salaa poikkeuksetta henkilötiedot tutkimuksen alussa antamalla niille ainutkertaiset avainkoodit, jottei rekisteröityjen henkilöllisyys paljastuisi. Tutkimuksia teettävät lääkealan yritykset eivät saa tietää koodien avaimia. Avaimet ovat tiedossa vain tutkijalla, jotta hän voi erityistapauksessa (esimerkiksi tarvittaessa lääketieteellistä jatkohoitoa) tunnistaa, kenestä on kyse. Periaatteet koskisivat EU:sta Yhdysvaltoihin siirrettyjä tietoja, jotka on koodattu tällä tavoin ja jotka ovat EU:n lainsäädännössä tarkoitettuja EU:n henkilötietoja.

15. Julkisten rekistereiden tiedot ja yleisesti saatavilla olevat tiedot

- a. Organisaation on sovellettava yleisesti saatavilla oleviin henkilötietoihin tietojen turvallisuutta ja eheyttä ja käyttötarkoituksen rajoittamista koskevaa periaatetta sekä muutoksenhaku-, täytäntöönpano- ja vastuuperiaatetta. Kyseisiä periaatteita sovelletaan myös henkilötietoihin, jotka on kerätty julkisista rekistereistä. Nämä rekisterit ovat eri hallinnon tasoja edustavien viranomaisten ylläpitämiä rekistereitä, jotka ovat suurelle yleisölle avoimia.
- b. Ilmoitusvelvollisuutta, valintamahdollisuutta ja tietojen edelleen siirtoon liittyvää vastuuvollisuutta koskevia periaatteita ei ole tarpeen soveltaa julkisista rekistereistä saatuu tietoon, jos tätä tietoa ei ole yhdistetty ei-julkiseen rekisteritietoon ja jos toimivaltaisen viranomaisen vahvistamia rekisterin käytön ehtoja noudatetaan. Ilmoitusvelvollisuutta, valintamahdollisuutta ja tietojen edelleen siirtoon liittyvää vastuuvollisuutta koskevia periaatteita ei ole yleensä tarpeen soveltaa myöskään yleisesti saatavilla olevaan tietoon, ellei eurooppalainen siirtäjä ilmoita, että kyseistä tietoa koskevien rajoitusten vuoksi organisaation on sovellettava kyseisiä periaatteita aikomaansa käyttötarkoitukseen. Organisaatio ei ole vastuussa siitä, miten julkaistusta aineistosta saatua tietoa käytetään.
- c. Jos todetaan, että organisaatio on tarkoituksellisesti julkaissut henkilötietoja järjestelyn periaatteiden vastaisesti, jotta se tai muut voisivat hyötyä tässä selostetuista poikkeuksista, organisaatio menettää tietosuojakehyksen edut.
- d. Tiedonsaantiperiaatetta ei tarvitse soveltaa julkiseen rekisteritietoon, jos siihen ei ole yhdistetty muuta henkilötietoa (yhdistämiseksi ei katsota pienten tietomäärien käyttöä julkisen rekisteritiedon luettelointiin tai järjestämiseen), mutta kaikkia toimivaltaisen viranomaisen vahvistamia rekisterin käytön ehtoja on tällöin kuitenkin noudatettava. Sen sijaan kun julkisten rekisterien sisältämää tietoa yhdistetään näihin rekistereihin kuulumattomiin tietoihin (muuhun kuin edellä mainittuun tietoon), organisaation on sallittava tiedonsaanti edellyttäen, ettei kyseiseen tietoon sovelleta muita sallittuja poikkeuksia.
- e. Tietoa, joka jo on yleisesti saatavilla, koskee sama sääntö kuin julkisista rekistereistä saatua tietoa. Tiedonsaantiperiaatetta ei tarvitse soveltaa, jos yleisesti saatavilla olevaa tietoa ei ole yhdistetty tietoon, joka ei ole yleisesti saatavilla. Yleisesti saatavilla olevia tietoja myyvät organisaatiot voivat periä tiedonhausta normaalisti perimänsä maksun. Henkilöt voivat vaihtoehtoisesti pyytää tiedot suoraan organisaatiolta, joka alun perin keräsi ne yhteen.

16. Viranomaisten pääsy tietoihin

- a. Lisätäkseen läpinäkyvyyttä sellaisten laillisten pyyntöjen osalta, jotka koskevat viranomaisten pääsyä henkilötietoihin, järjestelyyn osallistuvat organisaatiot voivat vapaaehtoisesti julkaista säännöllisiä avoimuusraportteja, joissa kerrotaan, kuinka monta henkilötietopyyntöä viranomaiset ovat niille lainvalvonnan ja kansallisen turvallisuuden vuoksi esittäneet. Raporttien julkaisemisen on kuitenkin oltava sovellettavien lakien mukaista.
 - b. Tietoja, jotka järjestelyyn osallistuvat organisaatiot ovat julkaisseet näissä raporteissa, voidaan hyödyntää yhdessä niiden tietojen kanssa, jotka tiedusteluyhteisö on julkaissut, sekä yhdessä muiden tietojen kanssa tehtäessä EU:n ja Yhdysvaltojen tietosuojakehyksen toiminnan määräaikaista yhteistä tarkastelua periaatteiden mukaisesti.
 - c. Se, että ilmoitusperiaatteen a kohdan xii alakohdan mukaista ilmoitusta ei ole tehty, ei poista eikä heikennä organisaation mahdollisuutta vastata mihin tahansa lailliseen pyyntöön.
-

LIITE I: VÄLIMIESMENETTELTYÄ KOSKEVA MALLI

Liitteessä I esitetään ehdot, joiden mukaisesti EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvat organisaatiot ovat velvollisia osallistumaan välimiesmenettelyyn muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti. Sitovaa välitysmahdollisuutta, jota jäljempänä selostetaan, sovelletaan vaateisiin, jotka koskevat EU:n ja Yhdysvaltojen tietosuojakehyksen soveltamisalaan kuuluvia tietoja ja jotka ovat jääneet vaille ratkaisua. Tämän vaihtoehdon tarkoituksena on tarjota nopea, riippumaton ja oikeudenmukainen mekanismi ratkaisun saamiseksi kaikkiin sellaisiin väitettyihin järjestelyn periaatteiden rikkomistapauksiin, joita ei ole kyetty ratkaisemaan muilla mahdollisilla tietosuojakehyksen mekanismeilla.

A. Soveltamisala

Välimiesmenettely on henkilön käytettävissä sellaisten vaateiden osalta, jotka ovat jääneet vaille ratkaisua. Välimiesmenettelyn avulla voidaan saada vastaus kysymykseen, onko järjestelyyn osallistuva organisaatio rikkonut järjestelyn velvoitteita kyseisen henkilön osalta ja onko kyseinen rikkominen edelleen täysin tai osittain korjaamatta. Välimiesmenettelyä voidaan käyttää ainoastaan tähän tarkoitukseen. Välimiesmenettelyä ei voida käyttää esimerkiksi asioissa, jotka liittyvät järjestelyn periaatteista⁽¹⁾ myönnettäviin poikkeuksiin tai EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman suojan riittävyttä koskeviin väitteisiin.

B. Korjaavat toimenpiteet, jotka voidaan määrätä

Välimiesmenettelyssä EU:n ja Yhdysvaltojen tietosuojakehyksen paneelilla, joka koostuu yhdestä tai kolmesta välimiehestä sen mukaan kuin osapuolet sopivat, on toimivalta määrätä yksilökohtaisesta, ei-rahallisesta kompensatiosta, joka on tarpeen järjestelyn periaatteiden noudattamatta jättämisen korjaamiseksi ja joka koskee ainoastaan kyseistä henkilöä. Tällaisia kompensatioita ovat henkilön mahdollisuus tutustua tietoihinsa sekä hänen tietojensa korjaaminen, poistaminen tai palauttaminen. EU:n ja Yhdysvaltojen tietosuojakehyksen paneelilla ei ole toimivaltuuksia määrätä muita korjaavia toimenpiteitä. Kun tietosuojakehyksen paneeli harkitsee, mitä korjaavia toimenpiteitä se määrää, sen on otettava huomioon muut korjaavat toimenpiteet, joita on jo määrätty muissa EU:n ja Yhdysvaltojen tietosuojakehyksen mekanismeissa. Vahingonkorvauksia, kustannusten korvauksia, palkkioita tai muita korjaavia toimenpiteitä ei voida määrätä. Kumpikin osapuoli vastaa omista asianajopalkkioistaan.

C. Toimet, jotka on tehtävä ennen välimiesmenettelyä

Henkilön, joka on päättänyt turvautua välimiesmenettelyyn, on ennen menettelyn vireillepanoa 1) otettava väitetty järjestelyn periaatteiden rikkominen esille suoraan organisaation kanssa ja annettava organisaatiolle tilaisuus ratkaista asia aikataulussa, joka selostetaan riitojenratkaisua ja täytäntöönpanoa koskevan täydentävän periaatteen d kohdan i alakohdassa, 2) hyödynnettävä järjestelyn periaatteiden mukaista riippumatonta muutoksenhakumekanismia, josta ei aiheudu kuluja henkilölle, sekä 3) otettava asia henkilön tietosuojaviranomaisen välityksellä esille kauppaministeriön kanssa ja annettava kauppaministeriölle tilaisuus ratkaista asia parhaansa mukaan aikataulussa, joka selostetaan kauppaministeriön kansainvälisen kaupan osaston kirjeessä. Tästä ei aiheudu kuluja henkilölle.

Välimiesmenettelyä ei voida käyttää, jos asia, joka koskee samaa henkilön väittämää järjestelyn periaatteiden rikkomista, 1) on aiemmin ollut sitovan välimiesmenettelyn kohteena, 2) on ratkaistu tuomioistuimen lopullisella päätöksellä sellaisen asian käsittelyn yhteydessä, jonka asianosainen henkilö on ollut, tai 3) on aiemmin ratkaistu osapuolten välisellä sopimuksella. Tätä vaihtoehtoa ei myöskään voida käyttää, jos 1) tietosuojaviranomaisella on tietosuojaviranomaisten tehtävää koskevan täydentävän periaatteen tai henkilöstötietoja koskevan täydentävän periaatteen mukainen toimivalta tai 2) se on toimivaltainen ratkaisemaan väitettyä rikkomista koskevan asian suoraan organisaation kanssa. Se, että tietosuojaviranomaisella on toimivalta ratkaista asia EU:ssa toimivan rekisterinpitäjän osalta, ei yksinään estä turvautumista välimiesmenettelyyn samassa asiassa sellaista muuta oikeussubjektia vastaan, jota kohtaan tietosuojaviranomaisella ei ole toimivaltaa.

D. Päätösten sitova luonne

Henkilön päätös turvautua sitovaan välimiesmenettelyyn on täysin vapaaehtoinen. Välimiespaneelin päätökset sitovat kaikkia menettelyn asianosaisia. Kun välitysmenettelyyn on turvauduttu, henkilö luopuu mahdollisuudesta hakea saman väitetyn rikkomisen nojalla hyvitystä toisella foorumilla. Jos ei-rahallinen kompensatio ei kuitenkaan täysin riitä korjaamaan väitettyä rikkomista, henkilön turvautuminen välimiesmenettelyyn ei estä häntä esittämästä normaaliin tapaan vahingonkorvausvaadetta tuomioistuimessa.

⁽¹⁾ Periaatteet, yleiskatsaus, 5 kohta.

E. Asian siirtäminen tuomioistuimeen ja täytäntöönpano

Henkilöt ja järjestelyyn osallistuvat organisaatiot voivat hakea muutosta Yhdysvaltojen lainsäädännön mukaisesti annettuun välimiespaneelin päätökseen tuomioistuimessa ja vaatia sen täytäntöönpanoa tuomioistuimessa välimiesmenettelystä annetun liittovaltion lain (Federal Arbitration Act) ⁽²⁾ nojalla. Asia on pantava vireille siinä liittovaltion piirituomioistuimessa, jonka alueelliseen toimivaltaan järjestelyyn osallistuvan organisaation ensisijainen liiketoimipaikka kuuluu.

Välimiesmenettelyllä on tarkoitus ratkaista yksittäisiä riita-asioita, eikä välimiesoikeuden päätöksiä ole tarkoitettu vakuuttaviksi ja sitoviksi ennakkopäätöksiksi muita osapuolia koskevissa asioissa, esimerkiksi tulevista välimiesmenettelyissä tai EU:n ja Yhdysvaltojen tuomioistuimissa käsiteltävissä asioissa tai liittovaltion kauppakomission menettelyissä.

F. Välimiespaneeli

Asianosaisten on valittava välimiehet EU:n ja Yhdysvaltojentietosuoja-kehityksen paneeliin luettelosta, jota käsitellään jäljempänä.

Kauppaministeriö ja komissio laativat sovellettavan lainsäädännön mukaisesti luettelon vähintään kymmenestä välimiehestä, jotka valitaan riippumattomuuden, nuhteettomuuden ja asiantuntemuksen perusteella. Tässä menettelyssä välimiehiin sovelletaan seuraavaa:

- 1) Välimiehet ovat luettelossa kolmen vuoden ajan, jollei poikkeuksellisista olosuhteista muuta johdu tai jollei heitä poisteta perustellusta syystä, ja kauppaministeriö voi jatkaa toimikautta vielä kolmella vuodella ilmoittamalla asiasta etukäteen komissiolle.
- 2) Välimiehet eivät saa ottaa ohjeita menettelyn asianosaisilta, järjestelyyn osallistuvalla organisaatiolta, Yhdysvalloilta, EU:lta, EU:n jäsenvaltiolta, muulta viranomaiselta, valtiolliselta elimeltä tai lainvalvontaviranomaiselta, eivätkä he saa olla etuyhteydessä mainittuihin tahoihin.
- 3) Välimiehillä on oltava lupa juristin ammatin harjoittamiseen Yhdysvalloissa, ja heidän on oltava yksityisyyden suoja koskevan Yhdysvaltojen lainsäädännön asiantuntijoita, joilla on asiantuntemusta myös EU:n tietosuojalainsäädännöstä.

⁽²⁾ Välimiesmenettelystä annetun liittovaltion lain 2 luvussa säädetään, että välityssopimus tai välitystuomio, joka liittyy sopimukseen perustuvaan tai muuhun kuin sopimukseen perustuvaan, kaupalliseksi katsottavaan oikeussuhteeseen, kuten liiketapahtumaan, sopimukseen tai yhteisymmärrykseen siten kuin ne kuvataan välimiesmenettelystä annetun liittovaltion lain 2 §:ssä, kuuluu New Yorkin yleissopimuksen soveltamisalaan (ulkomaisten välitystuomioiden tunnustamisesta ja täytäntöönpanosta New Yorkissa 10 päivänä kesäkuuta 1958 tehty yleissopimus, 21 U.S.T. 2519, T.I.A.S. No. 6997) (välimiesmenettelystä annettu liittovaltion laki, 9 U.S.C. 202 §. Välimiesmenettelystä annetussa liittovaltion laissa säädetään edelleen, että jos oikeussuhde on pelkästään Yhdysvaltojen kansalaisten välinen, oikeussuhteesta johtuvan välityssopimuksen tai välitystuomion ei katsota kuuluvan New Yorkin yleissopimuksen soveltamisalaan, ellei oikeussuhde koske ulkomailla sijaitsevaa omaisuutta, ellei se edellytä toimintaa tai täytäntöönpanoa ulkomailla tai ellei sillä ole jokin muu mielekäs yhteys yhteen tai useampaan vieraaseen valtioon. Samoin 2 luvussa todetaan, että välimiesmenettelyn asianosainen voi pyytää mitä tahansa tämän luvun mukaan toimivaltaista tuomioistuinta antamaan määräyksen, jossa vahvistetaan välitystuomio välimiesmenettelyn toista asianosaista vastaan. Tuomioistuin vahvistaa välitystuomion, jollei se tote, että välitystuomioon liittyy jokin New Yorkin yleissopimuksen mukainen tunnustamisen tai täytäntöönpanon hylkäys- tai lykkäysperuste. Ks. 207 §. Lisäksi 2 luvussa säädetään, että Yhdysvalloissa liittovaltion piirituomioistuimilla [...] on toimivalta tutkia ensimmäisenä oikeusasteena [...] New Yorkin yleissopimuksen nojalla vireille pannut kanteet ja oikeudenkäynnit riippumatta riidan raha-arvosta. Ks. 203 §.

Lisäksi 2 luvussa säädetään, että lain 1 lukua sovelletaan tämän luvun nojalla vireille pantuihin kanteisiin ja oikeudenkäynteihin, ellei 1 luku ole ristiriidassa tämän luvun tai Yhdysvaltojen ratifioiman New Yorkin yleissopimuksen kanssa. Ks. 208 §. Lain 1 luvussa puolestaan säädetään, että kaupankäyntiin liittyvän liiketapahtuman todisteeksi tehdyssä [...] sopimuksessa oleva kirjallinen määräys, jonka mukaan sopimuksen solmimisen jälkeen kyseisestä sopimuksesta tai liiketoimesta johtuvat riidat tai riidat, jotka syntyvät sen seurauksena, että on kieltäydytty sopimuksen tai liiketoimen täyttämisestä kokonaan tai osittain, ratkaistaan välimiesmenettelyssä, samoin kuin kirjallinen sopimus, jonka mukaan sopimuksesta, liiketoimesta tai mainitun kaltaisesta kieltäytymisestä johtuva olemassa oleva riita ratkaistaan välimiesmenettelyssä, ovat päteviä, peruuttamattomia ja täytäntöönpanokelpoisia, paitsi jos sopimuksen kumoaminen on perusteltua lain tai kohtuuden perusteella. Ks. 2 §. Lisäksi 1 luvussa säädetään, että jokainen välimiesmenettelyn osapuoli voi hakea näin määritellyssä tuomioistuimessa määräystä välitystuomion vahvistamisesta ja että tämän johdosta tuomioistuimen on annettava tällainen määräys, paitsi jos välitystuomio kumotaan tai sitä muutetaan tai korjataan siten kuin välimiesmenettelystä annetun liittovaltion lain 10 ja 11 §:ssä säädetään. Ks. 9 §.

G. Välimiesmenettelyyn sovellettavat säännöt

Kauppaministeriö ja komissio ovat sopineet sovellettavan lainsäädännön mukaisesti välimiesmenettelyä koskevien sääntöjen hyväksymisestä EU:n ja Yhdysvaltojen tietosuojakehyksen paneelin menettelytapasäännöiksi. ⁽³⁾ Jos menettelytapasääntöjä on muutettava, kauppaministeriö ja komissio sopivat kyseisten sääntöjen muuttamisesta tai toisen olemassa olevan, vakiintuneen yhdysvaltalaisen välimiesmenettelysäännösten valitsemisesta tarpeen mukaan. Säännöissä on otettava huomioon seuraavat näkökohdat:

1. Henkilö voi panna vireille sitovan välimiesmenettelyn toimittamalla asiasta ilmoituksen organisaatiolle. Vireillepanon edellytyksenä on, että välimiesmenettelyä edeltävät toimet on tehty. Ilmoitukseen on sisällytettävä yhteenveto toimista, joita on toteutettu C kohdan mukaisesti asian ratkaisemiseksi, kuvaus väitetystä rikkomisesta sekä henkilön valinnan mukaisesti todisteena esitettäviä asiakirjoja ja muuta todistusaineistoa ja/tai vaatimukseen sovellettavaa lakia koskevia näkemyksiä.
2. Laaditaan menettelyt sen varmistamiseksi, että yhteen rikkomiseen, josta henkilö esittää väitteitä, ei sovelleta päällekkäisiä korjaavia toimenpiteitä tai menettelyjä.
3. Menettely liittovaltion kauppakomissiossa voi olla meneillään samaan aikaan kuin välimiesmenettely.
4. Yhdysvaltojen, EU:n, EU:n jäsenvaltion, muun viranomaisen, valtiollisen elimen tai lainvalvontaviranomaisen edustajat eivät saa osallistua välimiesmenettelyyn, jos tietosuojaviranomainen voi EU:n kansalaisen pyynnöstä avustaa ilmoituksen valmistelussa. Tämä avustaminen voi liittyä vain ilmoitukseen, sillä tietosuojaviranomaisella ei ole pääsyä aineistoon, joka koskee menettelyä edeltävää todisteiden hankintaa (discovery) tai välimiesmenettelyä muutoin.
5. Välimiesmenettely tapahtuu Yhdysvalloissa, ja henkilö voi halutessaan osallistua menettelyyn videoneuvottelulaitteiden tai puhelimen välityksellä ilman, että tästä aiheutuu hänelle kustannuksia. Henkilökohtaista osallistumista ei vaadita.
6. Välimiesmenettelyn kieli on englanti, elleivät asianosaiset toisin sovi. Perustellusta pyynnöstä ja ottaen huomioon, onko henkilöllä edustajanaan asianajaja, välimiesmenettelyn istunto voidaan tulkata ja menettelyn aineisto kääntää ilman, että tästä aiheutuu henkilölle kustannuksia, paitsi jos EU:n ja Yhdysvaltojen tietosuojakehyksen paneelin mielestä tästä aiheutuu perusteettomia tai suhteettomia kustannuksia kyseisen yksittäisen menettelyn olosuhteissa.
7. Välimiehille toimitetut aineistot käsitellään luottamuksellisesti, ja niitä käytetään ainoastaan välimiesmenettelyn yhteydessä.
8. Menettelyä edeltävä todisteiden hankinta, joka liittyy tiettyyn henkilöön (individual-specific discovery), voidaan sallia, jos se on tarpeen. Asianosaiset käsittelevät näin saatuja aineistoja luottamuksellisesti ja käyttävät niitä ainoastaan kyseisessä välimiesmenettelyssä.
9. Välimiesmenettely olisi saatava päätökseen 90 päivän kuluessa siitä, kun henkilön ilmoitus on toimitettu organisaatiolle, jollei toisin ole sovittu asianosaisten kesken.

⁽³⁾ Kauppaministeriö on valinnut International Centre for Dispute Resolution -keskuksen, jäljempänä 'ICDR', joka on American Arbitration Association -yhdistyksen, jäljempänä 'AAA', kansainvälinen osasto, jäljempänä yhdessä 'ICDR-AAA', hallinnoimaan välimiesmenettelyjä järjestelyn periaatteiden liitteen I mukaisesti sekä hoitamaan periaatteiden liitteessä I yksilöityä välimiesrahastoa. Kauppaministeriö ja komissio sopivat 15. syyskuuta 2017 välimiesmenettelysäännösten valitsemisesta järjestelyn periaatteiden liitteessä I kuvattujen sitovien välimiesmenettelyjen menettelytapasäännöiksi. Ne sopivat myös välimiesten käytännösäännöistä, jotka ovat kauppaoikeuden alalla toimivien välimiesten yleisesti hyväksytyjen eettisten normien ja järjestelyn periaatteiden liitteen I mukaisia. Kauppaministeriö ja komissio sopivat, että välimiesmenettelyä koskevia sääntöjä ja käytännösääntöjä mukautetaan vastaamaan EU:n ja Yhdysvaltojen tietosuojakehykseen tehtäviä päivityksiä, ja kauppaministeriö tekee päivitykset yhdessä ICDR-AAA:n kanssa.

H. Kustannukset

Välimiesten olisi kohtuullisin toimenpitein pyrittävä minimoimaan välimiesmenettelyyn liittyvät kustannukset ja palkkiot.

Kauppaministeriö aikoo sovellettavan lainsäädännön mukaisesti edistää sellaisen rahaston ylläpitämistä, johon järjestelyyn osallistuvien organisaatioiden on suoritettava maksu. Maksu perustuu osittain organisaation kokoon. Rahastosta katetaan välitysmenettelyjen kustannukset, muun muassa välimiesten palkkiot vahvistettavaan enimmäismäärään saakka. Rahastoa hallinnoi kolmas osapuoli, joka raportoi säännöllisesti kauppaministeriölle rahaston toiminnasta. Kauppaministeriö tekee yhteistyötä kolmannen osapuolen kanssa rahaston toiminnan arvioimiseksi määräajoin. Tällöin arvioidaan esimerkiksi, onko tarvetta mukauttaa rahastoon tehtäviä maksuja ja välimiesten palkkioiden ylärajoja, ja tarkastellaan muun muassa välimiesmenettelyjen lukumäärää, kustannuksia ja kestoja. Tässä yhteydessä katsotaan, että järjestelyyn osallistuville organisaatioille ei pidä asettaa liiallista taloudellista raskautta. Kauppaministeriö ilmoittaa komissiolle tällaisten kolmannen osapuolen kanssa tehtyjen arviointien tuloksista ja toimittaa komissiolle ennakoilmoituksen mahdollisista maksujen määrään tehtävistä muutoksista. Asianajajien palkkiot eivät kuulu tämän säännöksen soveltamisalaan, eikä niitä kateta tämän säännöksen nojalla perustetusta rahastosta.

LIITE II



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

6. heinäkuuta 2023

Didier Reynders
Oikeusasioista vastaava komissaari
Euroopan komissio
Rue de la Loi / Wetstraat 200
1049 Bryssel
Belgia

Arvoisa komissaari Reynders,

Yhdysvaltojen puolesta minulla on kunnia toimittaa ohessa EU:n ja Yhdysvaltojen tietosuojakehystä koskeva asiakirja-aineisto. Yhdessä Yhdysvaltojen signaalitiedustelutoiminnan suojatoimien tehostamista koskevan toimeenpanoasetuksen 14086 (Enhancing Safeguards for United States Signals Intelligence Activities) ja 28 CFR osa 201:n, jolla muutetaan oikeusministeriön asetuksia tietosuojaa käsittelevän muutoksenhakutuomioistuimen (Data Protection Review Court) perustamiseksi, kanssa aineisto kertoo tärkeistä ja yksityiskohtaisista neuvotteluista yksityisyyden ja kansalaisoikeuksien suojan vahvistamiseksi. Neuvottelut ovat johtaneet uusiin takeisiin, joilla varmistetaan, että Yhdysvaltojen signaalitiedustelutoiminta on tarpeellista ja oikeasuhteista määriteltyjen kansallisten turvallisuustavoitteiden saavuttamiseksi, sekä Euroopan unionin (EU) kansalaisille tarkoitettuun uuteen mekanismiin, jonka avulla he voivat hakea muutosta, jos he katsovat, että signaalitiedustelutoimet kohdistuvat heihin laittomasti. Yhdessä nämä seikat varmistavat EU:n henkilötietojen yksityisyyden. EU:n ja Yhdysvaltojen tietosuojakehys luo perustan osallistavalle ja kilpailukykyiselle digitaaliselle. Molempien osapuolten tulisi olla ylpeitä kehukseen tehdyistä parannuksista, joilla tehostetaan yksityisyyden suojaa kaikkialla maailmassa. Tämä aineisto sekä toimeenpanoasetus, määräykset ja muut tiedot, jotka ovat saatavilla julkisista lähteistä, tarjoavat komissiolle erittäin vankan perustan, jonka pohjalta se voi tehdä uuden tietosuojan riittävyttä koskevan päätöksensä. ⁽¹⁾

Liitteenä ovat seuraavat aineistot:

- EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteet, mukaan lukien täydentävät periaatteet, jäljempänä yhdessä 'järjestelyn periaatteet', ja periaatteiden liite I (eli liite, jossa esitetään ehdot, joiden mukaisesti tietosuojakehykseen osallistuvat organisaatiot ovat velvollisia osallistumaan välimiesmenettelyyn tiettyjen sellaisten järjestelyn periaatteiden soveltamisalaan kuuluvia henkilötietoja koskevien vaateiden osalta, jotka ovat jääneet vaille ratkaisua);
- tietosuojakehysohjelmaa hallinnoivan kauppaministeriön kansainvälisen kaupan osaston (International Trade Administration) kirje, jossa kuvataan ministeriömme sitoumuksia sen varmistamiseen, että EU:n ja Yhdysvaltojen tietosuojakehys toimii tehokkaasti;
- liittovaltion kauppakomission (Federal Trade Commission) kirje, jossa selostetaan, kuinka kauppakomissio valvoo järjestelyn periaatteiden noudattamista;
- liikenneministeriön kirje, jossa selostetaan, kuinka liikenneministeriö valvoo järjestelyn periaatteiden noudattamista;
- kansallisen tiedusteluviraston johtajan (Office of the Director of National Intelligence) laatima kirje suojatoimista ja rajoituksista, joita sovelletaan Yhdysvaltojen kansallisiin turvallisuusviranomaisiin; sekä
- sekä oikeusministeriön kirje suojatoimista ja rajoituksista, jotka koskevat Yhdysvaltojen viranomaisten pääsyä tietoihin lainvalvonnan ja yleisen edun nimissä.

⁽¹⁾ Jos komission päätöstä, joka koskee EU:n ja Yhdysvaltojen tietosuojakehyksen tietosuojan riittävyttä, sovelletaan myös Islantiin, Liechtensteiniin ja Norjaan, EU:n ja Yhdysvaltojen tietosuojakehyspaketti kattaa sekä Euroopan unionin että nämä kolme maata.

EU:n ja Yhdysvaltojen tietosuojakehysaineisto julkaistaan kokonaisuudessaan kauppaministeriön tietosuojakehystä käsittelevällä verkkosivustolla, ja järjestelyn periaatteet ja periaatteiden liite I tulevat voimaan päivänä, jona Euroopan komission päätös tietosuojan riittävydestä tulee voimaan.

Voitte olla vakuuttuneita siitä, että Yhdysvallat ottaa nämä sitoumukset vakavasti. Odotamme innokkaasti yhteistyötä kanssanne pannessamme EU:n ja Yhdysvaltojen tietosuojakehystä täytäntöön ja käynnistäessämme yhdessä tämän prosessin seuraavan vaiheen.

Kunnioittavasti



Gina M. RAIMONDO

LIITE III



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

12. joulukuuta 2022

Didier Reynders
Oikeus-, kuluttaja- ja tasa-arvoasioista vastaava komissaari
Euroopan komissio
Rue de la Loi / Wetstraat 200
1049 Bryssel
Belgia

Arvoisa komissaari Reynders,

kansainvälisen kaupan osaston puolesta olen iloinen voidessani tehdä selkoa sitoumuksista, joita kauppaministeriö on tehnyt taatakseen henkilötietojen suojan hallintonsa toimesta ja tietosuojakehysohjelman valvonnan. Se, että EU:n ja Yhdysvaltojen tietosuojakehys on nyt valmis, on merkittävä virstanpylväs yksityisyyden suojalle ja yrityksille Atlantin molemmin puolin. Järjestelyn ansiosta EU:n kansalaiset voivat luottaa siihen, että heidän tietojensa suojataan ja että tietoihinsa liittyvien ongelmien ilmetessä heillä on käytössään oikeussuojakeinoja. Sen ansiosta tuhannet yritykset voivat jatkossakin investoida ja käydä kauppaa Atlantin yli molempien osapuolten talouksien ja kansalaisten eduksi. EU:n ja Yhdysvaltojen tietosuojakehys kertoo vuosia kestäneestä kovasta työstä ja yhteistyöstä Teidän ja Euroopan komissiossa, jäljempänä 'komissio', toimivien kollegoidenne kanssa. Odotamme innolla mahdollisuutta jatkaa työskentelyä komission kanssa sen varmistamiseksi, että tämä yhteinen järjestely toimii vaikuttavasti.

EU:n ja Yhdysvaltojen tietosuojakehys tarjoaa merkittäviä hyötyjä sekä yksityishenkilöille että yrityksille. Ensinnäkin se on merkittävä yksityisyyden suojan kokonaisuus, joka turvaa EU:n kansalaisten Yhdysvaltoihin siirrettäviä tietoja. Järjestely edellyttää siihen osallistuvilta yhdysvaltalaisilta organisaatioilta seuraavaa: niiden on laadittava järjestelyn kanssa sopusoinnussa olevat tietosuojaperiaatteet, niiden on annettava julkinen sitoumus EU:n ja Yhdysvaltojen tietosuojakehysten periaatteiden, täydentävät periaatteet mukaan lukien, jäljempänä yhdessä 'järjestelyn periaatteet', sekä periaatteiden liitteen I (eli liitteen, jossa esitetään ehdot, joiden mukaisesti EU:n ja Yhdysvaltojen tietosuojakehukseen osallistuvat organisaatiot ovat velvollisia osallistumaan välimiesmenettelyyn tiettyjen sellaisten järjestelyn periaatteiden soveltamisalaan kuuluvia henkilötietoja koskevien vaateiden osalta, jotka ovat jääneet vaille ratkaisua) noudattamisesta, niin että sitoumuksesta tulee Yhdysvaltojen lain mukaan täytäntöönpanokelpoinen⁽¹⁾, niiden on annettava vuosittain ministeriölle varmennus, jonka mukaan ne edelleen noudattavat järjestelyn periaatteita, niiden on järjestettävä EU:n kansalaisille maksuton ja riippumaton riitojenratkaisumekanismi ja niiden on oltava järjestelyn periaatteissa luetellun Yhdysvaltojen lakisääteisen elimen (esimerkiksi liittovaltion kauppakomission (Federal Trade Commission, FTC) ja liikenneministeriön (Department of Transportation, DOT)) tai jonkin järjestelyn periaatteiden tulevassa liitteessä luetellun Yhdysvaltojen lakisääteisen elimen tutkintaan ja lainvalvontaan liittyvän toimivallan alaisia. Vaikka organisaation päätös

⁽¹⁾ Organisaatioiden, jotka ovat antaneet oman varmennuksen EU:n ja Yhdysvaltojen tietosuojakehysten periaatteiden noudattamisesta ja haluavat hyödyntää tietosuojakehukseen osallistumisen etuja, on noudatettava "EU:n ja Yhdysvaltojen tietosuojakehysten periaatteita". Tämä sitoumus noudattaa "EU:n ja Yhdysvaltojen tietosuojakehysten periaatteita" on otettava huomioon tällaisten kehysten osallistuvien organisaatioiden tietosuojaperiaatteissa mahdollisimman pian, joka tapauksessa viimeistään kolmen kuukauden kuluttua "EU:n ja Yhdysvaltojen tietosuojakehysten periaatteiden" voimaantulosta. (Ks. omaa varmennusta koskevan täydentävän periaatteen e kohta.)

antaa oma varmennus on vapaaehtoinen, sääntönä on, että kun organisaatio on julkisesti sitoutunut noudattamaan EU:n ja Yhdysvaltojen tietosuojakehystä, sitoumus on Yhdysvaltojen lainsäädännön mukaan täytäntöönpanokelpoinen ja täytäntöönpanon toimittaa joko liittovaltion kauppakomissio, liikenneministeriö tai muu Yhdysvaltojen lakisääteinen elin sen mukaan, mikä viranomaisena on toimivaltainen järjestelyyn osallistuvan organisaation suhteen. Toiseksi EU:n ja Yhdysvaltojen tietosuojakehysten ansiosta yritykset Yhdysvalloissa, mukaan lukien Yhdysvalloissa toimivat eurooppalaisten yritysten tytäryhtiöt, voivat saada henkilötietoja Euroopan unionista. Näin helpotetaan tietovirtoja, jotka tukevat transatlanttista kauppaa. Yhdysvaltojen ja Euroopan unionin tietovirrat ovat maailman suurimmat ja muodostavat perustan Yhdysvaltojen ja EU:n 7,1 biljoonan Yhdysvaltain dollarin arvoiselle taloudelliselle suhteelle, joka luo edellytykset miljoonille työpaikoille Atlantin molemmiin puoliin. Yrityksiä, joille transatlanttiset tietovirrat ovat tärkeitä, on kaikilla teollisuuden aloilla, ja niiden joukossa on suuria Fortune 500 -yrityksiä sekä monia pieniä ja keskisuuria yrityksiä. Transatlanttisten tietovirtojen avulla yhdysvaltalaiset organisaatiot voivat käsitellä tietoja, joita ne tarvitsevat voidakseen tarjota tavaroita, palveluja ja työtilaisuuksia EU:n kansalaisille.

Kauppaministeriö on sitoutunut tekemään tiivistä ja tuottavaa yhteistyötä EU-kollegojen kanssa, jotta tietosuojakehysohjelmaa voidaan hallinnoida ja valvoa tehokkaasti. Tästä sitoumuksesta ovat osoituksena toimet, joilla kauppaministeriö kehittää ja parantaa jatkuvasti erilaisia resursseja organisaatioiden avuksi omaan varmennukseen liittyvässä prosessissa, verkkosivuston luominen kohdennetun tiedon tarjoamiseksi sidosryhmille, yhteistyö komission ja Euroopan tietosuojaviranomaisten kanssa sellaisten ohjeiden laatimiseksi, joilla selvennetään EU:n ja Yhdysvaltojen tietosuojakehysten tärkeitä osatekijöitä, tiedottaminen organisaatioiden tietosuojavaroitteiden ymmärtämisen edistämiseksi sekä organisaatioiden valvonta ja seuranta ohjelman vaatimusten noudattamisessa.

Jatkuva yhteistyömme arvostettujen EU:n viranomaisten kanssa antaa kauppaministeriölle mahdollisuuden varmistaa, että EU:n ja Yhdysvaltojen tietosuojakehys toimii käytännössä. Yhdysvaltojen hallitus on tehnyt pitkään komission kanssa yhteistyötä, jolla on pyritty saamaan aikaan yhteisiä tietosuojaperiaatteita. Yhteistyöllä on kurottu umpeen eroja oikeudellisissa toimintaperiaatteissa ja edistetty samalla kauppaa ja talouskasvua Euroopan unionissa ja Yhdysvalloissa. Uskomme, että EU:n ja Yhdysvaltojen tietosuojakehys, joka on esimerkki tästä yhteistyöstä, antaa komissiolle mahdollisuuden tehdä uuden tietosuojan riittävyttä koskevan päätöksen, jonka nojalla organisaatiot voivat käyttää EU:n ja Yhdysvaltojen tietosuojakehystä siirtääkseen henkilötietoja Euroopan unionista Yhdysvaltoihin EU:n lainsäädännön mukaisesti.

Kauppaministeriön toteuttama tietosuojakehysohjelman hallinto ja valvonta

Kauppaministeriö on vahvasti sitoutunut tietosuojakehysohjelman tehokkaaseen hallinnointiin ja valvontaan ja ryhtyy asianmukaisiin toimiin ja osoittaa asianmukaiset resurssit tämän tuloksen varmistamiseksi. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa, jäljempänä 'tietosuojakehysten osallistujaluettelo', yhdysvaltalaisista organisaatioista, jotka ovat toimittaneet oman varmennuksensa kauppaministeriölle ja vahvistaneet sitoumuksensa järjestelyn periaatteiden noudattamisesta. Kauppaministeriö päivittää luetteloa järjestelyyn osallistuvien organisaatioiden vuosittain tekemien uudelleenvarmennusten perusteella ja poistamalla siitä organisaatiot, jotka vetäytyvät siitä vapaaehtoisesti, jotka jättävät tekemättä kauppaministeriön menettelytapojen mukaisen vuotuisen uudelleenvarmennuksen tai joiden havaitaan jatkuvasti rikkovan järjestelyn periaatteita. Kauppaministeriö myös pitää yllä ja yleisön saatavilla virallista luetteloa sellaisista yhdysvaltalaisista organisaatioista, jotka on poistettu tietosuojakehysten osallistujaluettelosta, ja mainitsee aina perusteen, jonka vuoksi organisaatio on poistettu luettelosta. Mainittu virallinen luettelo pysyy yleisön saatavilla kauppaministeriön tietosuojakehystä käsittelevällä verkkosivustolla. Tietosuojakehystä käsittelevällä verkkosivustolla on näkyvästi esillä oleva selostus, jossa ilmoitetaan, että jokaisen tietosuojakehysten osallistujaluettelosta poistetun organisaation on lakattava esittämästä väitteitä, joiden mukaan se osallistuu EU:n ja Yhdysvaltojen tietosuojakehukseen ja noudattaa sitä ja että se voi vastaanottaa henkilötietoja EU:n ja Yhdysvaltojen tietosuojakehysten nojalla. Tällaisen organisaation on kuitenkin jatkettava järjestelyn periaatteiden soveltamista henkilötietoihin, jotka se on saanut sinä aikana, kun se on osallistunut EU:n ja Yhdysvaltojen tietosuojakehukseen, niin kauan kuin se säilyttää kyseisiä tietoja. Kauppaministeriö sitoutuu täyttääkseen yleisen ja jatkuvan sitoumuksensa tietosuojakehysohjelman tehokkaaseen hallinnointiin ja valvontaan toteuttamaan erityisesti seuraavat toimet:

Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät:

- Ennen kuin kauppaministeriö vahvistaa organisaation ensimmäisen oman varmennuksen tai vuotuisen uudelleenvarmennuksen, jäljempänä yhdessä 'oma varmennus', ja lisää organisaation tietosuojakehysten osallistujaluetteloon tai pitää sen siinä, se varmistaa, että organisaatio on vähintään noudattanut vaatimuksia, jotka on vahvistettu omaa varmennusta koskevassa täydentävässä periaatteessa sen osalta, mitä tietoja organisaation on toimitettava antaessaan kauppaministeriölle oman varmennuksen, ja toimitanut asianmukaisena ajankohtana tietosuojaperiaatteet, joissa tiedotetaan henkilöille kaikista 13:sta ilmoitusvelvollisuutta koskevassa periaatteessa vahvistetusta osatekijästä. Kauppaministeriö tarkastaa, että organisaatio on

- yksilöinyt organisaation, joka antaa oman varmennuksen, sekä kaikki oman varmennuksen antavan organisaation Yhdysvalloissa toimivat yksiköt tai tytäryhtiöt, jotka myös noudattavat järjestelyn periaatteita ja jotka organisaatio haluaa oman varmennuksensa kattavan,
- toimittanut vaaditut yhteystietonsa (esimerkiksi niiden oman varmennuksen antavaan organisaatioon kuuluvien tiettyjen henkilöiden ja/tai yhteyspisteiden yhteystiedot, jotka vastaavat valitusten, tiedonsaantipyyntöjen ja kaikkien muiden EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvien kysymysten käsittelystä,
- kuvaillut tarkoitukset, joihin organisaation on tarkoitus kerätä ja käyttää Euroopan unionista saatuja henkilötietoja,
- ilmoittanut, mitä henkilötietoja Euroopan unionista aiotaan siirtää EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla ja mitkä henkilötiedot organisaation oma varmennus näin ollen kattaa,
- jos organisaatiolla on julkiset verkkosivut, toimittanut verkko-osoitteen, jossa sen tietosuojaperiaatteet ovat saatavilla, tai jos julkisia verkkosivuja ei ole, toimittanut kauppaministeriölle kopion tietosuojaperiaatteistaan ja tiedon siitä, missä henkilöt, joita asia koskee (toisin sanoen kohteena oleva henkilöstö, jos on kyse henkilöstöä koskevasta tietosuojaperiaatteista, tai yleisö, jos kyseessä ovat muut kuin henkilöstöä koskevat tietosuojaperiaatteet) voivat tutustua kyseisiin periaatteisiin,
- sisällyttänyt tietosuojaperiaatteisiinsa asianmukaisena ajankohtana (eli ensin vain varmennuksen antamisen yhteydessä toimitetussa tietosuojaperiaatteiden luonnoksessa, jos kyse on ensimmäisestä omasta varmennuksesta, muussa tapauksessa lopullisessa ja tarvittaessa julkaistuissa tietosuojaperiaatteissa) ilmoituksen siitä, että se noudattaa järjestelyn periaatteita, ja linkin kauppaministeriön tietosuojakehystä koskevalle verkkosivustolle tai sivuston verkko-osoitteen (esimerkiksi kotisivu tai tietosuojakehyksen osallistujaluettelon verkkosivu),
- sisällyttänyt tietosuojaperiaatteisiinsa asianmukaisena ajankohtana kaikki 12 muuta ilmoitusvelvollisuutta koskevassa periaatteessa vahvistettua osatekijää (esimerkiksi mahdollisuuden saada asia tietyin edellytyksin sitovan välimiesmenettelyn käsiteltäväksi, vaatimus, jonka mukaan henkilötietoja on luovutettava lainmukaisen, julkisen viranomaisen esittämän pyynnön nojalla muun muassa kansalliseen turvallisuuteen tai lainvalvontaan liittyvien vaatimusten täyttämiseksi ja organisaation vastuu tapauksissa, joissa tietoja on siirretty edelleen kolmansille osapuolille),
- yksilöinyt, millä erityisellä lakisäateisellä elimellä (joka mainitaan järjestelyn periaatteissa tai niiden tulevassa liitteessä) on toimivalta käsitellä organisaatiosta tehtyt valitukset, jotka koskevat mahdollisia sopimattomia tai vilpillisiä käytäntöjä ja yksityisyyttä koskevien lakien ja asetusten rikkomista
- ilmoittanut kaikki yksityisyydensuojaohjelmat, joihin organisaatio osallistuu,
- ilmoittanut, onko menetelmä (eli seurantamenettely, joka sen on otettava käyttöön) sen varmistamiseksi, että organisaatio noudattaa periaatteita, 'oma varmennus' (eli sisäinen tarkastus) vai 'ulkopuolisen tahon tekemä arviointi' (eli kolmannen osapuolen suorittama tarkastus), ja jos organisaatio ilmoitti menetelmän olevan ulkopuolisen tahon tekemä arviointi, myös yksilöinyt kolmannen osapuolen, joka on tehnyt kyseisen arvioinnin,
- yksilöinyt asianmukaisen riippumattoman muutoksenhakumekanismin, joka on käytettävissä periaatteiden nojalla tehtyjen valitusten käsittelyä varten ja johon henkilöt, joita asia koskee, voivat asianmukaisesti turvautua maksutta.
- Jos organisaatio on valinnut yksityisen sektorin vaihtoehtoisen riidanratkaisuelimen tarjoaman riippumattoman muutoksenhakumekanismin, se on sisällyttänyt tietosuojaperiaatteisiinsa linkin sellaisen riippumattoman muutoksenhakumekanismin verkkosivustoon tai valituslomakkeeseen, joka voi tutkia ratkaisematta olevat järjestelyn periaatteiden nojalla tehtyt valitukset.
- Jos organisaation edellytetään tekevän (Euroopan unionista työsuhteen yhteydessä siirrettyjen henkilöstötietojen osalta) tai se on päättänyt tehdä yhteistyötä asianmukaisten tietosuojaviranomaisten kanssa järjestelyn periaatteiden nojalla tehtyjen valitusten tutkinnassa ja ratkaisemisessa, se on ilmoittanut sitoutuneensa tällaiseen yhteistyöhön tietosuojaviranomaisten kanssa ja niiden asiaan liittyvien neuvojen noudattamiseen toteuttaakseen erityisiä toimia järjestelyn periaatteiden noudattamiseksi.

- Kauppaministeriö tarkastaa myös, että organisaation oma varmennus on yhdenmukainen sen tietosuojaperiaatteiden kanssa. Jos oman varmennuksen antava organisaatio haluaa sen kattavan jonkin Yhdysvalloissa toimivista yksiköistään tai tytäryhtiöistään, joilla on erilliset tietosuojaperiaatteet, kauppaministeriö tarkastaa myös tällaisten järjestelyn kattamien yksikköjen tai tytäryhtiöiden tietosuojaperiaatteet varmistaakseen, että ne sisältävät kaikki ilmoitusperiaatteissa vaaditut tiedot.
- Kauppaministeriö tekee yhteistyötä lakisääteiden elinten (esimerkiksi liittovaltion kauppakomission ja liikenneministeriön) kanssa varmistaakseen, että organisaatiot ovat niiden omassa varmennuksessa yksilöidyn lakisäätöelimen toimivallan alaisia, jos kauppaministeriöllä on syytä epäillä, etteivät organisaatiot ole kyseisen toimivallan alaisia.
- Kauppaministeriö tekee yhteistyötä vaihtoehtoisten riitojenratkaisuelinten kanssa sen varmistamiseksi, että organisaatiot on aktiivisesti rekisteröity niiden omassa varmennuksessa yksilöityyn riippumattomaan muutoksenhakumekanismiin. Se myös tekee yhteistyötä kyseisten elinten kanssa sen varmistamiseksi, että organisaatiot on aktiivisesti rekisteröity niiden omassa varmennuksessa yksilöityä, jonkin ulkopuolisen tahon suorittamaa arviointia varten, jos kyseiset elimet tarjoavat kummankintyyppisiä palveluja.
- Kauppaministeriö tekee yhteistyötä sen kauppaministeriön valitseman kolmannen osapuolen kanssa, joka toimii tietosuojaviranomaisen paneelimaksun (eli vuosimaksun, jonka tarkoitus on kattaa tietosuojaviranomaisen paneelin toimintakustannukset) yhteydessä kerättyjen varojen säilyttäjänä. Näin kauppaministeriö tarkastaa, ovatko tietosuojaviranomaisen riippumattomaksi muutoksenhakumekanismiksi määrittäneet organisaatiot maksaneet kyseisen vuoden maksun.
- Kauppaministeriö tekee yhteistyötä sen kolmannen osapuolen kanssa, jonka kauppaministeriö on valinnut hallinnoimaan välimiesmenettelyjä järjestelyn periaatteiden liitteen I mukaisesti ja hallinnoimaan periaatteiden liitteessä I yksilöityä välimiesrahastoa. Näin kauppaministeriö tarkastaa, että organisaatiot ovat maksaneet osuutensa välimiesrahastoon.
- Jos kauppaministeriö havaitsee organisaatioiden omia varmennuksia tarkastellessaan ongelmia, se ilmoittaa organisaatioille, että niiden on puututtava kaikkiin tällaisiin ongelmiin kauppaministeriön asettamassa asianmukaisessa määräajassa ^(?). Kauppaministeriö ilmoittaa organisaatioille myös seuraavat seikat: Jos ne eivät toimi kauppaministeriön asettamien määräaikaisten sisällä tai eivät muuten anna kauppaministeriön menettelytapojen mukaista omaa varmennusta, niiden katsotaan luopuneen omasta varmennuksesta. Mikäli EU:n ja Yhdysvaltojen tietosuojakehykseen osallistumisesta tai sen määräysten noudattamisesta on annettu vääriä tietoja, kauppakomissio, liikenneministeriö tai muu asiaankuuluva valtiollinen elin voi ryhtyä asiassa lainvalvontatoimiin. Kauppaministeriö käyttää tiedottamisessaan organisaatioille niitä yhteydenottokeinoja, jotka organisaatiot ovat kauppaministeriölle ilmoittaneet.

Kauppaministeriö edistää yhteistyötä järjestelyn periaatteisiin liittyviä palveluja tarjoavien vaihtoehtoisten riitojenratkaisuelinten kanssa

- Kauppaministeriö tekee yhteistyötä riippumattomia muutoksenhakumekanismeja, joiden avulla voidaan tutkia ratkaisematta olevat, järjestelyn periaatteiden nojalla tehdyt valitukset, tarjoavien yksityisen sektorin vaihtoehtoisten riidanratkaisuelinten kanssa. Näin kauppaministeriö tarkastaa, että ne täyttävät vähintään riitojenratkaisua ja täytäntöönpanoa koskevassa täydentävässä periaatteessa asetetut vaatimukset. Kauppaministeriö tarkastaa, että organisaatio
- sisällyttää julkisille verkkosivuilleen tietoja EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteista ja sen puitteissa tarjoamistaan palveluista. Tietoihin on sisällyttävä 1) tiedot järjestelyn vaatimuksista, joiden mukaan on järjestettävä riippumaton muutoksenhakumekanismi, tai linkki tällaisiin vaatimuksiin, 2) linkki kauppaministeriön tietosuojakehystä käsittelevälle verkkosivulle, 3) tieto siitä, että elimen EU:n ja Yhdysvaltojen tietosuojakehyksen yhteydessä tuottamat riitojenratkaisupalvelut ovat henkilöille maksuttomia, 4) kuvaus siitä, kuinka järjestelyn periaatteisiin liittyvä valitus voidaan jättää käsiteltäväksi, 5) aikataulu, jonka mukaisesti järjestelyn periaatteisiin liittyvä valitus käsitellään, ja 6) kuvaus siitä, millaiset korjaavat toimet ovat mahdollisia. Kauppaministeriö ilmoittaa elimille hyvissä ajoin olennaisista muutoksista, jotka koskevat kauppaministeriön suorittamaa tietosuojakehysohjelman valvontaa ja hallinnointia, jos tällaiset muutokset ovat välittömiä, niitä on jo tehty ja ne ovat merkityksellisiä sen roolin kannalta, joka elimillä on EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa,

^(?) Esimerkiksi uudelleenvarmennuksen osalta odotetaan, että organisaatiot käsittelevät kaikki tällaiset ongelmat 45 päivän kuluessa, mikäli kauppaministeriö ei ole asettanut toista asianmukaista määräaikaa.

- julkaisee vuosittain kertomuksen, jossa esitetään niiden riitojenratkaisupalveluja koskevat tilastot. Luvut esitetään yhteenlaskettuina kokonaissummina. Tilastojen on sisällettävä 1) kertomusvuoden aikana saatujen järjestelyn periaatteisiin liittyvien valitusten yhteismäärä, 2) saatujen valitusten lajit, 3) riitojenratkaisuun liittyvät laatutoimenpiteet, kuten valitusten käsittelyajan pituus, ja 4) valitusten tulokset, erityisesti määrättyjen oikeussuojakeinojen tai seuraamusten määrät ja lajit. Kauppaministeriö antaa elimille erityisiä täydentäviä ohjeita siitä, mitä tietoja niiden olisi annettava kyseisistä vaatimuksista laadituissa vuosikertomuksissa (esimerkiksi luettelo kriteereistä, jotka valituksen on täytettävä, jotta sitä voidaan pitää vuosikertomuksessa huomioitavana järjestelyn periaatteisiin liittyvänä valituksena), sekä yksilöi muuntotyypiset tiedot, jotka elinten olisi annettava (esimerkiksi jos elin tarjoaa myös järjestelyn periaatteisiin liittyvän tarkastuspalvelun, kuvaus siitä, miten elin välttää kaikki tosiasialliset tai potentiaaliset eturistiriidat tilanteissa, joissa se tarjoaa organisaatiolle sekä tarkastuspalveluja että riidanratkaisupalveluja). Kauppaministeriön antamissa lisäohjeissa täsmennetään myös päivämäärä, johon mennessä elinten vuosikertomukset olisi julkaistava asianomaisen raportointikauden osalta.

Niiden organisaatioiden seuranta, jotka haluavat tulla poistetuiksi tai jotka on poistettu tietosuojakehyksen osallistujaluettelosta

- Jos organisaatio haluaa vetäytyä EU:n ja Yhdysvaltojen tietosuojakehyksestä, kauppaministeriö edellyttää, että organisaatio poistaa kaikista tietosuojaperiaatteistaan kaikki EU:n ja Yhdysvaltojen tietosuojakehystä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuu edelleen tietosuojakehykseen ja että se voi vastaanottaa henkilötietoja tietosuojakehyksen nojalla (ks. kuvaus kauppaministeriön sitoumuksesta etsiä organisaatioita, jotka totuudenvastaisesti väittävät osallistuvansa järjestelyyn). Kauppaministeriö edellyttää myös, että organisaatio täyttää ja toimittaa kauppaministeriölle asianmukaisen kyselyn varmistaakseen
- halunsa vetäytyä,
- mitä organisaatio tekee henkilötiedoille, jotka se sai EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla osallistuessaan EU:n ja Yhdysvaltojen tietosuojakehykseen: a) säilyttää tällaiset tiedot, jatkaa järjestelyn periaatteiden soveltamista tietoihin ja vahvistaa kauppaministeriölle vuosittain sitoumuksensa, jonka mukaan se jatkaa periaatteiden soveltamista tietoihin, b) säilyttää tällaiset tiedot ja antaa tiedoille ”riittävän” suojan muiden hyväksyttyjen keinojen avulla tai c) palauttaa tai hävittää kaikki tällaiset tiedot määrättyyn päivämäärään mennessä, sekä
- kuka organisaation sisällä toimii yhteyspisteenä järjestelyn periaatteisiin liittyvissä kysymyksissä.
- Jos organisaatio valitsi edellä kuvailun vaihtoehdon a, kauppaministeriö edellyttää myös, että organisaatio täyttää ja toimittaa kauppaministeriölle vuosittain järjestelystä vetäytymisensä jälkeen (eli viimeistään vuosi vetäytymisen jälkeen sekä tämän jälkeen aina kerran vuodessa, paitsi jos ja kunnes organisaatio joko antaa tällaisille tiedoille ”riittävän” suojan muiden hyväksyttyjen keinojen avulla tai palauttaa tai hävittää kaikki tällaiset tiedot ja ilmoittaa kauppaministeriölle tästä toimesta) asianmukaisen kyselyn todentaakseen, mitä se on tehnyt näille henkilötiedoille, mitä se tekee kaikille niille henkilötiedoille, joita se edelleen säilyttää, ja kuka organisaation sisällä toimii yhteyspisteenä järjestelyn periaatteisiin liittyvissä kysymyksissä.
- Jos organisaatio on antanut oman varmennuksensa raueta (eli se ei ole tehnyt vuosittaista järjestelyn periaatteiden noudattamista koskevaa uudelleenvarmennusta eikä sitä ole poistettu tietosuojakehyksen osallistujaluettelosta jostakin muusta syystä, kuten vetäytymisen vuoksi), kauppaministeriö ohjaa sen täyttämään ja toimittamaan kauppaministeriölle asianmukaisen kyselyn, jonka avulla tarkastetaan, haluaako se vetäytyä järjestelystä tai tehdä uudelleenvarmennuksen:
- Jos organisaatio haluaa vetäytyä järjestelystä, sen on todennettava, mitä se tekee henkilötiedoille, jotka se sai EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla osallistuessaan EU:n ja Yhdysvaltojen tietosuojakehykseen (ks. edellinen kuvaus siitä, mitä organisaation on todennettava, jos se haluaa vetäytyä järjestelystä).
- Jos organisaatio aikoo antaa uudelleenvarmennuksen, sen on todennettava edelleen, että sinä aikana, kun sen varmennus oli rauenneena, se sovelsi järjestelyn periaatteita EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa saatuihin henkilötietoihin, ja selvitettyä, mitä toimia se aikoo toteuttaa puuttuakseen ongelmiin, jotka ovat viivytäneet uudelleenvarmennuksen tekemistä.

- Jos organisaatio poistetaan tietosuojakehyksen osallistujaluettelosta jostakin seuraavista syistä: a) vetäytyminen EU:n ja Yhdysvaltojen tietosuojakehyksestä, b) järjestelyn periaatteiden noudattamista koskevan vuosittaisen uudelleenvarmennuksen tekemättä jättäminen (eli organisaatio joko aloitti vuotuisen uudelleenvarmennusprosessin mutta ei saattanut sitä päätökseen oikea-aikaisesti tai ei edes aloittanut prosessia) tai c) jatkuva järjestelyn periaatteiden noudattamatta jättäminen, kauppaministeriö lähettää ilmoituksen organisaation omassa varmennuksessa yksilöidylle yhteyshenkilöille. Ilmoituksessa kauppaministeriö yksilöi poistamisen syyn ja selvittää, että organisaation on lakattava esittämästä nimenomaisia tai epäsuoria väitteitä, joiden mukaan se osallistuu EU:n ja Yhdysvaltojen tietosuojakehykseen tai noudattaa sitä ja että se voi vastaanottaa henkilötietoja EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla. Ilmoituksessa, johon voi sisältyä myös muuta sisältöä, joka on mukautettu poistamisen syyhin, ilmoitetaan, että jos organisaatiot antavat virheellistä tietoa osallistumisestaan EU:n ja Yhdysvaltojen tietosuojakehykseen tai sen noudattamisesta esimerkiksi väittämällä osallistuvansa tietosuojakehykseen sen jälkeen, kun ne on poistettu tietosuojakehyksen osallistujaluettelosta, kauppakomissio, liikenneministeriö tai muu asiaankuuluva valtiollinen elin voi ryhtyä asiassa lainvalvontatoimiin.

Tietosuojakehyksen osallistumista koskevien totuudenvastaisten väitteiden havaitseminen ja niihin puuttuminen

- Kun organisaatio a) vetäytyy EU:n ja Yhdysvaltojen tietosuojakehyksestä, b) jättää toimittamatta vuotuisen uudelleenvarmennuksen, jossa se olisi todennut noudattavansa järjestelyn periaatteita (eli organisaatio joko aloitti vuotuisen uudelleenvarmennusprosessin mutta ei saattanut sitä päätökseen ajoissa tai ei edes aloittanut prosessia), c) poistetaan EU:n ja Yhdysvaltojen tietosuojakehyksen osallistujaluettelosta varsinkin "sen jatkuvasti rikottua järjestelyn periaatteita" tai d) ei tee ensimmäistä omaa varmennusta, jossa se toteaa noudattavansa järjestelyn periaatteita (eli se aloitti ensimmäisen oman varmennuksen mutta ei saattanut sitä päätökseen ajoissa), kauppaministeriö tarkastaa jatkuvasti viran puolesta, että organisaatio on poistanut kaikista julkistamistaan tietosuojaperiaateista kaikki EU:n ja Yhdysvaltojen tietosuojakehystä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuu tietosuojakehykseen ja että se voi vastaanottaa henkilötietoja EU:n ja Yhdysvaltojen tietosuojakehyksen nojalla. Mikäli kauppaministeriö havaitsee tällaisia viittauksia, se ilmoittaa organisaatiolle, että jos organisaatio edelleen esittää vääriä tietoja osallistumisestaan EU:n ja Yhdysvaltojen tietosuojakehykseen, kauppaministeriö siirtää tarvittaessa asian toimivaltaisen viraston käsiteltäväksi mahdollisia lainvalvontatoimia varten. Kauppaministeriö käyttää tiedottamisessaan organisaatiolle niitä yhteydenottokeinoja, jotka organisaatio on kauppaministeriölle ilmoittanut, tai tarvittaessa muita sopivia keinoja. Jos organisaatio ei poista viittausta tai kauppaministeriön menettelytapoja noudattaen anna omaa varmennusta siitä, että se noudattaa EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita, kauppaministeriö siirtää asian viran puolesta liittovaltion kauppakomissiolle, liikenneministeriölle tai muulle toimivaltaiselle lainvalvontavirastolle tai ryhtyy muihin asianmukaisiin toimiin varmistaakseen EU:n ja Yhdysvaltojen tietosuojakehyksen varmennusmerkin asianmukaisen käytön.
- Kauppaministeriö tarkkailee muutenkin, esittävätkö organisaatiot totuudenvastaisia väitteitä osallistumisestaan EU:n ja Yhdysvaltojen tietosuojakehykseen ja käyttävätkö ne tietosuojakehyksen varmennusmerkkiä epäasianmukaisesti. Tähän voivat syyllistyä esimerkiksi organisaatiot, jotka toisin kuin edellisessä kohdassa kuvaillut organisaatiot eivät koskaan ole edes aloittaneet omaa varmennusta. Tarkkailua suoritetaan esimerkiksi tekemällä internet-hakuja, joissa etsitään organisaatioiden tietosuojaperiaateista viittauksia EU:n ja Yhdysvaltojen tietosuojakehykseen. Jos kauppaministeriö tällaisia toimia toteuttaessaan havaitsee vääriä tietoja osallistumisesta EU:n ja Yhdysvaltojen tietosuojakehykseen ja tietosuojakehyksen varmennusmerkin epäasianmukaista käyttöä, kauppaministeriö ilmoittaa organisaatiolle, että jos organisaatio edelleen esittää vääriä tietoja osallistumisestaan tietosuojakehykseen, kauppaministeriö siirtää tarvittaessa asian toimivaltaisen viraston käsiteltäväksi mahdollisia lainvalvontatoimia varten. Kauppaministeriö käyttää tiedottamisessaan organisaatiolle niitä yhteydenottokeinoja, jotka organisaatio on mahdollisesti kauppaministeriölle ilmoittanut, tai tarvittaessa muita sopivia keinoja. Jos organisaatio ei poista viittausta tai kauppaministeriön menettelytapoja noudattaen anna omaa varmennusta siitä, että se noudattaa EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita, kauppaministeriö siirtää asian viran puolesta liittovaltion kauppakomissiolle, liikenneministeriölle tai muulle toimivaltaiselle lainvalvontavirastolle tai ryhtyy muihin asianmukaisiin toimiin varmistaakseen EU:n ja Yhdysvaltojen tietosuojakehyksen varmennusmerkin asianmukaisen käytön.
- Kauppaministeriö käsittelee ripeästi saamansa yksilöidyt, aiheelliset valitukset, jotka koskevat totuudenvastaisia väitteitä osallistumisesta EU:n ja Yhdysvaltojen tietosuojakehykseen (esimerkiksi valitukset, jotka on saatu tietosuojaviranomaisilta, yksityisen sektorin vaihtoehtoisten riitojenratkaisuelinten tarjoamista riippumattomista muutoksenhakumettelyistä, rekisteröidyltä, EU:n ja Yhdysvaltojen yrityksiltä ja muuntayppisiltä kolmansilta osapuolilta).
- Kauppaministeriö voi ryhtyä muihin asianmukaisiin korjaaviin toimenpiteisiin. Kauppaministeriölle annetut väärät tiedot ovat kanneperuste vääriä lausuntoja koskevan Yhdysvaltojen lain nojalla (False Statements Act, 18 U.S.C. § 1001).

Kauppaministeriö tarkastelee määräajoin viran puolesta periaatteiden noudattamista ja arvioi tietosuojakehysohjelmaa

- Kauppaministeriö seuraa jatkuvasti, noudattavatko EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvat organisaatiot järjestelyn periaatteita, ja pyrkii näin havaitsemaan kysymyksiä, jotka saattavat edellyttää jatkotoimia. Kauppaministeriö tekee jatkuvasti viran puolesta erityisesti rutiininomaisia tarkastuksia paikan päällä satunnaisesti valituissa EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvissa organisaatioissa sekä tapauskohtaisesti tarkastuksia paikan päällä tietyissä tietosuojakehykseen osallistuvissa organisaatioissa, jos niissä on havaittu mahdollisia vaatimusten noudattamiseen liittyviä puutteita (esimerkiksi sellaisia, joihin kolmas osapuoli on kiinnittänyt kauppaministeriön huomion). Tarkastuksilla pyritään toteamaan, a) ovatko valitusten, tiedonsaantipyyntöjen ja muiden EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvien ongelmien käsittelyyn liittyvät yhteyspisteet käytettävissä, b) ovatko organisaatioiden julkiset tietosuojaperiaatteet tarvittaessa helposti yleisön saatavilla sekä organisaatioiden julkisilla verkkosivustoilla että tietosuojakehyksen osallistujaluettelossa olevan linkin kautta, c) ovatko organisaation tietosuoja-periaatteet edelleen järjestelyn periaatteissa kuvailtujen omaa varmennusta koskevien vaatimusten mukaiset ja d) onko organisaation yksilöimä riippumaton muutoksenhakumekanismi käytettävissä EU:n ja Yhdysvaltojen tietosuoja-kehysten nojalla tehtyjen valitusten käsittelyä varten. Kauppaministeriö seuraa myös aktiivisesti uutisia, jotka antavat luotettavaa näyttöä siitä, etteivät EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvat organisaatiot ole noudattaneet vaatimuksia.
- Osana vaatimustenmukaisuuden arviointia kauppaministeriö edellyttää, että EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuva organisaatio täyttää ja toimittaa kauppaministeriölle yksityiskohtaisen kyselyn, jos a) kauppaministeriö on vastaanottanut organisaatiota koskevia yksilöityjä valituksia, jotka liittyvät järjestelyn periaatteiden noudattamiseen, eivätkä valitukset ole aiheettomia, b) organisaatio ei anna tyydyttävää vastausta EU:n ja Yhdysvaltojen tietosuojakehystä koskevaan kauppaministeriön tietopyyntöön tai c) on uskottavaa näyttöä siitä, että organisaatio ei noudata EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisia sitoumuksiaan. Jos kauppaministeriö on lähettänyt organisaatiolle tällaisen yksityiskohtaisen kyselyn eikä organisaatio vastaa kyselyyn tyydyttävästi, kauppaministeriö ilmoittaa organisaatiolle, että se siirtää tarvittaessa asian toimivaltaisen viraston käsiteltäväksi mahdollisia lainvalvontatoimia varten, jos kauppaministeriö ei saa organisaatiolta oikea-aikaista ja tyydyttävää vastausta. Kauppaministeriö käyttää tiedottamisessaan organisaatiolle niitä yhteydenottokeinoja, jotka organisaatio on kauppaministeriölle ilmoittanut, tai tarvittaessa muita sopivia keinoja. Jos organisaatio ei anna oikea-aikaista ja tyydyttävää vastausta, kauppaministeriö siirtää asian viran puolesta liittovaltion kauppakomissiolle, liikenneministeriölle tai muulle asianmukaiselle lainvalvontavirastolle tai ryhtyy muihin asianmukaisiin toimiin varmistaakseen vaatimusten noudattamisen. Kauppaministeriön on tarvittaessa kuultava toimivaltaista tietosuojaviranomaista periaatteiden noudattamisen tarkastelusta.
- Kauppaministeriö arvioi säännöllisesti tietosuojakehyksen hallintoa ja valvontaa sen varmistamiseksi, että seurannalla, mukaan lukien mahdolliset hakutyökalujen avulla toteutetut seurantatoimet (joilla esimerkiksi tarkistetaan vialliset linkit EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvien organisaatioiden tietosuojaperiaatteisiin), voidaan asianmukaisesti puuttua nykyisiin ongelmiin ja mahdollisesti esiin nouseviin uusiin ongelmiin.

Kauppaministeriö räätälöi tietosuojakehyksen verkkosivuston eri kohdeyleisöille

Kauppaministeriö muotoilee tietosuojakehyksen verkkosivuston niin, että se keskittyy seuraaviin kohdeyleisöihin: EU:n kansalaiset, EU:n yritykset, Yhdysvaltojen yritykset ja tietosuojaviranomaiset. Se, että sivustolle tulee aineistoa, joka on kohdennettu suoraan EU:n kansalaisille ja EU:n yrityksille, palvelee läpinäkyvyyttä monin tavoin. EU:n kansalaisille sivustolla selostetaan selkeästi seuraavat seikat: 1) oikeudet, jotka EU:n kansalaiset saavat EU:n ja Yhdysvaltojen tietosuoja-kehysten ansiosta, 2) muutoksenhakumekanismit, jotka EU:n kansalaisilla on käytössään, jos organisaatio on heidän käsityksensä mukaan rikkonut sitoumustaan noudattaa järjestelyn periaatteita, sekä 3) mistä löytää tietoja, jotka koskevat organisaation EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvää omaa varmennusta. EU:n yritysten on sivuston avulla helpompi tarkistaa, 1) osallistuuko organisaatio EU:n ja Yhdysvaltojen tietosuojakehykseen, 2) minkä tyyppisiä tietoja organisaation EU:n ja Yhdysvaltojen tietosuojakehykseen liittyvä oma varmennus kattaa, 3) millaisia tietosuojaperiaatteita sovelletaan varmennuksen kattamiin tietoihin sekä 4) millä menetelmällä organisaatio varmistaa, että se noudattaa järjestelyn periaatteita. Yhdysvaltojen yrityksille sivustolla selostetaan selkeästi seuraavat seikat: 1) hyödyt, jotka yritykset saavat EU:n ja Yhdysvaltojen tietosuojakehykseen osallistumisesta, 2) miten EU:n ja Yhdysvaltojen tietosuojakehykseen liitytään, miten tehdään uudelleenvarmennus ja miten EU:n ja Yhdysvaltojen tietosuojakehyksestä vetäydytään, sekä 3) miten Yhdysvallat hallinnoi ja valvoo EU:n ja Yhdysvaltojen tietosuojakehystä. Se, että sivustolle tulee aineistoa, joka on kohdennettu suoraan tietosuojaviranomaisille (esimerkiksi tieto kauppaministeriön tietosuojaviranomaisille tarkoitetusta yhteyspisteestä ja linkki järjestelyn periaatteisiin liittyvään sisältöön liittovaltion kauppakomission verkkosivustolla), palvelee sekä yhteistyötä että läpinäkyvyyttä. Kauppaministeriö työskentelee myös tapauskohtaisesti komission ja Euroopan tietosuojaneuvoston kanssa kehittääkseen ajankohtaista lisämateriaalia (esimerkiksi vastauksia usein esitettyihin kysymyksiin) käytettäväksi tietosuojakehyksen verkkosivustolla silloin, kun tällainen tieto helpottaisi tietosuojakehysohjelman tehokasta hallinnointia ja valvontaa.

Kauppaministeriö helpottaa yhteistyötään tietosuojaviranomaisten kanssa

Jotta yhteistyölle tietosuojaviranomaisten kanssa olisi paremmat edellytykset, kauppaministeriö ylläpitää erityistä yhteyspistettä, joka toimii linkkinä tietosuojaviranomaisten suuntaan. Jos tietosuojaviranomainen katsoo, että EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuva organisaatio ei noudata järjestelyn periaatteita eikä esimerkiksi ryhdy toimiin EU:n kansalaisen valituksen johdosta, tietosuojaviranomainen voi ottaa yhteyttä tähän erityiseen yhteyspisteeseen siinä tarkoituksessa, että organisaation toimintaa aletaan tutkia. Kauppaministeriö pyrkii parhaansa mukaan edistämään sitä, että valitukseen saadaan ratkaisu EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvan organisaation kanssa. Kauppaministeriö antaa tietosuojaviranomaiselle selonteon asian edistymisestä 90 päivän kuluessa valituksen vastaanottamisesta. Yhteyspisteelle ilmoitetaan myös organisaatioista, jotka väittävät totuudenvastaisesti osallistuvansa EU:n ja Yhdysvaltojen tietosuojakehykseen. Yhteyspiste pitää kirjaa kaikista valituksista, jotka kauppaministeriö on vastaanottanut tietosuojaviranomaisilta, ja ministeriö antaa myöhemmin selostettavassa yhteisessä tarkastelussa kertomuksen, jossa kunakin vuonna vastaanotettuja valituksia analysoidaan yhtenä kokonaisuutena. Yhteyspiste myös avustaa tietosuojaviranomaisia, jotka etsivät tietoja tietyn organisaation omasta varmennuksesta tai aiemmasta osallistumisesta EU:n ja Yhdysvaltojen tietosuojakehykseen, sekä vastaa tietosuojaviranomaisten tiedusteluihin, jotka koskevat tiettyjen EU:n ja Yhdysvaltojen tietosuojakehyksen vaatimusten täytäntöönpanoa. Kauppaministeriö tekee myös yhteistyötä komission ja tietosuojaneuvoston kanssa tietosuojaviranomaisten paneelin menettelyllisten ja hallinnollisten näkökohtien osalta, mukaan lukien asianmukaisten menettelyjen käyttöönotto tietosuojaviranomaisen paneelimaksun kautta kerättyjen varojen jakamiseksi. Käsityksemme mukaan komissio tekee yhteistyötä kauppaministeriön kanssa helpottaakseen kyseisten menettelyjen yhteydessä mahdollisesti ilmenevien ongelmien ratkaisemista. Lisäksi kauppaministeriö toimittaa tietosuojaviranomaisille EU:n ja Yhdysvaltojen tietosuojakehystä koskevaa materiaalia, jonka tietosuojaviranomaiset voivat sisällyttää omille verkkosivustoilleen ja näin lisätä järjestelyn läpinäkyvyyttä EU:n kansalaisten ja EU:n yritysten näkökulmasta. EU:n ja Yhdysvaltojen tietosuojakehystä ja siihen liittyviä oikeuksia ja velvollisuuksia koskevan tiedon lisääntyessä pitäisi olla helpompaa tunnistaa aiheeseen liittyvät ongelmat sitä mukaa kuin ne syntyvät ja sitten ratkaista ne asianmukaisesti.

Kauppaministeriö täyttää järjestelyn periaatteiden liitteen I mukaiset sitoumuksensa

Kauppaministeriö täyttää järjestelyn periaatteiden liitteen I mukaiset sitoumuksensa. Kauppaministeriö muun muassa ylläpitää luetteloa välimiehistä, jotka on valittu komission kanssa riippumattomuuden, nuhteettomuuden ja asiantuntemuksen perusteella, ja tekee tarvittaessa yhteistyötä sen kolmannen osapuolen kanssa, jonka kauppaministeriö on valinnut hallinnoimaan välimiesmenettelyjä järjestelyn periaatteiden liitteen I mukaisesti ja hallinnoimaan periaatteiden liitteessä I yksilöityä välimiesrahastoa. ⁽³⁾ Kauppaministeriö tekee yhteistyötä kolmannen osapuolen kanssa muun muassa todentaakseen, että kolmas osapuoli ylläpitää verkkosivustoa, joka sisältää ohjeita välimiesmenettelystä. Ohjeisiin kuuluvat muun muassa seuraavat tiedot: 1) miten käynnistetään menettely ja toimitetaan asiakirjoja, 2) kauppaministeriön ylläpitämä luettelo välimiehistä ja miten luettelosta valitaan välimiehet, 3) kauppaministeriön ja komission hyväksymät välimiesmenettelyyn sovellettavat säännöt ja välimiesten käytäntösäännöt ⁽⁴⁾ sekä 4) välimiesten palkkioiden kerääminen ja maksaminen. Lisäksi kauppaministeriö tekee yhteistyötä kolmannen osapuolen kanssa rahaston toiminnan arvioimiseksi määräajoin. Tällöin arvioidaan esimerkiksi, onko tarvetta mukauttaa välimiesrahastoon tehtäviä maksuja ja välimiesten palkkioiden ylärajoja (eli enimmäismääriä), ja tarkastellaan muun muassa välimiesmenettelyjen lukumäärää, kustannuksia ja kestoa. Tässä yhteydessä katsotaan, että EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvilla organisaatioilla ei pidä asettaa liiallista taloudellista rasitusta. Kauppaministeriö ilmoittaa komissiolle tällaisten kolmannen osapuolen kanssa tehtyjen arviointien tuloksista ja toimittaa komissiolle ennakkoilmoituksen mahdollisista maksujen määrään tehtävistä muutoksista.

EU:n ja Yhdysvaltojen tietosuojakehyksen toimintaa koskevat yhteiskatsaukset

Kauppaministeriö ja tarvittaessa muut virastot järjestävät säännöllisiä kokouksia komission, kiinnostuneiden tietosuojaviranomaisten ja tietosuojaneuvoston asianmukaisten edustajien kanssa. Kokouksissa kauppaministeriö selostaa EU:n ja Yhdysvaltojen tietosuojakehyksen toimintaa. Kokouksissa keskustellaan ajankohtaisista kysymyksistä, jotka liittyvät tietosuojakehysohjelman toimintaan, täytäntöönpanoon ja valvontaan. Kokouksiin voi tarvittaessa sisältyä keskustelua asiaan liittyvistä aiheista, kuten muista tiedonsiirtomekanismeista, jotka hyötyvät EU:n ja Yhdysvaltojen tietosuojakehyksestä.

⁽³⁾ Kauppaministeriö valitsi International Centre for Dispute Resolution -keskuksen (ICDR), joka on American Arbitration Association -yhdistyksen (AAA) kansainvälinen osasto, jäljempänä yhdessä 'ICDR-AAA', hallinnoimaan välimiesmenettelyjä järjestelyn periaatteiden liitteen I mukaisesti ja hallinnoimaan periaatteiden liitteessä I yksilöityä välimiesrahastoa.

⁽⁴⁾ Kauppaministeriö ja komissio sopivat 15 päivänä syyskuuta 2017 välimiesmenettelysäännösten valitsemisesta järjestelyn periaatteiden liitteessä I kuvattujen sitovien välimiesmenettelyjen menettelytapasäännöiksi. Ne sopivat myös välimiesten käytäntösäännöistä, jotka ovat kaupallisten välimiesten yleisesti hyväksyttyjen eettisten normien ja järjestelyn periaatteiden liitteen I mukaisia. Kauppaministeriö ja komissio sopivat, että välimiesmenettelyä koskevia sääntöjä ja käytäntösääntöjä mukautetaan vastaamaan EU:n ja Yhdysvaltojen tietosuojakehykseen tehtäviä päivityksiä, ja kauppaministeriö tekee päivitykset yhdessä ICDR-AAA:n kanssa.

Lainsäädännön muutokset

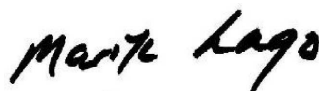
Kauppaministeriö pyrkii kohtuullisin toimin antamaan komissiolle tietoja merkittävistä muutoksista Yhdysvaltojen laeissa siltä osin kuin muutokset liittyvät EU:n ja Yhdysvaltojen tietosuojakehyksen kannalta merkityksellisiin tietosuojakäytäntöihin ja sellaisiin rajoituksiin ja suojatoimiin, jotka koskevat Yhdysvaltojen viranomaisten pääsyä henkilötietoihin ja näiden tietojen myöhempää käyttöä.

Yhdysvaltojen viranomaisten pääsy henkilötietoihin

Yhdysvallat on antanut Yhdysvaltojen signaalitiedustelutoiminnan suojatoimien tehostamista koskevan toimeenpanoasetuksen (Executive Order) 14086 (Enhancing Safeguards for United States Signals Intelligence Activities) ja 28 CFR osa 201:n, jolla muutetaan oikeusministeriön asetuksia tietosuojaa käsittelevän muutoksenhakutuomioistuimen (Data Protection Review Court) perustamiseksi. Nämä säädökset antavat henkilötiedoille vahvan suojan, joka koskee viranomaisten pääsyä tietoihin kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Annettu suoja koskee seuraavia asioita: yksityisyyden ja kansalaisoikeuksien suojan vahvistaminen sen varmistamiseksi, että Yhdysvaltojen signaalitiedustelutoiminta on tarpeellista ja oikeasuhteista määriteltyjen kansallisten turvallisuustavoitteiden saavuttamiseksi, uuden muutoksenhakumekanismin perustaminen riippumattoman ja sitovan viranomaisen puitteissa sekä Yhdysvaltojen signaalitiedustelutoiminnan nykyisen tiukan, monitasoisen valvonnan parantaminen. Näiden suojatoimien nojalla EU:n kansalaiset voivat hakea muutosta uuden monitasoisen muutoksenhakumekanismin kautta. Siihen kuuluu riippumaton tietosuojaa käsittelevä muutoksenhakutuomioistuin, joka koostuu Yhdysvaltojen viranomaisten ulkopuolelta valituista henkilöistä, joilla on täysi toimivalta päättää hakemuksista ja tarvittaessa suorista korjaavista toimenpiteistä. Kauppaministeriö pitää kirjaa EU:n kansalaisista, jotka tekevät vaatimukset täyttävän valituksen toimeenpanoasetuksen 14086 ja 28 CFR osa 201:n mukaisesti. Viiden vuoden kuluttua tämän kirjeen päiväyksestä ja sen jälkeen viiden vuoden välein kauppaministeriö ottaa yhteyttä asiaankuuluviin virastoihin selvittääkseen, onko tietosuojaa käsittelevälle muutoksenhakutuomioistuimelle toimitettujen vaatimukset täyttävien valitusten tarkasteluun tai tarkastelua koskevien hakemusten tarkasteluun liittyviä tietoja luokiteltu ei-salaisiksi. Jos tällaisia tietoja on luokiteltu ei-salaisiksi, kauppaministeriö tekee yhteistyötä asianomaisen tietosuojaviranomaisen kanssa tiedottaakseen asiasta kyseiselle EU:n kansalaiselle. Nämä parannukset vahvistavat, että Yhdysvaltoihin siirrettyjä EU:n henkilötietoja käsitellään tavalla, joka vastaa EU:n oikeudellisia vaatimuksia, jotka koskevat viranomaisten pääsyä tietoihin.

Järjestelyn periaatteiden, toimeenpanoasetuksen 14086, 28 CFR osa 201:n ja mukana toimittujen kirjeiden ja tietojen, muun muassa tietosuojakehysohjelman hallintoa ja valvontaa koskevien kauppaministeriön sitoumusten, perusteella meidän olettamuksemme on, että komissio tekee päätelmän, jonka mukaan EU:n ja Yhdysvaltojen tietosuojakehyksessä EU:n lainsäädännön edellyttämän riittävän suojan, ja tiedonsiirrot Euroopan unionista EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuville organisaatioille jatkuvat. Oletamme myös, että näiden järjestelyjen ehdot helpottavat edelleen EU:n vakiosopimuslausekkeisiin tai EU:n yrityksiä koskeviin sitoviin sääntöihin perustuvia siirtoja yhdysvaltalaisille organisaatioille.

Kunnioittavasti



Marisa LAGO



Office of the Chair

LIITE IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

9. kesäkuuta 2023

Didier Reynders
Oikeus-, kuluttaja- ja tasa-arvoasioista vastaava komissaari
Euroopan komissio
Rue de la Loi / Wetstraat 200
1049 Bryssel
Belgia

Arvoisa komissaari Reynders,

Yhdysvaltojen liittovaltion kauppakomissio kiittää mahdollisuudesta kertoa toimista, joilla se valvoo EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden toteutumista. Liittovaltion kauppakomissio on pitkään pyrkinyt suojelemaan kuluttajia ja yksityisyyttä kansainvälisissä yhteyksissä, ja olemme sitoutuneet varmistamaan tämän kehyksen kaupan alaa koskevien näkökohtien noudattamisen. Liittovaltion kauppakomissio on hoitanut tätä tehtävää vuodesta 2000 lähtien Yhdysvaltojen ja EU:n *Safe Harbor* -järjestelyn yhteydessä ja vuodesta 2016 lähtien EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn yhteydessä. ⁽¹⁾ Euroopan unionin tuomioistuin mitätöi 16. heinäkuuta 2020 tietosuojan riittävyyttä koskevan Euroopan komission päätöksen, johon EU:n ja Yhdysvaltojen Privacy Shield -järjestely perustui. Mitätöinti perustui ongelmiin, jotka eivät liittyneet kaupallisiin periaatteisiin, joiden noudattamista liittovaltion kauppakomissio valvoi. Yhdysvallat ja Euroopan komissio ovat sittemmin neuvotelleet EU:n ja Yhdysvaltojen tietosuojakehyksen vastauksena EU:n tuomioistuimen päätökseen.

Kirjoitan vahvistaakseni liittovaltion kauppakomission sitoutumisen EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteisiin. Erityisesti vahvistamme sitoumuksemme kolmella keskeisellä alueella: 1) annamme etusijan valitusten käsittelemiselle ja tutkimuksille, 2) haemme määräyksiä ja valvomme niiden noudattamista ja 3) teemme valvontayhteistyötä EU:n tietosuojaviranomaisten kanssa.

I. Johdanto

a. Liittovaltion kauppakomission työ yksityisyyden suojan valvonnassa ja alan toimintaperiaatteiden luomisessa

Liittovaltion kauppakomissiolla on laajat siviilioikeudellista lainvalvontaa koskevat toimivaltuudet, joilla se voi edistää kuluttajansuojaa ja kaupallisen alan kilpailua. Osana kuluttajansuojaan liittyviä tehtäviään liittovaltion kauppakomissio valvoo useiden lakien noudattamista suojellakseen kuluttajien ja heitä koskevan tiedon yksityisyyttä ja turvallisuutta.

⁽¹⁾ Puheenjohtaja Edith Ramirezin oikeus-, kuluttaja- ja tasa-arvoasioista vastaavalle Euroopan komission jäsenelle Věra Jourovälle lähettämä kirje, jossa selostetaan, kuinka liittovaltion kauppakomissio valvoo EU:n ja Yhdysvaltojen uuden Privacy Shield -järjestelyn noudattamista (29. helmikuuta 2016), saatavilla osoitteessa <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. Liittovaltion kauppakomissio sitoutui aiemmin myös valvomaan Yhdysvaltojen ja EU:n Safe Harbor -ohjelman noudattamista. Liittovaltion kauppakomission puheenjohtajan Robert Pitofskyn kirje Euroopan komission sisämarkkinoiden pääosaston johtajalle John Moggille (14. heinäkuuta 2000), saatavilla osoitteessa <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission>. Tämä kirje korvaa aiemmat sitoumukset.

Liittovaltion kauppakomissio valvoo liittovaltion kauppakomissiosta annetun lain noudattamista. Laissa kielletään kaupankäynnissä toteutettavat tai kaupankäyntiin vaikuttavat ”sopimattomat” ja ”vilpilliset” toimet tai käytännöt. ⁽²⁾ Liittovaltion kauppakomissio valvoo myös kohdennettuja lakeja, joilla suojataan terveyteen, luottoihin ja muihin rahoitusasioihin liittyviä tietoja sekä verkossa olevaa lapsia koskevaa tietoa. Liittovaltion kauppakomissio on antanut asetuksia kaikkien näiden kohdennettujen lakien täytäntöönpanemiseksi. ⁽³⁾

Liittovaltion kauppakomissio on viime aikoina myös toteuttanut useita aloitteita yksityisyyteen liittyvän työnsä vahvistamiseksi. Elokuussa 2022 se ilmoitti harkitsevansa sääntöjä, joilla torjutaan haitallista kaupallista valvontaa ja heikkoa tietoturvaa. ⁽⁴⁾ Hankkeen tavoitteena on luoda vankka julkinen rekisteri sen selvittämiseksi, olisiko kauppakomission hyväksyttävä sääntöjä, joilla puututaan kaupallisiin valvonta- ja tietoturvakäytäntöihin, ja millaiset näiden sääntöjen mahdollisesti pitäisi olla. Olemme ottaneet mielellämme vastaan EU:n sidosryhmien kommentteja tästä ja muista aloitteista.

Kauppakomission PrivacyCon-konferensseihin kokoontuu edelleen johtavia tutkijoita keskustelemaan kuluttajien yksityisyyteen ja tietoturvaan liittyvistä uusimmista tutkimuksista ja suuntauksista. Olemme myös lisänneet virastomme kykyä pysyä tekniikan kehityksen tasalla, koska se on useimmiten keskeistä yksityisyyssuhteissamme. Muodostamme kasvavaa tiimiä teknikoista ja poikkitieteellisistä tutkijoista. Kuten tiedätte, olemme myös ilmoittaneet käyvämme Teidän ja Euroopan komissiossa toimivien kollegojenne kanssa yhteistä vuoropuhelua, jossa käsitellään yksityisyyteen liittyviä aiheita, kuten harhauttavaa suunnittelua (nk. dark patterns) ja liiketoimintamalleja, joille on ominaista laajamittainen tiedonkeruu. ⁽⁵⁾ Laadimme hiljattain myös kongressille tarkoitetun raportin, jossa varoitettiin tekoälyn käyttöön liittyvistä haitoista, reagoidaksemme kongressin määrittämiin verkon haittoihin. Raportissa esitettiin virheellisyys, puolueellisuus, syrjintää ja haitalliseksi kääntyvään kaupalliseen valvontaan (surveillance creep) liittyviä huolenaiheita. ⁽⁶⁾

b. Yhdysvaltojen laissa annettu suoja, josta EU:n kuluttajat hyötyvät

EU:n ja Yhdysvaltojen tietosuojakehys on osa laajempaa Yhdysvalloissa noudatettavaa yksityisyyden suojaa, josta myös EU:n kuluttajat hyötyvät monin tavoin. Liittovaltion kauppakomissiosta annetussa laissa oleva sopimattomien tai vilpillisten toimien ja käytäntöjen kieltä ei rajoitu siihen, että sillä suojellaan yhdysvaltalaisia kuluttajia yhdysvaltalaisilta yrityksiltä, sillä kieltä kattaa käytännöt, jotka 1) aiheuttavat tai todennäköisesti aiheuttavat kohtuullisesti ennustettavissa olevia vahinkoja Yhdysvalloissa tai joihin 2) liittyy olennaista toimintaa Yhdysvalloissa. Lisäksi samat hyvitysmenetelmät ovat kauppakomission käytössä sekä ulkomaisten että kotimaisten kuluttajien suojaamiseksi. ⁽⁷⁾

Liittovaltion kauppakomissio valvoo myös, että kohdennettuja lakeja, joilla annetaan suojaa myös ei-yhdysvaltalaisille kuluttajille, noudatetaan. Tällaisia lakeja ovat esimerkiksi laki lasten yksityisyyden suojasta internetissä (Children's Online Privacy Protection Act, jäljempänä 'COPPA-laki'). COPPA-laissa asetetaan sivustojen ylläpitäjille vaatimuksia muun muassa siitä, että ne antavat vanhemmille suunnatun ilmoituksen ja hankkivat näiltä todennettavissa olevan suostumuksen sellaisten verkkosivustojen ja -palveluiden osalta, jotka on suunnattu lapsille, sekä sellaisten yleisten, kaikille suunnattujen

⁽²⁾ 15 U.S.C. 45 §:n a momentti. Kauppakomissiolla ei ole toimivaltaa rikoslain valvontaan eikä kansalliseen turvallisuuteen liittyvissä asioissa. Se ei voi myöskään ryhtyä useimpiin muihin valtionhallinnon toimivaltaan kuuluviin toimiin. Lisäksi liittovaltion kauppakomission toimivaltuuksissa, jotka koskevat kaupallisia toimintoja, on rajoituksia, jotka koskevat esimerkiksi pankkeja, lentoyhtiöitä, vakuutuslaitosten ja telepalveluyritysten tavanomaisia tiedonsiirtopalveluja. Kauppakomission toimivaltuudet eivät myöskään koske useimpia voittoa tavoittelemattomia yhteisöjä, mutta ne koskevat välttämättä yhteisöjä, jotka itse asiassa toimivat voiton saavuttamiseksi. Kauppakomissiolla on toimivaltuudet myös sellaisten voittoa tavoittelemattomien yhteisöjen osalta, jotka toimivat voittoa tavoittelevien jäsentensä hyväksi, muun muassa antamalla kyseisille jäsenille merkittäviä taloudellisia etuja. Joissakin tapauksissa liittovaltion kauppakomission toimivaltuudet ovat rinnakkaisia jonkin toisen lainvalvontaviranomaisen toimivaltuuksien kanssa. Yhteytemme liittovaltion ja osavaltioiden viranomaisiin ovat vankat, ja teemme tiivistä yhteistyötä koordinoitaksemme tutkimuksia ja siirtääksemme tarvittaessa asioita asianomaisten tahojen käsiteltäväksi.

⁽³⁾ Ks. FTC, Privacy and Security, <https://www.ftc.gov/business-guidance/privacy-security>.

⁽⁴⁾ Ks. tiedote, Fed. Trade Comm'n, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices* (11. elokuuta, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁽⁵⁾ Ks. oikeusasioista vastaavan Euroopan komission jäsenen Didier Reyndersin ja Yhdysvaltojen liittovaltion kauppakomission puheenjohtajan Lina Khanin yhteinen lehdistötiedote (30. maaliskuuta 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

⁽⁶⁾ Ks. tiedote, Fed. Trade Comm'n, *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems* 16. kesäkuuta, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁽⁷⁾ 15 U.S.C. 45 §:n a momentin 4 kohdan B alakohta. Lisäksi ”sopimattomat tai vilpilliset toimet tai käytännöt” käsittävät sellaiset ulkomaankauppaan liittyvät toimet tai käytännöt, i) jotka aiheuttavat tai todennäköisesti aiheuttavat Yhdysvalloissa vahinkoja, joiden syntymistä voidaan kohtuudella odottaa, tai ii) joihin liittyy olennaista toimintaa Yhdysvalloissa. 15 U.S.C. 45 §:n a momentin 4 kohdan A alakohta.

verkkosivustojen osalta, jotka tietoisesti keräävät henkilötietoja alle 13-vuotiailta lapsilta. Yhdysvaltalaisen verkkosivustojen ja -palveluiden, joihin sovelletaan COPPA-lakia ja jotka keräävät henkilötietoja ulkomaisista lapsista, on noudatettava COPPA-lakia. Myös ulkomaisten verkkosivustojen ja -palveluiden on noudatettava COPPA-lakia, jos ne on suunnattu yhdysvaltalaisille lapsille tai jos ne tietoisesti keräävät henkilötietoja yhdysvaltalaisilta lapsilta. Niiden Yhdysvaltojen liittovaltion lakien lisäksi, joiden noudattamista liittovaltion kauppakomissio valvoo, myös muissa liittovaltion ja osavaltioiden kuluttajansuojaa, tietoturvaloukkauksia ja yksityisyyden suojaa koskevissa laeissa voi olla EU:n kuluttajia hyödyttäviä säännöksiä.

c. Liittovaltion kauppakomission lainvalvontatoiminta

Liittovaltion kauppakomissio on nostanut kanteita sekä Yhdysvaltojen ja EU:n Safe Harbor -ohjelman että EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn yhteydessä. Se on myös valvonut EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn noudattamista senkin jälkeen, kun EU:n tuomioistuimien mitätöi tietosuojan riittävyyttä koskevan päätöksen, joka toimi EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn yhteydessä⁽⁸⁾. Useat kauppakomission viimeaikaiset valitukset ovat sisältäneet syytekohtia, joiden mukaan yritykset ovat rikkoneet EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn määräyksiä. Tämä koskee muun muassa seuraavia yrityksiä koskevia menettelyjä: Twitter⁽⁹⁾, CafePress⁽¹⁰⁾ ja Flo⁽¹¹⁾. Twitteriä vastaan toteutetuissa lainvalvontatoimissa Twitter määrättiin kauppakomission vaatimuksesta maksamaan 150 miljoonaa dollaria aikaisemman kauppakomission määräyksen rikkomisesta, johon liittyvät käytännöt koskivat yli 140:tä miljoonaa asiakasta. Yritys oli muun muassa rikkonut EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatetta 5 (Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaate). Lisäksi viraston määräys edellyttää, että Twitter sallii käyttäjien käyttää turvallisia monivaiheisia tunnistautumismenetelmiä, jotka eivät edellytä käyttäjiltä puhelinnumeroiden ilmoittamista.

Asiassa *CafePress* kauppakomissio väitti, että yritys ei suojannut kuluttajien arkaluonteisia tietoja, salasi merkittävän tietoturvaloukkauksen ja rikkoi EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatteita 2 (Valintaperiaate), 4 (Turvallisuusperiaate) ja 6 (Tietoihin pääsyä koskeva periaate). Kauppakomission määräyksessä vaaditaan, että yritys korvaa puutteelliset tunnistautumismenpiteet monivaiheisella tunnistautumisella, rajoittaa merkittävästi keräämiensä ja säilyttämiensä tietojen määrää, salaa sosiaaliturvatunnukset ja pyytää kolmatta osapuolta arvioimaan tietoturvaohjelmansa ja toimittamaan kauppakomissiolle kopion, joka voidaan julkaista.

Asiassa *Flo* kauppakomissio väitti, että hedelmällisyyden seurantasovellus paljasti käyttäjien terveystietoja kolmansille osapuolille, jotka olivat data-analytiikan tarjoajia, sitouduttuaan pitämään tällaiset tiedot yksityisinä. Kauppakomission valituksessa mainitaan erityisesti yrityksen vuorovaikutus EU:n kuluttajien kanssa ja se, että Flo rikkoi EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatteita 1 (Ilmoitusperiaate), 2 (Valintaperiaate), 3 (Henkilötietojen edelleen siirtämiseen liittyvä vastuuvollisuusperiaate) ja 5 (Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaate). Viraston määräyksessä vaaditaan muun muassa, että Flo ilmoittaa asianomaisille käyttäjille heidän henkilötietojensa luovuttamisesta ja ohjeistaa kaikkia kolmansia osapuolia, jotka ovat saaneet käyttäjien terveystietoja, hävittämään kyseiset tiedot. On tärkeää huomata, että liittovaltion kauppakomission määräyksellä suojellaan kaikkia yhdysvaltalaisen yrityksen kanssa asioivia kuluttajia ympäri maailman, ei pelkästään valituksen jättäneitä kuluttajia.

Monissa aiemmissa Yhdysvaltojen ja EU:n Safe Harbor -ohjelmaan ja EU:n ja Yhdysvaltojen Privacy Shield -järjestelyyn liittyneissä lainvalvonta-asioissa oli mukana organisaatioita, jotka olivat antaneet ensimmäisen oman varmennuksen kauppaministeriön kautta mutta eivät antaneet vuotuista uudelleenvarmennusta ja esittivät silti edelleen osallistuvansa järjestelyyn. Muissa tapauksissa oli kyse totuudenvastaisista väitteistä, jotka koskivat sellaisten organisaatioiden osallistumista, jotka eivät olleet koskaan tehneet ensimmäistä omaa varmennusta kauppaministeriön kautta. Jatkossa oletamme, että keskitymme proaktiivisissa lainvalvontatoimissamme edelleen sentyyppisiin EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden aineellisiin rikkomuksiin, joita väitettiin tapahtuneen Twitterin, CafePressin ja Flon kaltaisissa tapauksissa. Samalla kauppaministeriö jatkaa omaan varmennukseen liittyvän prosessin hallinnointia ja valvontaa, ylläpitää luetteloa EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvista organisaatioista ja käsittelee muita ohjelmaan osallistumista koskeviin väitteisiin liittyviä kysymyksiä.⁽¹²⁾ On tärkeää huomata, että organisaatioihin, jotka väittävät osallistuvansa EU:n ja Yhdysvaltojen tietosuojakehykseen, voidaan kohdistaa merkittäviä tietosuojakehyksen periaatteiden noudattamisen valvontaan liittyviä toimia silloinkin, kun ne eivät tee (uudelleen) omaa varmennusta kauppaministeriön kautta.

⁽⁸⁾ Ks. liite A, jossa luetellaan liittovaltion kauppakomission Safe Harbor- ja Privacy Shield -järjestelyihin liittyvät asiat.

⁽⁹⁾ Ks. tiedote, Fed. Trade Comm'n, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (25. toukokuuta 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

⁽¹⁰⁾ Ks. tiedote, Fed. Trade Comm'n, *FTC Takes Action Against CafePress for Data Breach Cover Up* (15. maaliskuuta 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

⁽¹¹⁾ Ks. tiedote, Fed. Trade Comm'n, *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others* (22. kesäkuuta 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⁾ Kansainvälisestä kaupasta vastaavan alivaltiosihteeri Marisa Lagon kirje oikeus-, kuluttaja- ja tasa-arvoasioista vastaavalle komissaarille Didier Reyndersille (12. joulukuuta 2022).

II. Etusijan antaminen valitusten käsittelemiselle ja tutkimukset

Samalla tavalla kuin Yhdysvaltojen ja EU:n Safe Harbor -ohjelmassa ja EU:n ja Yhdysvaltojen Privacy Shield -järjestelyssä liittovaltion kauppakomissio sitoutuu antamaan etusijan sellaisille EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamatta jättämisestä koskeville tapauksille, jotka on saatu kauppaministeriöstä ja EU:n jäsenvaltioista. Kauppakomissio asettaa etusijalle myös sellaiset EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamatta jättämisestä koskevat tapaukset, jotka on saatu yksityisyyden suojan itsesääntelystä vastaavilta elimiltä ja muilta riippumattomilta riitojenratkaisuelimiltä.

Jotta valitusten toimittaminen EU:n jäsenvaltioista olisi EU:n ja Yhdysvaltojen tietosuojakehyksessä helpompaa, liittovaltion kauppakomissio on laatinut vakioidun valitusten toimitusprosessin ja antanut EU:n jäsenvaltioille opastusta siitä, millaista tietoa kauppakomissio voisi parhaiten hyödyntää valitusten käsittelyssä. Osana tätä työtä liittovaltion kauppakomissio on nimenyt virastostaan yhteyspisteen EU:n jäsenvaltioilta tulevia valituksia varten. Tämä on erittäin hyödyllistä silloin, kun valituksen toimittava viranomainen on tutkinut väitetyn rikkomisen alustavasti ja pystyy tekemään liittovaltion kauppakomission kanssa yhteistyötä tutkimuksen aikana.

Kun liittovaltion kauppakomissio vastaanottaa tällaisen valituksen kauppaministeriöltä, EU:n jäsenvaltiolta, itsesääntelyorganisaatiolta tai muulta riippumattomalta riitojenratkaisuelimeltä, se voi ryhtyä useampaankin toimenpiteeseen asian hoitamiseksi. Kauppakomissio voi esimerkiksi tarkastaa organisaation tietosuojaperiaatteet, hankkia lisätietoja suoraan organisaatiolta tai kolmansilta osapuolilta, tehdä seurantatyötä yhdessä valituksen toimittaneen viranomaisen kanssa, arvioida, noudattaako rikkominen jotain kaavaa tai koskeeko se suurta määrää kuluttajia, päätellä, koskeeko valitus asioita, jotka kuuluvat kauppaministeriön toimivaltaan, arvioida, olisiko markkinaosapuolten virallisesta varoittamisesta hyötyä, ja tarvittaessa panna vireille lainvalvontamenettely.

Sen lisäksi, että liittovaltion kauppakomissio asettaa etusijalle EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteisiin liittyvät valitukset, jotka se vastaanottaa kauppaministeriöltä, EU:n jäsenvaltioilta ja yksityisyyden suojan itsesääntelyorganisaatioilta tai muilta riippumattomilta riitojenratkaisuelimiltä⁽¹³⁾, se tutkii edelleen tarvittaessa tietosuojakehyksen periaatteiden merkittäviä rikkomisia omasta aloitteestaan erilaisia välineitä käyttäen. Osana liittovaltion kauppakomission ohjelmaa, jonka kohteena ovat kaupallisia organisaatioita koskevat yksityisyydensuoja- ja tietoturva-asiat, virasto on selvittänyt rutiininomaisesti, onko tutkimuksen kohteena oleva yksikkö esittänyt EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä koskevia lausumia. Jos se on esittänyt niitä ja tutkimuksessa on tullut ilmi, että EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatteita on ilmeisesti rikottu, liittovaltion kauppakomissio on ottanut järjestelyn rikkomista koskevan väittämän osaksi lainvalvontatoimiaan. Kauppakomissio noudattaa jatkossakin tätä ennakoivaa lähestymistapaa, nyt EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamisen varmistamiseksi.

III. Määräysten hakeminen ja niiden noudattamisen valvonta

Liittovaltion kauppakomissio vahvistaa myös sitoumuksensa, jonka mukaan se hakee täytäntöönpanomääräyksiä ja valvoo niiden noudattamista varmistaakseen EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamisen. Kauppakomissio valvoo EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamista siten, että tuleviin kauppakomission määräyksiin, jotka koskevat tietosuojakehyksen periaatteita, sisällytetään erilaisia soveltuvia kieltoehtoja. Jos liittovaltion kauppakomission hallinnollisia määräyksiä rikotaan, voidaan siviilioikeudellisina seuraamuksina määrätä enintään 50 120 Yhdysvaltojen dollaria rikkomusta kohti tai, jos rikkomus jatkuu, 50 120 dollaria päivää kohti.⁽¹⁴⁾ Jos kielletyt käytännöt vaikuttavat suureen joukkoon kuluttajia, seuraamukset voivat nousta miljooniin dollareihin. Jokaiseen suostumusmääräykseen sisältyy myös raportointi- ja noudattamisehtoja. Määräyksen saaneen yksikön on tiettyjen vuosien ajan säilytettävä asiakirjat, jotka todistavat, että määräystä on noudatettu. Määräykset on annettava tiedoksi myös työntekijöille, joiden tehtävänä on varmistaa, että määräyksiä noudatetaan.

Liittovaltion kauppakomissio valvoo järjestelmällisesti, että olemassa olevia EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn periaatteita koskevia määräyksiä noudatetaan, kuten se tekee kaikkien määräystensä osalta, ja panee tarvittaessa vireille kanteita varmistaakseen määräysten noudattamisen.⁽¹⁵⁾ On tärkeää huomata, että liittovaltion kauppakomission määräyksellä suojellaan kaikkia yrityksen kanssa asioivia kuluttajia ympäri maailman, ei pelkästään valituksen jättäneitä kuluttajia. Lopuksi on todettava, että liittovaltion kauppakomissio pitää verkossa yllä luetteloa yrityksistä, joille on annettu määräys EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamisen valvonnan yhteydessä.⁽¹⁶⁾

⁽¹³⁾ Vaikka liittovaltion kauppakomissio ei ratkaise eikä sovittelu yksittäisiä kuluttajien tekemiä valituksia, se vahvistaa antavansa etusijan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita koskeville valituksille, jotka Euroopan tietosuojaviranomaiset sille toimittavat. Lisäksi kauppakomissio hyödyntää valituksia koskevia tietoja, jotka sisältyvät sen kuluttajavalitustietojen tietokantaan (Consumer Sentinel). Monilla muilla lainvalvontavirastoilla on pääsy tietokantaan. Tietokannan avulla kauppakomissio voi havaita trendejä, määrittää lainvalvontaprioriteetteja ja löytää mahdollisia tutkintakohteita. EU:n alueella asuvat henkilöt voivat jättää valituksen liittovaltion kauppakomissiolle käyttämällä samaa valitusjärjestelmää kuin Yhdysvaltojen kuluttajat, osoitteessa <https://reportfraud.ftc.gov/>. EU:n alueella asuvien henkilöiden kannalta saattaa olla hyödyllisintä jättää yksittäiset EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita koskevat valitukset oman jäsenvaltion tietosuojaviranomaiselle tai riippumattomalle riitojenratkaisuelimelle.

⁽¹⁴⁾ 15 U.S.C. 45 §:n m momentti; 16 C.F.R. 1.98 §. Määrä mukautetaan säännöllisesti inflaatioon.

⁽¹⁵⁾ Viime vuonna liittovaltion kauppakomissio päätti äänestyksellä yksinkertaistaa tutkintaprosessia, joka koskee toistuvien rikkomisiin syyllistyneitä organisaatioita. Ks. tiedote, Fed. Trade Comm'n, *FTC Authorizes Investigations into Key Enforcement Priorities* (1. heinäkuuta 2021), <https://www.ftc.gov/news-events/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

⁽¹⁶⁾ Ks. FTC, Privacy Shield, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

IV. Lainvalvontayhteistyö EU:n tietosuojaviranomaisten kanssa

Liittovaltion kauppakomissio katsoo, että EU:n tietosuojaviranomaisilla voi olla merkittävä tehtävä varmistettaessa EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamista, ja haluaa lisätä keskinäistä konsultointia ja lainvalvontayhteistyötä. Koordinoitu lähestymistapa onkin entistä ratkaisevampi vastattaessa haasteisiin, joita digitaalisten markkinoiden nykyinen kehitys ja dataintensiiviset liiketoimintamallit aiheuttavat. Liittovaltion kauppakomissio vaihtaa tietoja valituksia toimittaneiden valvontaviranomaisten kanssa ja muun muassa tiedottaa valitusten käsittelyn vaiheesta noudattaen luottamuksellisuutta koskevia lakeja ja rajoituksia. Sikäli kuin vastaanotettujen valitusten määrä ja tyyppi sallivat, valituksista annetaan myös arvio, jossa muuan muassa kuvataan keskeiset asiaan liittyvät kysymykset ja toimet, jotka liittovaltion kauppakomissio toimivaltansa rajoissa on pannut vireille lakien rikkomisen vuoksi. Liittovaltion kauppakomissio antaa valituksia toimittaneille viranomaisille palautetta myös siitä, minkä tyyppisiä valitukset ovat, sellaisten toimien tehostamiseksi, joilla voitaisiin puuttua lainvastaisiin menettelyihin. Jos valituksen toimittanut valvontaviranomainen pyytää tietoa valituksen käsittelyvaiheesta voidakseen käyttää tietoa omissa lainvalvontatoimissaan, liittovaltion kauppakomissio antaa vastauksen ottaen huomioon käsiteltävänä olevien valitusten määrän ja noudattaen luottamuksellisuuteen liittyviä ja muita lain vaatimuksia.

Liittovaltion kauppakomissio työskentelee tiiviisti myös Euroopan tietosuojaviranomaisten kanssa ja tarjoaa apua lainvalvonnan. Yhteistyössä olisi soveltuviissa tapauksissa kyse tietojen vaihdosta ja tutkimuksellisesta avusta Yhdysvaltojen verkkoturvallisuuslain (U.S. SAFE WEB Act) nojalla. Kyseinen laki antaa liittovaltion kauppakomissiolle valtuudet avustaa ulkomaisia lainvalvontaviranomaisia silloin, kun nämä valvovat sellaisten lakien noudattamista, joissa kielletyt menettelyt ovat olennaisilta osiltaan samanlaisia kuin liittovaltion kauppakomission valvomissa laeissa kielletyt menettelyt. ⁽¹⁷⁾ Kauppakomissio voi osana tätä apua verkkoturvallisuuslain vaatimuksia noudattaen jakaa tietoa, jota se on saanut omissa tutkimuksissaan, ryhtyä pakollisiin menettelyihin Euroopan tietosuojaviranomaisen puolesta tämän omassa tutkimuksessa sekä hankkia suullisia lausuntoja todistajilta tai vastaajilta Euroopan tietosuojaviranomaisen lainvalvontamenettelyn yhteydessä. Liittovaltion kauppakomissio käyttää näitä valtuuksia säännöllisesti avustaakseen muita viranomaisia eri puolilla maailmaa yksityisyydensuoja- ja kuluttajansuoja-asioissa.

Sen lisäksi, että liittovaltion kauppakomissio kuulee EU:n tietosuojaviranomaisia, kun se käsittelee näiden toimittamia yksittäisiä valituksia, se osallistuu säännöllisiin kokouksiin Euroopan tietosuojaneuvoston edustajien kanssa keskustellakseen yleisesti lainvalvontayhteistyön parantamisesta. Lisäksi liittovaltion kauppakomissio osallistuu kauppaministeriön, Euroopan komission ja Euroopan tietosuojaneuvoston edustajien ohella EU:n ja Yhdysvaltojen tietosuojakehyksen vuotuisen tarkasteluun keskustellakseen järjestelyn täytäntöönpanosta. Liittovaltion kauppakomissio edistää myös sellaisten työkalujen kehittämistä, joilla tehostetaan lainvalvontayhteistyötä Euroopan tietosuojaviranomaisten kanssa samoin kuin muiden yksityisyyden suojan toteutumista valvovien viranomaisten kanssa ympäri maailman. Liittovaltion kauppakomissio vahvistaa mielihyvin sitoumuksensa valvoa kaupalliseen sektoriin liittyviä EU:n ja Yhdysvaltojen tietosuojakehyksen näkökohtia. Katsomme kumppanuutemme EU:n kollegojen kanssa olevan ratkaiseva osa yksityisyyden suojan tarjoamista sekä Yhdysvaltojen että EU:n kansalaisille.

Kunnioittavasti



Lina M. KHAN

Chair, Federal Trade Commission

⁽¹⁷⁾ Kun liittovaltion kauppakomissio päättää, käyttääkö se verkkoturvallisuuslain mukaisia valtuuksiaan, se ottaa muun muassa huomioon seuraavaa: A) onko apua pyytävä virasto sitoutunut antamaan vastavuoroista apua liittovaltion kauppakomissiolle tai sitoutuuko se antamaan sitä vastaisuudessa, B) vaarantaisiko pyynnön noudattaminen Yhdysvaltojen yleistä etua ja C) koskevatko apua pyytävän viraston tutkimukset tai lainvalvontamenettelyt toimia ja käytäntöjä, jotka aiheuttavat tai todennäköisesti aiheuttavat vahinkoa merkittävälle määrälle ihmisiä. 15 U.S.C. 46 §:n j momentin 3 kohta. Kilpailulakien noudattamisen valvonta ei kuulu näiden valtuuksien soveltamisalaan.

Lisäys A

Privacy Shield- ja Safe Harbor -järjestelyjen noudattamisen valvonta

	Luettelonro/FTC:n asiakirjanro	Asia	Linkki
1	FTC:n asiakirjanro 2023062 Asia nro 3:22-cv-03070 (N.D. Cal.)	Yhdysvallat v. Twitter, Inc.	Twitter
2	FTC:n asia nro 192 3209	Asia Residual Pumpkin Entity, LLC, entinen toiminimi CafePress , ja PlanetArt, LLC, toiminimi CafePress	CafePress
3	FTC:n asia nro 192 3133 Luettelonro C-4747	Asia Flo Health, Inc.	Flo Health
4	FTC:n asia nro 192 3050 Luettelonro C-4723	Asia Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	FTC:n asia nro 192 3092 Luettelonro C-4709	Asia T&M Protection, LLC	T&M Protection
6	FTC:n asia nro 192 3084 Luettelonro C-4704	Asia TDARX, Inc.	TDARX
7	FTC:n asia nro 192 3093 Luettelonro C-4706	Asia Global Data Vault, LLC	Global Data
8	FTC:n asia nro 192 3078 Luettelonro C-4703	Asia Incentive Services, Inc.	Incentive Services
9	FTC:n asia nro 192 3090 Luettelonro C-4705	Asia Click Labs, Inc.	Click Labs
10	FTC:n asia nro 182 3192 Luettelonro C-4697	Asia Medable, Inc.	Medable
11	FTC:n asia nro 182 3189 Luettelonro 9386	Asia NTT Global Data Centers Americas, Inc., RagingWire Data Centers, Inc:n oikeudenomistajana	RagingWire
12	FTC:n asia nro 182 3196 Luettelonro C-4702	Asia Thru, Inc.	Thru
13	FTC:n asia nro 182 3188 Luettelonro C-4698	Asia DCR Workforce, Inc.	DCR Workforce
14	FTC:n asia nro 182 3194 Luettelonro C-4700	Asia LotaData, Inc.	LotaData
15	FTC:n asia nro 182 3195 Luettelonro C-4701	Asia EmpiriStat, Inc.	EmpiriStat

16	FTC:n asia nro 182 3193 Luettelonro C-4699	Asia 214 Technologies, Inc., myös toiminimi Trueface.ai	Trueface.ai
17	FTC:n asia nro 182 3107 Luettelonro 9383	Asia Cambridge Analytica, LLC	Cambridge Analytica
18	FTC:n asia nro 182 3152 Luettelonro C-4685	Asia SecurTest, Inc.	SecurTest
19	FTC:n asia nro 182 3144 Luettelonro C-4664	Asia VenPath, Inc.	VenPath
20	FTC:n asia nro 182 3154 Luettelonro C-4666	Asia SmartStart Employment Screening, Inc.	SmartStart
21	FTC:n asia nro 182 3143 Luettelonro C-4663	Asia mResource LLC , toiminimi Loop Works LLC	mResource
22	FTC:n asia nro 182 3150 Luettelonro C-4665	Asia IDmission LLC	IDmission
23	FTC:n asia nro 182 3100 Luettelonro C-4659	Asia ReadyTech Corporation	ReadyTech
24	FTC:n asia nro 172 3173 Luettelonro C-4630	Asia Decusoft, LLC	Decusoft
25	FTC:n asia nro 172 3171 Luettelonro C-4628	Asia Tru Communication, Inc.	Tru
26	FTC:n asia nro 172 3172 Luettelonro C-4629	Asia Md7, LLC	Md7
30	FTC:n asia nro 152 3198 Luettelonro C-4543	Asia Jhayrmaine Daniels (toiminimi California Skate-Line)	Jhayrmaine Daniels
31	FTC:n asia nro 152 3190 Luettelonro C-4545	Asia Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	FTC:n asia nro 152 3141 Luettelonro C-4540	Asia Golf Connect, LLC	Golf Connect
33	FTC:n asia nro 152 3202 Luettelonro C-4546	Asia Inbox Group, LLC	Inbox Group
34	Asia nro 152 3187 Luettelonro C-4542	Asia IOActive, Inc.	IOActive
35	FTC:n asia nro 152 3140 Luettelonro C-4549	Asia Jubilant Clinsys, Inc.	Jubilant
36	FTC:n asia nro 152 3199 Luettelonro C-4547	Asia Just Bagels Manufacturing, Inc.	Just Bagels

37	FTC:n asia nro 152 3138 Luettelonro C-4548	Asia NAICS Association, LLC	NAICS
38	FTC:n asia nro 152 3201 Luettelonro C-4544	Asia One Industries Corp.	One Industries
39	FTC:n asia nro 152 3137 Luettelonro C-4550	Asia Pinger, Inc.	Pinger
40	FTC:n asia nro 152 3193 Luettelonro C-4552	Asia SteriMed Medical Waste Solutions	SteriMed
41	FTC:n asia nro 152 3184 Luettelonro C-4541	Asia Contract Logix, LLC	Contract Logix
42	FTC:n asia nro 152 3185 Luettelonro C-4551	Asia Forensics Consulting Solutions, LLC	Forensics Consulting
43	FTC:n asia nro 152 3051 Luettelonro C-4526	Asia American Int'l Mailing, Inc.	AIM
44	FTC:n asia nro 152 3015 Luettelonro C-4525	Asia TES Franchising, LLC	TES
45	FTC:n asia nro 142 3036 Luettelonro C-4459	Asia American Apparel, Inc.	American Apparel
46	FTC:n asia nro 142 3026 Luettelonro C-4469	Asia Fantage.com, Inc.	Fantage
47	FTC:n asia nro 142 3017 Luettelonro C-4461	Asia Apperian, Inc.	Apperian
48	FTC:n asia nro 142 3018 Luettelonro C-4462	Asia Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	FTC:n asia nro 142 3019 Luettelonro C-4463	Asia Baker Tilly Virchow Krause, LLP	Baker Tilly
50	FTC:n asia nro 142 3020 Luettelonro C-4464	Asia BitTorrent, Inc.	BitTorrent
51	FTC:n asia nro 142 3022 Luettelonro C-4465	Asia Charles River Laboratories, Int'l	Charles River
52	FTC:n asia nro 142 3023 Luettelonro C-4466	Asia DataMotion, Inc.	DataMotion
53	FTC:n asia nro 142 3024 Luettelonro C-4467	Asia DDC Laboratories, Inc., toiminimi DNA Diagnostics Center	DDC
54	FTC:n asia nro 142 3028 Luettelonro C-4470	Asia Level 3 Communications, LLC	Level 3

55	FTC:n asia nro 142 3025 Luettelonro C-4468	Asia PDB Sports, Ltd. , toiminimi Denver Broncos Football Club, LLP	Broncos
56	FTC:n asia nro 142 3030 Luettelonro C-4471	Asia Reynolds Consumer Products, Inc.	Reynolds
57	FTC:n asia nro 142 3031 Luettelonro C-4472	Asia Receivable Management Services Corporation	Receivable Mgmt
58	FTC:n asia nro 142 3032 Luettelonro C-4473	Asia Tennessee Football, Inc.	Tennessee Football
59	FTC:n asia nro 102 3058 Luettelonro C-4369	Asia Myspace LLC	Myspace
60	FTC:n asia nro 092 3184 Luettelonro C-4365	Asia Facebook, Inc.	Facebook
61	FTC:n asia nro 092 3081 Siviilikanne nro 09-CV-5276 (C.D. Cal.)	Liittovaltion kauppakomissio v. Javian Karnani, ja Balls of Kryptonite, LLC , toiminimi Bite Size Deals, LLC, ja Best Priced Brands, LLC	Balls of Kryptonite
62	FTC:n asia nro 102 3136 Luettelonro C-4336	Asia Google, Inc.	Google
63	FTC:n asia nro 092 3137 Luettelonro C-4282	Asia World Innovators, Inc.	World Innovators
64	FTC:n asia nro 092 3141 Luettelonro C-4271	Asia Progressive Gaitways LLC	Progressive Gaitways
65	FTC:n asia nro 092 3139 Luettelonro C-4270	Asia Onyx Graphics, Inc.	Onyx Graphics
66	FTC:n asia nro 092 3138 Luettelonro C-4269	Asia ExpatEdge Partners, LLC	ExpatEdge
67	FTC:n asia nro 092 3140 Luettelonro C-4281	Asia Directors Desk LLC	Directors Desk
68	FTC:n asia nro 092 3142 Luettelonro C-4272	Asia Collectify LLC	Collectify

LIITE V



THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. heinäkuuta 2023

Komissaari Didier Reynders
Euroopan komissio
Rue de la Loi / Wetstraat 200
1049 Bryssel
Belgia

Arvoisa komissaari Reynders,

Yhdysvaltojen liikenneministeriö kiittää mahdollisuudesta selostaa tehtäviään, jotka liittyvät EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden valvontaan. EU:n ja Yhdysvaltojen tietosuojakehyks on erittäin tärkeä, kun kaupankäynnin yhteydessä annettavia henkilötietoja suojellaan yhä verkostoituneemmassa maailmassa. Järjestelyn avulla yritykset voivat tehdä merkittäviä liiketoimia globaalissa taloudessa samaan aikaan, kun EU:n kuluttajien yksityisyyden suoja säilyy korkeatasoisena.

Liikenneministeriö ilmaisi ensimmäisen kerran julkisesti sitoumuksensa valvoa Yhdysvaltojen ja EU:n Safe Harbor -ohjelman noudattamista kirjeessä, jonka se toimitti Euroopan komissiolle yli 22 vuotta sitten. Sitoumukset toistettiin ja niitä laajennettiin vuonna 2016 lähetetyssä kirjeessä, joka koski EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä. Liikenneministeriö vakuutti kirjeissä, että se valvoisi tarmokkaasti Yhdysvaltojen ja EU:n Safe Harbor -ohjelman ja myöhemmin EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn yksityisyydensuojaperiaatteiden noudattamista. Liikenneministeriö ulottaa tämän sitoumuksen koskemaan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita ja dokumentoi sen tässä kirjeessä.

Liikenneministeriö vahvistaa sitoumuksensa erityisesti seuraavilla keskeisillä alueilla: 1) etusijan antaminen EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden väitetyjä rikkomisia koskeville tutkintatoimille, 2) asianmukaisten lainvalvontatoimien kohdistaminen yksiköihin, jotka esittävät totuudenvastaisia tai vilpillisiä väitteitä osallistumisesta EU:n ja Yhdysvaltojen tietosuojakehykseen, ja 3) EU:n ja Yhdysvaltojen tietosuojakehyksen rikkomisen vuoksi annettujen täytäntöönpanomääräysten seuranta ja julkistaminen. Annamme tietoa kustakin sitoumuksesta ja tarvittaessa taustoitamme liikenneministeriön tehtäviä kuluttajien yksityisyyden suojaamisessa ja EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamisen varmistamisessa.

1. Tausta

A. Liikenneministeriön toimivalta, joka liittyy yksityisyyden suojaamiseen

Ministeriö on vahvasti sitoutunut varmistamaan kuluttajien lentoyhtiöille ja lipunkirjoittajille antamien tietojen yksityisyyden.

Liikenneministeriön valtuudet tällä osa-alueella vahvistetaan Yhdysvaltojen laissa, ks. 49 U.S.C 41712 §, jossa kielletään liikenteenharjoittajaa tai lipunvälittäjää harjoittamasta sopimatonta tai vilpillistä menettelyä lentoliikenteessä tai lentokuljetusten myynnissä. Lainkohta vastaa liittovaltion kauppakomissiosta annetun lain 5 jaksoa (15 U.S.C. § 45).

Liikenneministeriö antoi hiljattain sääntöjä, joissa määritellään sopimattomat ja vilpilliset käytännöt ja jotka vastaavat sekä liikenneministeriön että liittovaltion kauppakomission aiempia sääntöjä (14 CFR § 399.79). Tarkemmin sanottuna menettely on 'sopimaton', jos se aiheuttaa tai todennäköisesti aiheuttaa merkittäviä haittoja, jotka eivät ole kohtuudella vältettävissä ja joiden vastapainoksi kuluttajille tai kilpailutilanteelle ei koidu yhtä suuria hyötyjä.

Menettely on 'vilpillinen', jos se johtaa kuluttajia virheellisesti kuvittelemaan, että heidän toimintansa on järkevää tietystä tilanteesta, ja liittyy olennaiseen asiaan. Asia on olennainen, jos se on todennäköisesti vaikuttanut kuluttajan käyttäytymiseen tai päätökseen tuotteen tai palvelun osalta. Näiden yleisten periaatteiden lisäksi liikenneministeriö tulkitsee 41712 §:ää siten, että se kieltää lentoliikenteen harjoittajaa ja lipunkirjoittajaa 1) rikkomasta tietosuojaperiaatteita, 2) rikkomasta liikenneministeriön vahvistamia määräyksiä, joissa tietyt yksityisyyden suojaan liittyvät käytännöt todetaan sopimattomiksi tai vilpillisiksi, 3) rikkomasta lakia lasten yksityisyyden suojasta internetissä (Children's Online Privacy Protection Act, jäljempänä 'COPPA-laki') tai liittovaltion kauppakomission määräyksiä, joilla COPPA-lakia pannaan täytäntöön, ja 4) jättämästä EU:n ja Yhdysvaltojen tietosuojakehykseen osallistuvana organisaationa noudattamatta EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita. ⁽¹⁾

Kuten edellä todetaan, liittovaltion lain mukaan liikenneministeriöllä on yksinomainen toimivalta säännellä lentoyhtiöiden yksityisyydensuojakäytäntöjä, ja se jakaa toimivallan liittovaltion kauppakomission kanssa niiden yksityisyydensuojakäytäntöjen osalta, joita lipunkirjoittajat soveltavat lentoliikennepalvelujen myynnissä.

Kun lentoliikenteen harjoittaja tai lentoliikennepalvelujen myyjä julkisesti sitoutuu noudattamaan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita, ministeriöllä on oikeus käyttää 41712 §:n mukaisia toimivaltuuksia varmistaakseen, että periaatteita noudatetaan. Jos siis matkustaja antaa tietoja EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita noudattamaan sitoutuneelle lentoliikenteen harjoittajalle tai lipunkirjoittajalle ja jos lentoliikenteen harjoittaja tai lipunkirjoittaja ei noudata kyseisiä periaatteita, kyseessä on 41712 §:n rikkomus.

B. Täytäntöönpanokäytännöt

Liikenneministeriössä toimiva lentoliikenteen kuluttajansuojavirasto (OACP) ⁽²⁾ tutkii 49 U.S.C. 41712 §:n soveltamisalaan kuuluvia tapauksia. Se valvoo 41712 §:ssä säädettyä sopimattomien ja vilpillisten käytäntöjen kieltä pääasiassa neuvottelujen avulla, valmistelemalla kieltomääräyksiä (cease and desist order) ja laatimalla siviilioikeudellisia seuraamuksia (civil penalty) koskevia päätösluonnoksia. Tiedot mahdollisista rikkomisista tulevat yksikölle paljolti valituksista, joita yksikkö vastaanottaa yksityishenkilöiltä, matkatoimistoilta, lentoyhtiöiltä sekä yhdysvaltalaisilta ja ulkomaisilta viranomaisilta. Kuluttajat voivat käyttää liikenneministeriön verkkosivustoa tehdäkseen yksityisyyden suojaa koskevan valituksen lentoyhtiötä tai lipunkirjoittajaa vastaan. ⁽³⁾

Jos asiassa ei saavuteta kohtuullista ja asianmukaista sovintoa, virastolla on toimivaltuudet panna vireille lainvalvontamenettely. Menettelyyn kuuluu istunto, jossa esitetään todisteita ja jota johtaa liikenneministeriön hallintolainkäytöstä vastaava tuomari. Tuomarilla on valtuudet antaa kieltomääräyksiä ja määrätä siviilioikeudellisia seuraamuksia. Seurauksena 41712 §:n rikkomisesta voi olla kieltomääräyksen antaminen ja enintään 37 377 Yhdysvaltojen dollarin suuruisen siviilioikeudellisen seuraamuksen määrääminen kutakin 41712 §:n rikkomusta kohti.

Liikenneministeriöllä ei ole toimivaltuuksia määrätä vahingonkorvauksia tai rahallisia hyvityksiä yksittäisille kantelijoille. Liikenneministeriöllä on kuitenkin toimivaltuudet hyväksyä sovinto, joka syntyy viraston tutkimusten tuloksena ja hyödyttää suoraan kuluttajia (esimerkiksi siten, että heille maksetaan rahaa tai annetaan arvositteitä) sen sijaan, että rikkoja maksaisi vastaavan määrän rahamääräisinä seuraamuksina Yhdysvaltojen hallitukselle. Tätä on tapahtunut aiemmin ja voi sopivissa olosuhteissa tapahtua myös EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden yhteydessä. Jos lentoyhtiö toistuvasti rikkoo 41712 §:ää, kyseisen yhtiön halukkuus noudattaa sääntöjä voidaan kyseenalaistaa, mikä saattaa törkeissä tapauksissa johtaa siihen, ettei lentoyhtiön enää katsota olevan toimilupakelpoinen ja että se tämän seurauksena menettää toimilupansa.

Liikenneministeriö on tähän mennessä saanut suhteellisen vähän valituksia, joissa väitetään lipunkirjoittajien tai lentoyhtiöiden loukanneen yksityisyyttä. Jos sellaisia tulee, ne tutkitaan edellä esitettyjen periaatteiden mukaisesti.

C. Liikenneministeriön tuottama oikeussuoja, josta EU:n kuluttajat hyötyvät

Sopimattomien ja vilpillisten käytäntöjen kieltä lentoliikennepalvelujen harjoittamisessa tai myynnissä sovelletaan 41712 §:n nojalla yhdysvaltalaisiin ja ulkomaisiin lentoliikenteen harjoittajiin ja lipunkirjoittajiin. Liikenneministeriö ryhtyy usein toimiin yhdysvaltalaisista tai ulkomaista lentoyhtiötä vastaan sellaisten käytäntöjen vuoksi, jotka koskevat sekä yhdysvaltalaisia että ulkomaisia kuluttajia ja joita lentoyhtiö on noudattanut tarjotessaan lentoliikennepalveluja Yhdysvaltoihin tai Yhdysvalloista. Liikenneministeriö aikoo jatkossakin ryhtyä kaikkiin käytettävissä oleviin korjaaviin toimenpiteisiin suojataksaan ulkomaisia ja yhdysvaltalaisia kuluttajia sääntelyn alaisten yksiköiden sopimattomilta ja vilpillisiltä käytännöiltä lentoliikennepalveluissa.

⁽¹⁾ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

⁽²⁾ Entinen Ilmailualan lainvalvonnasta ja oikeudellisista menettelyistä vastaava yksikkö.

⁽³⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

Liikenneministeriö valvoo lentoyhtiöiden osalta myös sitä, että kohdennettuja lakeja, joilla annetaan suojaa myös ei-yhdysvaltalaisille kuluttajille, noudatetaan. Tällainen laki on esimerkiksi COPPA-laki. COPPA-laissa asetetaan sivustojen ylläpitäjille muun muassa vaatimus, että ne antavat vanhemmille suunnatun ilmoituksen ja hankkivat näiltä todennettavissa olevan suostumuksen sellaisten verkkosivustojen ja -palveluiden osalta, jotka on suunnattu lapsille, sekä sellaisten yleisten, kaikille suunnattujen verkkosivustojen osalta, jotka tietoisesti keräävät henkilötietoja alle 13-vuotiailta lapsilta. Yhdysvaltalaisen verkkosivuston ja -palveluiden, joihin sovelletaan COPPA-lakia ja jotka keräävät henkilötietoja ulkomaisista lapsista, on noudatettava COPPA-lakia. Myös ulkomaisten verkkosivustojen ja -palveluiden on noudatettava COPPA-lakia, jos ne on suunnattu yhdysvaltalaisille lapsille tai jos ne tietoisesti keräävät henkilötietoja yhdysvaltalaisilta lapsilta. Jos yhdysvaltalaiset tai ulkomaiset lentoyhtiöt, jotka harjoittavat toimintaa Yhdysvalloissa, rikkovat COPPA-lakia, liikenneministeriöllä on toimivalta ryhtyä lainvalvontatoimiin.

II. EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamisen valvonta

Jos lentoyhtiö tai lipunkirjoittaja päättää osallistua EU:n ja Yhdysvaltojen tietosuojakehykseen ja liikenneministeriö vastaanottaa valituksen, jossa väitetään, että lentoyhtiö tai lipunkirjoittaja on rikkonut EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita, ministeriö toteuttaa määrätietoisesti seuraavat toimet varmistaakseen, että EU:n ja Yhdysvaltojen tietosuojakehystä noudatetaan.

A. Etusijan antaminen rikkomusväitteiden tutkinnalle

Liikenneministeriössä toimiva lentoliikenteen kuluttajansuojavirasto tutkii jokaisen valituksen, jossa väitetään, että EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita on rikottu (myös EU:n tietosuojaviranomaisilta vastaanotetut valitukset), ja ryhtyy lainvalvontatoimiin, jos ilmenee, että rikkomisesta on näytöä.

Lisäksi virasto tekee yhteistyötä liittovaltion kauppakomission ja kauppaministeriön kanssa ja antaa etusijan sellaisten väitteiden tutkimiselle, joiden mukaan sääntelyn alaiset yksiköt eivät noudata EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa tehtyä yksityisyyden suojaan liittyviä sitoumuksia.

Kun virastolle esitetään väite, jonka mukaan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita on rikottu, se voi ryhtyä monenlaisiin toimiin asian tutkimiseksi. Se voi esimerkiksi tarkastaa lipunkirjoittajan tai lentoyhtiön tietosuojaperiaatteet, hankkia lisätietoja lipunkirjoittajalta, lentoyhtiöltä tai kolmansilta osapuolilta, ryhtyä seurantatoimiin yhdessä valituksen toimittaneen yksikön kanssa ja arvioida, noudattaako rikkominen jotakin kaavaa tai koskeeko se huomattavaa määrää kuluttajia. Lisäksi se toteaa, onko asiassa elementtejä, jotka kuuluvat kauppaministeriön tai liittovaltion kauppakomission toimivaltaan, arvioi, olisiko kuluttajien tai yritysten kouluttaminen hyödyllistä, ja tarpeen mukaan panee vireille lainvalvontatoimia.

Jos ministeriö saa tiedon lipunkirjoittajien mahdollisista EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden rikkomisista, se koordinoi asiaa liittovaltion kauppakomission kanssa. Ministeriö ilmoittaa liittovaltion kauppakomissiolle ja kauppaministeriölle myös EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita koskevien lainvalvontatoimien tuloksista.

B. Puuttuminen totuudenvastaisiin tai vilpillisiin väitteisiin järjestelyyn osallistumisesta

Liikenneministeriö sitoutuu jatkossakin tutkimaan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden noudattamatta jättämistä, muun muassa totuudenvastaisia tai vilpillisiä väitteitä osallistumisesta EU:n ja Yhdysvaltojen tietosuojakehykseen. Ministeriö antaa etusijan kauppaministeriöstä tuleville valituksille, joissa se on todennut, että organisaatio väittää perusteettomasti osallistuvansa EU:n ja Yhdysvaltojen tietosuojakehykseen tai käyttää luvatta tietosuojakehyksen varmennusmerkkiä.

Lisäksi on todettava, että jos organisaatio sitoutuu noudattamaan EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteita tietosuojaperiaatteissaan, se, että organisaatio ei anna omaa varmennusta kauppaministeriössä tai että se laiminlyö varmennuksen voimassa pitämisen, ei sinänsä itsestään selvästi vapauta organisaatiota lainvalvontatoimilta, joihin liikenneministeriö ryhtyy organisaation antamien sitoumusten vuoksi.

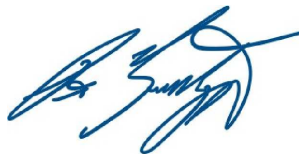
C. EU:n ja Yhdysvaltojen tietosuojakehyksen rikkomisen vuoksi annettujen täytäntöönpanomääräysten seuranta ja julkistaminen

Liikenneministeriössä toimiva lentoliikenteen kuluttajansuojavirasto sitoutuu myös jatkossa – kun tämä on tarpeen EU:n ja Yhdysvaltojen tietosuojakehyksen noudattamisen varmistamiseksi. Varsinkin siinä tapauksessa, että virasto antaa määräyksen, jonka mukaan lentoyhtiön tai lipunkirjoittajan on lopetettava EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteiden ja 41712 §:n rikkominen ja pidättäydyttävä siitä myös tulevaisuudessa, virasto valvoo, että kyseinen toimija noudattaa kieltomääräystä. Virasto pitää lisäksi huolen siitä, että EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteisiin liittyvissä asioissa annetut määräykset ovat saatavilla sen verkkosivustolla.

Odotamme innolla, että EU:n ja Yhdysvaltojen tietosuojakehystä koskeva yhteistyömme liittovaltion kumppanien ja EU:n sidosryhmien kanssa jatkuu.

Toivon, että tässä esitetyistä tiedoista on hyötyä. Annan mielelläni lisätietoja ja vastaan asiaa koskeviin kysymyksiin.

Kunnioittavasti



Pete BUTTIGIEG

LIITE VI



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

23. kesäkuuta 2023

Ana Gallego Torres
Oikeus- ja kuluttaja-asioiden pääosaston pääjohtaja
Euroopan komissio
Rue Montoyer/Montoyerstraat 59
1049 Bryssel
Belgia

Arvoisa pääjohtaja Gallego Torres,

Tässä kirjeessä esitetään lyhyt yhteenveto tärkeimmistä tutkintavälineistä, joiden avulla yhdysvaltalaisilta yrityksiltä saadaan liiketoimintaan liittyviä ja muita tietoja lainvalvontatarkoituksia ja (siviilioikeudellisen ja sääntelyyn liittyvän) yleisen edun nimissä. Kirjeessä kerrotaan myös tietoihin pääsyä koskevista rajoituksista, jotka oikeusperustassa on määrätty. ⁽¹⁾ Kaikki tässä kirjeessä selostetut oikeudelliset menettelyt ovat syrjimättömiä siinä mielessä, että niitä käytetään tietojen hankkimiseksi yrityksiltä Yhdysvalloissa, myös sellaisilta yrityksiltä, jotka antavat oman varmennuksensa EU:n ja Yhdysvaltojen tietosuojakehyksessä, eikä rekisteröidyn kansalaisuudella tai asuinpaikalla ole merkitystä. Yhdysvaltojen perustuslain neljännellä lisäyksellä on erityistä merkitystä viranomaisten takavarikoidessa tietoja. Lisäyksessä säädetään seuraavaa: ⁽²⁾

Yhdysvaltojen perustuslain neljännellä lisäyksellä on erityistä merkitystä viranomaisten takavarikoidessa tietoja. Lisäyksessä säädetään seuraavaa: "Kansalaisten oikeutta olla turvassa henkilöönsä, taloonsa, asiakirjoihinsa ja muuhun omaisuuteensa kohdistuvilta kohtuuttomilta etsinnöiltä ja takavarikoinneilta älköön loukattako, älköönkä etsintälupaa annettako muutoin kuin todennäköisestä syystä, joka on vahvistettu valalla tai juhlallisella vakuutuksella, ja etsintäluvassa on erityisesti mainittava etsinnän tapahtumapaikka sekä pidätettävät henkilöt ja takavarikoitavat esineet." Yhdysvaltojen perustuslaki, neljäs lisäys. Yhdysvaltojen korkein oikeus totesi asiassa *Berger v. New Yorkin osavaltio* seuraavaa: "kuten tämä tuomioistuim on lausunut lukemattomia kertoja, tämän lisäyksen perustarkoituksena on suojella kansalaisten yksityisyyttä ja turvallisuutta viranomaisten mielivaltaista tunkeutumista vastaan". Ks. 388 U.S. 41, 53 (1967) (asiassa on viittaus tapaukseen *Camara v. San Franciscon kaupungin tuomioistuin*, 387 U.S. 523, 528 (1967)). Neljännessä lisäyksessä edellytetään, että lainvalvontaviranomaisten on kotimaisissa rikostutkimuksissa yleensä hankittava tuomioistuimelta etsintälupa ennen etsinnän toteuttamista. Ks. *Katz v. Yhdysvallat*, 389 U.S. 347, 357 (1967). Etsintäluvan antamista koskevia normeja, kuten todennäköistä syytä ja erityisyyttä koskevia vaatimuksia, sovelletaan fyysistä etsintää ja

⁽¹⁾ Tässä tiivistelmässä ei selosteta kansalliseen turvallisuuteen liittyviä tutkintavälineitä, joita lainvalvonnassa käytetään terrorismia koskeissa tai muissa kansalliseen turvallisuuteen liittyvissä tutkimuksissa. Näin ollen tässä ei selosteta esimerkiksi kansallista turvallisuutta koskevia kirjeitä, joilla hankitaan tiettyjä yritysten lainakertomuksissa, kirjanpidoissa ja sähköisissä tilausasiakas- ja liiketapahtumarekistereissä olevia tietoja, 12 U.S.C. § 3414; 15 U.S.C. 1681u §; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, FISA-lain nojalla tehtävistä toimista (sähköinen tarkkailu, etsintäluvat, liiketoimintatietojen hankkiminen ja muu tietojen kerääminen), ks. 50 U.S.C. § 1801 ja sitä seuraavat pykälät.

⁽²⁾ Tässä kirjeessä käsitellään liittovaltion lainvalvonta- ja sääntelyviranomaisia. Osavaltioiden lainvalvontaviranomaiset tutkivat osavaltioiden lakien rikkomiset, ja niitä koskevat asiat käsitellään osavaltioiden tuomioistuimissa. Osavaltioiden lainvalvontaviranomaiset käyttävät etsintämääräyksiä ja haasteita, jotka annetaan osavaltioiden lakien mukaisesti. Tämä tapahtuu suurimmaksi osaksi samalla tavalla kuin tässä kirjeessä selostetaan, mutta erona on, että oikeudellista menettelyä koskeva suoja, jota annetaan osavaltioiden perustuslakien mukaan, voi mennä pidemmälle kuin Yhdysvaltojen perustuslaissa annettu suoja. Osavaltion laissa säädettyjen suojatoimenpiteiden on oltava vähintään yhtä kattavia kuin Yhdysvaltojen perustuslaissa määrätty suojatoimet, ja tämä koskee myös perustuslain neljättä lisäystä (mutta ei rajoitu siihen).

takavarikointia koskeviin lupiin sekä tallennettua viestintää koskevan lain nojalla annettuihin sähköisen viestinnän tallennettua sisältöä koskeviin lupiin, kuten jäljempänä on selostettu. Kun etsintä lupavaatimusta ei sovelleta, hallituksen on silti noudatettava toimissaan neljännen lisäyksen edellyttämää ”kohtuutta”. Näin ollen perustuslaissa itsessään varmistetaan, että Yhdysvaltojen hallituksen valta takavarikoida kansalaisten tietoja ei ole rajatonta tai mielivaltaista. ⁽³⁾

Lainvalvontaviranomaiset:

Liittovaltion syyttäjät, jotka ovat oikeusministeriön virkamiehiä, ja liittovaltion tutkijat, mukaan lukien oikeusministeriön alaisen lainvalvontaviraston FBI:n tutkijat, voivat velvoittaa yhdysvaltalaiset yritykset luovuttamaan asiakirjoja ja muita tietoja rikostutkintaa varten hyödyntämällä useita pakollisia oikeudellisia menettelyjä. Näitä ovat suuren valamiehistön haasteet, hallinnolliset haasteet ja etsintäluvut. Muita viestintätietoja voidaan hankkia sellaisten rikostutkimuksia koskevien liittovaltion oikeudellisten välineiden nojalla, jotka liittyvät lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiin.

Suuren valamiehistön haaste tai tuomioistuinhaaste: Rikosoikeudellisia haasteita käytetään kohdennettujen lainvalvontatutkimusten tukena. Suuren valamiehistön haaste on virallinen kehoitus avustaa valamiehistöä tutkimuksessa, joka koskee tiettyä rikoslain rikkomusepäilyä. Haaste annetaan tavallisesti liittovaltion syyttäjän pyynnöstä. Suuret valamiehistöt kuuluvat tuomioistuimen tutkintahaaraan, ja niiden jäsenet valitsee tuomari tai avustava tuomari. Haasteessa voidaan vaatia, että henkilö todistaa menettelyssä tai luovuttaa liiketoimintatietoja, sähköisesti tallennettua tietoa tai muita aineellisia esineitä. Tietojen tulee olla merkityksellisiä tutkimuksen kannalta. Haaste ei saa olla kohtuuton eli laajuudeltaan ja rasittavuudeltaan liiallinen. Haasteen vastaanottaja voi vastustaa haastetta esittämällä näihin seikkoihin perustuvan väitteen. Ks. liittovaltion rikosprosessisääntöjen kohta 17. Sen jälkeen, kun asia on tullut suuren valamiehistön käsittelyyn, asiakirjojen hankkimiseksi voidaan rajoitetuissa olosuhteissa käyttää tuomioistuinhaastetta.

Hallinnollisiin haasteisiin liittyvät valtuudet: Hallinnollista haastetta voidaan käyttää rikosoikeudellisissa tai siviilioikeudellisissa tutkimuksissa. Useissa liittovaltion laeissa säädetään hallinnollisten haasteiden käyttämisestä rikoslain täytäntöönpanon yhteydessä. Tällöin on kyse tutkimuksista, jotka koskevat terveydenhuoltoalan petoksia, lasten kaltoinkohtelua, salaisen palvelun turvatoimia tai valvottuja aineita, tai kyse on valvontaviranomaisen tutkimuksista, jotka kohdistuvat hallituksen virastoihin. Näissä tutkimuksissa voidaan vaatia luovuttamaan tutkinnan kannalta merkityksellisiä liiketoimintatietoja, sähköisesti tallennettua tietoa tai muita aineellisia esineitä. Jos viranomaiset hakevat tuomioistuimelta hallinnollisen haasteen vahvistamista, haasteen vastaanottaja voi – aivan kuten suuren valiokunnan haasteen vastaanottaja – esittää väitteen, jonka mukaan haaste on kohtuuton eli laajuudeltaan ja rasittavuudeltaan liiallinen.

Tuomioistuimen määräykset, jotka liittyvät lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiin: Sellaisten rikosoikeussäännösten nojalla, jotka koskevat lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiin liittyviä lupia, lainvalvontaviranomaiset voivat hankkia tuomioistuimen määräyksen, jolla ne voivat – vahvistettuaan, että tiedot ovat tarpeen meillä olevassa rikostutkimuksessa – saada tiettyä puhelinnumeroa tai sähköpostiosoitetta koskevaa reaaliaikaista, ei-sisällöllistä numeronvalinta-, reititys-, osoitteenmuodostus- ja merkinantotietoa. Ks. 18 U.S.C. 3121–3127 §. Tällaisen välineen asentaminen tai käyttäminen muuten kuin lain mukaisesti on liittovaltion rikos.

Laki sähköisen viestinnän tietosuojasta (Electronic Communications Privacy Act): Viranomaisten pääsystä internetpalveluntarjoajien, puhelinyhtiöiden ja muiden kolmansien osapuolten tilausasiakastietoihin, tietoliikennetietoihin ja viestinnän tallennettuun sisältöön on omat sääntönsä. Ne ovat sähköisen viestinnän tietosuojasta annetun lain II osastossa, jota kutsutaan myös tallennettua viestintää koskevaksi laiksi, ks. 18 U.S.C. 2701–2712 §. Laissa säädetään yksityisyyden suojan järjestelmästä, jossa rajoitetaan lainvalvontaviranomaisten pääsyä tietoihin siten, että se ei voi ulottua pidemmälle kuin mitä perustuslaillisten säännösten nojalla vaaditaan internetpalveluntarjoajien asiakkailta ja tilausasiakkailta. Lain mukaan yksityisyyden suoja kasvaa sitä mukaa kuin tiedonkeruun häiritsevyys lisääntyy. Lainvalvontaviranomaisten on hankittava haaste, jos he haluavat saada tilausasiakkaiden rekisteröintitietoja, internetprotokolla- eli IP-osoitteita ja niihin liittyviä

⁽³⁾ Mitä tulee edellä käsiteltyihin neljännen lisäyksen mukaisiin periaatteisiin, jotka koskevat yksityisyyteen ja turvallisuuteen liittyvien etujen suojaamista, yhdysvaltalaiset tuomioistuimet soveltavat näitä periaatteita säännöllisesti teknologian kehityksen mahdollistamiin lainvalvontaviranomaisten uudentyyppisiin tutkintavälineisiin. Korkein oikeus päätti esimerkiksi vuonna 2018, että kun hallitus hankkii lainvalvontaan liittyvässä tutkimuksessa matkapuhelinyhtiöltä pidemmän ajanjakson historiallisia sijaintitietoja, kyseessä on ”etsintä”, johon sovelletaan neljännen lisäyksen sisältämää etsintä lupavaatimusta. *Carpenter v. Yhdysvallat*, 138 S. Ct. 2206 (2018).

aikaleimoja tai laskutustietoja. Useimpien muiden tallennettujen, ei-sisällöllisten tietojen osalta, kuten sellaisten sähköpostiotsikoiden osalta, joista ei ilmene viestin aihe, lainvalvontaviranomaisten on esitettävä tuomarille erityisiä seikkoja, jotka osoittavat, että pyydytetyt tiedot ovat merkityksellisiä ja olennaisia vireillä olevan rikostutinnan kannalta. Jotta lainvalvontaviranomaiset voivat saada pääsyn sähköisen viestinnän tallennettuun sisältöön, niiden on yleensä hankittava tuomarilta määräys sillä perusteella, että on perusteltu syy uskoa kyseisellä tilillä todennäköisesti olevan todisteita rikoksesta. Tallennettua viestintää koskevassa laissa säädetään myös siviili- ja rikosoikeudellisista seuraamuksista. ⁽⁴⁾

Tarkkailua koskevat tuomioistuimen määräykset puhelinkuuntelua koskevan liittovaltion lain nojalla: Lisäksi lainvalvontaviranomaiset voivat rikostutkintaa varten salakuunnella reaaliaikaisesti langallista, suullista tai sähköistä viestintää puhelinkuuntelua koskevan liittovaltion lain nojalla. Ks. 18 U.S.C. 2510–2523 §. Tämän välineen käyttäminen edellyttää aina tuomioistuimen määrystä. Tuomarin on siinä tultava muun muassa johtopäätökseen, jonka mukaan on todennäköisiä syitä uskoa, että langallisen tai sähköisen salakuuntelun avulla saadaan todisteita liittovaltion rikoksesta tai syytettyä välttelevän etsintäkuulutetun olinpaikasta. Laissa säädetään siviilioikeudellisista ja rikosoikeudellisista seuraamuksista, jos salakuuntelua koskevia säännöksiä rikotaan.

Etsintälupa – Liittovaltion rikosprosessisääntöjen kohta 41: Yhdysvalloissa lainvalvontaviranomaiset voivat tutkia kiinteistön fyysisesti, jos niillä on siihen tuomarin antama lupa. Lainvalvontaviranomaisten on osoitettava tuomarille todennäköisin syin, että rikos on tapahtunut tai on tapahtumassa ja että rikokseen liittyvää on todennäköisesti löydettävissä etsintäluvassa yksilöidystä paikasta. Tätä välinettä käytetään usein silloin, kun kiinteistön fyysinen tutkiminen on tarpeen sillä perusteella, että jos haaste tai muu tietojen toimittamista koskeva määräys annettaisiin tiedoksi yritykselle, syntyisi vaara todisteiden hävittämisestä. Henkilö, johon kohdistuu etsintä tai jonka omaisuutta etsintä koskee, voi vaatia, että laittomalla etsinnällä saadut todisteet hylätään, jos nämä todisteet esitetään häntä vastaan rikosoikeudenkäynnissä. Ks. *Mapp v. Ohio*, 367 U.S. 643 (1961). Kun tietojen haltijaa vaaditaan oikeuden määräyksen nojalla antamaan tiedot, tähän veloitettu osapuoli voi riitauttaa vaatimuksen kohtuuttomana rasitteena. Ks. Yhdysvaltojen lain soveltamisesta 610 F.2d 1148, 1157 (3d Cir. 1979) (tuomion mukaan asianmukainen menettely edellyttää kuulemisen pitämistä rasitteesta ennen kuin puhelinyhtiö veloitetaan tukemaan etsintää) ja Yhdysvaltojen lain soveltamisesta 616 F.2d 1122 (9th Cir. 1980) (tuomiossa päädytään samaan johtopäätökseen tuomioistuimen valvontavaltuuksista).

Oikeusministeriön suuntaviivat ja toimintaperiaatteet: Sen lisäksi, että perustuslaissa ja tavallisissa laeissa sekä vahvistetuissa säännöissä rajoitetaan edellä selostetulla tavalla viranomaisten pääsyä tietoihin, oikeusministeri on vahvistanut suuntaviivoja, joissa asetetaan lisärajoituksia lainvalvontaviranomaisten pääsyle tietoihin ja joihin sisältyy myös yksityisyyden ja kansalaisvapauksien suojaan liittyviä toimia. Esimerkiksi oikeusministerin vahvistamissa, FBI:n kotimaisia operaatioita koskeissa yleisissä suuntaviivoissa syyskuulta 2008 (saatavilla osoitteessa <http://www.justice.gov/archive/opa/docs/guidelines.pdf>) asetetaan rajoituksia tutkintamenetelmien käytölle etsittäessä tietoa, joka liittyy liittovaltion rikosten tutkintaan. Näissä suuntaviivoissa edellytetään, että FBI käyttää tutkintamenetelmiä, jotka häiritsevät niin vähän kuin mahdollista ja joissa otetaan huomioon vaikutukset yksityisyyteen ja kansalaisvapauksiin ja mahdolliset vahingot henkilön maineelle. Lisäksi suuntaviivojen mukaan on selvää, että FBI:n on toteutettava tutkimuksensa ja muut toimensa lainmukaisella ja kohtuullisella tavalla, jossa kunnioitetaan vapautta ja yksityisyyttä ja jossa vältetään aiheuttamasta tarpeetonta häiriötä lainkuuliaisille ihmisille. Ks. FBI-suuntaviivojen sivu 5. FBI on pannut nämä suuntaviivat täytäntöön antamalla ohjeen, joka koskee viraston kotimaisia tutkimuksia ja operaatioita (saatavilla osoitteessa <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>). Tämä on kattava käsikirja, joka sisältää tutkimusvälineiden käyttöä koskevat yksityiskohtaiset rajoitukset ja ohjeistusta sen varmistamiseksi, että jokaisessa tutkimuksessa suojellaan kansalaisvapauksia ja yksityisyyttä. Muita sääntöjä ja toimintaperiaatteita, joilla rajoitetaan liittovaltion syyttäjien tutkimustoimia, on selostettu oikeudenkäytön käsikirjassa, joka on saatavilla osoitteessa <https://www.justice.gov/jm/justicemanual>.

Siviilihallinto- ja sääntelyviranomaisten (yleisen edun mukaiset) valtuudet:

⁽⁴⁾ Lisäksi sähköisen viestinnän tietosuojasta annetun lain 2705 §:n b momentissa annetaan hallitukselle lupa hankkia tuomioistuimen määräys, joka perustuu todistettuun tarpeeseen suojautua paljastamiselta ja jossa kielletään viestintäpalvelujen tarjoajaa ilmoittamasta vapaaehtoisesti käyttäjilleen kyseisen lain mukaisen oikeudellisen menettelyn kohteeksi joutumisesta. Varaoikeusministeri Rod Rosenstein laati lokakuussa 2017 oikeusministeriön asianajajille ja edustajille muistion, jossa annetaan ohjeita sen varmistamiseksi, että tällaisia turvaamismääräyksiä koskevat hakemukset räätälöidään tutkinnan erityisten tosiseikkojen ja huolenaiheiden mukaan, sekä vahvistetaan yleinen yhden vuoden enimmäisaika sille, kuinka kauan hakemuksella voidaan pyrkiä viivyttämään ilmoitusta. Toukokuussa 2022 varaoikeusministeri Lisa Monaco antoi aihetta koskevia lisäohjeita, joissa muun muassa vahvistettiin sisäiset oikeusministeriön hyväksymisvaatimukset hakemuksille, jotka koskevat turvaamismääräyksen jatkamista alkuperäisen vuoden pituisen ajanjakson jälkeen, ja edellytettiin turvaamismääräysten soveltamisen päättämistä tutkinnan päättyessä.

Yhdysvalloissa on asetettu merkittäviä rajoituksia myös sille, miten siviilihallintoon ja sääntelyyn liittyvien (ns. yleisen edun mukaisten) syiden nojalla voidaan vaatia tietoja yrityksiltä. Virastot, joilla on siviilihallinto- ja sääntelytehtäviä, voivat toimittaa yrityksille haasteita, joissa ne vaativat luovuttamaan liiketoimintatietoja, sähköisesti tallennettua tietoa tai muita aineellisia esineitä. Näiden virastojen toimivaltaa esittää hallinnollisia tai siviilihallinnollisia haasteita on rajattu. Tämä johtuu paitsi virastojen perustamissäännöksistä myös siitä, että haasteet tarkastetaan riippumattomassa oikeudellisessa menettelyssä ennen niiden mahdollista oikeudellista täytäntöönpanoa. Ks. esimerkiksi liittovaltion rikosprosessisääntöjen kohta 45. Virastot voivat pyytää pääsyä ainoastaan tietoihin, joilla on merkitystä virastojen sääntelytoimivaltaan kuuluvissa asioissa. Lisäksi hallinnollisen haasteen vastaanottaja voi nostaa kanteen tuomioistuimessa ja vastustaa haasteen täytäntöönpanoa esittämällä näyttöä, jonka mukaan virasto ei ole noudattanut perusvaatimusten mukaista kohtuullisuutta, kuten edellä on selostettu.

On olemassa muita oikeusperustoja, joihin vedoten yritykset voivat vastustaa hallinnollisten virastojen tietopyyntöjä ja joissa on kyse siitä, että yritykset toimivat tietyillä erityisillä aloilla ja että niiden hallussa oleva tieto on tietyn tyyppistä. Esimerkiksi rahoituslaitokset voivat vastustaa hallinnollisia haasteita, joissa vaaditaan tietynlaisia tietoja, sillä perusteella, että tietojen luovutuksella rikottaisiin pankkisalaisuudesta annettua lakia ja sen täytäntöönpanoasetuksia. 31 U.S.C. 5318 §. 31 C.F.R. X luku. Muut yritykset voivat tukeutua luottokelpoisuusraportointia koskevaan Fair Credit Reporting Act -lakiin (15 U.S.C. § 1681b) tai moniin muihin alakohtaisiin lakeihin. Jos viraston haastetoimivaltaa käytetään väärin, seurauksena voi olla viraston vahingonkorvausvastuu tai ao. virkamiesten henkilökohtainen vahingonkorvausvastuu. Ks. esimerkiksi kansalaisten pankkitietoja koskeva Right to Financial Privacy Act -laki, 12 U.S.C. §§ 3401–3423. Näin ollen Yhdysvaltojen tuomioistuimet valvovat, että sääntelyhaastepyyntöt ovat asiallisia, ja valvovat riippumattomasti liittovaltion virastojen toimia.

Lopuksi on todettava, että kaikkien lakisääteisten valtuuksien, jotka hallintoviranomaisilla on tietojen fyysiseen takavarikoimiseen yritykseltä Yhdysvalloissa, on oltava neljänteen lisäykseen perustuvien vaatimusten mukaisia. Ks. See v. Seattlen kaupunki, 387 U.S. 541 (1967).

Loppupäätelmä:

Kaikkien lainvalvonta- ja sääntelytoimintojen on noudatettava sovellettavaa lainsäädäntöä Yhdysvalloissa, mukaan lukien perustuslakia, lakeja, sääntöjä ja asetuksia. Toiminnoissa on myös noudatettava sovellettavia toimintaperiaatteita, kuten liittovaltion lainvalvontatoimia koskevia oikeusministerin suuntaviivoja. Edellä kuvatussa lainsäädännössä rajoitetaan Yhdysvaltojen lainvalvonta- ja sääntelyviranomaisten mahdollisuuksia hankkia tietoja yrityksiltä Yhdysvalloissa – koskivatpa ne Yhdysvaltojen tai muiden maiden kansalaisia – ja lisäksi annetaan mahdollisuus siihen, että kaikki viranomaisten tietopyyntöt, jotka perustuvat laissa myönnettyihin valtuuksiin, voidaan saattaa oikeudellisen valvonnan kohteeksi tuomioistuimessa.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

LIITE VII

KANSALLISEN TIEDUSTELUVIRASTON PÄÄLAKIMIEHEN TOIMISTO

WASHINGTON, DC 20511

9. joulukuuta 2022

Leslie B. Kiernan,
päälakimies
U.S. Department of
Commerce 1401 Constitution
Ave., NW Washington, DC 20230

Arvoisa Leslie B. Kiernan,

Presidentti Biden allekirjoitti 7. lokakuuta 2022 toimeenpanoasetuksen 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, joka tukee Yhdysvaltojen signaalitiedustelutoimintaan sovellettavia yksityisyyden suojaa ja kansalaisvapauksia koskevia tiukkoja suojoitoimia. Tällaisia suojoitoimia ovat seuraavat: signaalitiedustelutoiminnan edellytetään täyttävän luetellut oikeutetut tavoitteet, tällainen toiminta kielletään nimenomaisesti, jos tarkoituksena on tiettyjen kiellettyjen tavoitteiden saavuttaminen, otetaan käyttöön uudenlaisia menettelyjä sen varmistamiseksi, että signaalitiedustelutoiminta edistää näitä oikeutettuja tavoitteita eikä kiellettyjä tavoitteita, vaaditaan, että signaalitiedustelutoimintaa toteutetaan ainoastaan sen jälkeen, kun on kaikkien olennaisten tekijöiden kohtuullisen arvioinnin perusteella todettu, että toiminta on tarpeen jotakin tiedustelutoiminnan validoitua painopistettä varten, ja ainoastaan siinä laajuudessa ja tavalla, joka on oikeassa suhteessa siihen tiedustelutoiminnan validoituun painopisteeseen, jota varten se on hyväksytty, sekä ohjataan tiedusteluyhteisön yksiköjä päivittämään periaatteitaan ja menettelyjään siten, että ne vastaavat toimeenpanoasetuksen edellyttämiä signaalitiedustelutoiminnan suojoitoimia. Merkittävintä on, että toimeenpanoasetuksella otetaan myös käyttöön riippumaton, sitova mekanismi, jonka avulla toimeenpanoasetuksen mukaisesti nimetyistä, vaatimukset täyttävistä valtioista tulevat henkilöt voivat hakea muutosta, jos he uskovat joutuneensa Yhdysvaltojen lainvastaisen signaalitiedustelutoiminnan kohteeksi, mukaan lukien toiminta, joka rikkoo toimeenpanoasetuksessa vahvistettuja suojoitoimia.

Presidentti Bidenin antama toimeenpanoasetus 14086 muodosti päätöspisteen Euroopan komission ja Yhdysvaltojen edustajien välisille, yli vuoden kestäneille yksityiskohtaisille neuvotteluille, ja ohjaa toimia, joita Yhdysvallat aikoo toteuttaa pannakseen täytäntöön EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa antamansa sitoumukset. Tietosuojakehyksen laatimista edistäneen yhteistyöhengen mukaisesti olen ymmärtänyt, että olette saanut Euroopan komissiolta kaksi kysymyskokonaisuutta siitä, miten tiedusteluyhteisö aikoo panna toimeenpanoasetuksen täytäntöön. Käsittelen mielelläni näitä kysymyksiä tässä kirjeessä.

Ulkomaantiedustelun valvontaa koskevan vuoden 1978 lain (Foreign Intelligence Surveillance Act of 1978, FISA-laki) 702 §

Ensimmäinen kysymyskokonaisuus koskee FISA-lain 702 §:ää, joka mahdollistaa ulkomaisten tiedustelutietojen keräämisen kohdistamalla tiedustelutoimintaa muihin kuin yhdysvaltalaisiin henkilöihin, joiden voidaan kohtuudella olettaa oleskelevan Yhdysvaltojen ulkopuolella, siten, että sähköisten viestintäpalvelujen tarjoajia veloitetaan avustamaan tässä. Kysymykset koskevat erityisesti kyseisen säännöksen ja toimeenpanoasetuksen 14086 välistä vuorovaikutusta sekä muita suojoitoimia, joita sovelletaan FISA-lain 702 §:n nojalla harjoitettavaan toimintaan.

Ensinnäkin voimme vahvistaa, että tiedusteluyhteisö soveltaa toimeenpanoasetuksessa 14086 vahvistettuja suojoitoimia FISA-lain 702 §:n mukaisiin toimiin.

Lisäksi hallituksen FISA-lain 702 §:n käyttöön sovelletaan lukuisia muita suojatoimia. Kaikkiin FISA-lain 702 §:n mukaisiin sertifiointipäätöksiin on esimerkiksi saatava sekä oikeusministerin että kansallisen tiedusteluviraston (DNI) johtajan allekirjoitus, ja hallituksen on toimitettava kaikki tällaiset sertifiointipäätökset ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen (FISC) hyväksyttäväksi. Tuomioistuin koostuu riippumattomista tuomareista, joiden toimikausi, jota ei voi uusia, kestää seitsemän vuotta mutta joilla on elinikäinen oikeus pysyä tuomarin virassaan. Sertifiointipäätöksissä yksilöidään kerättävien ulkomaantiedustelutietojen luokat. Tietojen, jotka kerätään kohdistamalla tiedustelutoimintaa muihin kuin yhdysvaltalaisiin henkilöihin, joiden voidaan kohtuudella olettaa oleskelevan Yhdysvaltojen ulkopuolella, on vastattava ulkomaantiedustelutietojen lakisääteistä määritelmää. Sertifiointipäätöksissä on ollut tietoa kansainvälisestä terrorismista ja muista aiheista, kuten joukkotuhoaseita koskevan tiedon hankkimisesta. Jokainen vuosittainen sertifiointipäätös on toimitettava FISC-tuomioistuimen hyväksyttäväksi sertifiointipäätösten hakemuspaketissa, joka sisältää oikeusministerin ja kansallisen tiedusteluviraston sertifiointipäätökset, tiettyjen tiedusteluvirastojen johtajien valahtoiset todistukset ja hallitusta sitovat kohdentamismenettelyt, minimointimenettelyt ja kyselymenettelyt. Kohdentamismenettelyissä edellytetään muun muassa, että tiedusteluyhteisö arvioi kohtuudella kaikkien olosuhteiden perusteella, että kohdentamisella kerätään todennäköisesti FISA-lain 702 §:n mukaisessa sertifiointipäätöksessä yksilöityä ulkomaantiedustelutietoa.

Lisäksi kerätessään tietoja FISA-lain 702 §:n nojalla tiedusteluyhteisön on annettava kirjallinen selvitys siitä, millä perusteella arvioidaan, että kohdentamishetkellä kohteella odotetaan olevan hallussaan tai sen odotetaan vastaanottavan tai todennäköisesti välittävän FISA-lain 702 §:n mukaisessa sertifiointipäätöksessä yksilöityä ulkomaantiedustelutietoa, vahvistettava, että FISA-lain 702 §:ssä säädettyissä kohdentamismenettelyissä vahvistettu kohdentamisvaatimus täyttyy edelleen, ja lopetettava kerääminen, jos vaatimus ei enää täyty. Ks. Yhdysvaltojen hallituksen ilmoitus FISC-tuomioistuimelle (U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 *Summary of Notable Section 702 Requirements*), s. 2 ja 3 (15. heinäkuuta 2015).

Koska tiedusteluyhteisön on kirjattava arvionsa, jonka mukaan FISA-lain 702 §:n mukaiset tavoitteet täyttävät sovellettavat kohdentamisvaatimukset, ja vahvistettava säännöllisesti arvion validiteetti, FISC-tuomioistuin on helpompaa valvoa tiedusteluyhteisön kohdentamistoimia. Oikeusministeriön tiedusteluvalvonnasta vastaavat asianajajat tarkastelevat jokaista kirjattua kohdentamisarviointia ja perustelua kahden kuukauden välein. Nämä asianajajat suorittavat tätä valvontaa ulkomaantiedusteluoperaatioista riippumatta. Tätä tehtävää hoitava oikeusministeriön osasto vastaa vakiintuneen FISC-säännön mukaisesti siitä, että FISC-tuomioistuimelle ilmoitetaan sovellettavien menettelyjen mahdollisista rikkomisista. Tämän raportoinnin sekä FISC-tuomioistuimen ja tämän oikeusministeriön osaston välisten säännöllisten tapaamisten, joissa käsitellään FISA-lain 702 §:n mukaisen kohdentamisen valvontaa, avulla FISC-tuomioistuin voi valvoa, että kohdentamisessa ja muissa menettelyissä noudatetaan FISA-lain 702 §:ää, ja muutoin varmistaa, että hallituksen toiminta on lainmukaista. FISC-tuomioistuin voi tehdä tämän monella tavalla, muun muassa tekemällä sitovia korjaavia päätöksiä, joilla perutaan hallituksen toimivalta kerätä tietoja tietyistä kohteista tai muuttaa tai lykätä FISA-lain 702 §:n mukaista tiedonkeruuta. FISC-tuomioistuin voi myös vaatia hallitusta raportoimaan tai tiedottamaan tarkemmin siitä, miten se noudattaa kohdentamis- ja muita menettelyjä, tai vaatia muutoksia näihin menettelyihin.

Signaalitiedustelutiedon valikoimaton keruu

Toinen kysymyskokonaisuus koskee signaalitiedustelutiedon valikoimatonta keruuta, joka on toimeenpanoasetuksessa 14086 määritelty seuraavasti: sellaisen signaalitiedustelutiedon suuren määrän luvallinen keruu, joka teknisistä tai operationaalisista syistä tehdään käyttämättä erottelutekijöitä (esimerkiksi erityisiä tunnisteita tai valintakriteerejä).

Näistä kysymyksistä toteamme ensiksi, että valikoimatonta keruuta ei sallita FISA-laissa eikä kansallista turvallisuutta koskevilla kirjeillä. FISA-lain osalta voidaan todeta seuraavaa:

- FISA-lain I osastossa säädetään sähköisen tarkkailun ja III osastossa koti- tai paikanetsinnän luvallisuudesta. Kummassakin osastossa edellytetään tuomioistuimen määräystä (tietyin poikkeuksin, kuten hätätilanteissa) ja vaaditaan aina, että on oltava perusteltu syy olettaa kohteen olevan vieras valta tai vieraan vallan asiamies. Ks. 50 U.S.C. 1805–1824 §.
- Yhdysvaltojen FREEDOM Act -lailla muutettiin vuonna 2015 FISA-lain IV osastoa, jossa sallitaan lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien (pen registers, trap and trace devices) käyttö tuomioistuimen määräyksen nojalla (paitsi hätätilanteissa), siten, että hallituksen on nyt perusteltava pyynnöt ”erityisen valintakriteerin” avulla. Ks. 50 U.S.C. 1842 §:n c momentin 3 kohta.

- FISA-lain V osastossa, jonka mukaan Yhdysvaltojen liittovaltion poliisi (FBI) voi hankkia tietyn tyyppisiä liiketoimintatietoja, edellytetään tuomioistuimen määräystä, joka perustuu hakemukseen, jossa todetaan, että on olemassa erityisiä ja ymmärrettäviä tosiseikkoja, joiden perusteella on syytä uskoa, että tietoihin liittyvä henkilö on vieras valta tai vieraan vallan asiamies. Ks. 50 U.S.C. 1862 §:n b momentin 2 kohdan B alakohta ⁽¹⁾.
- Lopuksi voidaan todeta, että FISA-lain 702 §:n mukaan ulkomaantiedustelutietojen hankinnan kohteena voi olla henkilöjä, joiden voidaan kohtuudella uskoa olevan Yhdysvaltojen ulkopuolella. Ks. 50 U.S.C. 1881a §:n a momentti. Kuten yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaava lautakunta on todennut, hallituksen FISA-lain 702 §:n nojalla toteuttama tietojenkeruu koostuu yksinomaan yksittäisiin henkilöihin kohdistuvista toimista ja sellaisen viestinnän hankkimisesta, joka liittyy näihin henkilöihin, joilta hallituksella on syytä olettaa saavansa tietynlaista ulkomaantiedustelutietoa, niin että ohjelmassa ei toimita keräämällä viestintää valikoimatta. Yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan kertomus FISA-lain 702 §:n nojalla toteutetusta tarkkailuohjelmasta (*Privacy and Civil Liberties Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 103 (2.7.2014)). ⁽²⁾

Vuoden 2015 FREEDOM Act -laissa säädetään kansallista turvallisuutta koskevien kirjeiden osalta erityisestä valintakriteeristä, jota vaaditaan tällaisten kirjeiden käyttämiseksi. Ks. 12 U.S.C. 3414 §:n a momentin 2 kohta; 15 U.S.C. 1681u §; 15 U.S.C. 1681v §:n a momentti; 18 U.S.C. 2709 §:n b momentti.

Lisäksi toimeenpanoasetuksessa 14086 säädetään, että kohdennettu keruu on asetettava etusijalle ja että kun tiedusteluyhteisö toteuttaa valikoimatonta keruuta, signaalitiedustelutiedon valikoimaton keruu on sallittua vain, jos on määritetty..., että jotakin tiedustelutoiminnan validoitua painopistettä varten tarvittavia tietoja ei voida kohtuudella saada kohdennetulla keruulla. Ks. EO 14086 2 §:n c momentin ii kohdan A alakohta.

Lisäksi kun tiedusteluyhteisö toteaa, että valikoimaton keruu täyttää nämä vaatimukset, toimeenpanoasetuksessa 14086 säädetään lisäsuojatoimista. Toimeenpanoasetuksessa edellytetään erityisesti, että valikoimatonta keruuta toteuttaessaan tiedusteluyhteisö soveltaa kohtuullisia menetelmiä ja teknisiä toimenpiteitä kerättävien tietojen rajaamiseksi vain siihen, mikä on tarpeen tiedustelutoiminnan validoidun painopisteen puitteissa siten, että samalla minimoidaan asiaankuulumattomien tietojen kerääminen. Ks. *sama* säädös. Asetuksessa säädetään myös, että signaalitiedustelutoimintaa, johon kuuluu valikoimattoman keruun avulla saatujen signaalitiedustelutietojen kysely, toteutetaan ainoastaan sen jälkeen, kun on kaikkien olennaisten tekijöiden kohtuullisen arvioinnin perusteella todettu, että toiminta on tarpeen tiedustelutoiminnan validoidun painopisteen puitteissa. Ks. *saman säädöksen* 2 §:n a momentin ii kohdan A alakohta. Asetuksessa tämä periaate on pantu täytäntöön myös toteamalla, että tiedusteluyhteisö voi tehdä kyselyjä valikoimatta hankituista ei-minimoiduista signaalitiedustelutiedoista ainoastaan kuuden sallitun tavoitteen puitteissa ja että tällaiset kyselyt on tehtävä sellaisten periaatteiden ja menettelyjen mukaisesti, joissa otetaan asianmukaisesti huomioon [kyselyjen] vaikutus kaikkien henkilöiden yksityisyyteen ja kansalaisvapauksiin riippumatta heidän kansalaisuudestaan tai asuinpaikastaan. Ks. *saman säädöksen* 2 §:n c momentin iii kohdan D alakohta. Lisäksi asetuksessa säädetään kerättyjen tietojen käsittelystä, suojauksesta ja pääsynvalvonnasta. Ks. *saman säädöksen* 2 §:n c momentin iii kohdan A ja B alakohta.

* * * * *

Toivomme, että näistä selvityksistä on apua. Ottakaa yhteyttä virastoomme, jos Teillä on vielä kysyttävää siitä, miten Yhdysvaltojen tiedusteluyhteisö aikoo panna täytäntöön toimeenpanoasetusta 14086.

⁽¹⁾ Vuosina 2001–2020 FISA-lain V osastossa sallittiin FBI:n hakevan FISC-tuomioistuimelta lupaa hankkia ”aineellisia esineitä”, jotka ovat merkityksellisiä tiettyjen hyväksyttyjen tutkimusten kannalta. Ks. USA PATRIOT Act -laki, Pub. L. No. 107-56, 115 Stat. 272, 215 § (2001). Tällä sanamuodolla, joka on rauennut eikä näin ollen ole enää voimassa olevaa lainsäädäntöä, annettiin toimivalta, jonka nojalla hallitus aiemmin keräsi puhelinliikenteen metadatat valikoimattomasti. USA FREEDOM Act -lailla oli kuitenkin jo ennen säännöksen raukeamista muutettu lakia siten, että siinä vaadittiin hallitusta perustelemaan FISC-tuomioistuimelle tehtävä hakemus ”erityisellä valintakriteerillä”. Ks. USA FREEDOM Act -laki, Pub. L. No. 114-23, 129 Stat. 268, 103 § (2015).

⁽²⁾ 703 ja 704 §:ssä, joissa annetaan tiedusteluyhteisölle valtuudet kohdentaa tiedustelua Yhdysvaltojen ulkopuolella oleviin yhdysvaltalaisiin henkilöihin, edellytetään tuomioistuimen määräystä (paitsi hätätilanteissa) ja aina todennäköistä syytä uskoa, että kohde on vieras valta, vieraan vallan asiamies tai vieraan vallan virkamies tai työntekijä. Ks. 50 U.S.C. 1881b §, 1881c §.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. FONZONE', followed by a horizontal line that ends in a vertical bar.

Christopher C. FONZONE,
päälakimies

LIITE VIII

Lyhenneluettelo

Tässä päätöksessä esiintyvät seuraavat lyhenteet:

AAA	American Arbitration Association (Yhdysvaltain sovitteluelinten yhdistys)
AG-asetus	Attorney General Regulation on the Data Protection Review Court (oikeusministerin asetus tietosuoja-asioiden muutoksenhakutuomioistuimesta)
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (oikeusministerin ohjeet FBI:n Yhdysvaltojen sisäisistä operaatioista)
APA	Administrative Procedure Act (hallintomenettelylaki)
CIA	Central Intelligence Agency (keskustiedustelupalvelu)
CNSS	Committee on National Security Systems (kansallisten turvallisuusjärjestelmien komitea)
Unionin tuomioistuin	Euroopan unionin tuomioistuin
Päätös	Komission täytäntöönpanopäätös Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman tietosuojan tason riittävydestä
DHS	Department of Homeland Security (sisäisen turvallisuuden ministeriö)
DNI	Director of National Intelligence (kansallisen tiedusteluviraston johtaja)
DoC	U.S. Department of Commerce (Yhdysvaltojen kauppaministeriö)
DoJ	U.S. Department of Justice (Yhdysvaltojen oikeusministeriö)
DoT	U.S. Department of Transportation (Yhdysvaltojen liikenneministeriö)
DPA	Data Protection Authority (tietosuojaviranomainen)
DPF List	Data Privacy Framework List (tietosuojakehykseen osallistuvien organisaatioiden luettelo)
DPRC	Data Protection Review Court (tietosuoja-asioiden muutoksenhakutuomioistuin)
ECOA	Equal Credit Opportunity Act (yhtäläisiä luotonsaantimahdollisuuksia koskeva laki)
ECPA	Electronic Communications Privacy Act (laki sähköisen viestinnän tietosuojasta)
EEA	European Economic Area (Euroopan talousalue, ETA)
EO 12333	Executive Order 12333 'United States Intelligence Activities' (toimeenpanoasetus Yhdysvaltojen tiedustelutoiminnasta)
EO 14086, EO	Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' (toimeenpanoasetus Yhdysvaltojen signaalitiedustelutoiminnan suojaustoimien tehostamisesta)
EU-U.S. DPF, DPF	EU:n ja Yhdysvaltojen tietosuojakehys
EU-U.S. DPF Panel	EU-U.S. Data Privacy Framework Panel (EU:n ja Yhdysvaltojen tietosuojakehyksen paneeli)
FBI	Federal Bureau of Investigation (Yhdysvaltojen liittovaltion poliisi)
FCRA	Fair Credit Reporting Act (luottokelpoisuusraportointia koskeva laki)
FISA	Foreign Intelligence Surveillance Act (ulkomaantiedustelun valvontaa koskeva laki)

FISC	Foreign Intelligence Surveillance Court (ulkomaantiedustelun valvonnasta vastaava tuomioistuin)
FISCR	Foreign Intelligence Surveillance Court of Review (ulkomaantiedustelun valvonnan muutoksenhakutuomioistuin)
FOIA	Freedom of Information Act (tiedonvapautta koskeva laki)
FRA	Federal Records Act (liittovaltion rekisterilaki)
FTC	U.S. Federal Trade Commission (liittovaltion kauppakomissio)
HIPAA	Health Insurance Portability and Accountability Act (sairausvakuutuslaki)
ICDR	International Centre for Dispute Resolution (kansainvälinen riidanratkaisukeskus)
IOB	Intelligence Oversight Board (tiedustelutoiminnan valvontalautakunta)
NIST	National Institute for Standards and Technology (kansallinen standardi- ja teknologiainstituutti)
NSA	National Security Agency (kansallinen turvallisuusvirasto)
NSL	National Security Letter (kansallista turvallisuutta koskeva kirje)
ODNI	Office of the Director of National Intelligence (kansallisen tiedustelujohtajan toimisto)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (kansallisen tiedustelujohtajan alaisuudessa toimiva kansalaisvapauksien suojelusta vastaava virkahenkilö)
OMB	Office of Management and Budget (hallinto- ja talousarviovirasto)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (yksityisyyden ja kansalaisvapauksien suojasta vastaava oikeusministeriön toimisto)
PCLOB	Privacy and Civil Liberties Oversight Board (yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaava lautakunta)
PIAB	President's Intelligence Advisory Board (tiedustelutoimintaa käsittelevä presidentin neuvoa-antava lautakunta)
PPD 28	Presidential Policy Directive 28 (presidentin määräys)
Asetus (EU) 2016/679	Euroopan parlamentin ja neuvoston asetukset (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta
SAOP	Senior Agency Official for Privacy (viraston tietosuojavastaava)
Periaatteet	EU:n ja Yhdysvaltojen tietosuojakehyksen periaatteet
U.S.	United States (Yhdysvallat)
Unioni	Euroopan unioni