

II

(Muut kuin lainsäätämismääräyksessä hyväksyttävät säädökset)

PÄÄTÖKSET

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 riittävydestä

(tiedoksiannettu numerolla C(2016) 4176)

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY ⁽¹⁾ ja erityisesti sen 25 artiklan 6 kohdan,

on kuullut Euroopan tietosuojavaltuutettua ⁽²⁾,

1. JOHDANTO

- (1) Direktiivissä 95/46/EY vahvistetaan säännöt henkilötietojen siirtämisestä jäsenvaltioista kolmansiin maihin siinä määrin kuin kyseiset siirrot kuuluvat sen soveltamisalaan.
- (2) Direktiivin 95/46/EY 1 artiklan ja sen johdanto-osan 2 ja 10 kappaleen tarkoituksena on turvata tehokas ja kattava suoja luonnollisten henkilöiden perusvapauksille ja -oikeuksille, erityisesti perusoikeudelle yksityiselämän kunnioittamiseen henkilötietojen käsittelyssä, ja lisäksi näiden perusvapauksien ja -oikeuksien suojan korkeatasoisuus ⁽³⁾.
- (3) Euroopan unionin tuomioistuimen oikeuskäytännössä on painotettu sekä Euroopan unionin perusoikeuskirjan 7 artiklassa taattua yksityiselämän kunnioittamista koskevaa perusoikeutta että 8 artiklassa taattua henkilötietojen suojan perusoikeutta ⁽⁴⁾.
- (4) Direktiivin 95/46/EY 25 artiklan 1 kohdan mukaan jäsenvaltioiden on säädettävä siitä, että henkilötietoja voidaan siirtää kolmanteen maahan vain, jos kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso ja jos direktiivin muiden säännösten täytäntöönpanemiseksi annettuja jäsenvaltion lakeja noudatetaan ennen tietojen siirtämistä. Komissio voi todeta, että kolmannessa maassa taataan tietosuojan riittävä taso kyseisen maan lainsäädännön tai niiden kansainvälisten sitoumusten perusteella, jotka se on tehnyt henkilöiden oikeuksien turvaamiseksi. Tässä tapauksessa, jollei direktiivin muiden säännösten mukaisesti säädetyistä kansallisista säännöksistä muuta johdu, henkilötietoja voidaan siirtää jäsenvaltioista ilman lisätakeita.

⁽¹⁾ EYVL L 281, 23.11.1995, s. 31.

⁽²⁾ Ks. lausunto 4/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyttä koskevasta päätösluonnoksesta, julkaistu 30.5.2016.

⁽³⁾ Asia C-362/14, Maximilian Schrems v. Data Protection Commissioner ("Schrems"), ECLI:EU:C:2015:650, 39 kohta.

⁽⁴⁾ Asia C-553/07, Rijkeboer, ECLI:EU:C:2009:293, 47 kohta; yhdistetyt asiat C-293/12 ja C-594/12, Digital Rights Ireland ym., ECLI:EU:C:2014:238, 53 kohta; asia C-131/12, Google Spain ja Google, ECLI:EU:C:2014:317, 53, 66 ja 74 kohta.

- (5) Direktiivin 95/46/EY 25 artiklan 2 kohdan mukaan kolmannessa maassa taattavaa tietosuojan tasoa olisi arvioitava kaikkien tiettyyn siirtoon tai siirtojen ryhmään liittyvien olosuhteiden pohjalta, mukaan lukien kyseisessä kolmannessa maassa voimassa olevat yleiset tai alakohtaiset oikeussäännöt.
- (6) Komission päätöksessä 2000/520/EY ⁽⁵⁾ katsottiin direktiivin 95/46/EY 25 artiklan 2 kohdan soveltamiseksi, että niin sanotut safe harbor -periaatteet, jotka on pantu täytäntöön Yhdysvaltojen kauppaministeriön julkaisemissa tavallisimmissa kysymyksissä annettujen ohjeiden mukaisesti, takaavat riittävän suojan henkilötiedoille, jotka siirretään unionista Yhdysvalloissa toimiville organisaatioille.
- (7) Komission 27 päivänä marraskuuta 2013 antamissa tiedonannoissa COM(2013) 846 final ⁽⁶⁾ ja COM(2013) 847 final ⁽⁷⁾ komissio katsoi, että safe harbor -järjestelmän perustaa oli tarkistettava ja vahvistettava useiden tekijöiden vuoksi. Näitä tekijöitä olivat muun muassa tietovirtojen voimakas kasvu ja niiden kriittinen merkitys transatlanttiselle taloudelle, safe harbor -järjestelmään liittyneiden yhdysvaltalaisen yritysten määrän nopea kasvu ja tiettyjen Yhdysvaltojen tiedusteluohjelmien laajuus ja kattavuus, mikä herätti epäilyjä suojelun tasosta, joka järjestelmällä voitaisiin taata. Lisäksi komissio havaitsi eräitä puutteita safe harbor -järjestelmässä.
- (8) Komissio esitti 13 suositusta safe harbor -järjestelmän tarkistamiseksi komission keräämien todisteiden perusteella. Näitä todisteita olivat muun muassa EU:n ja Yhdysvaltojen kontaktiryhmän ⁽⁸⁾ työhön perustuvat tiedot ja EU:n ja Yhdysvaltojen *ad hoc* -tietosuojatyöryhmässä ⁽⁹⁾ Yhdysvaltojen tiedusteluohjelmista saadut tiedot. Suosituksissa keskityttiin yksityisyyden suojaa koskevien aineellisoikeudellisten periaatteiden vahvistamiseen, yhdysvaltalaisen oman varmennuksen antaneiden yritysten tietosuojaperiaatteiden avoimuuden lisäämiseen, Yhdysvaltojen viranomaisten toteuttaman, näiden periaatteiden noudattamista koskevan valvonnan, seurannan ja täytäntöönpanon parantamiseen, kohtuuhintaisten riitojenratkaisumekanismien saatavuuteen sekä tarpeeseen varmistaa, että päätöksen 2000/520/EY mukaista kansalliseen turvallisuuteen perustuvaa poikkeusta käytetään vain siinä määrin kuin se on ehdottoman välttämätöntä ja oikeasuhteista.
- (9) Euroopan unionin tuomioistuin julisti 6 päivänä lokakuuta 2015 asiassa C-362/14 (Maximillian Schrems v. Data Protection Commissioner) ⁽¹⁰⁾ antamassaan tuomiossa päätöksen 2000/520/EY pätemättömäksi. Tarkastelematta yksityisyyden suojaa koskevien safe harbor -periaatteiden sisältöä tuomioistuin katsoi, että komissio ei ollut todennut kyseisessä päätöksessä, että Yhdysvallat tosiasiallisesti takaa tietosuojan riittävän tason sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta ⁽¹¹⁾.
- (10) Tältä osin unionin tuomioistuin täsmensi, että vaikka direktiivin 95/46/EY 25 artiklan 6 kohdan ilmaisu "tietosuojan riittävä taso" ei tarkoita tietosuojan tasoa, joka olisi täysin sama kuin unionin oikeusjärjestyksessä taattu taso, sen on kuitenkin ymmärrettävä tarkoittavan vaatimusta, että kolmas maa takaa perusvapauksien ja -oikeuksien suojan sellaisen tason, joka pääosiltaan vastaa tasoa, joka taataan unionissa direktiivin 95/46/EY nojalla, luettuna perusoikeuskirjan valossa. Vaikka keinot, joita kyseinen kolmas maa tässä yhteydessä käyttää, voivat poiketa niistä, joita unionissa käytetään, keinojen on käytännössä osoittauduttava tehokkaiksi ⁽¹²⁾.
- (11) Unionin tuomioistuin arvosteli sitä, ettei päätös 2000/520/EY sisällä riittäviä toteamuksia siitä, että Yhdysvalloissa olisi valtiollisia sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista puuttumista henkilöiden, joiden tietoja siirretään unionista Yhdysvaltoihin, perusoikeuksiin myös silloin, kun kyseinen puuttuminen olisi kyseisen maan valtiollisille elimille sallittua niiden pyrkiessä kansallisen turvallisuuden kaltaisiin legitiimeihin tavoitteisiin, eikä siitä, että tällaista puuttumista vastaan on olemassa tehokasta oikeussuojaa ⁽¹³⁾.

⁽⁵⁾ Komission päätös 2000/520/EY, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä (EYVL L 215, 28.8.2000, s. 7).

⁽⁶⁾ Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon (COM(2013) 846 final, 27.11.2013).

⁽⁷⁾ Komission tiedonanto Euroopan parlamentille ja neuvostolle safe harbor -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta (COM(2013) 847 final, 27.11.2013).

⁽⁸⁾ Ks. esimerkiksi Euroopan unionin neuvosto, yksityisyyden suojaa ja henkilötietojen suojaamista käsittelevä EU:n ja Yhdysvaltojen korkean tason kontaktiryhmän loppuraportti, asiakirja 9831/08, 28. toukokuuta 2008, saatavilla osoitteessa: <http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf>

⁽⁹⁾ Kertomus EU:n ja Yhdysvaltojen *ad hoc* -tietosuojatyöryhmän EU:n yhteispuheenjohtajien havainnoista, 27.11.2013, saatavilla osoitteessa: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>

⁽¹⁰⁾ Ks. alaviite 3.

⁽¹¹⁾ Schrems, 97 kohta.

⁽¹²⁾ Schrems, 73–74 kohta.

⁽¹³⁾ Schrems, 88–89 kohta.

- (12) Komissio aloitti vuonna 2014 neuvottelut Yhdysvaltojen viranomaisten kanssa keskustellakseen safe harbor -järjestelmän vahvistamisesta komission tiedonantoon COM(2013) 847 final sisältyvien 13 suosituksen mukaisesti. Sen jälkeen, kun Euroopan unionin tuomioistuin oli antanut tuomion asiassa Schrems, neuvotteluja tiivistettiin, jotta mahdollisesti saataisiin aikaan uusi tietosuojan riittävyttä koskeva päätös, joka täyttäisi direktiivin 95/46/EY 25 artiklan vaatimukset, sellaisina kuin unionin tuomioistuin on niitä tulkinnut. Asiakirjat, jotka ovat tämän päätöksen liitteenä ja jotka julkaistaan myös Yhdysvaltojen Federal Register -lehdessä, ovat näiden keskustelujen tulosta. Yksityisyyden suojaa koskevat periaatteet (liite II) sekä Yhdysvaltojen viranomaisten viralliset lausumat ja sitoumukset, jotka sisältyvät liitteissä I ja III–VII oleviin asiakirjoihin, muodostavat EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn.
- (13) Komissio on analysoinut huolellisesti Yhdysvaltojen lainsäädäntöä ja käytäntöä, mukaan lukien kyseiset viralliset lausumat ja sitoumukset. Johdanto-osan 136–140 kappaleessa esitettyjen havaintojen perusteella komissio päättää, että Yhdysvallat takaa tietosuojan riittävän tason henkilötiedoille, jotka siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa unionista Yhdysvalloissa sijaitseville oman varmennuksen antaneille organisaatioille.

2. EU:N JA YHDYSVALTOJEN VÄLINEN PRIVACY SHIELD -JÄRJESTELY

- (14) EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely perustuu omaan varmennukseen, jolla yhdysvaltalaiset organisaatiot sitoutuvat tiettyihin yksityisyyden suojaa koskeviin periaatteisiin eli EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn periaatteisiin, mukaan lukien täydentävät periaatteet, jäljempänä yhdessä 'järjestelyn periaatteet', jotka on antanut Yhdysvaltojen kauppaministeriö ja jotka sisältyvät tämän päätöksen liitteeseen II. Sitä sovelletaan sekä rekisterinpitäjiin että henkilötietojen käsittelijöihin (edustajiin) siten, että henkilötietojen käsittelijöiden on oltava sopimuksen nojalla velvollisia toimimaan ainoastaan EU:n rekisterinpitäjän ohjeiden perusteella ja avustamaan sitä vastattaessa henkilöille, jotka käyttävät järjestelyn periaatteiden mukaisia oikeuksiaan ⁽¹⁴⁾.
- (15) Rajoittamatta direktiivin 95/46/EY nojalla annettujen kansallisten säännösten soveltamista, tällä päätöksellä sallitaan siirrot unionissa olevalta rekisterinpitäjältä tai henkilötietojen käsittelijältä Yhdysvalloissa sijaitseville organisaatioille, jotka ovat antaneet Yhdysvaltojen kauppaministeriölle oman varmennuksen järjestelyn periaatteiden noudattamisesta ja ovat sitoutuneet noudattamaan niitä. Periaatteita sovelletaan ainoastaan yhdysvaltalaisen organisaation suorittamaan henkilötietojen käsittelyyn siltä osin kuin tällaisten organisaatioiden suorittama käsittely ei kuulu unionin lainsäädännön soveltamisalaan ⁽¹⁵⁾. Privacy Shield -järjestely ei vaikuta henkilötietojen käsittelyä jäsenvaltioissa koskevan unionin lainsäädännön soveltamiseen ⁽¹⁶⁾.

⁽¹⁴⁾ Ks. liite II, 111.10.a kohta. Kohdassa I.8.c olevan määritelmän mukaisesti EU:n rekisterinpitäjä määrittää henkilötietojen käsittelyn tarkoituksen ja keinot. Lisäksi edustajan kanssa tehtävästä sopimuksesta on käytävä ilmi, onko sallittua siirtää tietoja edelleen (ks. III.10. a.ii.2 kohta).

⁽¹⁵⁾ Tämä pätee myös silloin, kun henkilötietoja siirretään unionista työsuhteen yhteydessä. Vaikka järjestelyn periaatteissa painotetaan EU:n työnantajan ensisijaista vastuuta (ks. liite II, III.9.d.i kohta), niissä tehdään selväksi, että sen toiminta kuuluu unionissa ja/tai kyseisessä jäsenvaltiossa sovellettavien sääntöjen soveltamisalaan, ei periaatteiden piiriin. Ks. liite II, III.9.a.i, b.ii, c.i ja d.i kohta.

⁽¹⁶⁾ Tämä koskee myös käsittelyä, joka tapahtuu käyttämällä välineitä, jotka sijaitsevat unionissa, mutta joita käyttää organisaatio, joka on perustettu unionin ulkopuolella (ks. direktiivin 95/46/EY 4 artiklan 1 kohdan c alakohta). Yleistä tietosuoja-asetusta sovelletaan 25 päivästä toukokuuta 2018 alkaen i) henkilötietojen käsittelyyn, joka suoritetaan unioniin sijoittautuneen rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toteutettavan toiminnan yhteydessä (myös silloin, kun käsittely tapahtuu Yhdysvalloissa), tai ii) rekisteröityä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy a) tavaroiden tai palvelujen tarjoamiseen, riippumatta siitä, onko se rekisteröidylle maksullista, näille rekisteröidylle unionissa; b) näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa. Ks. Euroopan parlamentin ja neuvoston asetusta (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 artiklan 1 ja 2 kohta (EUVL L 119, 4.5.2016, s. 1).

- (16) Privacy Shield -järjestelyn tarjoamaa henkilötietojen suojaa sovelletaan kaikkiin EU:n rekisteröityihin⁽¹⁷⁾, joiden henkilötietoja on siirretty unionista sellaisille Yhdysvalloissa oleville organisaatioille, jotka ovat antaneet kauppaministeriölle oman varmennuksen järjestelyn periaatteiden noudattamisesta.
- (17) Järjestelyn periaatteita sovelletaan välittömästi varmennuksen jälkeen. Tietojen edelleen siirtämiseen liittyvää vastuuvuorollisuutta koskevaan periaatteeseen sovelletaan kuitenkin poikkeusta, jos Privacy Shield -järjestelyyn oman varmennuksen antaneella organisaatiolla on jo olemassa olevia kaupallisia suhteita kolmansien osapuolten kanssa. Kun otetaan huomioon, että kyseisten kaupallisten suhteiden saattaminen tietojen edelleen siirtämiseen liittyvää vastuuvuorollisuutta koskevaan periaatteeseen sisältyvien sääntöjen mukaisiksi voi viedä hieman aikaa, organisaation on tehtävä niin mahdollisimman pian ja joka tapauksessa viimeistään yhdeksän kuukauden kuluttua oman varmennuksen antamisesta (edellyttäen, että tämä tapahtuu kahden ensimmäisen kuukauden kuluessa päivästä, jona Privacy Shield -järjestely tulee voimaan). Tämän siirtymäkauden aikana organisaation on sovellettava ilmoitus- ja valintaperiaatteita (jolloin EU:n rekisteröity voi jättäytyä tiedonsiirron ulkopuolelle), ja jos henkilötietoja siirretään edustajana toimivalle kolmannelle osapuolelle, on varmistettava, että viimeksi mainittu tarjoaa vähintään saman suojelun tason kuin järjestelyn periaatteet edellyttävät⁽¹⁸⁾. Siirtymäkausi tarjoaa kohtuullisen ja asianmukaisen tasapainon, kun on toisaalta kyse tietosuojaa koskevan perusoikeuden kunnioittamisesta ja toisaalta yritysten oikeutetusta tarpeesta saada riittävästi aikaa mukautua uuteen järjestelyyn silloin, kun tämä riippuu myös niiden kaupallisista suhteista kolmansien osapuolten kanssa.
- (18) Järjestelmää hallinnoi ja valvoo Yhdysvaltojen kauppaministeriö niiden antamiensa sitoumusten perusteella, jotka sisältyvät Yhdysvaltojen kauppaministerin lausumiin (tämän päätöksen liite I). Järjestelyn periaatteiden valvonnan osalta Yhdysvaltojen liittovaltion kaupakomissio (Federal Trade Commission, FTC) ja liikenneministeriö ovat antaneet lausumia, jotka sisältyvät tämän päätöksen liitteisiin IV ja V.

2.1 Yksityisyyden suojaa koskevat periaatteet

- (19) Osana EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa toteutettavaa omaa varmennusta organisaatioiden on sitouduttava noudattamaan järjestelyn periaatteita⁽¹⁹⁾.
- (20) *Ilmoitusperiaatteen* mukaan organisaatioiden on annettava rekisteröidyille tiedot useista heidän henkilötietojensa käsittelyyn liittyvistä keskeisistä aiheista (esim. kerättävien tietojen laji, tietojen käsittelyn tarkoitus, oikeus tutustua tietoihin ja valinnaoikeus, tietojen edelleen siirtämistä koskevat ehdot ja vastuu). Lisäksi sovelletaan muita suojatoimia, erityisesti organisaatioille asetettua vaatimusta julkistaa tietosuojaperiaatteensa (joissa otetaan huomioon järjestelyn periaatteet) ja esittää linkit kauppaministeriön verkkosivustolle (ja lisätiedot omasta varmennuksesta, rekisteröityjen oikeuksista ja käytettävissä olevista muutoksenhakumenettelyistä), johdanto-osan 30 kappaleessa mainittuun Privacy Shield -luetteloon ja asianmukaisen vaihtoehtoisen riitojenratkaisuelimen verkkosivustolle.
- (21) *Tietojen eheyttä ja käyttötarkoituksen rajoittamista koskevan periaatteen* mukaan henkilötiedot on rajoitettava siihen, mikä on tarpeen tietojen käsittelyn kannalta, ja niihin tietoihin, jotka ovat käyttötarkoitukseensa nähden luotettavia, sekä niihin, jotka ovat tarkkoja, täydellisiä ja ajantasaisia. Organisaatio ei saa käsitellä henkilötietoja tavalla, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta tai tarkoitusta, johon kyseinen rekisteröity oli sittemmin antanut suostumuksensa. Organisaatioiden on varmistettava, että henkilötiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia.

⁽¹⁷⁾ Nyt käsillä oleva päätös on ETA:n kannalta merkityksellinen. Euroopan talousalueesta tehdyn sopimuksen (ETA-sopimuksen) mukaan Euroopan unionin sisämarkkinat ulottuvat kolmeen ETA-valtioon (Islanti, Liechtenstein ja Norja). Tietosuojaa koskeva unionin lainsäädäntö, mukaan lukien direktiivi 95/46/EY, kuuluu ETA-sopimuksen soveltamisalaan ja on sisällytetty sen liitteeseen XI. ETA:n sekakomitean on päätettävä tämän päätöksen ottamisesta osaksi ETA-sopimusta. Kun tätä päätöstä sovelletaan Islantiin, Liechtensteiniin ja Norjaan, EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely kattaa myös nämä kolme maata ja Privacy Shield -paketissa olevien viittausten EU:hun ja sen jäsenvaltioihin on katsottava tarkoittavan myös Islantia, Liechtensteiniä ja Norjaa.

⁽¹⁸⁾ Ks. liite II, 111.6.e kohta.

⁽¹⁹⁾ Erityisiä sääntöjä, joihin sisältyy ylimääräisiä suojatoimia, sovelletaan henkilöstötietoihin, jotka on kerätty työsuhteen yhteydessä, kuten yksityisyyden suojaa koskeviin periaatteisiin sisältyvissä henkilöstötietoja koskevassa täydentävässä periaatteessa on vahvistettu (ks. liite II, III.9 kohta). Esimerkiksi työnantajien olisi otettava huomioon työntekijöiden esittämät yksityisyyttä koskevat toiveet rajoittamalla pääsyä henkilötietoihin, muuttamalla ne tunnistamattomiksi tai käyttämällä koodeja tai salanimiä. Tärkeintä on, että organisaatiot velvoitetaan tekemään yhteistyötä ja noudattamaan unionin tietosuojaviranomaisten neuvoja, kun on kyse tällaisista tiedoista.

- (22) Jos uusi (muutettu) käyttötarkoitus on olennaisesti erilainen, mutta silti yhteensopiva alkuperäisen tarkoituksen kanssa, *valintaperiaatteen* mukaan rekisteröidyillä on oikeus vastustaa henkilötietojensa käsittelyä (opt out). *Valintaperiaate* ei korvaa periaatteiden vastaisen tietojen käsittelyn nimenomaista kieltä (20). Suoramarkkinoinnissa sovelletaan erityisiä sääntöjä, jotka yleensä mahdollistavat henkilötietojen käytön kieltämisen ”milloin tahansa” (21). Arkaluonteisten tietojen tapauksessa organisaatioiden on tavallisesti hankittava rekisteröidyn nimenomainen myönteinen suostumus (opt in).
- (23) *Tietojen eheyttä ja käyttötarkoituksen rajoittamista koskevan periaatteen* mukaan henkilötiedot voidaan säilyttää muodossa, jossa henkilö tunnistetaan tai voidaan tunnistaa (eli henkilötietojen muodossa) ainoastaan niin kauan kuin on tarpeen sitä tarkoitusta varten, johon tiedot alun perin kerättiin tai joka myöhemmin hyväksyttiin. Tämä velvoite ei estä Privacy Shield -järjestelyyn liittyneitä organisaatioita käsittelemästä henkilötietoja pidempää aikaa, mutta ainoastaan niin kauan ja siinä määrin kuin tällainen käsittely kohtuudella palvelee jotain seuraavista tarkoituksista: arkistointi yleisen edun nimissä, journalismi, kirjallisuus ja taide, tieteellinen ja historiantutkimus ja tilastollinen analyysi. Henkilötietojen säilyttäminen pidempään näitä tarkoituksia varten edellyttää järjestelyn periaatteiden mukaisia suojatoimia.
- (24) *Turvallisuusperiaatteen* mukaan organisaatioiden, jotka luovat, ylläpitävät, käyttävät tai levittävät henkilötietoja, on toteutettava ”kohtuullisia ja asianmukaisia” turvallisuustoimenpiteitä, ottaen huomioon tietojen käsittelyyn liittyvät riskit ja tietojen luonne. Alihankintana teetettävän tietojen käsittelyn osalta organisaatioiden on tehtävä alihankkijan kanssa sopimus, jossa taataan samantasoinen suoja kuin järjestelyn periaateissa, ja varmistettava sen asianmukainen täytäntöönpano.
- (25) *Tiedonsaantiperiaatteen* (22) mukaan rekisteröidyillä on oikeus ilman perusteluja ja ainoastaan kohtuullista maksua vastaan saada organisaation vahvistus siitä, käsittelee kyseinen organisaatio heihin liittyviä henkilötietoja, ja saada tiedot kohtuullisessa ajassa. Tätä oikeutta voidaan rajoittaa vain poikkeuksellisissa olosuhteissa; mahdollisen tiedonsaantioikeuden epäämisen tai rajoittamisen on oltava välttämätön ja asianmukaisesti perusteltu, ja organisaation on osoitettava, että nämä vaatimukset täyttyvät. Rekisteröidyillä on oltava mahdollisuus oikaista, muuttaa tai poistaa henkilötietonsa, jos ne ovat epätarkkoja tai niitä on käsitelty vastoin järjestelyn periaatteita. Aloilla, joilla yritykset todennäköisimmin käyttävät henkilötietojen automatisoitua käsittelyä, kun ne tekevät henkilöön vaikuttavia päätöksiä (esim. luotonanto, asuntolainatarjoukset, työllisyys), Yhdysvaltojen lainsäädäntö tarjoaa erityisiä suojatoimia kielteisiä päätöksiä vastaan (23). Henkilöillä on yleensä näiden säädösten mukaan oikeus saada tietoonsa päätöksen (esim. luoton hylkääminen) perustana olleet erityiset syyt, riitauttaa puutteelliset tai virheelliset tiedot (sekä lainvastaisten perusteiden käyttö), ja hakea muutosta. Nämä säännöt tarjoavat suojaa niissä todennäköisesti melko harvoissa tapauksissa, joissa Privacy Shield -organisaatio tekisi automatisoidut päätökset itse (24). Kun kuitenkin otetaan huomioon, että automatisoitua käsittelyä käytetään yhä enemmän (mukaan lukien profilointi) perustana yksityishenkilöihin vaikuttavassa uudenaikaisen digitaalitalouden päätöksenteossa, kyseessä on ala, jota on seurattava tiiviisti. Seurannan helpottamiseksi Yhdysvaltojen viranomaisten kanssa on sovittu, että automatisoitua päätöksentekoa koskeva vuoropuhelu, mukaan lukien näkemysten vaihto EU:n ja Yhdysvaltojen lähtökohtien yhtäläisyyksistä ja eroista tältä osin, on tarvittaessa osa ensimmäistä vuosittaista tarkastelua ja myöhempiä tarkasteluja.

(20) Tämä koskee kaikkia Privacy Shield -järjestelyn puitteissa tehtyjä tiedonsiirtoja, myös silloin, kun ne koskevat työsuhteen yhteydessä kerättyjä tietoja. Vaikka oman varmennuksen antanut yhdysvaltalainen organisaatio voi periaatteessa käyttää henkilöstötietoja muihin kuin työsuhteeseen liittyviin tarkoituksiin (esim. tietynlainen markkinointiviestintä), sen on noudatettava käyttötarkoituksen vastaisen käsittelyn kieltä ja lisäksi se voi tehdä näin ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Yhdysvaltalaiselle organisaatiolle asetettu kieltä ryhtyä rankaisutoimiin työntekijää vastaan valintaoikeuden käyttämisestä, mukaan lukien kaikki työllistymismahdollisuuksia koskevat rajoitukset, varmistaa, että huolimatta alistaisuus- ja riippuvuussuhteesta työntekijään ei kohdistu paineita, vaan tämä voi sen vuoksi käyttää valintaoikeuttaan vapaasti.

(21) Ks. liite II, 111.12 kohta.

(22) Ks. myös tietoihin pääsyä koskeva täydentävä periaate (liite II, III.8 kohta).

(23) Ks. esim. Equal Credit Opportunity Act (ECOA, 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 (FHA, 42 U.S.C. § 3601 ja sitä seuraavat pykälät).

(24) EU:ssa kerättyjen henkilötietojen siirron yhteydessä henkilön (asiakas) sopimussuhde on useimmissa tapauksissa solmittu EU:n rekisterinpitäjän kanssa (joka näin ollen yleensä tekee automatisoituun käsittelyyn perustuvan päätöksen), jonka on noudatettava EU:n tietosuojasääntöjä. Tähän sisältyvät skenaariot, joissa käsittelyn suorittaa Privacy Shield -organisaatio, joka toimii EU:n rekisterinpitäjän edustajana.

- (26) Järjestelyyn osallistuvilla organisaatioilla on *muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen* ⁽²⁵⁾ mukaan oltava vankat mekanismit sen varmistamiseksi, että muita järjestelyn periaatteita noudatetaan ja että EU:n rekisteröityjen, joiden henkilötietoja on käsitelty säännösten vastaisella tavalla, käytettävissä on muutoksenhakumahdollisuus, mukaan lukien tehokkaat oikeussuojakeinot. Kun organisaatio on vapaaehtoisesti päättänyt antaa oman varmennuksen ⁽²⁶⁾ EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa, sen on todella noudatettava järjestelyn periaatteita. Jotta organisaatio voi jatkaa osallistumistaan Privacy Shield -järjestelyyn saadakseen henkilötietoja unionista, sen on vuosittain varmennettava uudelleen osallistumisensa järjestelyyn. Organisaatioiden on myös toteutettava toimenpiteitä sen varmistamiseksi ⁽²⁷⁾, että niiden julkaistut tietosuojaperiaatteet vastaavat järjestelyn periaatteita ja että niitä tosiasiallisesti noudatetaan. Tämä voidaan tehdä joko itsearviointijärjestelmän avulla, johon on sisällyttävä 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 ja pistokokeita. Lisäksi organisaation on otettava käyttöön tehokas oikeussuojamekanismi mahdollisten valitusten käsittelemiseksi (ks. myös johdanto-osan 43 kappale) ja sen on oltava liittovaltion kauppakomission, Yhdysvaltojen liikenneministeriön tai muun valtuutetun lakisäätöelimen tutkinta- ja täytäntöönpanovallan alainen järjestelyn periaatteiden noudattamisen varmistamiseksi.
- (27) Erityisiä sääntöjä sovelletaan niin sanottuun "tietojen edelleen siirtämiseen" eli henkilötietojen siirtämiseen organisaatiolta rekisterinpitäjänä tai henkilötietojen käsitelijänä toimivalle kolmannelle osapuolelle, riippumatta siitä, sijaitseeko viimeksi mainittu Yhdysvalloissa vai Yhdysvaltojen (ja unionin) ulkopuolisessa kolmannessa maassa. Näiden sääntöjen tarkoituksena on varmistaa, että EU:n rekisteröityjen henkilötiedoille taattu suoja ei vaarannu eikä sitä voida kiertää siirtämällä tietoja kolmansille osapuolille. Tämä koskee erityisesti monimutkaisempia käsittelyketjuja, jotka ovat tyypillisiä tämän päivän digitaalitaloudelle.
- (28) Tietojen edelleen siirtämiseen liittyvää *vastuuvellisuutta koskevan periaatteen* ⁽²⁸⁾ nojalla edelleen siirtäminen voi tapahtua vain i) rajoitetusti ja tiettyihin tarkoituksiin, ii) sopimuksen (tai vastaavan konsernin sisäisen järjestelyn ⁽²⁹⁾) perusteella ja iii) vain, jos sopimuksessa määrätään samasta suojelun tasosta kuin järjestelyn periaateissa. Tähän sisältyy vaatimus siitä, että periaatteiden soveltamista voidaan rajoittaa vain siinä määrin kuin se on tarpeen kansallisen turvallisuuden, lainvalvonnan ja muiden yleisen edun mukaisten tarkoitusten nimissä ⁽³⁰⁾. Tämä olisi luettava yhdessä *ilmoitusperiaatteen* kanssa ja, kun kyseessä on tietojen siirtäminen rekisterinpitäjänä toimivalle kolmannelle osapuolelle ⁽³¹⁾, *valintaperiaatteen* kanssa, jonka mukaan rekisteröidyille on ilmoitettava (muun muassa) mahdollisen kolmannen vastaanottajan tyyppi/nimi, edelleensirron tarkoitus samoin kuin tarjottu valinta-oikeus. Rekisteröidyille on myös ilmoitettava mahdollisuudesta kieltää tiedonsiirto (opt out) tai arkaluonteisten tietojen tapauksessa myös siitä, että niiden on annettava nimenomainen "myönteinen" suostumus (opt in) tietojen siirrolle. Ottaen huomioon *tietojen eheyttä ja käyttötarkoituksen rajoittamista koskevan periaatteen* velvoite tarjota samantasoinen suoja kuin mikä taataan järjestelyn periaateissa edellyttää, että kolmas osapuoli voi käsitellä sille lähetettyjä henkilökohtaisia tietoja vain tarkoituksiin, jotka eivät ole ristiriidassa niiden tarkoitusten kanssa, joita varten tiedot alun perin kerättiin tai joihin henkilö myöhemmin antoi luvan.
- (29) Vellollisuutta tarjota periaateissa 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 teetettävää käsittelyä varten. Kaikissa tapauksissa kolmantena osapuolena olevan vastaanottajan kanssa tehdyssä sopimuksessa on määrättävä siitä, että kyseinen osapuoli ilmoittaa Privacy Shield -järjestelyyn osallistuvalla organisaatiolle, jos se toteaa, ettei se voi enää täyttää tätä vaatimusta. Kun tällaiseen toteamukseen on päädytty, kolmannen osapuolen on lopetettava tietojen käsittely tai ryhdyttävä muihin kohtuullisiin ja asianmukaisiin

⁽²⁵⁾ Ks. riitojenratkaisua ja täytäntöönpanoa koskeva täydentävä periaate (liite II, III.11 kohta).

⁽²⁶⁾ Ks. myös omaa varmennusta koskeva täydentävä periaate (liite II, III.6 kohta).

⁽²⁷⁾ Ks. myös tarkastusta koskeva täydentävä periaate (liite II, III.7 kohta).

⁽²⁸⁾ Ks. myös täydentävä periaate tietojen edelleen siirtämistä koskevista pakollisista sopimuksista (liite II, III.10 kohta).

⁽²⁹⁾ Ks. täydentävä periaate tietojen edelleen siirtämistä koskevista pakollisista sopimuksista (liite II, III.10.b kohta). Vaikka tämä periaate mahdollistaa myös muihin kuin sopimuksellisiin välineisiin perustuvat siirrot (esim. 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 oman varmennuksen antaneella yhdysvaltalaisella organisaatiolla säilyy vastuu järjestelyn periaatteiden noudattamisesta, sillä on voimakas kannustin käyttää välineitä, jotka ovat todella tehokkaita käytännössä.

⁽³⁰⁾ Ks. liite II, I.5 kohta.

⁽³¹⁾ Henkilöillä ei ole tietojen siirtoa koskevaa kielto-oikeutta, 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.

toimiin tilanteen korjaamiseksi ⁽³²⁾. Kun periaatteiden noudattamiseen liittyviä ongelmia esiintyy (alihankinnan) käsittelyketjussa, Privacy Shield -järjestelyyn osallistuvan organisaation, joka toimii henkilötietojen rekisterinpitäjänä, on todistettava, että se ei ole vastuussa vahingon aiheuttaneesta tapahtumasta, tai muuten se joutuu vastuuseen muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti. Lisäsuojatoimia sovelletaan, kun tietoja siirretään edelleen edustajana toimivalle kolmannelle osapuolelle ⁽³³⁾.

2.2 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn avoimuus, hallinto ja valvonta

- (30) EU:n ja Yhdysvaltojen välisessä Privacy Shield -järjestelyssä määrätään valvonta- ja täytäntöönpanomekanismeista, jotta voidaan tarkastaa ja varmistaa, että oman varmennuksen antaneet yhdysvaltalaiset yritykset noudattavat järjestelyn periaatteita ja että mahdolliseen periaatteiden noudattamatta jättämiseen puututaan. Nämä mekanismit on esitetty järjestelyn periaatteissa (liite II) ja kauppaministeriön (liite I), liittovaltion kauppakomission (liite IV) ja liikenneministeriön (liite V) antamissa sitoumuksissa.
- (31) EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn asianmukaisen soveltamisen varmistamiseksi asianomaisten osapuolten, kuten rekisteröityjen, tiedonviejien ja kansallisten tietosuojaviranomaisten, on voitava tunnistaa järjestelyn periaatteita noudattavat organisaatiot. Sen vuoksi Yhdysvaltojen kauppaministeriö on sitoutunut pitämään yllä ja saattamaan yleisön saataville luettelon organisaatioista, jotka ovat ilmoittaneet noudattavansa järjestelyn periaatteita ja jotka kuuluvat ainakin yhden tämän päätöksen liitteissä I ja II tarkoitetun täytäntöönpanoviranomaisen toimivallan piiriin, jäljempänä 'Privacy Shield -luettelo' ⁽³⁴⁾. Kauppaministeriö päivittää luettelon organisaatioiden vuosittain antamien uudelleenvarmennusten perusteella ja aina kun organisaatio peruuttaa osallistumisensa EU:n ja Yhdysvaltojen väliseen Privacy Shield -järjestelyyn tai se poistetaan järjestelyn piiristä. Se myös ylläpitää ja saattaa yleisön saataville virallisen luettelon organisaatioista, jotka on poistettu luettelosta, ja ilmoittaa kussakin tapauksessa poistamisen syyn. Lisäksi se luo linkin Privacy Shield -järjestelyyn liittyvistä liittovaltion kauppakomission käsittelemistä tapauksista laadittuun luetteloon, jota ylläpidetään kauppakomission verkkosivustolla.
- (32) Kauppaministeriö julkaisee sekä Privacy Shield -luettelon että uudelleenvarmennukset erityisellä verkkosivustolla. Oman varmennuksen antaneiden organisaatioiden on puolestaan ilmoitettava ministeriön verkkosivuilla olevan luettelon internetosoite. Lisäksi organisaation tietosuojaperiaatteissa, jos ne ovat saatavilla verkossa, on oltava hyperlinkki Privacy Shield -verkkosivustolle sekä hyperlinkki sellaisen riippumattoman muutoksenhakumekanismiin verkkosivustolle tai valituslomakkeeseen, joka voi tutkia ratkaisemattomat valitukset. Kauppaministeriö tarkastaa järjestelmällisesti järjestelyyn osallistuvan organisaation varmennuksen ja uudelleenvarmennuksen yhteydessä, että kyseisen organisaation tietosuojaperiaatteet ovat järjestelyn periaatteiden mukaiset.
- (33) Organisaatiot, jotka ovat toistuvasti jättäneet noudattamatta järjestelyn periaatteita, poistetaan Privacy Shield -luettelosta ja niiden on palautettava tai poistettava henkilötiedot, jotka ne ovat vastaanottaneet EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa. Muissa luettelosta poistamista koskeissa tapauksissa, esimerkiksi silloin kun organisaatio vetäytyy vapaaehtoisesti järjestelystä tai ei anna uutta varmennusta, organisaatio voi säilyttää henkilötiedot, jos se vahvistaa kauppaministeriölle vuosittain sitoumuksensa jatkaa periaatteiden soveltamista tai tarjoaa riittävän suojan henkilötiedoille muiden hyväksytyjen keinojen avulla (esimerkiksi käyttämällä sopimusta, joka vastaa täysin komission hyväksymien vakiomuotoisten sopimuslausakkeiden vaatimuksia). Tällöin organisaation on nimettävä organisaatiossaan yhteyspiste kaikkia Privacy Shield -järjestelyyn liittyviä kysymyksiä varten.
- (34) Kauppaministeriö valvoo organisaatioita, jotka eivät ole enää EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn jäseniä, koska ne ovat joko vapaaehtoisesti vetäytyneet järjestelystä tai koska niiden antaman varmennuksen voimassaolo on päättynyt, sen selvittämiseksi, aikovatko ne palauttaa, poistaa tai säilyttää ⁽³⁵⁾

⁽³²⁾ 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 Privacy Shield -järjestelyyn kuuluvan organisaation on toteutettava tämä toimet, sillä se vastaa ohjeidensa mukaisesti toimivan edustajan suorittamasta tietojen käsittelystä.

⁽³³⁾ Tällaisessa tapauksessa kyseisen yhdysvaltalaisen organisaation on myös 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 saatuaan tätä koskevan ilmoituksen.

⁽³⁴⁾ Tietoja Privacy Shield -luettelon pitämisestä on liitteissä I ja II (I.3, I.4, III.6.d ja III.11.g kohta)

⁽³⁵⁾ Ks. esim. liite II, I.3, III.6.f ja III.11.g.i kohta.

aikaisemmin järjestelyn puitteissa saamansa henkilötiedot. Jos organisaatiot säilyttävät nämä tiedot, niiden on jatkettava järjestelyn periaatteiden soveltamista. Jos kauppaministeriö on poistanut organisaatiot järjestelystä, koska ne ovat jatkuvasti jättäneet noudattamatta järjestelyn periaatteita, se varmistaa, että nämä organisaatiot palauttavat tai poistavat järjestelyn puitteissa saamansa henkilötiedot.

- (35) Jos organisaatio jostain syystä jättäytyy EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn ulkopuolelle, sen on poistettava kaikki julkiset lausumat, jotka antaisivat ymmärtää, että se osallistuu edelleen Privacy Shield -järjestelyyn tai että se on oikeutettu järjestelyn etuihin, erityisesti kaikki sen julkaistuissa tietosuojaperiaatteissa olevat viittaukset Privacy Shield -järjestelyyn. Lisäksi kauppaministeriö etsii aktiivisesti järjestelyyn osallistumista koskevia totuudenvastaisia väitteitä ja puuttuu niihin myös entisten jäsenten tapauksessa ⁽³⁶⁾. Liittovaltion kauppakomissio, liikenneministeriö tai muut asiaankuuluvat Yhdysvaltojen täytäntöönpanoviranomaiset voivat ryhtyä toimiin sellaisten virheellisten tietojen johdosta, jotka organisaatio on antanut yleisölle harhaanjohtavien lausumien tai käytäntöjen muodossa järjestelyn periaatteiden noudattamisesta; kauppaministeriölle toimitetut väärät tiedot voivat johtaa toimiin totuudenvastaisia lausuntoja koskevan lain (False Statements Act, 18 U.S.C. § 1001) nojalla ⁽³⁷⁾.
- (36) Kauppaministeriö valvoo viran puolesta totuudenvastaisia väitteitä osallistumisesta Privacy Shield -järjestelyyn tai Privacy Shield -varmennusmerkin epäasianmukaista käyttöä, ja tietosuojaviranomaiset voivat ottaa yhteyttä ministeriön yhteyspisteeseen, jotta organisaation toimintaa voitaisiin tarkastella. Jos organisaatio on vetäytynyt EU:n ja Yhdysvaltojen välisestä Privacy Shield -järjestelystä tai laiminlyönyt uudelleenvarmennuksen taikka se poistetaan Privacy Shield -luettelosta, kauppaministeriö varmistaa jatkuvasti, että organisaatio on poistanut julkaistuista tietosuojaperiaatteistaan kaikki sellaiset viittaukset Privacy Shield -järjestelyyn, jotka antaisivat ymmärtää sen osallistuvan edelleen järjestelyyn, ja jos organisaatio jatkaa totuudenvastaisen väitteiden esittämistä, kauppaministeriö voi viedä asian liittovaltion kauppakomission, liikenneministeriön tai muun toimivaltaisen viranomaisen käsiteltäväksi mahdollisia täytäntöönpanotoimia varten. Se myös lähettää kyselylomakkeet niille organisaatioille, joiden omat varmennukset raukeavat tai jotka ovat vapaaehtoisesti vetäytyneet EU:n ja Yhdysvaltojen välisestä Privacy Shield -järjestelystä, sen tarkistamiseksi, aikooko organisaatio palauttaa tai poistaa Privacy Shield -järjestelyn puitteissa saamansa henkilötiedot tai aikooko se jatkaa järjestelyn periaatteiden soveltamista kyseisiin henkilötietoihin, ja jos henkilötiedot aiotaan säilyttää, kuka organisaatiossa toimii yhteyspisteinä järjestelyyn liittyvissä kysymyksissä.
- (37) Kauppaministeriö tarkastaa viran puolesta jatkuvasti ⁽³⁸⁾, esimerkiksi lähettämällä yksityiskohtaisia kyselylomakkeita, että oman varmennuksen antaneet organisaatiot noudattavat sovellettavia periaatteita. Se tekee järjestelmällisesti tarkastuksia myös silloin, kun se on saanut tietyn (aiheellisen) valituksen, kun organisaatio ei anna tyydyttävää vastausta sen tiedusteluihin tai kun on uskottavia todisteita siitä, että organisaatio ei ehkä noudata järjestelyn periaatteita. Tarvittaessa kauppaministeriö myös kuulee tietosuojaviranomaisia tällaisista periaatteiden noudattamista koskevista tarkasteluista.

2.3 Oikeussuojakeinot, valitusten käsittely ja täytäntöönpano

- (38) EU:n ja Yhdysvaltojen välisessä Privacy Shield -järjestelyyn sisältyvässä *muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteissa* edellytetään, että organisaatiot tarjoavat sellaisille henkilöille mahdollisuuden muutoksenhakuun, joihin järjestelyn periaatteiden noudattamatta jättäminen on vaikuttanut. Näin EU:n rekisteröidyillä on mahdollisuus tehdä valitus, kun yhdysvaltalaiset oman varmennuksen antaneet yritykset eivät noudata periaatteita, ja saada valitukset ratkaistua, tarvittaessa päätöksellä, jossa määrätään tehokkaasta korjaustoimenpiteestä.
- (39) Oman varmennuksen osana organisaatioiden on täytettävä muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen vaatimukset ottamalla käyttöön tehokkaat ja helposti saatavilla olevat riippumattomat muutoksenhakumenettelyt, jotta kunkin henkilön valitukset ja riitatapaukset voidaan tutkia ja ratkaista nopeasti ilman kyseiselle henkilölle aiheutuvia kuluja.
- (40) Organisaatiot voivat valita joko unionissa tai Yhdysvalloissa sijaitsevan riippumattoman muutoksenhakumenettelyn. Tähän sisältyy mahdollisuus sitoutua vapaaehtoisesti yhteistyöhön EU:n tietosuojaviranomaisten kanssa.

⁽³⁶⁾ Ks. liitteen I jakso "Kauppaministeriö etsii organisaatioita, jotka totuuden vastaisesti väittävät osallistuvansa järjestelyyn ja puuttuu tapauksiin".

⁽³⁷⁾ Ks. liite II, III.6.h ja III.11.f kohta.

⁽³⁸⁾ Katso liite I.

Tällaista mahdollisuutta ei kuitenkaan ole silloin, kun organisaatiot käsittelevät henkilöstötietoja, jolloin yhteistyö tietosuojaviranomaisten kanssa on pakollista. Muita vaihtoehtoja ovat riippumaton vaihtoehtoinen riitojenratkaisu ja yksityisen sektorin kehittämät *yksityisyysdensuojaohjelmat*, joiden säännöt sisältävät järjestelyn periaatteet. Viimeksi mainittuihin on sisällyttävä tehokkaat täytäntöönpanomekanismit muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti. Organisaatioiden on korjattava mahdolliset periaatteiden noudattamatta jättämistä koskevat ongelmat. Niiden on myös vahvistettava, että ne kuuluvat liittovaltion kauppakomission, liikenneministeriön tai jonkin muun Yhdysvaltojen toimivaltaisen lakisääteisen elimen tutkinta- ja täytäntöönpanovallan piiriin.

- (41) Näin ollen Privacy Shield -järjestely tarjoaa rekisteröidyille useita mahdollisuuksia käyttää oikeuksiaan ja tehdä valituksia, kun oman varmennuksen antaneet yhdysvaltalaiset yritykset eivät noudata järjestelyn periaatteita, sekä saada valituksensa ratkaistua, tarvittaessa päätöksellä, jossa määrätään tehokkaasta korjaustoimenpiteestä. Henkilöt voivat tehdä valituksen suoraan organisaatiolle, organisaation nimeämälle riippumattomalle riitojenratkaisuelimelle, kansallisille tietosuojaviranomaisille tai liittovaltion kauppakomissiolle.
- (42) Jos valitusta ei ole voitu ratkaista millään näistä muutoksenhaku- tai täytäntöönpanomekanismeilla, henkilöillä on myös oikeus turvautua Privacy Shield -paneelin sitovaan välimiesmenettelyyn (tämän päätöksen liitteen II liite 1). Lukuun ottamatta välimiespaneelia, joka edellyttää, että kaikki tietyt oikeussuojakeinot on jo käytetty, henkilöt voivat vapaasti turvautua mihin tahansa valitsemaansa oikeussuojakeinoon tai niihin kaikkiin eikä niiden tarvitse valita yhtä mekanismia toisen sijaan tai käyttää niitä tietyssä järjestyksessä. On kuitenkin viisaampaa noudattaa tiettyä loogista järjestystä, kuten jäljempänä esitetään.
- (43) Ensinnäkin EU:n rekisteröidyt voivat saattaa järjestelyn periaatteiden noudattamatta jättämiseen liittyvät tapaukset käsiteltäväksi ottamalla suoraan yhteyttä kyseiseen *yhdysvaltalaiseen oman varmennuksen antaneeseen yritykseen*. Valitusten käsittelyn helpottamiseksi organisaation on otettava käyttöön tehokas oikeussuojamekanismi. Organisaation tietosuojaperiaateissa on sen vuoksi ilmoitettava selvästi yhteyspiste, joka on joko organisaatiossa tai sen ulkopuolella ja joka käsittelee valitukset (mukaan lukien unionissa mahdollisesti sijaitsevat asiaankuuluvat elimet, jotka voivat vastata tiedusteluihin tai valituksiin), ja riippumattomat valitusten käsittelymekanismit.
- (44) Saatuaan valituksen joko suoraan kyseiseltä henkilöltä tai kauppaministeriöltä, kun tietosuojaviranomaiset ovat siirtäneet asian käsittelyn sille, organisaation on toimitettava vastaus EU:n rekisteröidylle 45 päivän kuluessa. Vastauksessa on arvioitava valituksen aiheellisuus ja annettava tiedot siitä, miten organisaatio aikoo korjata ongelman. Samoin organisaatioiden on vastattava viipymättä järjestelyn periaatteiden noudattamiseen liittyviin tiedusteluihin ja muihin tietopyyntöihin, jotka on tehnyt Yhdysvaltojen kauppaministeriö tai tietosuojaviranomainen⁽³⁹⁾ (jos organisaatio on sitoutunut tekemään yhteistyötä tietosuojaviranomaisten kanssa). Organisaatioiden on säilytettävä dokumentaatio tietosuojaperiaatteidensa täytäntöönpanosta ja esitettävä ne pyynnöstä riippumattomalle muutoksenhakumekanismin tai liittovaltion kauppakomissiolle (tai muulle Yhdysvaltojen viranomaiselle, jolla on toimivalta tutkia sopimattomia ja vilpillisiä käytäntöjä), tutkinnan tai periaatteiden noudattamatta jättämistä koskevan valituksen yhteydessä.
- (45) Toiseksi henkilöt voivat esittää valituksen 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 muutoksenhakumenettelyn. Tällaisen elimen määräämien 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 on julkistettava periaatteiden noudattamatta jättämistä koskevat havainnot. Organisaation nimeämien riippumattomien riitojenratkaisuelimien on sisällytettävä niiden julkisille verkkosivuille asiaankuuluvat tiedot, jotka koskevat EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä ja niiden sen puitteissa tarjoamia palveluja. Niiden on julkaistava vuosittain vuosikertomus, jossa esitetään näitä palveluja koskevat kootut tilastot⁽⁴⁰⁾.

⁽³⁹⁾ Tämän käsittelevän viranomaisen on nimittänyt tietosuojaviranomaisten paneeli tietosuojaviranomaisten roolia koskevan täydentävän periaatteen mukaisesti (liite II, III.5 kohta).

⁽⁴⁰⁾ Vuosikertomukseen on sisällyttävä 1) kertomusvuoden aikana saatujen Privacy Shield -järjestelyyn 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.

- (46) Periaatteiden noudattamista koskevien tarkastelumenettelyjen osana kauppaministeriö varmistaa, että oman varmennuksen antaneet yhdysvaltalaiset yritykset ovat todella rekisteröityneet niihin riippumattomiin muutoksenhakumekanismeihin, joihin ne väittävät rekisteröityneensä. Organisaatioiden ja vastuussa olevien riippumattomien muutoksenhakumekanismien on vastattava nopeasti Privacy Shield -järjestelyä koskeviin kauppaministeriön tiedusteluihin ja tietopyyntöihin.
- (47) 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 sopimattomia ja vilpillisiä käytäntöjä) tai toimivaltaiselle tuomioistuimelle ⁽⁴¹⁾. 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 katsotaan periaatteiden jatkuvaksi noudattamatta jättämiseksi. Tämän seurauksena organisaatio poistetaan luettelosta, kun kauppaministeriö on ilmoittanut tästä kyseiselle organisaatiolle 30 päivää ennen ja antanut periaatteita rikkoneelle organisaatiolle mahdollisuuden esittää vastineensa ⁽⁴²⁾. Jos organisaatio luettelosta poistamisen jälkeen väittää edelleen osallistuvansa Privacy Shield -järjestelyyn, kauppaministeriö siirtää asian liittovaltion kauppakomission tai muun toimivaltaisen viraston käsiteltäväksi ⁽⁴³⁾.
- (48) Kolmanneksi henkilöt voivat tehdä valituksen myös kansalliselle tietosuojaviranomaiselle. Organisaatiot ovat velvollisia tekemään yhteistyötä, kun tietosuojaviranomaiset tutkivat valituksia ja tekevät niitä koskevia päätöksiä, joko silloin, kun valitus koskee työsuhteen yhteydessä kerättyjä henkilöstötietojen käsittelyä tai kun asianomainen organisaatio on vapaaehtoisesti suostunut tietosuojaviranomaisten valvontaan. Organisaatioiden on erityisesti vastattava tiedusteluihin, noudatettava tietosuojaviranomaisen antama lausuntoa, mukaan lukien korjaavat tai korvaavat toimenpiteet, ja toimitettava tietosuojaviranomaiselle kirjallinen vahvistus siitä, että kyseiset toimenpiteet on toteutettu.
- (49) Tietosuojaviranomaisten lausunto toimitetaan unionin tasoisen epävirallisen tietosuojaviranomaisten paneelin kautta, mikä auttaa yhtenäisen ja johdonmukaisen lähestymistavan varmistamisessa tietyn valituksen osalta ⁽⁴⁴⁾. Lausunto annetaan, kun kiistan molemmilla osapuolilla on ollut asianmukainen tilaisuus esittää haluamansa huomiot ja todistusaineisto. Paneeli antaa lausunnon niin nopeasti kuin asianmukainen menettely sallii ja yleensä 60 päivän kuluessa valituksen vastaanottamisesta. Jos organisaatio ei noudata lausuntoa 25 päivän kuluessa niiden antamisesta eikä anna mitään tyydyttävää selitystä viivästykselle, paneeli ilmoittaa aikomuksestaan joko saattaa asia kauppakomissiolle (tai muulle toimivaltaiselle yhdysvaltalaiselle täytäntöönpanoviranomaiselle) tai katsoa, että yhteistyötä koskevaa sitoumusta on rikottu vakavasti. Ensimmäisessä tapauksessa tämä voi johtaa FTC-lain (tai vastaavan säädöksen) 5 §:n mukaisiin täytäntöönpanotoimiin. Toisessa tapauksessa paneeli ilmoittaa asiasta kauppaministeriölle, joka katsoo, että jos organisaatio kieltäytyy noudattamasta tietosuojaviranomaisten paneelin lausuntoa, kyseessä on periaatteiden jatkuva noudattamatta jättäminen. Tällöin organisaatio poistetaan Privacy Shield -luettelosta.
- (50) 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 jäsenvaltion kansallisissa tuomioistuimissa.
- (51) Henkilöt voivat tehdä valituksen tietosuojaviranomaisille 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 Privacy Shield -järjestelyyn osallistuva organisaatio ei ole noudattanut periaatteita, kauppaministeriö perustaa erityisen yhteyspisteen pitämään yhteyttä tietosuojaviranomaisiin ja avustamaan niitä tutkimuksissa, jotka koskevat järjestelyn periaatteiden noudattamista organisaatiossa ⁽⁴⁵⁾. Samoin liittovaltion kauppakomissio on sitoutunut perustamaan yhteyspisteen ⁽⁴⁶⁾ ja avustamaan tietosuojaviranomaisia tutkimuksissa Yhdysvaltojen verkkoturvallisuuslain (U.S. SAFE WEB Act) ⁽⁴⁷⁾ mukaisesti.

⁽⁴¹⁾ Ks. liite II, III.11.e kohta.

⁽⁴²⁾ Ks. liite II, III.11.g kohta, erityisesti ii ja iii alakohta.

⁽⁴³⁾ Ks. liitteen I jakso "Kauppaministeriö etsii organisaatioita, jotka totuuden vastaisesti väittävät osallistuvansa järjestelyyn ja puuttuu tapauksiin".

⁽⁴⁴⁾ Tietosuojaviranomaisten olisi laadittava tietosuojaviranomaisten epävirallisen paneelin työjärjestys niiden työhönsä ja keskinäiseen yhteistyöhön liittyvän toimivaltansa perusteella.

⁽⁴⁵⁾ Ks. liitteen I jakso "Kauppaministeriö lisää yhteistyötään tietosuojaviranomaisten kanssa" ja "Kauppaministeriö edistää periaatteiden rikkomuksia koskevien valitusten ratkaisemista", sekä liite II, II.7.e kohta.

⁽⁴⁶⁾ Ks. liite IV, s. 6.

⁽⁴⁷⁾ Ks. edellinen viite.

- (52) Neljänneksi kauppaministeriö on sitoutunut vastaanottamaan, tarkastamaan ja parhaansa mukaan käsittelemään valitukset organisaatioista, jotka eivät ole noudattaneet järjestelyn periaatteita. Tätä varten kauppaministeriö laatii tietosuojaviranomaisille erityismenettelyt, joiden puitteissa valitukset siirretään erityiselle yhteyspisteelle, niitä seurataan ja niiden johdosta toteutetaan lisätoimia yritysten kanssa ratkaisun löytymisen helpottamiseksi. Yksittäisten valitusten käsittelyn jouduttamiseksi yhteyspiste toimii suoraan asiaankuuluvan tietosuojaviranomaisen kanssa sovellettavien periaatteiden noudattamista koskeissa kysymyksissä ja erityisesti ilmoittaa tälle valitusten käsittelyn etenemisestä enintään 90 päivän kuluessa siitä, kun asia on siirretty käsiteltäväksi. Tämä antaa rekisteröidyille mahdollisuuden tehdä valitus suoraan kansalliselle tietosuojaviranomaiselle, kun yhdysvaltalaiset oman varmuuden antaneet yritykset eivät noudata sovellettavia periaatteita, ja saada valitus siirrettyä Yhdysvaltojen kauppaministeriölle, joka on EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä hallinnoiva viranomainen. Kauppaministeriö on myös sitoutunut laatimaan EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn toimintaa koskevan vuotuisen tarkastelun yhteydessä kertomuksen, jossa sen vuoden aikana saamia valituksia analysoidaan kootussa muodossa ⁽⁴⁸⁾.
- (53) Jos kauppaministeriö toteaa viran puolesta tehtyjen tarkastusten, valitusten tai muiden tietojen perusteella, että organisaatio on jatkuvasti jättänyt noudattamatta järjestelyn periaatteita, se poistaa tällaisen organisaation Privacy Shield -luettelosta. Jos organisaatio kieltäytyy noudattamasta minkä tahansa yksityisyyden suojan itsesääntelystä vastaavan tahon, riippumattoman riitojenratkaisuelimen tai valtiollisen elimen, mukaan lukien tietosuojaviranomainen, lopullista päätöstä, se katsotaan periaatteiden jatkuvaksi noudattamatta jättämiseksi.
- (54) Viidenneksi Privacy Shield -järjestelyyn osallistuvan organisaation on kuuluttava Yhdysvaltojen viranomaisten, erityisesti liittovaltion kauppakomission (Federal Trade Commission, FTC) ⁽⁴⁹⁾ tutkinta- ja täytäntöönpanovallan piiriin, jotta voidaan tehokkaasti varmistaa periaatteiden noudattaminen. Liittovaltion kauppakomissio asettaa etusijalle sellaiset järjestelyn periaatteiden noudattamatta jättämisestä koskevat tapaukset, jotka on saatu riippumattomilta riitojenratkaisu- tai itsesääntelyelimiltä, kauppaministeriöltä ja tietosuojaviranomaisilta (jotka toimivat joko omasta aloitteestaan tai valitusten perusteella), sen määrittämiseksi, onko FTC-lain 5 §:ää rikottu ⁽⁵⁰⁾. Liittovaltion kauppakomissio on sitoutunut luomaan vakiomuotoisen siirtomenettelyn, nimeämään yhteyspisteen tietosuojaviranomaisten sille tekemille siirroille ja vaihtamaan tietoja siirroista. Lisäksi se ottaa suoraan vastaan henkilöiden tekemiä valituksia ja toteuttaa Privacy Shield -järjestelyyn liittyviä tutkimuksia omasta aloitteestaan, erityisesti osana yksityisyyden suojaa koskevia laajempia tutkimuksiaan.
- (55) Liittovaltion kauppakomissio voi toteuttaa täytäntöönpanotoimia antamalla hallinnollisia määräyksiä ("suostumusmääräys", consent order), ja se valvoo järjestelmällisesti tällaisten määräysten noudattamista. Jos organisaatio ei noudata määräyksiä, liittovaltion kauppakomissio voi viedä asian toimivaltaisen tuomioistuimen käsiteltäväksi hakeakseen siviilioikeudellisia seuraamuksia ja muita korjaavia toimenpiteitä, mukaan lukien seuraamukset lainvastaisen toiminnan aiheuttamasta vahingosta. Vaihtoehtoisesti liittovaltion kauppakomissio voi pyytää suoraan alustavaa tai pysyvää kieltotuomiota tai muita korjaavia toimenpiteitä liittovaltion tuomioistuimessa. Privacy Shield -järjestelyyn kuuluvalla organisaatiolla annettuun suostumusmääräykseen liittyy omatoimista raportointia koskevia säännöksiä ⁽⁵¹⁾, ja organisaatioiden on julkaistava kaikki liittovaltion kauppakomissiolle toimitettuun, periaatteiden noudattamista koskevaan kertomukseen tai arviointikertomukseen sisältyvät, Privacy Shield -järjestelyyn liittyvät osuudet. Lisäksi liittovaltion kauppakomissio pitää verkossa yllä luetteloa yrityksistä, joille on annettu kauppakomission tai tuomioistuimen määräys Privacy Shield -järjestelyyn liittyvissä tapauksissa.
- (56) Kuudenneksi, jos valitusta ei ole ratkaistu tyydyttävästi minkään muun oikeussuojamekanismin avulla, EU:n rekisteröity voi turvautua viimesijaisena muutoksenhakumekanismina toimivan Privacy Shield -paneelin sitovaan välimiesmenettelyyn. Organisaatioiden on ilmoitettava henkilöille, että nämä voivat tietyin edellytyksin pyytää sitovaa välimiesmenettelyä, ja niillä on velvollisuus esittää vastineensa, kun henkilö on turvautunut tähän mahdollisuuteen toimittamalla ilmoituksen asianomaiselle organisaatiolle ⁽⁵²⁾.

⁽⁴⁸⁾ Ks. liite I, jakso "Kauppaministeriö edistää periaatteiden rikkomuksia koskevien valitusten ratkaisemista".

⁽⁴⁹⁾ Privacy Shield -järjestelyyn kuuluvan organisaation on ilmoitettava julkisesti, että se on sitoutunut noudattamaan järjestelyn periaatteita, julkistettava tietosuojaperiaatteensa järjestelyn periaatteiden mukaisesti ja pantava ne täysimääräisesti 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.

⁽⁵⁰⁾ 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. FTC-lain 20 §), ja se voi viedä asian tuomioistuimeen, jos tällaisia määräyksiä ei noudateta.

⁽⁵¹⁾ Kauppakomission tai tuomioistuimen määräyksissä voidaan vaatia yrityksiä toteuttamaan yksityisyydensuojaohjelmia ja antamaan kauppakomissiolle säännöllisesti kertomus järjestelyn periaatteiden noudattamisesta tai riippumattoman kolmannen osapuolen arviointi kyseisistä ohjelmista.

⁽⁵²⁾ Ks. liite II, II.1.xi ja III.7.c kohta.

- (57) Välimiespaneeli koostuu vähintään 20:stä välimiehestä, jotka kauppaministeriö ja komissio ovat nimittäneet heidän riippumattomuutensa, nuhteettomuutensa ja Yhdysvaltojen yksityisyyden suojaa koskevasta lainsäädännöstä ja unionin tietosuojalainsäädännöstä saamansa kokemuksen perusteella. Kunkin yksittäisen kiistan osalta osapuolet valitsevat välimiehistä yhden välimiehen tai kolmen välimiehen paneelin⁽⁵³⁾. Menettelyssä sovelletaan tavanomaisia välimiesmenettelysääntöjä, joista kauppaministeriö ja komissio sopivat. Nämä säännöt täydentävät jo laadittua kehystä, joka sisältää useita tämän mekanismin käyttömahdollisuuksia parantavia piirteitä EU:n rekisteröityjen kannalta: i) kansallinen tietosuojaviranomainen voi avustaa rekisteröityä tämän valmistellessa vaatimustaan paneelin käsiteltäväksi; ii) vaikka välimiesmenettely tapahtuu Yhdysvalloissa, EU:n rekisteröidyt voivat osallistua menettelyyn video- tai puhelinneuvottelun avulla, josta ei aiheudu henkilölle kustannuksia; iii) vaikka välimiesmenettelyssä käytettävä kieli on tavallisesti englanti, istunto voidaan yleensä tulkata ja aineisto kääntää⁽⁵⁴⁾ perustellusta pyynnöstä ilman että tästä aiheutuu rekisteröidylle kustannuksia; iv) vaikka kunkin osapuolen on maksettava omat asianajopalkkionsa, kauppaministeriö perustaa Privacy Shield -järjestelyyn osallistuvien organisaatioiden vuotuisista rahoitusosuuksista rahaston, josta katetaan välimiesmenettelyn tukikelpoiset kustannukset sellaiseen enimmäismäärään asti, jonka Yhdysvaltojen viranomaiset määrittävät komissiota kuultuaan.
- (58) Privacy Shield -paneelilla on valtuudet määrätä yksilökohtaisesta, ei-rahallisesta kompensaatista (individual-specific, non-monetary equitable relief)⁽⁵⁵⁾, joka on tarpeen järjestelyn periaatteiden noudattamatta jättämisen korjaamiseksi. Vaikka paneeli ottaa päätöstä tehdessään huomioon muut Privacy Shield -mekanismien perusteella toteutetut korjaavat toimenpiteet, henkilöt voivat silti turvautua välimiesmenettelyyn, jos ne pitävät näitä muita toimenpiteitä riittämättöminä. Näin EU:n rekisteröidyt voivat vedota välimiesmenettelyyn kaikissa tapauksissa, joissa Yhdysvaltojen toimivaltaisten viranomaisten (esimerkiksi liittovaltion kauppakomission) toiminnan tai toimimatta jättämisen vuoksi valituksia ei ole ratkaistu tyydyttävästi. Välimiesmenettelyyn ei voida vedota, jos tietosuojaviranomaisella on toimivalta ratkaista vaade yhdysvaltalaisen oman varmennuksen antaneen yrityksen osalta, toisin sanoen tapauksissa, joissa organisaatio on joko velvollinen tekemään yhteistyötä tietosuojaviranomaisten kanssa ja noudattamaan ohjeita työsuhteen yhteydessä kerättyjen henkilöstötietojen käsittelyn osalta tai on vapaaehtoisesti sitoutunut tekemään niin. Henkilöt voivat panna välimiesoikeuden päätöksen täytäntöön Yhdysvaltojen tuomioistuimissa liittovaltion välimiesmenettelystä annetun lain (Federal Arbitration Act) nojalla, ja varmistaa siten, että heidän käytössään on oikeussuojakeinoja, jos yritys ei noudata päätöstä.
- (59) Seitsemänneksi, jos organisaatio ei kunnioita sitoumustaan noudattaa järjestelyn periaatteita ja julkaistuja tietosuojaperiaatteita, muita oikeussuojakeinoja voi olla käytettävissä Yhdysvaltojen osavaltioiden lainsäädännön nojalla tapauksissa, joissa on kyse vahingonkorvauslainsäädännön (tort law) mukaisista korjaavista toimenpiteistä tai harhaanjohtavista lausumista, sopimattomista tai vilpillisistä toimista tai käytännöistä taikka sopimusrikkomuksista.
- (60) Lisäksi jos tietosuojaviranomainen EU:n rekisteröidyn esittämän vaateen saatuaan katsoo, että henkilötietoja siirretään Yhdysvalloissa sijaitsevalle organisaatiolle EU:n tietosuojalainsäädännön vastaisesti, mukaan lukien tapaukset, joissa EU:n tiedonviejällä on syytä uskoa, että organisaatio ei noudata järjestelyn periaatteita, se voi myös käyttää toimivaltaansa suhteessa tiedonviejään ja tarvittaessa määrätä, että tietojen siirto on keskeytettävä.
- (61) Tässä jaksossa esitettyjen tietojen perusteella komissio katsoo, että Yhdysvaltojen kauppaministeriön hyväksymät järjestelyn periaatteet varmistavat sellaisen henkilötietojen suojan tason, joka olennaisilta osin vastaa direktiivissä 95/46/EY vahvistetuissa aineellisoikeudellisissa peruseriaateissa taattua tasoa.
- (62) Lisäksi järjestelyn periaatteiden tehokas soveltaminen taataan läpinäkyvillä velvoitteilla ja Privacy Shield -järjestelyn hallinnolla ja periaatteiden noudattamista koskevilla tarkastelumenettelyillä, joista huolehtii kauppaministeriö.
- (63) Lisäksi komissio katsoo, että kokonaisuutena tarkasteltuna Privacy Shield -järjestelyyn kuuluvien valvonta-, muutoksenhaku- ja täytäntöönpanomekanismien avulla voidaan havaita tapaukset, joissa järjestelyyn liittynyt organisaatio rikkoo järjestelyn periaatteita, ja rangaista niistä käytännössä ja tarjota oikeussuojakeinoja rekisteröidylle, jotta tämä voi tutustua itseään koskeviin henkilötietoihin ja saada nämä tiedot oikaistuiksi tai poistetuiksi.

⁽⁵³⁾ Osapuolet sopivat paneelin välimiesten määrästä.

⁽⁵⁴⁾ Paneeli voi kuitenkin todeta tiettyyn välimiesmenettelyyn liittyvien olosuhteiden vuoksi, että kustannusten kattaminen johtaisi perusteettomiin tai suhteettomiin kustannuksiin.

⁽⁵⁵⁾ Henkilöt eivät voi vaatia välimiesmenettelyssä vahingonkorvausta, mutta välimiesmenettelyyn vetoaminen ei sulje pois mahdollisuutta hakea vahingonkorvausta tavanomaisissa yhdysvaltalaisissa tuomioistuimissa.

3. YHDYSVALTALAISTEN VIRANOMAISTEN PÄÄSY EU:N JA YHDYSVALTOJEN VÄLISEN PRIVACY SHIELD -JÄRJESTELYN PUITTEISSA SIIRRETTYIHIN HENKILÖTIETOIHIIN JA NIIDEN KÄYTTÖ

- (64) Kuten liitteen II I.5 kohdasta ilmenee, järjestelyn periaatteiden noudattamista rajoitetaan siinä määrin kuin se on tarpeen kansallisen turvallisuuden, yleisen edun tai lainvalvonnan vaatimusten vuoksi.
- (65) Komissio on arvioinut Yhdysvaltojen lainsäädännön mukaiset rajoitukset ja suojatoimet siltä osin kuin on kyse yhdysvaltalaisten viranomaisten pääsystä EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa siirrettyihin henkilötietoihin ja niiden käytöstä kansallisen turvallisuuden, lainvalvonnan ja muiden yleisen edun mukaisten tarkoitusten nimissä. Lisäksi Yhdysvaltojen hallitus on toimittanut komissiolle kansallisen tiedusteluviraston johtajan (Office of the Director of National Intelligence, ODNI) ⁽⁵⁶⁾ kautta yksityiskohtaisia lausumia ja sitoumuksia, jotka sisältävät tämän päätöksen liitteeseen VI. Yhdysvaltojen hallitus on myös ulkoministerin allekirjoittamalla ja tämän päätöksen liitteessä III olevalla kirjeellä sitoutunut luomaan uuden valvontamekanismin, joka liittyy tietoihin pääsyyn kansallisen turvallisuuden vuoksi, eli tiedusteluyhteisöstä riippumattoman, tietosuojasta vastaavan oikeusasiamiehen viran. Lisäksi tämän päätöksen liitteeseen VII sisältyvässä Yhdysvaltojen oikeusministeriön lausumassa kuvataan rajoituksia ja suojatoimia, joita sovelletaan viranomaisten pääsyyn tietoihin ja niiden käyttöön lainvalvonnan ja muiden yleisen edun mukaisten tarkoitusten nimissä. Avoimuuden lisäämiseksi ja näiden sitoumusten oikeudellisen luonteen huomioon ottamiseksi jokainen lueteltu ja tämän päätöksen liitteenä oleva asiakirja julkaistaan Yhdysvaltojen Federal Register -lehdessä.
- (66) Jäljempänä selvitetään tarkemmin komission päätelmiä rajoituksista, jotka koskevat yhdysvaltalaisten viranomaisten pääsyä Euroopan unionista Yhdysvaltoihin siirrettyihin henkilötietoihin ja niiden käyttöä sekä tehokkaan oikeussuojan olemassaoloa.

3.1. Yhdysvaltalaisten viranomaisten pääsy tietoihin ja niiden käyttö kansallisen turvallisuuden nimissä

- (67) Komission analyysi osoittaa, että Yhdysvaltojen lainsäädäntö sisältää useita rajoituksia EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa siirrettyihin tietoihin pääsulle ja niiden käytölle kansallisen turvallisuuden nimissä sekä valvontamekanismeja ja oikeussuojakeinoja, jotka tarjoavat riittävät suojatoimet tietojen suojaamiseksi tehokkaasti laittomalta pääsylvä ja väärinkäytösten riskiltä ⁽⁵⁷⁾. Tätä oikeudellista kehystä on vahvistettu huomattavasti vuoden 2013 jälkeen, jolloin komissio julkaisi kaksi tiedonantoa, kuten jäljempänä esitetään (ks. johdanto-osan 7 kappale).

3.1.1 Rajoitukset

- (68) Yhdysvaltojen perustuslain mukaan kansallisen turvallisuuden varmistaminen kuuluu presidentin toimivaltaan armeijan ylipäällikkönä ja ylipäätä toimeenpanevana viranomaisena, ja ulkomaantiedustelun osalta presidentti johtaa Yhdysvaltojen ulkoasioita ⁽⁵⁸⁾. Vaikka kongressilla on valtuudet asettaa rajoituksia, minkä se onkin tehnyt monessa suhteessa, presidentti voi näissä rajoissa johtaa Yhdysvaltojen tiedusteluyhteisön toimintaa erityisesti toimeenpanoasetusten (Executive Orders) tai presidentin määräysten (Presidential Directives) avulla. Tätä sovelletaan tietenkin myös niillä aloilla, joilla ei ole kongressin antamia ohjeita. Tällä hetkellä kaksi keskeistä oikeudellista välinettä tässä yhteydessä ovat toimeenpanoasetus 12333 ("toimeenpanoasetus (E.O.) 12333") ⁽⁵⁹⁾ ja presidentin määräys "Presidential Policy Directive 28".

⁽⁵⁶⁾ Kansallisen tiedusteluviraston johtaja (DNI) toimii tiedusteluyhteisön päällikkönä ja presidentin ja kansallisen turvallisuusneuvoston pääneuvonantajana. Ks. vuoden 2004 Intelligence Reform and Terrorism Prevention Act, Pub. L. 108-458, 17.12.2004. Kansallisen tiedusteluviraston johtaja muun muassa määrittää vaatimukset tiedusteluyhteisön suorittaman kansallisen tiedustelutoiminnan toimeksiantajille ja tiedustelutietojen keräämiselle, analysoinnille, tuottamiselle ja levittämiseksi sekä johtaa ja ohjaa näitä toimintoja esimerkiksi laatimalla ohjeita tietoihin tai tiedustelutietoihin pääsystä ja niiden käytöstä ja jakamisesta. Ks. toimeenpanoasetuksen (E.O.) 12333 1.3 (a) ja (b) §.

⁽⁵⁷⁾ Ks. Schrems, 91 kohta.

⁽⁵⁸⁾ Yhdysvaltojen perustuslaki, II artikla. Ks. myös johdanto presidentin määräykseen PPD-28.

⁽⁵⁹⁾ E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). Siltä osin kuin toimeenpanoasetus on julkisesti saatavilla, siinä määritellään Yhdysvaltojen tiedustelutoiminnan tavoitteet, tarkoitus, tehtävät ja vastuut (mukaan lukien tiedusteluyhteisön eri toimijoiden roolit) ja vahvistetaan tiedustelutoiminnassa noudatettavat yleisperiaatteet (erityisesti tarve antaa erityisiä menettelysääntöjä). Toimeenpanoasetuksen (E.O.) 12333 3.2 §:n mukaan presidentti, kansallisen turvaneuvoston tukemana, ja DNI antavat ne asianmukaiset määräykset ja ohjeet ja määrittävät ne menettelyt, jotka ovat tarpeen asetuksen täytäntöönpanemiseksi.

- (69) Presidentin määräyksessä PPD-28 (Presidential Policy Directive 28), joka annettiin 17 päivänä tammikuuta 2014, asetetaan useita rajoituksia signaalitiedustelutoiminnalle⁽⁶⁰⁾. Kyseinen määräys sitoo Yhdysvaltojen tiedusteluviranomaisia⁽⁶¹⁾ ja pysyy voimassa Yhdysvaltojen hallinnossa tapahtuvista muutoksista huolimatta⁽⁶²⁾. PPD-28 on erityisen tärkeä ei-yhdysvaltalaisille henkilöille, myös EU:n rekisteröidyille. Siinä säädetään muun muassa, että:
- a) tietojen keruun signaalitiedustelun avulla on perustuttava säädökseen tai presidentin hyväksyntään ja se on suoritettava Yhdysvaltojen perustuslain (erityisesti sen neljännen lisäyksen) ja Yhdysvaltojen lainsäädännön mukaisesti;
 - b) kaikkia henkilöitä olisi kohdeltava ihmisarvoisesti ja kunnioittavasti, riippumatta heidän kansalaisuudestaan tai siitä, missä he mahdollisesti asuvat;
 - c) kaikki henkilöt ovat oikeutettuja yksityisyyden suojaan heidän henkilötietojensa käsittelyssä;
 - d) yksityisyyden suoja ja kansalaisvapaudet muodostavat olennaisen osan Yhdysvaltojen signaalitiedustelutoiminnan suunnittelussa;
 - e) Yhdysvaltojen signaalitiedustelutoiminnassa on sen vuoksi huomioitava asianmukaiset suojatoimet kaikkien henkilöiden henkilötietojen osalta riippumatta heidän kansallisuudestaan tai siitä, missä he mahdollisesti asuvat.
- (70) PPD-28:n mukaan signaalitiedustelutietoja voidaan kerätä ainoastaan, jos tarkoituksena on ulkomaantiedustelu tai vastatiedustelu kansallisen tai ministeriötason tehtävien tukemiseksi, ei mihinkään muuhun tarkoitukseen (esim. kilpailuedun antamiseksi yhdysvaltalaisille yhtiöille). Tältä osin ODNI selittää, että tiedusteluyhteisön toimijoiden ”olisi vaadittava, että keruun olisi mahdollisuuksien mukaan keskityttävä tiettyihin ulkomaisiin tiedustelukohteisiin tai -aiheisiin erottelutekijöiden avulla (esim. erityiset viestintävälineet, valintakriteerit ja tunnisteet)”⁽⁶³⁾. Lisäksi lausumat varmistavat, että tiedustelutietojen keräämistä koskevien päätösten tekemistä ei jätetä yksittäisten tiedustelupalvelun edustajien harkintavaltaan, vaan niihin sovelletaan sellaisia toimintaperiaatteita ja menettelytapoja, jotka Yhdysvaltojen tiedusteluyhteisön eri toimijoiden (virastot) on otettava käyttöön PPD-28:n panemiseksi täytäntöön⁽⁶⁴⁾. Tämän vuoksi asianmukaisten valintakriteerien tutkiminen ja määrittäminen tapahtuu yleisen kansallisia tiedusteluprioriteetteja koskevan kehyksen (National Intelligence Priorities Framework) puitteissa. Näin varmistetaan, että korkean tason poliittiset päättäjät asettavat tiedustelun painopisteet ja että niitä tarkistetaan säännöllisesti, jotta ne vastaavat ajankohtaisia kansallisia turvallisuushuolia, ja että niissä otetaan huomioon mahdolliset riskit, myös ne, jotka kohdistuvat yksityisyyden suojaan⁽⁶⁵⁾. Tämän perusteella viraston henkilöstö tutkii ja määrittelee erityiset valintakriteerit, joiden avulla on tarkoitus kerätä painopisteitä vastaavia ulkomaantiedustelutietoja⁽⁶⁶⁾. Valintakriteerejä on tarkistettava säännöllisesti, jotta nähdään, tarjoavatko ne edelleen arvokasta tiedustelutietoa painopisteiden mukaisesti⁽⁶⁷⁾.
-
- ⁽⁶⁰⁾ Toimeenpanoasetuksen (E.O.) 12333 mukaan Yhdysvaltojen kansallisen turvallisuusviraston (National Security Agency, NSA) johtaja on signaalitiedustelun operatiivinen johtaja, joka johtaa yhtenäistä signaalitiedustelutoiminnan organisaatiota.
- ⁽⁶¹⁾ Termin ”tiedusteluyhteisö” määritelmästä ks. E.O. 12333 3.5 (h) § ja PPD-28:n alaviite 1.
- ⁽⁶²⁾ Ks. oikeusministeriön oikeudellisen neuvonantajan muistio presidentti Clintonille (Memorandum by the Office of Legal Counsel, Department of Justice (DOJ), to President Clinton), 29.1.2000. Tämän oikeudellisen lausunnon mukaan presidentin määräyksellä on sama oikeudellinen vaikutus kuin toimeenpanoasetuksella.
- ⁽⁶³⁾ ODNI:n lausumat (liite VI), s. 3.
- ⁽⁶⁴⁾ Ks. PPD-28:n 4(b) ja (c) kohta. Julkisten tietojen mukaan vuoden 2015 tarkastelussa vahvistettiin nykyiset kuusi käyttötarkoitusta. Ks. ODNI, Signals Intelligence Reform, 2016 Progress Report.
- ⁽⁶⁵⁾ ODNI:n lausumat (liite VI), s. 6, viitaten tiedusteluyhteisöä koskevaan määräykseen nro 204 (Intelligence Community Directive 204). Ks. myös PPD-28:n 3 kohta.
- ⁽⁶⁶⁾ ODNI:n lausumat (liite VI), s. 6. Ks. esimerkiksi NSA Civil Liberties and Privacy Office (NSA CLPO), NSA’s Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014. Ks. myös ODNI Status Report 2014. Ulkomaantiedustelun valvontaa koskevan FISA-lain 702 pykälän mukaisesti tietoihin pääsystä tehtäviä pyyntöjä koskeviin tiedusteluihin sovelletaan ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen (FISC) hyväksymiä minimointimenettelyjä. Ks. NSA CLPO, NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014.
- ⁽⁶⁷⁾ Ks. Signals Intelligence Reform, 2015 Anniversary Report. Ks. myös ODNI:n lausumat (liite VI), s. 6, 8–9 ja 11.

- (71) Lisäksi PPD-28:ssa olevat vaatimukset, joiden mukaan tiedusteluaineiston keruun on aina ⁽⁶⁸⁾ oltava "mahdollisimman räätälöityä" ja että tiedusteluyhteisön on asetettava etusijalle muiden tietojen saatavuus ja asianmukaiset ja toteuttamiskelpoiset vaihtoehdot ⁽⁶⁹⁾, ovat kohdennetun keruun priorisointia valikoimattoman keruun sijaan koskevan yleissäännön mukaiset. ODN:n antaman vakuutuksen mukaan näillä vaatimuksilla varmistetaan erityisesti, että valikoimaton keruu ei ole "laajamittaista" eikä "kohdentamatonta" ja että poikkeus ei mene säännön edelle ⁽⁷⁰⁾.
- (72) Vaikka PPD-28:n mukaan tiedusteluyhteisön toimijoiden on joskus tietyissä olosuhteissa kerättävä valikoimattomia signaalitiedustelutietoja esimerkiksi havaitakseen ja arvioidakseen uusia tai kehittyviä uhkia, siinä ohjataan nämä toimijat antamaan etusija vaihtoehdoille, jotka mahdollistavat kohdennetun signaalitiedustelun ⁽⁷¹⁾. Tästä seuraa, että valikoimaton keruu suoritetaan vain, jos kohdennettu keruu erottelutekijöitä (ts. tiettyyn kohteeseen liittyvä tunnistus, kuten kohteen sähköpostiosoite tai puhelinnumero) käyttämällä ei ole mahdollista "teknisistä tai toiminnallisista syistä" ⁽⁷²⁾. Tämä koskee sekä tapaa, jolla signaalitiedustelutiedot kerätään, että sitä, mitä todellisuudessa kerätään ⁽⁷³⁾.
- (73) ODN:n lausumien mukaan tiedusteluyhteisö pyrkii rajoittamaan keruuta "mahdollisimman paljon" myös silloin, kun se ei voi käyttää erityisiä tunnistuksia keruun kohdentamiseksi. Tämän varmistamiseksi se "soveltaa suodattimia ja muita teknisiä keinoja keskittääkseen keruun niihin välineisiin, jotka todennäköisesti sisältävät ulkomaantiedustelun kannalta arvokasta viestintätietoa" (ja näin ollen vastaavat Yhdysvaltojen poliittisten päättäjien esittämiä vaatimuksia edellä johdanto-osan 70 kappaleessa kuvatun prosessin mukaisesti). Tämän seurauksena valikoimaton keruu kohdennetaan vähintään kahdella tavalla. Ensinnäkin sen on aina liityttävä tiettyihin ulkomaantiedustelun tavoitteisiin (esim. signaalitiedustelutietojen hankkimiseksi tietyllä alueella toimivan terroristiryhmän toiminnasta) ja keskityttävä sellaisen viestinnän keruuseen, jolla on tämä yhteys. ODN:n vakuutusten mukaan tämä näkyy siitä, että "Yhdysvaltojen signaalitiedustelutoiminta koskee vain murto-osaa internetviestinnästä" ⁽⁷³⁾. Toiseksi ODN:n lausumissa selitetään, että käytettävät suodattimet ja muut tekniset keinot suunnitellaan niin, että keruu keskitetään mahdollisimman tarkasti, jotta varmistetaan, että kerätyn "merkityksellisen tiedon" määrä on mahdollisimman pieni.
- (74) Myös silloin kun Yhdysvallat pitää tarpeellisenä kerätä valikoimattomia signaalitiedustelutietoja johdanto-osan 70–73 kappaleessa esitettyjen edellytysten mukaisesti, määräyksessä PPD-28 rajoitetaan tällaisten tietojen käyttö erityiseen luetteloon, johon sisältyy kuusi kansalliseen turvallisuuteen liittyvää käyttötarkoitusta, kaikkien henkilöiden yksityisyyden suojan ja kansalaisvapauksien suojelemiseksi heidän kansalaisuudestaan tai asuinpaikastaan riippumatta ⁽⁷⁴⁾. Näihin sallittuihin käyttötarkoituksiin kuuluvat toimenpiteet, joiden avulla voidaan havaita ja torjua uhkia, jotka johtuvat vakoilusta, terrorismista, joukkotuhoaseista, tai uhkia, jotka

⁽⁶⁸⁾ Ks. alaviite 63.

⁽⁶⁹⁾ On myös huomattava, että toimeenpanoasetuksen (E.O.) 12333 2.4 §:n mukaan tiedusteluyhteisön toimijoiden "on käytettävä Yhdysvalloissa mahdollisimman vähän häiritseviä keruutekniikkoja". Rajoituksista, jotka koskevat kaiken valikoimattoman keruun korvaamista kohdennetulla keruulla, katso kansallisen tutkimusneuvoston suorittaman arvioinnin tulokset, joista Euroopan unionin perusoikeusvirasto on raportoinut, Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015), s. 18.

⁽⁷⁰⁾ ODN:n lausumat (liite VI), s. 4.

⁽⁷¹⁾ Ks. myös PPD-28:n 5(d) kohta, jonka mukaan kansallisen tiedusteluviraston johtajan on yhteistyössä asiaankuuluvien tiedusteluyhteisön toimijoiden johtajien ja tiede- ja teknologiapolitiikan viraston (Office of Science and Technology Policy) kanssa annettava presidentille "raportti, jossa arvioidaan mahdollisuutta luoda ohjelmisto, jonka avulla tiedusteluyhteisö voi helpommin toteuttaa kohdennetun tietojen keruun valikoimattoman vähän häiritseviä keruutekniikkoja". Julkisten tietojen mukaan tämän raportin tulos oli, että "ei ole olemassa ohjelmistopohjaista vaihtoehtoa, joka tarjoaa täydellisen vaihtoehdon valikoimattomalle keruulle, jonka tarkoituksena on havaita eräät kansalliseen turvallisuuteen kohdistuvat uhkat". Ks. Signals Intelligence Reform, 2015 Anniversary Report.

⁽⁷²⁾ Ks. alaviite 63.

⁽⁷³⁾ ODN:n lausumat (liite VI). Tällä vastataan erityisesti kansallisten tietosuojaviranomaisten tietosuojan tason riittävyttä koskevasta päätösluonnoksesta antamassaan lausunnossa ilmaisemiin huolenaiheisiin. Ks. 29 artiklan mukaisen tietosuojatyöryhmän lausunto 01/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan tason riittävyttä koskevasta päätösluonnoksesta (annettu 13.4.2016), s. 38, ja alaviite 47.

⁽⁷⁴⁾ Ks. PPD-28:n 2 kohta.

kohdistuvat verkkoturvallisuuteen, asevoimiin tai sotilashenkilöistöön, samoin kuin kansainvälisen rikollisuuden uhkia, jotka liittyvät muihin viiteen käyttötarkoitukseen. Niitä tarkistetaan vähintään vuosittain. Yhdysvaltojen hallituksen lausumien mukaan tiedusteluyhteisön toimijat ovat vahvistaneet analysoimattomiin signaalitiedustelutietoihin liittyviä pyyntöjä koskevia analyttisiä menetelmiään ja standardejaan, jotta ne olisivat näiden vaatimusten mukaisia; kohdennettujen pyyntöjen käyttö "varmistaa, että vain ne tiedot, joilla on mahdollisesti tiedusteluarvoa, esitetään analytikoille tutkittavaksi" ⁽⁷⁵⁾.

- (75) Nämä rajoitukset ovat erityisen tärkeitä EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa toimitettujen henkilötietojen kannalta erityisesti tapauksissa, joissa henkilötietojen keruu oli tarkoitus suorittaa Yhdysvaltojen ulkopuolella, mukaan lukien niiden siirtäminen transatlanttisia kaapeleita pitkin unionista Yhdysvaltoihin. Kuten Yhdysvaltojen viranomaiset ovat ODN:n lausumissa vahvistaneet, tällaiseen tietojen keruuseen sovelletaan kyseisissä lausumissa esitettyjä rajoituksia ja suojatoimia, myös niitä, jotka on vahvistettu PPD-28:ssa ⁽⁷⁶⁾.
- (76) Vaikka näitä periaatteita ei olekaan ilmaistu kyseisin oikeudellisin termein, niissä otetaan huomioon tarpeellisuutta ja suhteellisuutta koskevien periaatteiden keskeinen sisältö. Kohdennettu tietojenkeruu on selvästi etusijalla, kun taas valikoimaton keruu rajoittuu (poikkeuksellisiin) tilanteisiin, joissa kohdennettu keruu ei ole mahdollinen teknisistä tai toiminnallisista syistä. Myös silloin kun *valikoimatonta keruuta* ei voida välttää, tällaisten tietojen myöhempi "käyttö" tietoihin pääsyn kautta *rajoittuu tiukasti* tiettyihin, kansalliseen turvallisuuteen liittyviin laillisiin tarkoituksiin ⁽⁷⁷⁾.
- (77) Nämä vaatimukset sitovat koko tiedusteluyhteisöä, koska ne sisältyvät presidentin ylimpänä toimeenpanevana viranomaisena antamaan määräykseen, ja ne on pantu täytäntöön sellaisten viraston sääntöjen ja menettelyjen avulla, joilla yleiset periaatteet muunnetaan päivittäisiä toimintoja koskeviksi erityisohjeiksi. Vaikka PPD-28 ei sido kongressia, kongressi on itse toteuttanut toimenpiteitä, joilla varmistetaan, että henkilötietojen keruu Yhdysvalloissa ja niihin pääsy on kohdennettua, eikä sitä toteuteta "yleiseltä pohjalta".
- (78) Saatavilla olevien tietojen, kuten Yhdysvaltojen hallitukselta saatujen lausumien, perusteella voidaan todeta, että Yhdysvaltojen tiedusteluvirastot voivat sen jälkeen, kun tiedot on siirretty Yhdysvalloissa sijaitseville organisaatioille, jotka ovat antaneet oman varmennuksen EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa, pyytää henkilötietoja ainoastaan silloin ⁽⁷⁸⁾, kun pyyntö on ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act, FISA) mukainen tai sen on tehnyt Yhdysvaltojen liittovaltion poliisi (Federal Bureau of Investigation, FBI) niin sanotun kansallista turvallisuutta koskevan kirjeen (National Security Letter, NSL) ⁽⁷⁹⁾ perusteella. FISA-laki sisältää useita oikeusperustoja, joita voidaan käyttää EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa siirrettyjen, EU:n rekisteröityjä koskevien henkilötietojen keräämiseksi

⁽⁷⁵⁾ ODN:n lausumat (liite VI), s. 4. Ks. myös Intelligence Community Directive 203.

⁽⁷⁶⁾ ODN:n lausumat (liite VI), s. 2. Vastaavasti sovelletaan toimeenpanoasetuksessa (E.O.) 12333 esitettyjä rajoituksia (esim. kerättyjen tietojen on vastattava presidentin asettamia tiedustelun painopisteitä).

⁽⁷⁷⁾ Ks. Schrems, 93 kohta.

⁽⁷⁸⁾ Lisäksi FBI:n suorittama tietojen keruu voi perustua myös lainvalvontavaltuuksiin (ks. tämän päätöksen 3.2 jakso).

⁽⁷⁹⁾ Lisätietoja NSL:n käytöstä ks. ODN:n lausumat (liite VI), s. 13–14 ja alaviite 38. Kuten lausumassa todetaan, FBI voi käyttää NSL:ää pyytääkseen vain muuta kuin sisällöllistä tietoa, jolla on merkitystä hyväksytylle kansallista turvallisuutta koskevalle tutkimukselle kansainväliseltä terrorismilta tai salaiselta tiedustelutoiminnalta suojautumiseksi. EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa tapahtuvien tietosiirtojen osalta tärkein lakisääteinen lupa näyttää sisältyvän sähköisen viestinnän tietosuojaa koskevaan lakiin (Electronic Communications Privacy Act, 18 U.S.C. § 2709), jossa edellytetään, että kaikissa tilaaja- tai tapahtumatietoja koskevissa pyynnöissä käytetään "kriteeriä, joka nimenomaisesti yksilöi henkilön, yhteisön, puhelinnumeron tai tilin".

ja käsittelemiseksi. Näitä oikeusperustoja ovat FISA-lain 104 §⁽⁸⁰⁾, joka kattaa perinteisen yksilöllisen sähköisen valvonnan, ja 402 §⁽⁸¹⁾, joka käsittelee lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien (pen registers, trap and trace devices) asennusta. Muut kaksi keskeistä välinettä ovat FISA-lain 501 § (entinen U.S. PATRIOT ACT -lain 215 §) ja 702 §⁽⁸²⁾.

- (79) Tältä osin USA FREEDOM Act -laissa, joka annettiin 2 päivänä kesäkuuta 2015, kielletään valikoimattomien tietojen kerääminen FISA-lain 402 §:n (lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien käyttö lupa), FISA-lain 501 §:n (aikaisemmin U.S. PATRIOT ACT -lain 215 §)⁽⁸³⁾ ja NSL-kirjeiden perusteella. Sen sijaan siinä vaaditaan erityisten valintakriteerien käyttöä⁽⁸⁴⁾.
- (80) Vaikka FISA-laki sisältää muita oikeusperustoja kansalliselle tiedustelutoiminnalle, myös signaalitiedustelulle, komission arviointi osoittaa, että julkisten viranomaisten toimet rajoitetaan myös näissä oikeusperustoissa EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa siirrettyjen henkilötietojen osalta tietojen kohdennettuun keruuseen ja niihin pääsyyn.
- (81) Tämä on selvää kun on kyse perinteisestä yksilöllisestä sähköisestä valvonnasta FISA-lain 104 §:n nojalla⁽⁸⁵⁾. FISA-lain 702 §:n, joka muodostaa perustan kahdelle tärkeälle Yhdysvaltojen tiedusteluvirastojen tiedusteluohjelmalle (PRISM, UPSTREAM), mukaan tiedonhaut suoritetaan kohdennetusti käyttämällä yksittäisiä valintakriteerejä, joilla yksilöidään tietyt viestintävälineet, kuten kohteen sähköpostiosoite tai puhelinnumero, mutta ei avainkäsitteitä tai kohteena olevien henkilöiden nimiä⁽⁸⁶⁾. Kuten Privacy and Civil Liberties Oversight Board

⁽⁸⁰⁾ 50 U.S.C. § 1804. Vaikka tämä oikeusperusta edellyttää "lausumaa tosiseikoista ja olosuhteista, joihin hakija vetoaa perustellakseen näkemyksensä, että a) sähköisen valvonnan kohteena on ulkovalta tai ulkovaltan edustaja", viimeksi mainittuun voi sisältyä ei-yhdysvaltalaisia henkilöitä, jotka harjoittavat kansainvälistä terrorismia tai joukkotuhoaseiden kansainvälistä levittämistä (mukaan luettuna valmistelevat toimet) (50 U.S.C. § 1801 (b)(1)). EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa siirrettyihin henkilötietoihin on kuitenkin vain teoreettinen yhteys, sillä tosiasioita koskevassa lausumassa on myös perusteltava näkemys, että "kutakin viestintävälinettä tai paikkaa, johon sähköistä valvontaa kohdistetaan, käyttää tai aikoo käyttää ulkovalta tai ulkovaltan edustaja". Joka tapauksessa tämän valtuutuksen käyttö edellyttää hakemuksen tekemistä ulkomaantiedustelun valvonnasta vastaavalle tuomioistuimelle (FISC), joka arvioi muun muassa, onko toimitettujen tosiseikkojen perusteella todennäköistä, että näin todella on.

⁽⁸¹⁾ 50 U.S.C. § 1842 ja § 1841(2) sekä 18 osaston § 3127. 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). Se edellyttää hakemuksen tekemistä ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen (tai yhdysvaltalaisen alemman oikeusasteen tuomarin) määräyksen saamiseksi ja 1841(4) §:ssä tarkoitettun erityisen valintakriteerin käyttöä, eli kriteerin, joka nimenomaisesti yksilöi henkilön, tilin tms. ja jota käytetään niin suuressa määrin kuin on kohtuullista haluttujen tietojen laajuuden rajoittamiseksi.

⁽⁸²⁾ FISA-lain 501 §:ssä (entinen U.S. PATRIOT ACT -lain 215 §) valtuutetaan FBI pyytämään tuomioistuimen määräystä, jonka tarkoituksena on "aineellisten esineiden" (erityisesti puhelinliikenteen metadatan mutta myös liiketoimintaa koskevien tietojen) saanti ulkomaantiedustelua varten. Sen sijaan 702 § sallii Yhdysvaltojen tiedusteluyhteisön toimijoille mahdollisuuden pyytää pääsyä tietoihin, myös internetviestinnän sisältöön, Yhdysvalloista käsin mutta niin, että kohteena ovat tietyt ei-yhdysvaltalaiset henkilöt Yhdysvaltojen ulkopuolella.

⁽⁸³⁾ Tämän säännöksen perusteella FBI voi pyytää "aineellisia esineitä" (esim. tiedostot, paperit, asiakirjat) osoittamalla ulkomaantiedustelun valvonnasta vastaavalle tuomioistuimelle (FISC), että on perusteltuja syitä uskoa, että ne ovat merkityksellisiä FBI:n tietyn tutkimuksen kannalta. FBI:n on käytettävä tiedonhaussa FISC-tuomioistuimen hyväksymiä valintakriteerejä, joiden osalta on "kohtuullinen, perusteltu epäily" siitä, että tällainen kriteeri liittyy yhteen tai useampaan ulkovaltaan tai niiden edustajiin, jotka osallistuvat kansainväliseen terrorismiin tai niiden valmisteluun. Ks. PCLOB, Sec. 215 Report, s. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016, s. 4–6.

⁽⁸⁴⁾ ODN:n lausumat (liite VI), s. 13 (alaviite 38).

⁽⁸⁵⁾ Ks. alaviite 81.

⁽⁸⁶⁾ PCLOB, Sec. 702 Report, s. 32–33 viittauksineen. Yksityisyyden suojasta vastaavan toimiston mukaan Yhdysvaltojen kansallisen turvallisuusviraston (NSA) on varmistettava, että kohteen ja valintakriteerin välillä on yhteys, ja dokumentoitava ulkomaantiedustelutiedot, jotka on tarkoitus hankkia. Kahden NSA:n 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 Surveillance Act Section 702, 16.4.2014.

(PCLOB) on huomauttanut, 702 §:n mukaisen valvonnan ”kohteena ovat tietyt [ei-yhdysvaltalaiset] henkilöt, jotka on määritetty yksilöllisesti” ⁽⁸⁷⁾. Päätymislausekkeen vuoksi FISA-lain 702 §:ää on tarkasteltava uudelleen vuonna 2017, jolloin komission on arvioitava EU:n rekisteröityjen käytettävissä olevia suojatoimia.

- (82) Lisäksi Yhdysvaltojen hallitus on lausumissaan antanut Euroopan komissiolle nimenomaisen vakuutuksen siitä, että Yhdysvaltojen tiedusteluyhteisö ”ei harjoita kehenkään, esimerkiksi tavallisiin unionin kansalaisiin, kohdistuvaa kohdentamatonta valvontaa” ⁽⁸⁸⁾. Yhdysvalloissa kerättyjen henkilötietojen osalta tätä lausuntoa tukevat empiiriset todisteet, jotka osoittavat, että *tietopyynnöt*, jotka on tehty käyttämällä NSL-kirjettä tai FISA-lain mukaisesti joko yksittäin tai yhdessä, koskevat ainoastaan suhteellisen pientä määrää kohteita, kun tilannetta verrataan internetin yleiseen tietovirtaan ⁽⁸⁹⁾.
- (83) Kerättyihin tietoihin *pääsyn* ja *tietoturvan* osalta PPD-28:ssa edellytetään, että pääsy ”on rajoitettu vain luvan omaavaan henkilöstöön, joille tiedot ovat tarpeen tehtävänsä suorittamiseksi” ja että henkilötiedot ”on käsiteltävä ja säilytettävä arkaluonteisiin tietoihin sovellettavien suojatoimien mukaisesti sellaisissa olosuhteissa, jotka antavat riittävän suojan ja estävät sellaisilta henkilöiltä niihin pääsyn, joilla ei ole lupaa päästä tietoihin”. Tiedusteluhenkilöstö saa PPD-28:ssa vahvistettuja periaatteita koskevaa asianmukaista ja riittävää koulutusta ⁽⁹⁰⁾.
- (84) Yhdysvaltojen tiedusteluviranomaisten keräämien, EU:n rekisteröityjen henkilötietojen *säilyttämisestä* ja edelleen *levittämisestä* PPD-28:ssa todetaan, että kaikkia henkilöitä (myös ei-yhdysvaltalaisia) olisi kohdeltava ihmisarvoisesti ja kunnioittavasti, että kaikki henkilöt ovat oikeutettuja yksityisyyden suojaan henkilötietojensa käsittelyssä ja että tiedusteluyhteisön toimijoiden on sen vuoksi laadittava politiikkoja, jotka tarjoavat tällaisille tiedoille asianmukaiset suojatoimet, jotka ”on kohtuudella suunniteltu niin, että ne minimoivat [tietojen] levittämisen ja säilyttämisen” ⁽⁹¹⁾.

⁽⁸⁷⁾ PCLOB, Sec. 702 Report, s. 111. Ks. myös ODNIn lausumat (liite VI), s. 9, (”[FISA-lain] 702 §:n mukainen keruu ei ole” laajamittaista ja kohdentamatonta ”vaan että siinä keskitytään tarkasti keräämään ulkomaantiedustelutietoja yksittäin tunnistetuilta perustelluilta kohteilta”), ja s. 13, alaviite 36 (viittaus FISC-tuomioistuimen vuonna 2014 antamaan lausuntoon); NSA CLPO, NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Jopa UPSTREAMin tapauksessa NSA voi pyytää tietojen hankkimista ainoastaan käytettävien valintakriteerien lähtevästä tai saapuvasta tai niitä koskevasta sähköisestä viestinnästä.

⁽⁸⁸⁾ ODNIn lausumat (liite VI), s. 18. Ks. myös s. 6, jonka mukaan sovellettavat menettelyt ”osoittavat selkeän sitoumuksen estää mielivaltaisen ja kohdentamaton signaalitiedustelutietojen keruu ja panna täytäntöön – hallituksemme korkeimmalta tasolta lähtien – kohtuusperiaate”.

⁽⁸⁹⁾ Ks. Statistical Transparency Report Regarding Use of National Security Authorities, 22.4.2015. Internetin yleisestä tietovirrasta, ks. esim. perusoikeusvirasto, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), s. 15–16. UPSTREAM-ohjelmasta on todettava, että FISC-tuomioistuimen vuonna 2011 antaman ja julkistaman lausunnon mukaan yli 90 prosenttia FISA-lain 702 §:n nojalla hankitusta sähköisestä viestinnästä tuli PRISM-ohjelmasta ja alle 10 prosenttia UPSTREAM-ohjelmasta. Ks. FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), alaviite 21 (saatavilla osoitteessa <http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>).

⁽⁹⁰⁾ Ks. PPD-28:n 4(a)(ii) kohta. Ks. myös ODNIn, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, heinäkuu 2014, s. 5, jonka mukaan ”tiedusteluyhteisön politiikkojen olisi vahvistettava nykyisiä analyyttisiä menetelmiä ja standardeja, joiden mukaan analyytikkojen on pyrittävä jäsentämään tiedustelukysymykset tai muut hakuehdot ja -tekniikat tunnistaaakseen tiedustelutiedot, jotka ovat merkityksellisiä perustellun tiedustelu- tai lainvalvontatehtävän kannalta; keskitettävä tiedustelukysymykset henkilöistä niihin tiedustelutietojen luokkiin, jotka vastaavat tiedustelun tai lainvalvonnan tiedontarvetta; ja minimoitava sellaisten henkilötietojen tarkastelu, jotka eivät ole merkityksellisiä tiedustelun tai lainvalvonnan tiedontarpeen kannalta”. Ks. esim. CIA, Signals Intelligence Activities, s. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, s. 3. Signaalitiedustelutoiminnan uudistamista koskevan vuoden 2016 edistyskertomuksen mukaan tiedusteluyhteisön toimijat (kuten FBI, CIA ja NSA) ovat toteuttaneet toimia, joiden tarkoituksena on saada henkilöstö tietoiseksi PPD-28:n vaatimuksista luomalla uusia tai muuttamalla olemassa olevia koulutustoimia.

⁽⁹¹⁾ ODNIn lausumien mukaan näitä rajoituksia sovelletaan riippumatta siitä, onko tiedot kerätty valikoimattomasti vai kohdennetusti, ja riippumatta henkilön kansalaisuudesta.

- (85) Yhdysvaltojen hallituksen mukaan tämä kohtuusvaatimus tarkoittaa sitä, että tiedusteluyhteisön toimijoiden ei tarvitse ottaa käyttöön "mitä tahansa teoriassa mahdollista toimenpidettä" vaan että niiden on "tasapainotettava toimensa yksityisyyttä ja kansalaisvapauksia koskevien oikeutettujen etujen suojelemiseksi signaalitiedustelu-toiminnan käytännön vaatimusten kanssa" ⁽⁹²⁾. Tältä osin ei-yhdysvaltalaisia henkilöitä kohdellaan samoin kuin yhdysvaltalaisia Yhdysvaltojen oikeusministerin hyväksymien menettelyjen perusteella ⁽⁹³⁾.
- (86) Näiden sääntöjen mukaan tietoja säilytetään yleensä enintään viisi vuotta, ellei laissa ole erityissäännöstä tai ellei kansallisen tiedusteluviraston johtaja yksityisyyden suojaa koskevia kysymyksiä huolellisesti arvioituaan ja ODN:n kansalaisvapauksien suojasta vastaavan neuvonantajan samoin kuin viraston kansalaisvapauksiin liittyviä tehtäviä hoitavien virkamiesten näkemykset huomioon ottaen määrää, että tietojen säilyttämisen jatkaminen on kansallisen turvallisuuden edun mukaista ⁽⁹⁴⁾. Tietojen levittäminen on rajattu tapauksiin, joissa tiedot ovat merkityksellisiä keruun tarkoituksen kannalta ja näin ollen ne vastaavat hyväksytyn ulkomaantiedustelun tai lainvalvonnan tiedontarvetta ⁽⁹⁵⁾.
- (87) Yhdysvaltojen hallituksen antamien vakuutusten mukaan henkilötietoja ei saa levittää pelkästään sillä perusteella, että asianomainen henkilö ei ole yhdysvaltalainen ja että "ulkomaalaisen henkilön tavanomaiseen toimintaan kohdistuvaa signaalitiedustelua ei katsottaisi ulkomaantiedusteluksi, jota voitaisiin levittää tai säilyttää pysyvästi pelkästään tämän seikan perusteella, ellei se muutoin vastaa hyväksyttyä ulkomaantiedustelutiedon tarvetta" ⁽⁹⁶⁾.
- (88) Edellä olevan perusteella komissio katsoo, että Yhdysvalloissa on käytössä sääntöjä, joilla pyritään rajoittamaan puuttumista kansallisen turvallisuuden nimissä sellaisten henkilöiden perusoikeuksiin, joiden henkilötietoja siirretään unionista Yhdysvaltoihin EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn nojalla, siihen mikä on ehdottomasti tarpeen oikeutetun tavoitteen saavuttamiseksi.
- (89) Kuten edellä oleva analyysi osoittaa, Yhdysvaltojen lainsäädännössä varmistetaan, että valvonta- ja tarkkailutoimenpiteitä käytetään ainoastaan ulkomaantiedustelutiedon hankkimiseksi – mikä on oikeutettu poliittinen tavoite ⁽⁹⁷⁾ – ja niitä räätälöidään mahdollisimman paljon. Erityisesti on huomattava, että valikoimaton keruu

⁽⁹²⁾ Ks. ODN:n lausumat (liite VI).

⁽⁹³⁾ Ks. PPD-28:n 4(a)(i) kohta ja toimeenpanoasetuksen (E.O.) 12333 2.3 §.

⁽⁹⁴⁾ PPD-28:n 4(a)(i) kohta; ODN:n lausumat (liite VI), s. 7. Esimerkiksi FISA-lain 702 §:n nojalla kerättyjen henkilötietojen osalta NSA:n FISC-hyväksytyissä minimointimenettelyissä on sääntönä, että PRISM-ohjelman metadataa ja analysoimaton sisältöä ei säilytetä viittä vuotta kauempaa, kun taas UPSTREAM-datan säilytysaika on enintään kaksi vuotta. NSA käyttää säilytysaikojen noudattamisessa automaattista prosessia, jossa kerätyt tiedot poistetaan kulloisenkin säilytysajan päätyttyä. Ks. NSA Sec. 702 FISA Minimization Procedures, 7 kohta ja 6(a)(1) kohta; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Samoin FISA-lain 501 §:n (ent. U.S. PATRIOT ACT -lain 215 §) mukainen säilytysaika on enintään viisi vuotta, elleivät henkilötiedot kuulu ulkomaantiedustelutietoihin, joiden levittäminen on asianmukaisesti hyväksytty, tai ellei oikeusministeriö anna NSA:lle kirjallista ohjetta siitä, että tiedot kuuluvat säilytysvelvollisuuden piiriin käynnissä olevassa tai tulevassa oikeudenkäynnissä. Ks. NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016.

⁽⁹⁵⁾ Erityisesti FISA-lain 501 §:n (ent. U.S. PATRIOT ACT -lain 215 §) tapauksessa henkilötietoja voidaan levittää vain terrorismin torjumiseksi tai todisteena rikoksesta; FISA-lain 702 §:n tapauksessa ainoastaan jos on kyse perustellusta ulkomaantiedusteluun tai lainvalvontaan liittyvästä käyttötarkoituksesta. Vrt. NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016. Ks. myös NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

⁽⁹⁶⁾ ODN:n lausumat (liite VI), s. 7 (viitaten tiedusteluyhteisöä koskevaan määräykseen nro 203 (Intelligence Community Directive, ICD 203).

⁽⁹⁷⁾ Unionin tuomioistuin on selvittänyt, että kansallinen turvallisuus muodostaa oikeutetun poliittisen tavoitteen. Ks. Schrems, 88 kohta. Ks. myös asia Digital Rights Ireland ym., tuomion 42–44 ja 51 kohta, jossa unionin tuomioistuin katsoi, että vakavan rikollisuuden, erityisesti järjestäytyneen rikollisuuden ja terrorismin, torjuminen voi riippua suuressa määrin nykyaikaisten tutkintatekniikojen käytöstä. Lisäksi toisin kuin rikostutkinnassa, joka tyypillisesti koskee vastuun määrittämistä taannehtivasti ja syyllisyyttä aikaisemmasta toiminnasta, tiedustelutoiminnassa keskitytään usein kansalliseen turvallisuuteen kohdistuvien uhkien ehkäisemiseen ennen kuin vahinko on tapahtunut. Näin ollen tällaisen tutkimuksen on usein katettava useampia mahdollisia toimijoita ("kohteita") ja laajempi maantieteellinen alue. Vrt. Euroopan ihmisoikeustuomioistuin, Weber ja Saravia v. Saksa, päätös 29.6.2006, hakemus nro 54934/00, 105–118 kohta (ns. strateginen seuranta).

voidaan hyväksyä ainoastaan poikkeuksellisesti, jos kohdennettu keruu ei ole mahdollinen, ja siihen liitetään ylimääräisiä suojatoimia, joilla kerättyjen tietojen määrä ja niihin pääsy minimoidaan (pääsy on kohdennettava ja sallittava ainoastaan tiettyihin tarkoituksiin).

- (90) Komission arvioinnin mukaan tämä vastaa unionin tuomioistuimen tuomiossa Schrems vahvistamaa standardia. Tuomion mukaan säännöstyössä, jolla puututaan perusoikeuskirjan 7 ja 8 artiklassa taattuihin perusoikeuksiin, on säädettävä "vähimmäisvaatimuksista" ⁽⁹⁸⁾, minkä lisäksi tuomiossa todetaan, että "siihen, mikä on ehdottomasti tarpeen, ei siis rajoitu säännöstö, jossa sallitaan yleisesti kaikkien henkilöiden, joiden henkilötiedot on siirretty unionista Yhdysvaltoihin, kaikkien henkilötietojen säilyttäminen tekemättä mitään erottelua, rajoitusta tai poikkeusta tavoiteltavan päämäärän mukaan ja säätämättä objektiivisesta perusteesta, jolla voitaisiin rajoittaa viranomaisten pääsyä tietoihin ja rajata niiden myöhempi käyttö tarkoituksiin, jotka ovat täsmällisiä, täysin rajallisia ja omiaan oikeuttamaan puuttumisen, jota niin henkilötietoihin pääsy kuin niiden käyttökin merkitsevät" ⁽⁹⁹⁾. Rajoittamatonta kaikkien henkilöiden tietojen keruuta ja säilyttämistä ilman rajoituksia ei harrasteta, ei myöskään rajoittamatonta pääsyä tietoihin. Lisäksi komissiolle annetut lausumat, mukaan lukien vakuutus siitä, että Yhdysvaltojen signaalitiedustelutoiminta koskee vain murto-osaa internetviestinnästä, sulkevat pois mahdollisuuden "yleisestä" pääsystä ⁽¹⁰⁰⁾ sähköisen viestinnän sisältöön.

3.1.2 Tehokas oikeussuoja

- (91) Komissio on arvioinut sekä Yhdysvalloissa käytössä olevat valvontamekanismit siltä osin kuin on kyse Yhdysvaltojen tiedusteluviranomaisten puuttumisesta Yhdysvaltoihin siirrettyihin henkilötietoihin että EU:n rekisteröityjen käytettävissä olevat oikeussuojakeinot.

Valvonta

- (92) Yhdysvaltojen tiedusteluyhteisöön sovelletaan erilaisia tarkastelu- ja valvontamekanismeja, jotka kuuluvat valtionhallinnon kolmeen haaraan. Näitä ovat toimeenpanohaaran sisäiset ja ulkoiset elimet, useat kongressin valiokunnat sekä tuomioistuINVALVONTA, viimeksi mainittu erityisesti ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act) soveltamisalaan kuuluvan toiminnan osalta.
- (93) Ensinnäkin toimeenpanohaaran sisällä valvotaan laajasti Yhdysvaltojen viranomaisten tiedustelutoimintaa.
- (94) PPD-28:n 4(a)(iv) kohdan mukaan tiedusteluyhteisön toimintaperiaatteisiin ja menettelytapoihin "on sisällytettävä asianmukaisia toimenpiteitä, joilla helpotetaan henkilötietojen suojatoimien täytäntöönpanon valvontaa"; näihin toimenpiteisiin on kuuluttava säännölliset tarkastukset ⁽¹⁰¹⁾.

⁽⁹⁸⁾ Ks. Schrems, 91 kohta oikeuskäytäntöviittauksiin.

⁽⁹⁹⁾ Schrems, 93 kohta.

⁽¹⁰⁰⁾ Vrt. Schrems, 94 kohta.

⁽¹⁰¹⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7. Ks. esim. CIA, Signals Intelligence Activities, s. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, III(A)(4) ja (B)(4) kohta; NSA, PPD-28 Section 4 Procedures, 12.1.2015, 8.1 ja 8.6(c) kohta.

- (95) Tältä osin on otettu käyttöön useita valvontakerroksia, mukaan lukien kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavat virkamiehet, valvontaviranomaiset, ODN:n kansalaisvapauksista ja yksityisyyden suojaasta vastaava toimisto (ODNI Civil Liberties and Privacy Office), PCLOB ja presidentin tiedusteluvalvontakomitea (President's Intelligence Oversight Board). Näitä valvontatehtäviä tukevat määräysten noudattamisesta vastaava henkilöstö kaikissa virastoissa ⁽¹⁰²⁾.
- (96) Kuten Yhdysvaltojen hallitus on todennut ⁽¹⁰³⁾, kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavia virkamiehiä, jotka vastaavat valvonnasta, on niissä ministeriöissä, joilla on tiedusteluvastuita, ja tiedusteluvirastoissa ⁽¹⁰⁴⁾. Vaikka näiden viranomaisten toimivalta voi vaihdella jonkin verran perustana olevan lainsäädännön mukaan, ne yleensä kattavat menettelyjen valvonnan sen varmistamiseksi, että kyseessä oleva ministeriö/virasto ottaa asianmukaisesti huomioon yksityisyyden suojaan ja kansalaisvapauksiin liittyvät huolenaiheet ja että se 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 ODN:n tapaam. toimivalta tutkia valituksia ⁽¹⁰⁵⁾). Ministeriön/viraston johtajan on puolestaan varmistettava, että virkamies saa kaikki tiedot ja pääsee tutustumaan kaikkeen aineistoon, joka on tarpeen hänen tehtävänsä suorittamiseksi. Kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavat virkamiehet raportoivat säännöllisesti kongressille ja PCLOBille muun muassa seuraavista: ministeriön/viraston vastaanottamien valitusten lukumäärä ja luonne sekä yhteenvedot niihin annetuista päätöksistä, suoritettut arvioinnit ja tarkastelut ja virkamiehen toteuttamien toimien vaikutus ⁽¹⁰⁶⁾. Kansallisten tietosuojaviranomaisten arvion mukaan kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavien virkamiesten suorittamaa sisäistä valvontaa voidaan pitää suhteellisen tehokkaana, vaikka tietosuojaviranomaisten mielestä kyseisten virkamiesten riippumattomuus ei ole vaaditulla tasolla ⁽¹⁰⁷⁾.
- (97) Lisäksi kullakin tiedusteluyhteisön toimijalla on oma valvontaviranomaisensa (Inspector General), jonka tehtävänä on muun muassa valvoa ulkomaantiedustelua ⁽¹⁰⁸⁾. Tähän sisältyy ODN:n yhteydessä oleva 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 ⁽¹⁰⁹⁾. Valvontaviranomaiset muodostavat lakisääteisesti riippumattomia ⁽¹¹⁰⁾ yksiköitä, joiden tehtävänä on suorittaa tarkastuksia ja tutkimuksia, jotka koskevat kansalliseen tiedusteluun liittyviä, kyseessä olevan viraston ohjelmia ja niiden toteuttamia toimia, mukaan lukien valtaoikeuksien väärinkäyttö tai lain rikkominen ⁽¹¹¹⁾. Niillä on oikeus saada käyttöönsä kaikki tiedot, raportit, tarkastusaineistot, arvioinnit, asiakirjat, työpaperit, suositukset tai muu asianmukainen aineisto, tarvittaessa haasteteitse, ja ne voivat

⁽¹⁰²⁾ Esimerkiksi NSA:n vaatimusten noudattamisesta vastaavan osaston palveluksessa on yli 300 henkeä. Ks. ODN:n lausumat (liite VI), s. 7.

⁽¹⁰³⁾ Ks. oikeusasiamiesmekanismi (liite III), 6 kohdan b alakohdan i–iii alakohta.

⁽¹⁰⁴⁾ Ks. 42 U.S.C. § 2000ee-1. Tämä koskee esimerkiksi Yhdysvaltojen ulkoasiainministeriötä, oikeusministeriötä (myös FBI:tä), sisäisen turvallisuuden ministeriötä, puolustusministeriötä, NSA:ta, CIA:ta ja ODN:ia.

⁽¹⁰⁵⁾ Yhdysvaltojen hallitus on todennut, että jos ODN:n kansalaisvapauksista ja yksityisyyden suojaasta vastaava toimisto vastaanottaa valituksen, se myös koordinoi muiden tiedusteluyhteisön toimijoiden kanssa, miten kyseinen valitus olisi edelleen käsiteltävä tiedusteluyhteisössä. Ks. oikeusasiamiesmekanismi (liite III), 6 kohdan b alakohdan ii alakohta.

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

⁽¹⁰⁷⁾ 29 artiklan mukaisen tietosuojatyöryhmän lausunto 01/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskevasta päätösluonnoksesta (13.4.2016), s. 41.

⁽¹⁰⁸⁾ ODN:n lausumat (liite VI), s. 7. Ks. esim. NSA, PPD-28 Section 4 Procedures, 12.1.2015, 8.1 kohta; CIA, Signals Intelligence Activities, s. 7 (Responsibilities).

⁽¹⁰⁹⁾ Tämän valvontaviranomaisen (jonka virka perustettiin lokakuussa 2010) nimittää presidentti, ja nimityksen vahvistaa senaatti. Valvontaviranomaisen voi erottaa ainoastaan presidentti, ei DNI.

⁽¹¹⁰⁾ 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 tutkimusta, 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. esim. Inspector General Act of 1978, 8 § (puolustusministeriön valvontaviranomainen); 8E § (oikeusministeriön valvontaviranomainen), 8G (d)(2)(A) ja (B) § (NSA:n valvontaviranomainen); 50. U.S.C. § 403q (b) (CIA:n valvontaviranomainen); Intelligence Authorization Act For Fiscal Year 2010, § 405(f) (tiedusteluyhteisön valvontaviranomainen). Kansallisten tietosuojaviranomaisten arvion mukaan "valvontaviranomaiset täyttävät todennäköisesti organisatorisen riippumattomuuden kriteerin, siten kuin unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin ovat sen määrittäneet, ainakin siitä hetkestä alkaen, jolloin uutta nimitysprosessia sovelletaan kaikkiin valvontaviranomaisiin". Ks. 29 artiklan mukaisen tietosuojatyöryhmän lausunto 01/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskevasta päätösluonnoksesta (13.4.2016), s. 40.

⁽¹¹¹⁾ Ks. ODN:n lausumat (liite VI), s. 7. Ks. myös Inspector General Act of 1978, sellaisena kuin se on muutettuna, Pub. L. 113-126, 7.7.2014.

ottaa todistajanlausuntoja ⁽¹¹²⁾. Vaikka valvontaviranomaiset voivat antaa vain ei-sitovia suosituksia korjaavista toimista, niiden raportit, mukaan lukien jatkotoimia (tai niiden puutetta) koskevat, julkistetaan ja lähetetään kongressille, joka voi tällä perusteella harjoittaa valvontatehtäväänsä ⁽¹¹³⁾.

- (98) Lisäksi yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan (Privacy and Civil Liberties Oversight Board, PCLOB), joka on toimeenpanohaaraan kuuluva ⁽¹¹⁴⁾ puolueiden välinen, riippumaton viisijäseninen elin ⁽¹¹⁵⁾, jonka presidentti nimittää kuusivuotiskaudeksi ja jonka nimityksen senaatti hyväksyy, vastuualaan kuuluu terrorismin vastainen politiikka ja sen täytäntöönpano yksityisyyden suojan ja kansalaisvapauksien suojelemiseksi. Tarkastellessaan tiedusteluyhteisön toimintaa kyseinen elin voi saada käyttöönsä kaikki asiaankuuluvat tiedot, raportit, tarkastusaineistot, arvioinnit, asiakirjat, työpaperit ja suositukset, mukaan lukien salaisiksi luokitellut tiedot, suorittaa haastatteluja ja kuulla todistajia. Se saa raportteja useiden liittovaltion ministeriöiden/virastojen ⁽¹¹⁶⁾ kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavilta virkamiehiltä, ja se voi antaa niille suosituksia. Lisäksi se raportoi säännöllisesti kongressin valiokunnille ja presidentille ⁽¹¹⁷⁾. PCLOBin tehtävänä on myös toimeksiantonsa puitteissa laatia arviointiraportti PPD-28:n täytäntöönpanosta.
- (99) Lisäksi edellä mainittuja valvontamekanismeja täydentää *tiedustelutoiminnan valvonnasta vastaava lautakunta* (Intelligence Oversight Board), joka on perustettu presidentin tiedustelutoimintaa käsittelevän neuvoa-antavan lautakunnan osaksi ja joka valvoo, että Yhdysvaltojen tiedusteluviranomaiset noudattavat perustuslakia ja kaikkia sovellettavia sääntöjä.
- (100) Valvonnan helpottamiseksi tiedusteluyhteisön toimijoita kannustetaan suunnittelemaan tietojärjestelmiä, jotka mahdollistavat henkilötietoja koskevien tiedustelujen tai muiden hakujen seurannan, tallennuksen ja arvioinnin ⁽¹¹⁸⁾. Valvonnasta vastaavat ja sääntöjen noudattamista valvovat elimet tarkastavat säännöllisesti tiedusteluyhteisön toimijoiden käytännöt, joita ne soveltavat signaalitiedusteluun sisältyvien henkilötietojen suojaan, ja sen, noudattavatko toimijat kyseisiä menettelyjä ⁽¹¹⁹⁾.
- (101) Näitä valvontatehtäviä tuetaan myös vaatimuksilla raportoida laajasti tapauksista, joissa sääntöjä ei ole noudatettu. Erityisesti virastojen soveltamilla menettelyillä on varmistettava, että kun huomataan, että signaalitiedustelun avulla kerättyjen, mitä tahansa kansallisuutta olevan henkilön henkilötietoihin liittyy merkittävä sääntöjen noudattamiseen liittyvä ongelma, tässä ongelmasta on ilmoitettava välittömästi kyseisen tiedusteluyhteisön toimijan johtajalle, joka puolestaan ilmoittaa asiasta kansallisen tiedusteluviraston johtajalle, jonka on PPD-28:n nojalla päätettävä, tarvitaanko korjaavia toimia ⁽¹²⁰⁾. Lisäksi toimeenpanoasetuksen (E.O.) 12333 mukaisesti kaikkien tiedusteluyhteisön toimijoiden on raportoitava tiedustelutoiminnan valvonnasta vastaavalle lautakunnalle sääntöjen noudattamatta jättämistä koskevat tapaukset ⁽¹²¹⁾. Näillä mekanismeilla varmistetaan, että asiaa

⁽¹¹²⁾ Ks. Inspector General Act of 1978, § 6.

⁽¹¹³⁾ Ks. ODNI:n lausumat (liite VI), s. 7. Ks. myös Inspector General Act of 1978, §§ 4(5) ja 5. Lain Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259, 7.10.2010, 405(b)(3) ja (4) §:n mukaan tiedusteluyhteisön valvontaviranomainen tiedottaa sekä DNI:lle että kongressille korjaavien toimenpiteiden tarpeesta ja niiden edistymisestä.

⁽¹¹⁴⁾ Kansallisten tietosuojaviranomaisten arvioinnin mukaan PCLOB on aikaisemmin "osoittanut itsenäisen toimivaltansa". Ks. 29 artiklan mukaisen tietosuojatyöryhmän lausunto 01/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskevasta päätösluonnoksesta (13.4.2016), s. 42.

⁽¹¹⁵⁾ Lisäksi PCLOBin vakinaisen henkilöstön määrä on noin 20. Ks. <https://www.pclob.gov/about-us/staff.html>.

⁽¹¹⁶⁾ Näitä ovat ainakin oikeusministeriö, puolustusministeriö, sisäisen turvallisuuden ministeriö, kansallisen tiedusteluviraston johtaja ja keskustiedustelupalvelu (CIA), sekä mahdolliset muut PCLOBin raporttien kannalta relevanteiksi katsomat ministeriöt, virastot tai toimeenpanohaaran toimijat.

⁽¹¹⁷⁾ Ks. 42 U.S.C. § 2000ee. Ks. myös oikeusasiamiesmekanismi (liite III), 6 kohdan b alakohdan iv alakohta. PCLOBin on muun muassa raportoitava, jos jokin toimeenpanohaaraan kuuluva virasto kieltäytyy noudattamasta sen neuvoja.

⁽¹¹⁸⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7–8.

⁽¹¹⁹⁾ Samoin, s. 8. Ks. myös ODNI:n lausumat (liite VI), s. 9.

⁽¹²⁰⁾ ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, s. 7. Ks. esim. NSA, PPD-28 Section 4 Procedures, 12.1.2015, 7.3 ja 8.7(c) ja (d) kohta; FBI, Presidential Policy Directive 28 Policies and Procedures, III.(A)(4) ja (B)(4) kohta; CIA, Signals Intelligence Activities, s. 6 (Compliance) ja s. 8 (Responsibilities).

⁽¹²¹⁾ Ks. toimeenpanoasetus (E.O.) 12333, § 1.6(c).

käsitellään tiedusteluyhteisön korkeimmalla tasolla. Jos tapaus liittyy ei-yhdysvaltalaiseen henkilöön, kansallisen tiedusteluviraston johtajan on ulkoministeriä ja ilmoituksen tehneen yksikön tai viraston johtajaa kuultuaan päätettävä, olisiko ryhdyttävä toimenpiteisiin asiasta ilmoittamiseksi asianomaiselle ulkovaltojen hallitukselle niin, että suojellaan lähteitä, menetelmiä ja yhdysvaltalaisia henkilöistöä ⁽¹²²⁾.

- (102) Toiseksi näiden toimeenpanohaaran valvontamekanismien lisäksi Yhdysvaltojen kongressilla, erityisesti *edustajainhuoneen ja senaatin tiedustelu- ja oikeusasioden valiokunnilla*, on kaikkeen Yhdysvaltojen harjoittamaan ulkomaanti-edusteluun, myös signaalitiedusteluun, liittyviä valvontavelvoitteita. Kansallista turvallisuutta koskevan lain (National Security Act) mukaan ”presidentti varmistaa, että kongressin tiedusteluvaliokunnille tiedotetaan täysimääräisesti ja viipymättä Yhdysvaltojen tiedustelutoiminnasta, mukaan lukien tässä alaluvussa edellytetty merkittävä ennakoitu tiedustelutoiminta” ⁽¹²³⁾. Samoin ”presidentti varmistaa, että kaikesta laittomasta tiedustelutoiminnasta ilmoitetaan viipymättä kongressin tiedusteluvaliokunnille samoin kuin mahdollisista korjaavista toimista, jotka on toteutettu tai jotka aiotaan toteuttaa laittoman toiminnan johdosta” ⁽¹²⁴⁾. Näiden valiokuntien jäsenillä on pääsy sekä salaisiksi luokiteltuihin tietoihin että tiedustelumenetelmiin ja -ohjelmiin ⁽¹²⁵⁾.
- (103) Myöhemmillä säädöksillä on laajennettu ja tarkennettu raportointivaatimuksia, jotka koskevat sekä tiedusteluyhteisön toimijoita, asianomaisia valvontaviranomaisia että oikeusministeriä. Esimerkiksi FISA-laissa edellytetään, että oikeusministeri ”tiedottaa täysimääräisesti” tiettyjen kyseisen lain pykälien mukaisesti senaatin ja edustajainhuoneen tiedustelu- ja oikeusasioden valiokunnille hallituksen toimista ⁽¹²⁶⁾. Se edellyttää myös, että hallitus antaa kongressin valiokunnille jäljennökset ”kaikista ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimen (Foreign Intelligence Surveillance Court) tai ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimen (Foreign Intelligence Surveillance Court of Review) päätöksistä, määräyksistä tai lausunnoista, joihin sisältyy [FISA-lain säännösten] merkittävää tulkintaa”. Erityisesti mitä tulee FISA-lain 702 §:n mukaiseen valvontaan, tällaista toimintaa valvotaan 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 liitteenä erityisesti oikeusministeriön ja ODN:n selvitykset sääntöjen noudattamisesta ja kuvaus mahdollisista tapauksista, joissa sääntöjä ei ole noudatettu ⁽¹²⁷⁾, ja oikeusministerin ja DNI:n erillinen puolivuositainen arvio, jossa selvitetään kohdentamiseen ja minimointiin liittyvien menettelyjen noudattamista, mukaan lukien niiden menettelyjen noudattaminen, joiden tarkoituksena on varmistaa, että tiedonkeruu liittyy perusteltuun ulkomaantiedustelutavoitteeseen ⁽¹²⁸⁾. Kongressi saa myös valvontaviranomaisten kertomukset. Kyseisillä viranomaisilla on valtuudet arvioida, noudattavatko virastot kohdentamiseen ja minimointiin liittyviä menettelyjä sekä oikeusministerin ohjeita.
- (104) Vuoden 2015 USA Freedom Act -lain mukaan Yhdysvaltojen hallituksen on vuosittain ilmoitettava kongressille (ja yleisölle) muun muassa haettujen ja myönnettyjen FISA-määräysten (FISA orders and directives) lukumäärä sekä arviot valvonnan kohteena olevien yhdysvaltalaisien ja ei-yhdysvaltalaisien henkilöiden määrästä ⁽¹²⁹⁾. Lisäksi laissa edellytetään, että kansallista turvallisuutta koskevien kirjeiden (NSL) määrästä annetaan julkinen raportti

⁽¹²²⁾ PPD-28, 4(a)(iv) kohta.

⁽¹²³⁾ Ks. § 501(a)(1) (50 U.S.C. § 413(a)(1)). Tässä säännöksessä vahvistetaan yleiset vaatimukset, jotka koskevat kongressin toteuttamaa kansallisen turvallisuuden alan valvontaa.

⁽¹²⁴⁾ Ks. § 501(b) (50 U.S.C. § 413(b)).

⁽¹²⁵⁾ Vrt. § 501(d) (50 U.S.C. § 413(d)).

⁽¹²⁶⁾ Ks. 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

⁽¹²⁷⁾ Ks. 50 U.S.C. § 1881f.

⁽¹²⁸⁾ Ks. 50 U.S.C. § 1881a(l)(1).

⁽¹²⁹⁾ Ks. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 602(a). Lisäksi 402 §:n mukaan ”kansallisen tiedusteluviraston johtaja toteuttaa oikeusministeriä kuultuaan kunkin ulkomaantiedustelun valvonnan vastaavan tuomioistuimen tai ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimen antaman sellaisen päätöksen, määräyksen tai lausunnon turvallisuusluokituksen poistamista koskevan tarkastelun (601(e) §:n mukaisesti), johon sisältyy jonkin lain säännöksen merkittävä tulkinta, mukaan lukien uusi tai merkittävä tulkinta ”erityinen valintakriteeri”, ja kyseisen tarkastelun mukaisesti saattaa julkisesti saataville mahdollisimman suuressa määrin kyseisen päätöksen, määräyksen tai lausunnon”.

sekä yhdysvaltalaisista että ei-yhdysvaltalaisista osalta (samalla FISA-määräysten ja -sertifiointipäätösten sekä NSL-pyyntöjen vastaanottajat voivat antaa avoimuusraportin tietyin edellytyksin) ⁽¹³⁰⁾.

- (105) Kolmanneksi ulkomaantiedustelun valvonnasta vastaava tuomioistuin (FISC) ⁽¹³¹⁾ voi tarkastella Yhdysvaltojen viranomaisten FISA-lakiin perustuvaa tiedustelutoimintaa ja joissain tapauksessa toimenpiteille on hankittava kyseisen tuomioistuimen ennakkohyväksyntä. FISC on riippumaton tuomioistuin ⁽¹³²⁾, jonka päätöksistä voi valittaa ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimelle (FISCR) ⁽¹³³⁾ ja viimeksi Yhdysvaltojen korkeimmalle oikeudelle ⁽¹³⁴⁾. Ennakkohyväksynnän saamiseksi pyynnön esittäneiden viranomaisten (FBI, NSA, CIA jne.) on toimitettava hakemusluonnos oikeusministeriön kansallisen turvallisuuden osaston lakimiehille, jotka tutkivat hakemuksen ja pyytävät tarvittaessa lisätietoja ⁽¹³⁵⁾. Kun hakemus on valmis, se on hyväksyttävä oikeusministerillä, varaoikeusministerillä tai kansallisesta turvallisuudesta vastaavalla apulaisoikeusministerillä ⁽¹³⁶⁾. Tämän jälkeen oikeusministeriö toimittaa hakemuksen FISC-tuomioistuimelle, joka arvioi sen ja tekee alustavan päätöksen siitä, miten asiassa edetään ⁽¹³⁷⁾. Kuulemisessa FISC-tuomioistuimella on valtuudet ottaa todistajanlausuntoja, joihin voi sisältyä asiantuntijaneuvoja ⁽¹³⁸⁾.

- (106) FISC-tuomioistuimen (ja FISCR:n) tukena on viisihenkinen pysyvä paneeli. Sen jäsenillä on kokemusta kansalliseen turvallisuuteen ja kansalaisvapauksiin liittyvissä kysymyksissä ⁽¹³⁹⁾. Tuomioistuin nimittää ryhmästä yhden toimimaan *amicus curiae* ominaisuudessa tehtäväänsä avustaa määräystä tai muutoksenhakua koskeissa hakemuksissa, joissa tuomioistuimen mukaan on kyse lainsäädännön uudesta tai merkittävästä tulkinnasta, ellei tuomioistuin katso, että kyseinen nimitys ei ole asianmukainen ⁽¹⁴⁰⁾. 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 ⁽¹⁴¹⁾.

⁽¹³⁰⁾ USA FREEDOM Act, § 602(a) ja 603(a).

⁽¹³¹⁾ Tiettyjen valvontamuotojen ollessa kyseessä myös Yhdysvaltojen korkeimman oikeuden presidentin julkisesti nimittämä alemman oikeusasteen tuomari voi käsitellä hakemuksia ja antaa määräyksiä.

⁽¹³²⁾ FISC-tuomioistuin koostuu yhdestätoista Yhdysvaltojen korkeimman oikeuden presidentin nimittämästä tuomarista. 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 edellyttää, että tuomarit valitaan vähintään seitsemästä Yhdysvaltojen tuomiopiiristä. Ks. FISA, 103 § (50 U.S.C. § 1803 (a)); PCLOB, Sec. 215 Report, s. 174–187. Tuomareiden tukena on kokeneita lakimiesavustajia, jotka muodostavat tuomioistuimen oikeudellisen henkilöstön ja jotka valmistelevat tietojen keruupyyntöjen oikeudellisen analyysin. Ks. PCLOB, Sec. 215 Report, s. 178; ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen puheenjohtajan Reggie B. Waltonin kirje senaatin oikeusasioiden valiokunnan puheenjohtajalle Patrick J. Leahylle (29. heinäkuuta 2013) ("Waltonin kirje"), s. 2–3.

⁽¹³³⁾ FISCR-tuomioistuin koostuu kolmesta tuomarista, jotka Yhdysvaltojen korkeimman oikeuden presidentti nimittää. Heidät valitaan Yhdysvaltojen liittovaltion piirituomioistuinten tai muutoksenhakutuomioistuinten tuomareista, ja kunkin toimikausi on porrastettu ja kestää seitsemän vuotta. Ks. FISA, 103 § (50 U.S.C. § 1803(b)).

⁽¹³⁴⁾ Ks. 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h) ja 1881 a (i)(4).

⁽¹³⁵⁾ Esimerkiksi lisätiedot valvonnan kohteesta, tekniset tiedot valvontamenetelmistä tai vakuutukset siitä, miten hankittuja tietoja käytetään ja levitetään. Ks. PCLOB, Sec. 215 Report, s. 177.

⁽¹³⁶⁾ 50 U.S.C. §§ 1804 (a) ja 1801 (g).

⁽¹³⁷⁾ FISC-tuomioistuin voi hyväksyä hakemuksen, pyytää lisätietoja, päättää kuulemisen tarpeellisuudesta tai ilmoittaa hakemuksen mahdollisesta epäämisestä. Hallitus tekee lopullisen hakemuksen tämän alustavan määrittelyn perusteella. Hakemukseen voi sisältyä tuomarin alustavien huomautuksiin perustuvia merkittäviä muutoksia alkuperäiseen hakemukseen verrattuna. Vaikka FISC-tuomioistuin hyväksyy suurimman osan lopullisista hakemuksista, huomattavaan osaan niistä sisältyy merkittäviä muutoksia alkuperäiseen hakemukseen verrattuna. Esimerkiksi heinä–syyskuussa 2013 hyväksytyistä hakemuksista tällaisia oli 24 prosenttia. Ks. PCLOB, Sec. 215 Report, s. 179; Waltonin kirje, s. 3.

⁽¹³⁸⁾ Ks. PCLOB, Sec. 215 Report, s. 179, alaviite 619.

⁽¹³⁹⁾ 50 U.S.C. § 1803 (i)(1) ja (3)(A). Tällä uudella lainsäädännöllä pantiin täytäntöön PCLOBin suositukset, joiden mukaan perustettaisiin yksityisyyden suojan ja kansalaisvapauksien asiantuntijoiden pooli. Pooliin kuuluvat voivat toimia *amicus curiae*na ja esittää tuomioistuimelle oikeudellisia argumentteja, jotka koskevat yksityisyyden suojan ja kansalaisvapauksien kehittämistä. Ks. PCLOB, Sec. 215 Report, s. 183–187.

⁽¹⁴⁰⁾ 50 U.S.C. § 1803 (i)(2)(A). ODNin toimittamien tietojen mukaan tällaisia nimityksiä on jo tehty. Ks. Signals Intelligence Reform, 2016 Progress Report.

⁽¹⁴¹⁾ 50 U.S.C. § 1803 (i)(2)(B).

- (107) FISC-tuomioistuimen valvontatoimissa on eroavaisuuksia siltä osin kuin on kyse kahdesta FISA-lain mukaisesta valvontaa koskevasta lakisääteisestä luvasta, jotka ovat tärkeimmät EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn mukaisten tiedonsiirtojen kannalta.

- (108) FISA-lain 501 §:ssä⁽¹⁴²⁾ sallitaan ”aineellisten esineiden (mukaan lukien kirjanpito- ja tiedostot, työpaperit, asiakirjat ja muu materiaali)” keruu. Kyseisen pykälän mukaan FISC-tuomioistuimelle toimitettavan hakemuksen on sisällettävä tosiasioita koskeva lausuma, joka osoittaa, että on perusteltua syytä uskoa, että etsityt aineelliset esineet ovat merkityksellisiä sellaisen luovutuksen kannalta (muu kuin uhka-arviointi), jonka tarkoituksena on hankkia ei-yhdysvaltalaisesta henkilöstä koskevia ulkomaantiedustelutietoja tai suojautua kansainväliseltä terrorismilta tai laittomalta tiedustelutoiminnalta. Lisäksi hakemuksessa on oltava luettelo oikeusministerin hyväksymistä minimointimenettelyistä, jotka koskevat kerättyjen tietojen säilyttämistä ja levittämistä⁽¹⁴³⁾.

- (109) Sen sijaan FISC-tuomioistuin ei FISA-lain 702 §:n⁽¹⁴⁴⁾ nojalla anna lupaa yksittäisille valvontatoimenpiteille. Sen sijaan se hyväksyy valvontaohjelmia (kuten PRISM, UPSTREAM) oikeusministerin ja kansallisen tiedusteluviraston johtajan valmistelemien vuotuisten sertifiointihakemusten perusteella. FISA-lain 702 §:n mukaan ulkomaantiedustelutietojen hankinnan kohteena voi olla henkilöjä, joiden voidaan kohtuudella uskoa olevan Yhdysvaltojen ulkopuolella⁽¹⁴⁵⁾. Yhdysvaltojen kansallinen turvallisuusvirasto NSA suorittaa kohdentamisen kahdessa vaiheessa. Ensinnäkin NSA:n analyttikot tunnistavat ne ulkomailta olevat ei-yhdysvaltalaiset henkilöt, joiden valvonta johtaa analyttikkojen arvion mukaan sertifiointipäätöksessä määriteltyyn ulkomaantiedustelutietoon. Sen jälkeen kun henkilöt on tunnistettu ja heidän kohdentamisensa on hyväksytty NSA:n kattavassa arviointijärjestelmässä⁽¹⁴⁶⁾, kehitetään valintakriteerit ja sovelletaan niitä (”tasked selectors”). Näiden kriteerien avulla tunnistetaan kohteiden käyttämät viestintävälineet (esimerkiksi sähköpostiosoitteet)⁽¹⁴⁷⁾. Kuten edellä todettiin, FISC-tuomioistuimen antamiin sertifiointipäätöksiin ei sisälly tietoa kohteena olevista yksittäisistä ihmisistä, vaan niiden avulla yksilöidään ulkomaantiedustelutietojen luokat⁽¹⁴⁸⁾. Vaikka FISC-tuomioistuin ei arvioi todennäköisen syyn perusteella tai muulla tavalla, onko henkilöt kohdennettu asianmukaisesti ulkomaantiedustelutietojen hankkimiseksi⁽¹⁴⁹⁾, se valvoo, että ”hankinnan huomattavana tarkoituksena on hankkia ulkomaantiedustelutietoja”⁽¹⁵⁰⁾. Itse asiassa FISA-lain 702 §:n mukaan NSA voi kerätä Yhdysvaltojen ulkopuolella tietoja ei-yhdysvaltalaisista henkilöistä vain, jos voidaan kohtuudella olettaa, että tiettyä viestintävälinettä käytetään ulkomaantiedustelutiedon (esim. kansainväliseen terrorismiin, ydinaseiden levittämiseen tai vihamielisten tietoverkkojen toimintaan liittyvien tietojen) välittämiseen. Tällaisiin määrityksiin voidaan hakea muutosta tuomioistuimessa⁽¹⁵¹⁾. Sertifiointeissa on myös otettava huomioon kohdentamista ja minimointia koskevat menettelyt⁽¹⁵²⁾. Oikeusministeri ja kansallisen tiedusteluviraston johtaja tarkastavat, että vaatimuksia noudatetaan,

⁽¹⁴²⁾ 50 U.S.C. § 1861.

⁽¹⁴³⁾ 50 U.S.C. § 1861 (b).

⁽¹⁴⁴⁾ 50 U.S.C. § 1881.

⁽¹⁴⁵⁾ 50 U.S.C. § 1881a (a).

⁽¹⁴⁶⁾ PCLOB, Sec. 702 Report, s. 46.

⁽¹⁴⁷⁾ 50 U.S.C. § 1881a (h).

⁽¹⁴⁸⁾ 50 U.S.C. § 1881a (g). PCLOBin mukaan nämä luokat ovat tähän mennessä koskeneet pääasiassa kansainvälistä terrorismia ja sellaisia aiheita kuin joukkotuhousteiden hankinta. Ks. PCLOB, Sec. 702 Report, s. 25.

⁽¹⁴⁹⁾ PCLOB, Sec. 702 Report, s. 27.

⁽¹⁵⁰⁾ 50 U.S.C. § 1881a.

⁽¹⁵¹⁾ ”Liberty and Security in a Changing World”, Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies, 12.12.2013, s. 152.

⁽¹⁵²⁾ 50 U.S.C. § 1881a (i).

ja virastojen on raportoitava kaikista vaatimustenvastaisista tapauksista FISC-tuomioistuimelle ⁽¹⁵³⁾ (sekä kongressille ja presidentin tiedustelutoiminnan valvonnasta vastaavalle lautakunnalle), joka tällä perusteella voi muuttaa lupaa ⁽¹⁵⁴⁾.

- (110) Lisäksi FISC-tuomioistuimen valvonnan tehostamiseksi Yhdysvaltojen viranomaiset ovat luvanneet panna täytäntöön PCLOBin suositusten, jonka mukaan kyseiselle tuomioistuimelle toimitetaan asiakirjat 702 §:n mukaisista kohdentamispäätöksistä, mukaan lukien satunnaisotannalla poimittu otos käyttöön otetuista valintakriteereistä, jotta se voi arvioida, miten ulkomaantiedustelun tarkoitusta koskeva vaatimus täytetään käytännössä ⁽¹⁵⁵⁾. Yhdysvaltojen viranomaiset ovat myös hyväksyneet ja toteuttaneet toimenpiteitä tarkoituksenaan tarkistaa NSA:n kohdentamismenettelyjä dokumentoidakseen paremmin kohdentamispäätöksien perustana olevat ulkomaantiedusteluun liittyvät syyt ⁽¹⁵⁶⁾.

Oikeussuojakeinot

- (111) EU:n rekisteröityjen käytettävissä on useita Yhdysvaltojen lainsäädännön mukaisia keinoja, jos he ovat huolissaan siitä, että Yhdysvaltojen tiedusteluyhteisön toimijat ovat mahdollisesti käsitelleet (keränneet, saaneet käyttöönsä jne.) heidän henkilötietojaan, ja siitä, onko tässä tapauksessa noudatettu Yhdysvaltojen lainsäädännössä sovellettuja rajoituksia. Nämä keinot liittyvät erityisesti kolmeen alaan: FISA-lakiin perustuva tietoihin pääsy; henkilötietojen tahallinen, laiton käyttö hallituksen virkamiesten toimesta; ja tietoihin pääsy Freedom of Information Act -lain (FOIA) nojalla ⁽¹⁵⁷⁾.
- (112) Ensinnäkin ulkomaantiedustelun valvontaa koskevassa laissa säädetään useista korjaavista toimenpiteistä, jotka ovat myös ei-yhdysvaltalaisen henkilöiden käytettävissä, laittoman sähköisen valvonnan riittauttamiseksi ⁽¹⁵⁸⁾. Tähän sisältyy henkilöiden mahdollisuus nostaa Yhdysvaltoja vastaan siviilikanne rahamääräisen vahingonkorvauksen saamiseksi, kun heitä koskevia tietoja on laittomasti ja tahallisesti käytetty tai luovutettu ⁽¹⁵⁹⁾; nostaa Yhdysvaltojen hallituksen virkamiehiä vastaan kanne niiden henkilökohtaisessa ominaisuudessa ("lain varjolla") rahamääräisen vahingonkorvauksen saamiseksi ⁽¹⁶⁰⁾; ja riittauttaa 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 ⁽¹⁶¹⁾.
- (113) Toiseksi Yhdysvaltojen hallitus esitti komissiolle useita muita keinoja, joita EU:n rekisteröidyt voisivat käyttää ryhtyäkseen oikeudellisiin toimenpiteisiin hallituksen virkamiehiä vastaan, kun hallituksen virkamiehet ovat

⁽¹⁵³⁾ FISC-tuomioistuimen työjärjestyksen säännössä 13(b) edellytetään, että hallitus toimittaa tuomioistuimelle kirjallisen ilmoituksen välittömästi sen jälkeen, kun se on havainnut, että tuomioistuimen antama valtuutus tai hyväksyntä on pantu täytäntöön tavalla, joka ei ole tuomioistuimen luvan tai hyväksynnän taikka sovellettavan lain mukainen. Se edellyttää myös, että hallitus ilmoittaa tuomioistuimelle kirjallisesti vaatimusten noudattamatta jättämistä koskevan tapauksen kannalta merkityksellisistä tosiseikoista ja olosuhteista. Yleensä hallitus esittää säännön 13(a) mukaisen lopullisen ilmoituksen sen jälkeen, kun merkitykselliset seikat ovat tiedossa ja luvattomasti kerätyt tiedot on tuhottu. Ks. Waltonin kirje, s. 10.

⁽¹⁵⁴⁾ 50 U.S.C. § 1881 (l). Ks. myös PCLOB, Sec. 702 Report, s. 66–76; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. FISA-lain 702 §:n mukaista henkilötietojen keräämistä tiedustelutarkoituksessa valvotaan toimeenpanohaarassa sekä sisäisesti että ulkoisesti. Sisäiseen valvontaan kuuluu muun muassa sisäisiä vaatimustenmukaisuusohjelmia kohdentamis- ja minimointimenettelyjen noudattamisen arvioimiseksi ja valvomiseksi; vaatimusten noudattamatta jättämistä koskevista tapauksista raportointi sekä sisäisesti että ulkoisesti ODNille, oikeusministeriölle, kongressille ja FISC-tuomioistuimelle; ja samoille elimille toimitetut vuotuiset selvitykset. Ulkoinen valvonta koostuu lähinnä ODN:n, oikeusministeriön ja valvontaviranomaisten suorittamista kohdentamis- ja minimointitarkasteluista. ODN, oikeusministeriö ja valvontaviranomaiset raportoivat puolestaan kongressille ja FISC-tuomioistuimelle, myös vaatimusten noudattamatta jättämistä koskevista tapauksista Merkittävistä vaatimusten noudattamatta jättämistä koskevista tapauksista on ilmoitettava FISC-tuomioistuimelle välittömästi, muille toimitetaan neljännesvuosittain asiaa koskeva raportti. Ks. PCLOB, Sec. 702 Report, s. 66–77.

⁽¹⁵⁵⁾ PCLOB, Recommendations Assessment Report, 29.1.2015, s. 20.

⁽¹⁵⁶⁾ PCLOB, Recommendations Assessment Report, 29.1.2015, s. 16.

⁽¹⁵⁷⁾ Lisäksi turvallisuusluokiteltuja tietoja koskevista menettelyistä annetussa laissa (Classified Information Procedures Act) säädetään, että oikeuskäsittelyssä, jossa Yhdysvaltojen on osoitettava, että materiaali koostuu turvallisuusluokitelluista tiedoista (esimerkiksi siksi, että niitä on suojattava luvattomalta luovuttamiselta kansalliseen turvallisuuteen liittyvistä syistä), Yhdysvaltojen on ilmoitettava vastaajalle ne osat materiaalista, joihin se aikoo kohtuudella nojautua perustellakseen rikkomuksen sen osan, joka koskee turvallisuusluokiteltuja tietoja.

⁽¹⁵⁸⁾ Ks. tältä osin ODN:n lausumat (liite VI), s. 16.

⁽¹⁵⁹⁾ 18 U.S.C. § 2712.

⁽¹⁶⁰⁾ 50 U.S.C. § 1810.

⁽¹⁶¹⁾ 50 U.S.C. § 1806.

lainvastaisesti päässeet henkilötietoihin tai käyttäneet niitä, myös väitettyihin kansalliseen turvallisuuteen liittyviin tarkoituksiin (eli Computer Fraud and Abuse Act ⁽¹⁶²⁾; Electronic Communications Privacy Act ⁽¹⁶³⁾; ja Right to Financial Privacy Act ⁽¹⁶⁴⁾). Kaikki nämä kanneperusteet koskevat tiettyjä tietoja, kohteita ja/tai pääsylajeja (esim. tietokoneen etäyhteys internetin kautta) ja tietyin edellytyksin (esim. tarkoituksellinen/tahallinen toiminta, virkatehtävien ulkopuolinen toiminta, aiheutunut vahinko) ⁽¹⁶⁵⁾. Hallintomenettelylaki (Administrative Procedure Act, 5 U.S.C. § 702) 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. 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” ⁽¹⁶⁶⁾.

- (114) Lopuksi on todettava, että Yhdysvaltojen hallitus on viittannut FOIAan, jota ei-yhdysvaltalaiset henkilöt voivat käyttää keinona saada käyttöönsä liittovaltion virastoissa olevia asiakirjoja, myös silloin, kun niihin sisältyy kyseisen henkilön henkilötietoja ⁽¹⁶⁷⁾. FOIAN painopisteen vuoksi yksittäiset henkilöt eivät voi sen nojalla ryhtyä toimenpiteisiin henkilötietoihin pääsyä vastaan, vaikka henkilöt voisivatkin periaatteessa saada sen perusteella käyttöönsä tietoja, jotka ovat kansallisten tiedusteluvirastojen hallussa. Kuitenkin mahdollisuudet vaikuttavat tältä osin rajallisilta, koska virastot voivat olla paljastamatta tietoja, jotka kuuluvat tiettyjen luettelujen poikkeusten piiriin, mukaan lukien pääsy luokiteltuihin kansallista turvallisuutta koskeviin tietoihin sekä lainvalvonnassa tehtyjen tutkimusten tietoihin ⁽¹⁶⁸⁾. On kuitenkin huomattava, että henkilöt voivat riitauttaa kansallisten tiedusteluvirastojen tällaisten poikkeusten käytön, sillä ne voivat hakea muutosta sekä hallintoviranomaiselta että tuomioistuimelta.
- (115) Vaikka henkilöiden, myös EU:n rekisteröityjen, käytettävissä on tämän vuoksi useita oikeussuojakeinoja, kun he ovat olleet laittoman (sähköisen) valvonnan kohteena kansallisen turvallisuuden nimissä, on kuitenkin selvää, että tämä ei koske eräitä Yhdysvaltojen tiedusteluviranomaisten käytössä olevia oikeusperustoja (esim. toimeenpanoasetus (E.O.) 12333). Lisäksi on todettava, että vaikka periaatteessa ei-yhdysvaltaisten henkilöiden käytettävissä on oikeussuojakeinoja, esimerkiksi kun on kyse FISAn mukaisesta valvonnasta, käytössä olevat kanneperusteet ovat vähäiset ⁽¹⁶⁹⁾ ja henkilöiden (myös yhdysvaltaisten) nostamat kanteet jätetään tutkimatta, jos ne eivät pysty osoittamaan kanneoikeuttaan ⁽¹⁷⁰⁾. Tämä rajoittaa pääsyä yleisiin tuomioistuihin ⁽¹⁷¹⁾.
- (116) Tarjotakseen kaikille EU:n rekisteröidyille ylimääräisen oikeussuojakeinon, Yhdysvaltojen hallitus on päättänyt perustaa uuden oikeusasiamiesmekanismin, kuten tämän päätöksen liitteessä III olevassa Yhdysvaltojen ulkoministerin kirjeessä komissiolle esitetään. Tämän järjestelmän perustana on PPD-28:n perusteella nimettävä johtava koordinaattori (valtiosuhteeri), joka toimii ulkoministeriössä yhteyspisteenä ja jonka kautta ulkomaiset hallitukset voivat esittää Yhdysvaltojen signaalitiedustelua koskevia kysymyksiä, mutta oikeusasiamiehen tehtävä menee tätä alkuperäistä suunnitelmaa huomattavasti pidemmälle.

⁽¹⁶²⁾ 18 U.S.C. § 1030.

⁽¹⁶³⁾ 18 U.S.C. §§ 2701–2712.

⁽¹⁶⁴⁾ 12 U.S.C. § 3417.

⁽¹⁶⁵⁾ ODN:n lausumat (liite VI), s. 17.

⁽¹⁶⁶⁾ 5 U.S.C. § 706 (2)(A).

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

⁽¹⁶⁸⁾ 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).

⁽¹⁶⁹⁾ Ks. ODN:n lausumat (liite VI), s. 16. Annettujen selvitysten perusteella käytettävissä olevat keinot edellyttävät joko vahingon olemassaoloa (18 U.S.C. § 2712; 50 U.S.C. § 1810) tai sen osoittamista, että hallitus aikoo käyttää tai luovuttaa kyseiseen henkilöön kohdistuvasta sähköisestä valvonnasta hankittuja tai johdettuja tietoja asianomaista henkilöä vastaan oikeudellisissa tai hallinnollisissa menettelyissä Yhdysvalloissa (50 U.S.C. § 1806). Kuten unionin tuomioistuin on toistuvasti korostanut, yksityisyyden suojaa koskevaan perusoikeuteen puuttumisen olemassaolon osoittaminen ei riipu siitä, onko kyseiselle henkilölle aiheutunut kielteisiä seurauksia tämän puuttumisen vuoksi. Ks. Schrems, 89 kohta oikeuskäytäntöviittauksineen.

⁽¹⁷⁰⁾ Tämä hyväksyttävyyssperuste on peräisin Yhdysvaltojen perustuslain III artiklan riitaisuusvaatimuksesta (‘case or controversy’ requirement).

⁽¹⁷¹⁾ Ks. Clapper v. Amnesty Int’l USA, 133 S.Ct. 1138, 1144 (2013). NSL:n käytöstä USA FREEDOM Act -laissa (502(f)–503 §) säädetään, että kieltoa paljastaa kirjeeseen liittyviä tietoja tarkistettava ajoittain ja että NSL:n vastaanottajille on ilmoitettava, kun toiseikat eivät enää tue tätä kieltoa (ks. ODN:n lausumat (liite VI), s. 13). Tämä ei takaa, että EU:n rekisteröidyille ilmoitettaisiin, että kyseinen henkilö on tutkimuksen kohteena.

- (117) Yhdysvaltojen hallituksen sitoumusten mukaan oikeusasiamiesmekanismi takaa etenkin, että yksittäiset valitukset tutkitaan ja käsitellään asianmukaisesti ja että henkilöt saavat riippumattoman vahvistuksen sille, että Yhdysvaltojen lakeja on noudatettu, tai jos tällaisia lakeja on rikottu, että noudattamatta jättäminen on korjattu ⁽¹⁷³⁾. Mekanismiin kuuluu tietosuojasta vastaava oikeusasiamies eli alivaltiosihteeri ja muuta henkilöstöä sekä muita toimivaltaisia valvontaelimiä, jotka valvovat tiedusteluyhteisön eri toimijoita, joiden yhteistyöhön oikeusasiamies tukeutuu valituksia käsitellessään. Varsinkin silloin, kun henkilön kysymys koskee sitä, onko valvonta ja tarkkailu Yhdysvaltojen lainsäädännön mukaista, oikeusasiamies voi tukeutua riippumattomiin valvontaelimiin, joilla on tutkintavaltuudet (kuten ministeriöiden ja virastojen valvontaviranomaiset tai PCLOB). Kussakin tapauksessa ulkoministeri varmistaa, että oikeusasiamiehen käytettävissä on keinot sen varmistamiseksi, että sen vastaukset henkilöiden pyyntöihin perustuvat kaikkiin tarvittaviin tietoihin.
- (118) Tämän yhdistelmä rakenteen avulla oikeusasiamiesmekanismi takaa riippumattoman valvonnan ja oikeussuojakeinot. Lisäksi yhteistyö muiden valvontaelinten kanssa varmistaa, että käytettävissä on tarvittavaa asiantuntemusta. Se, että mekanismi velvoittaa oikeusasiamiehen vahvistamaan, onko sovellettavia periaatteita noudatettu tai miten noudattamatta jättämistä koskeva tilanne korjataan, heijastaa Yhdysvaltojen hallituksen sitoumusta käsitellä ja ratkaista EU:n kansalaisten tekemät valitukset.
- (119) Ensinnäkin toisin kuin puhtaasti hallitusten välisessä järjestelmässä oikeusasiamies vastaanottaa yksittäisiä valituksia ja vastaa niihin. Valitukset voidaan osoittaa jäsenvaltioissa oleville kansallisten turvallisuuspalveluiden ja/tai viranomaisten suorittamien henkilötietojen käsittelyn valvonnasta vastaaville viranomaisille, jotka toimittavat valitukset EU:n keskitetylle elimelle, josta ne siirretään edelleen Privacy Shield -järjestelyn oikeusasiamiehelle ⁽¹⁷³⁾. Tämä hyödyttää EU:n kansalaisia, jotka voivat kääntyä lähellä olevan kansallisen viranomaisen puoleen omalla kielellään. Tämän viranomaisen tehtävänä on tukea henkilöä, joka esittää oikeusasiamiehelle pyynnön, joka sisältää perustiedot ja jota voidaan siten pitää ”täydellisenä”. Henkilön ei tarvitse osoittaa, että Yhdysvaltojen hallitus on todella päässyt hänen henkilötietoihinsa käsiksi signaalitiedustelun kautta.
- (120) Toiseksi Yhdysvaltojen hallitus sitoutuu varmistamaan, että oikeusasiamies voi tehtävissään tukeutua muiden Yhdysvaltojen lainsäädännön mukaisten valvonnasta ja sääntöjen noudattamisesta vastaavien mekanismien kanssa tehtävään yhteistyöhön. Tähän osallistuvat toisinaan kansalliset tiedusteluviranomaiset, erityisesti silloin, kun pyynnön on tulkittava koskevan oikeutta tutustua asiakirjoihin tiedonvapautta koskevan FOIA-lain nojalla. Muissa tapauksissa, erityisesti silloin kun pyynnöt koskevat valvonnan yhteensopivuutta Yhdysvaltojen lainsäädännön kanssa, tällaiseen yhteistyöhön osallistuu riippumattomia valvontaelimiä (esim. virastojen/ministeriöiden valvontaviranomaiset), joiden vastuulla ja toimivallassa on perusteellisen tutkinnan suorittaminen (ja erityisesti heillä on mahdollisuus tutustua kaikkiin asiaa koskeviin asiakirjoihin ja valtuudet pyytää tietoja ja lausuntoja) ja ryhtyä toimenpiteisiin, jos sovellettavia periaatteita ei noudateta ⁽¹⁷⁴⁾. Oikeusasiamies voi siirtää asioita myös PCLOBin käsiteltäväksi ⁽¹⁷⁵⁾. Jos jokin näistä valvontaelimistä toteaa, että periaatteita ei ole noudatettu, kyseisen tiedusteluyhteisön toimijan (esim. tiedusteluviraston) on korjattava tilanne, sillä vain siten oikeusasiamies voi antaa Yhdysvaltojen hallituksen sitoumuksen mukaisen ”positiivisen” vastauksen henkilölle (toisin sanoen sen, että

⁽¹⁷²⁾ Jos valituksen tekijä haluaa käyttöönsä Yhdysvaltojen viranomaisten hallussa olevia asiakirjoja, sovelletaan FOIA-lain (Freedom of Information Act) sääntöjä ja menettelyjä. Tähän kuuluu mahdollisuus hakea FOIA-laissa säädettyjen edellytysten mukaisesti muutosta oikeustietse (riippumattoman valvonnan sijaan) siinä tapauksessa, että vaatimus hylätään.

⁽¹⁷³⁾ Oikeusasiamiesmekanismiin (liite III, 4 kohdan f alakohta) mukaan oikeusasiamies on suoraan yhteydessä kansalaisten valituksia käsittelevän EU:n elimen kanssa, ja tämä elin puolestaan vastaa yhteydenpidosta pyynnön esittäneen kansalaisen kanssa. Jos suora yhteydenpito on osa perustana olevia prosesseja, jotka voivat johtaa pyydettyyn hyvitykseen (esim. FOIA-tiedonsaantipyynnö, ks. 5 jakso), yhteydenpito tapahtuu sovellettavien menetelmien mukaisesti.

⁽¹⁷⁴⁾ Ks. oikeusasiamiesmekanismi (liite III), 2 kohdan a alakohta. Ks. myös johdanto-osan 96–97 kappale.

⁽¹⁷⁵⁾ Ks. oikeusasiamiesmekanismi (liite III), 2 kohdan c alakohta. Yhdysvaltojen hallituksen antamien selitysten mukaan PCLOB tarkastelee jatkuvasti Yhdysvaltojen viranomaisten terrorismin vastaisia politiikkoja ja menettelyjä sekä niiden täytäntöönpanoa määrittääkseen, ”turvaavatko viranomaisten toimet asianmukaisesti yksityisyyden suojan ja kansalaisvapaudet ja ovatko ne yksityisyyden suojaan ja kansalaisvapauksia koskevien sovellettavien lakien, asetusten ja politiikkojen mukaisia”. Se myös ”vastaanottaa yksityisyyden suojaan ja kansalaisvapauksiin liittyviä tehtäviä hoitavilta virkamiehiltä raportteja ja muita tietoja ja tarkastelee niitä sekä antaa tarvittaessa niiden toimintaa koskevia suosituksia”.

mahdollinen noudattamatta jättäminen on korjattu). Yhteistyön osana oikeusasiamiehelle myös ilmoitetaan tutkinnan tuloksesta, ja oikeusasiamiehellä on käytettävissään keinot varmistaa, että se saa kaikki tarvittavat tiedot vastauksensa laatimiseksi.

- (121) Lopuksi on todettava, että oikeusasiamies on Yhdysvaltojen tiedusteluyhteisöstä riippumaton eikä ota vastaan sen ohjeita ⁽¹⁷⁶⁾. Tämä on erityisen tärkeää, kun otetaan huomioon, että oikeusasiamiehen on "vahvistettava", että i) valitus on tutkittu asianmukaisesti ja että ii) sovellettavaa Yhdysvaltojen lainsäädäntöä – erityisesti liitteessä VI esitettyjä rajoituksia ja suojatoimia – on noudatettu, tai jos periaatteita ei noudateta, rikkominen on korjattu. Riippumattoman vahvistuksen antamiseksi oikeusasiamiehen on saatava tutkintaa koskevat tarvittavat tiedot arvioidakseen valitukseen annetun vastauksen virheettömyyden. Lisäksi ulkoasiainministeri on sitoutunut varmistamaan, että valtiosihteeri toimii oikeusasiamiehen tehtävässä puolueettomasti ja ettei mikään vaikuta epäasianmukaisesti oikeusasiamiehen antamiin vastauksiin.
- (122) Tällä mekanismilla varmistetaan, että valitukset tutkitaan ja ratkaistaan huolellisesti ja että ainakin valvonnan ja tarkkailun alalla tähän työhön osallistuvat riippumattomat valvontaelimet, joilla on tarvittava asiantuntemus ja tutkintavaltuudet, sekä oikeusasiamies, joka pystyy suorittamaan tehtävänsä ilman epäasianmukaista, erityisesti poliittista, vaikutusta. Lisäksi henkilöt voivat tehdä valituksen tarvitsematta osoittaa, että he ovat olleet valvonnan ja tarkkailun kohteena, tai he voivat ainoastaan antaa viitteitä siitä ⁽¹⁷⁷⁾. Näiden tekijöiden perusteella komissio on vakuuttunut siitä, että väärinkäyttöä vastaan on olemassa riittävät ja tehokkaat takeet.
- (123) Edellä olevan perusteella komissio päättää, että Yhdysvallat varmistaa tehokkaan oikeussuojan sen estämiseksi, että tiedusteluviranomaiset puuttuisivat niiden henkilöiden perusoikeuksiin, joiden tietoja siirretään unionista Yhdysvaltoihin EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa.
- (124) Komissio ottaa tältä osin huomioon unionin tuomioistuimen asiassa Schrems antaman tuomion, jonka mukaan "säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ole tehokasta oikeussuojaa koskevan perusoikeuden, sellaisena kuin se vahvistetaan Euroopan unionin perusoikeuskirjan 47 artiklassa, keskeisen sisällön mukainen" ⁽¹⁷⁸⁾. Komission arviointi osoittaa, että Yhdysvallat tarjoaa tällaiset oikeussuojakeinot esimerkiksi oikeusasiamiesmekanismin käyttöönoton muodossa. Oikeusasiamiesmekanismi tarjoaa riippumattoman valvonnan ja tutkintavaltuudet. Komissio arvioi mekanismin vaikuttavuutta seurattessaan jatkuvasti Privacy Shield -järjestelyä, esimerkiksi vuotuisessa yhteisessä uudelleentarkastelussa, johon myös oikeusasiamies osallistuu.

3.2 Yhdysvaltojen viranomaisten pääsy tietoihin ja niiden käyttö lainvalvonnan ja kansallisen turvallisuuden nimissä

- (125) EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn puitteissa siirrettyihin henkilötietoihin pääsystä lainvalvonnan nimissä Yhdysvaltojen hallitus on (oikeusministeriön kautta) antanut vakuutuksen sovellettavista rajoituksista ja suojatoimista, jotka komission arvion mukaan osoittavat tietosuojan riittävän tason.

⁽¹⁷⁶⁾ Ks. Roman Zakharov v. Venäjä, Euroopan ihmisoikeustuomioistuimen tuomio 4.12.2015 (suuri jaosto), hakemus nro 47143/06, 275 kohta ("vaikka on periaatteessa suotavaa antaa tuomarille valvontavastuu, ei-oikeudellisten elinten suorittaman valvonnan voidaan katsoa olevan ihmisoikeussopimuksen mukaista, jos kyseinen valvontaviranomainen on tarkkailun suorittavista viranomaisista riippumaton ja sillä on riittävät ja tehokkaat valvontavaltuudet").

⁽¹⁷⁷⁾ Ks. Kennedy v. Yhdistynyt kuningaskunta, tuomio 18.5.2010, hakemus nro 26839/05, 167 kohta.

⁽¹⁷⁸⁾ Schrems, 95 kohta. Kuten tuomion 91 ja 96 kohdasta ilmenee, 95 kohta koskee unionin oikeusjärjestyksessä taattua suojan tasoa, jota kolmannessa maassa tarjottavan suojan tason on "pääosin vastattava". Tuomion 73 ja 74 kohdan mukaan tämä ei tarkoita, että suojelun tason olisi oltava täysin sama tai että kolmannen maan käyttämien keinojen olisi oltava täysin samat, vaikkakin keinojen on käytännössä osoittauduttava tehokkaiksi.

- (126) Näiden tietojen mukaan lainvalvontaviranomaisten Yhdysvaltojen perustuslain neljännen lisäyksen ⁽¹⁷⁹⁾ perusteella suorittamien etsintöjen ja takavarikkojen edellytyksenä on pääasiallisesti ⁽¹⁸⁰⁾ tuomioistuimen määräys, kun ”perusteltu syy” on näytetty toteen. Niissä erityisissä ja poikkeuksellisissa tapauksissa, joissa määräystä koskevaa vaatimusta ei sovelleta ⁽¹⁸¹⁾, lainvalvontaan sovelletaan ”kohtuustestiä” ⁽¹⁸²⁾. Se, onko etsintä tai takavarikko kohtuullinen ”määritetään arvioimalla toisaalta missä määrin se loukkaa henkilön yksityisyyttä ja toisaalta missä määrin sitä tarvitaan hallituksen oikeutettujen etujen edistämiseksi” ⁽¹⁸³⁾. Yleisesti ottaen Yhdysvaltojen perustuslain neljännessä lisäyksessä taataan yksityisyyden suoja ja ihmisarvoinen kohtelu ja suojellaan hallituksen virkamiesten mielivaltaisilta ja yksityisyyden suojaan puuttuvilta toimilta ⁽¹⁸⁴⁾. Näihin käsitteisiin sisältyy unionin lainsäädännössä vahvistettu tarpeellisuuden ja oikeasuhteisuuden ajatus. Kun lainvalvontaviranomaisilla ei ole enää tarvetta käyttää takavarikoituja esineitä todisteena, ne olisi palautettava ⁽¹⁸⁵⁾.
- (127) Vaikka neljännen lisäyksen mukainen oikeus ei ulotu sellaisiin ei-yhdysvaltalaisiin henkilöihin, jotka eivät asu Yhdysvalloissa, he kuitenkin hyötyvät välillisesti sen tarjoamasta suojasta, sillä tiedot ovat yhdysvaltalaisen yritysten hallussa, jolloin lainvalvontaviranomaisten on joka tapauksessa pyydettävä tuomioistuimen lupaa (tai vähintään noudatettava kohtuusvaatimusta) ⁽¹⁸⁶⁾. Lisäsuojaa tarjoavat erityiset oikeusperustat samoin kuin oikeusministeriön ohjeet, joissa rajoitetaan lainvalvontaviranomaisten pääsyä tietoihin tarpeellisuuden ja oikeasuhteisuuden perusteella (esim. vaatimalla, että FBI käyttää mahdollisimman vähän häiritseviä tutkimuskeinoja, kun otetaan huomioon vaikutukset yksityisyyteen ja kansalaisvapauksiin) ⁽¹⁸⁷⁾. Yhdysvaltojen hallituksen antamien lausumien mukaan samantasoista tai korkeampaa suojaa sovelletaan osavaltiotasolla toteutettaviin lainvalvontaviranomaisten tutkimuksiin (kun on kyse tutkimuksista, jotka suoritetaan osavaltion lakien mukaisesti) ⁽¹⁸⁸⁾.
- (128) Vaikka tuomioistuimen tai suuren valamiehistön (tuomioistuimen tutkintahaara, jonka tuomari valitsee) ennakkolupaa ei vaadita kaikissa tapauksissa ⁽¹⁸⁹⁾, hallinnolliset haasteet on rajattu erityistapauksiin, ja niihin voi hakea muutosta riippumattomassa tuomioistuimessa ainakin silloin, kun hallitus esittää täytäntöönpanoa tuomioistuimessa ⁽¹⁹⁰⁾.
-
- ⁽¹⁷⁹⁾ Yhdysvaltojen perustuslain neljännessä lisäyksessä säädetään seuraavaa: ”Kansalaisten oikeutta olla turvassa henkilöön, taloonsa, asiakirjoihinsa ja muuhun omaisuuteensa kohdistuvilta kohtuuttomilta etsinnöiltä ja takavarikoinneilta alkoon loukattako, alköönkä etsintälupaa annettako muutoin kuin todennäköisestä syystä, joka on vahvistettu valalla tai juhlallisella vakuutuksella, ja etsintäluvassa on erityisesti mainittava etsinnän tapahtumapaikka sekä pidettävät henkilöt ja takavarikoitavat esineet.” Vain tuomarit (myös alemmassa oikeusasteessa toimivat) voivat myöntää etsintälupia. Sähköisesti tallennettujen tietojen jäljentämistä koskeviin liittovaltion lupiin sovelletaan myös rikosprosessia koskevien liittovaltion sääntöjen sääntöä nro 41.
- ⁽¹⁸⁰⁾ Yhdysvaltojen korkein oikeus on useasti todennut, että ilman lupaa tehtyt etsinnät ovat ”poikkeuksellisia”. Ks. esim. *Johnson v. Yhdysvallat*, 333 U.S. 10, 14 (1948); *McDonald v. Yhdysvallat*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. v. Yhdysvallat*, 429 U.S. 338, 352-53, 355 (1977). Lisäksi korkein oikeus painottaa säännöllisesti, että ”perustavanlaatuisin perustuslain sääntö tällä alalla on se, että oikeusprosessin ulkopuolella ilman tuomarin antamaa ennakkolupaa toteutetut etsinnät ovat neljännen lisäyksen mukaan itsessään kohtuuttomia, ja niihin voidaan soveltaa vain muutamaa erityisesti perusteltua ja hyvin määriteltyä poikkeusta”. Ks. esim. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. v. Yhdysvallat*, 429 U.S. 338, 352-53, 358 (1977).
- ⁽¹⁸¹⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
- ⁽¹⁸²⁾ PCLOB, Sec. 215 Report, s. 107, jossa viitataan asiaan *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
- ⁽¹⁸³⁾ PCLOB, Sec. 215 Report, s. 107, jossa viitataan asiaan *Samson v. California*, 547 S. Ct. 843, 848 (2006).
- ⁽¹⁸⁴⁾ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.
- ⁽¹⁸⁵⁾ Ks. esim. *Yhdysvallat v. Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).
- ⁽¹⁸⁶⁾ Vrt. *Roman Zakharov v. Venäjä*, tuomio 4.12.2015 (suuri jaosto), hakemus nro 47143/06, 269 kohta, jonka mukaan ”vaatimus osoittaa tietojen hankkimista koskeva lupa viestintäpalveluja tarjoavalle yritykselle ennen pääsyä henkilön viestintään on yksi tärkeistä suojatoimista, joilla ehkäistään lainvalvontaviranomaisten syyllistymisen väärinkäyttöön ja varmistetaan, että asianmukainen lupa hankitaan kaikissa tiedonhankintatapauksissa”.
- ⁽¹⁸⁷⁾ Oikeusministeriön lausumat (liite VII), s. 4, viittauksineen.
- ⁽¹⁸⁸⁾ Oikeusministeriön lausumat (liite VII), alaviite 2.
- ⁽¹⁸⁹⁾ Komission saamien tietojen mukaan ja ottamatta huomioon tiettyjä aloja, joilla ei todennäköisesti ole merkitystä EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa suoritettujen tiedonsiirtojen kannalta (esim. terveydenhuollon petoksia, lasten hyväksikäyttöä tai valvottuja aineita koskevien tapausten tutkimukset), tämä koskee sähköisen viestinnän tietosuojaa koskevan lain (Electronic Communications Privacy Act, ECPA) mukaan pääasiassa tiettyjä viranomaisia, eli kun on kyse tilaajia, viestintäistuntoja ja laskutusta koskeviin perustietoihin liittyvistä pyynnöistä (18 U.S.C. § 2703 (c)(1),(2), esim. osoite ja palvelun laji ja pituus) ja yli 180 päivän ikäisten sähköpostien sisältöä (18 U.S.C. § 2703(a)(b)). Jälkimmäisessä tapauksessa asianomaiselle henkilölle on ilmoitettava asiasta, joten tällä on mahdollisuus riitauttaa pyyntö tuomioistuimessa. Ks. myös oikeusministeriön katsaus, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3. luku; *The Stored Communications Act*, s. 115–138.
- ⁽¹⁹⁰⁾ Yhdysvaltojen hallituksen lausumien mukaan hallinnollisten haasteiden vastaanottajat voivat riitauttaa ne tuomioistuimessa sillä perusteella, että ne ovat kohtuuttomia, eli menevät liian pitkälle tai ovat epäoikeudenmukaisia taikka hankalia. Ks. oikeusministeriön lausumat (liite VI), s. 2.

- (129) Sama koskee hallinnollisten haasteiden käyttöä yleisen edun nimissä. Lisäksi Yhdysvaltojen hallituksen lausumien mukaan samantapaisia sisältöä koskevia rajoituksia sovelletaan niin, että virastot voivat saada käyttöönsä ainoastaan tietoja, joilla on merkitystä niiden toimivaltaan kuuluvissa asioissa, ja että virastojen on noudatettava kohtuuseriaatetta.
- (130) Yhdysvaltojen lainsäädännössä säädetään lisäksi useista mahdollisuuksista käyttää oikeussuojakeinoja viranomaista tai jotain sen virkamiestä vastaan, kun nämä viranomaiset käsittelevät henkilötietoja. Näitä oikeussuojakeinoja, joihin kuuluvat erityisesti hallintomenettelylaki (Administrative Procedure Act, APA), tiedonvapautta koskeva laki (Freedom of Information Act, FOIA) ja sähköisen viestinnän tietosuojalaki (Electronic Communications Privacy Act, ECPA), voivat käyttää kaikki henkilöt heidän kansalaisuudestaan riippumatta sovellettavat edellytykset huomioon ottaen.
- (131) Hallintomenettelylaissa ⁽¹⁹¹⁾ olevien muutoksenhakua tuomioistuimessa koskevien säännösten 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 ⁽¹⁹²⁾. 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” ⁽¹⁹³⁾.
- (132) Erityisesti sähköisen viestinnän tietosuojalain II osastossa ⁽¹⁹⁴⁾ säädetään lakimääräisten yksityisyyden suojaa koskevien oikeuksien järjestelmästä, ja sitä sovelletaan pääsyyntä viestintäpalveluja tarjoavien kolmansien osapuolten hallussa olevaan langallisen, suullisen tai sähköisen viestinnän sisältöön lainvalvonnan nimissä ⁽¹⁹⁵⁾. 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 hallituksen virkamiestä vastaan, kun tämä on tahallisesti syyllistynyt laittomiin tekoihin, tai Yhdysvaltoja vastaan todelliseen vahinkoon perustuvan ja rangaistusluonteisen vahingonkorvauksen sekä kielto- tai vahvistustuomion saamiseksi.
- (133) Tiedonvapautta koskevan lain (FOIA, 5 U.S.C. § 552) nojalla kenellä tahansa henkilöllä on oikeus saada käyttöönsä liittovaltion viraston hallussa olevia tietoja ja kaikki hallinnolliset keinot käytettyään panna oikeutensa täytäntöön tuomioistuimessa, lukuun ottamatta tietoja, joita ei paljasteta poikkeuksen tai erityisen lainvalvontaan liittyvän syyn perusteella ⁽¹⁹⁶⁾.

⁽¹⁹¹⁾ 5 U.S.C. § 702.

⁽¹⁹²⁾ Yleensä vain ”lopullinen” viraston toimi – pikemmin kuin ”alustava, menettelyllinen tai välillinen” viraston toimi – on tuomioistuinvälvönnän alainen. Ks. 5 U.S.C. § 704.

⁽¹⁹³⁾ 5 U.S.C. § 706(2)(A).

⁽¹⁹⁴⁾ 18 U.S.C. §§ 2701–2712.

⁽¹⁹⁵⁾ ECPA suojaa tietoja, jotka ovat kahdenlaisten verkkopalveluyritysten hallussa: i) sähköiset viestintäpalvelut, esimerkiksi puhelin tai sähköposti; ii) etäkäyttöpalvelut kuten tallenne- ja käsittelypalvelut.

⁽¹⁹⁶⁾ Nämä poikkeukset ovat kuitenkin rajoitettuja. Esimerkiksi 5 U.S.C. 552(b)(7) §:n mukaan FOIA-oikeudet on suljettu pois kun on kyse ”tiedoista tai tiedoista, jotka on laadittu lainvalvontaa varten, mutta vain siinä määrin, että tällaisten lainvalvontatiedostojen tai -tietojen luovuttaminen A) johtaisi siihen, että sen voitaisiin kohtuudella olettaa haittaavan lainvalvontamenettelyjä, B) riistäisi henkilöltä oikeuden oikeudenmukaiseen oikeudenkäyntiin tai puolueettomaan käsittelyyn tuomioistuimessa, C) johtaisi siihen, että sen voitaisiin kohtuudella odottaa muodostavan luvattoman 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 koonnut rikoslain täytäntöönpanon valvonnasta vastaava viranomainen rikostutkimuksen kuluessa tai virasto, joka suorittaa laillista kansalliseen turvallisuuteen liittyvää tiedustelua koskevaa tutkimusta, luottamuksellisen lähteen toimittamat tiedot, E) johtaisi lainvalvontatutkimuksissa tai syytteen nostamisessa käytettyjen tekniikoiden ja menettelyjen paljastumiseen tai lainvalvontatutkimuksissa 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 luovuttamisen 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 ii), että 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 (c)(1))

- (134) Lisäksi useissa muissa säädöksissä (Wiretap Act ⁽¹⁹⁷⁾, Computer Fraud and Abuse Act ⁽¹⁹⁸⁾, Federal Torts Claim Act ⁽¹⁹⁹⁾, Right to Financial Privacy Act ⁽²⁰⁰⁾ ja Fair Credit Reporting Act ⁽²⁰¹⁾) annetaan henkilöille oikeus nostaa kanne Yhdysvaltojen viranomaista tai virkamiestä vastaan henkilötietojensa käsittelyn vuoksi.
- (135) Näin ollen komissio katsoo, että Yhdysvalloissa on käytössä sääntöjä, joilla pyritään rajoittamaan puuttumista lainvalvonnan tai muun julkisen edun nimissä sellaisten henkilöiden perusoikeuksiin ⁽²⁰²⁾, joiden henkilötietoja siirretään unionista Yhdysvaltoihin EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn nojalla, siihen mikä on ehdottomasti tarpeen oikeutetun tavoitteen saavuttamiseksi. Lisäksi säännöt varmistavat tehokkaan oikeussuojan tällaista perusoikeuksiin puuttumista vastaan.

4. EU:N JA YHDYSVALTOJEN VÄLISEN PRIVACY SHIELD -JÄRJESTELYN MUKAINEN RIITTÄVÄ TIETOSUOJAN TASO

- (136) Komissio katsoo edellä esitetyn perusteella, että Yhdysvallat takaa riittävän suojan henkilötiedoille, jotka siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa unionista Yhdysvalloissa oleville oman varmennuksen antaneille organisaatioille.
- (137) Komissio katsoo erityisesti, että Yhdysvaltojen kauppaministeriön hyväksymät järjestelyn periaatteet varmistavat kokonaisuutena tarkastellen sellaisen henkilötietojen suojan tason, joka olennaisilta osin vastaa direktiivissä 95/46/EY vahvistetuissa peruseriaa- teissa taattua tasoa.
- (138) Lisäksi järjestelyn periaatteiden tehokas soveltaminen taataan läpinäkyvillä velvoitteilla ja Privacy Shield -järjestelyn hallinnolla, josta huolehtii kauppaministeriö.
- (139) Lisäksi komissio katsoo, että kokonaisuutena tarkasteltuna Privacy Shield -järjestelyyn kuuluvien valvonta- ja muutoksenhakumekanismien avulla voidaan havaita tapaukset, joissa järjestelyyn liittynyt organisaatio rikkoo järjestelyn periaatteita, ja rangaista niistä käytännössä ja tarjota oikeussuojakeinoja rekisteröidylle, jotta tämä voi tutustua itseään koskeviin henkilötietoihin ja saada nämä tiedot oikaistuiksi tai poistetuiksi.
- (140) Lisäksi komissio katsoo Yhdysvaltojen oikeusjärjestystä koskevien käytettävissä olevien tietojen, mukaan lukien Yhdysvaltojen hallituksen antamat lausumat ja sitoumukset, perusteella, että Yhdysvaltojen viranomaisten mahdollinen puuttuminen niiden henkilöiden perusoikeuksiin, joiden tietoja siirretään Privacy Shield -järjestelyn puitteissa unionista Yhdysvaltoihin, kansallisen turvallisuuden, lainvalvonnan tai muun yleisen edun nimissä ja tästä seuraavat rajoitukset, joita asetetaan oman varmennuksen antaneille organisaatioille yksityiseen suojaa koskevien periaatteiden noudattamisen osalta, rajoitetaan siihen, mikä on ehdottomasti tarpeen oikeutetun tavoitteen saavuttamiseksi, ja että tällaista perusoikeuksiin puuttumista vastaan on olemassa tehokkaita oikeussuojakeinoja.

⁽¹⁹⁷⁾ 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 tai se paljastetaan tai sitä käytetään tahallisesti, voi nostaa siviilikanteen kyseisen lain rikkomisesta, tietyissä olosuhteissa myös yksittäistä virkamiestä tai Yhdysvaltoja vastaan. Osoitteiden ja muunlaisen muun kuin sisällöllisen tiedon (esim. IP-osoite, sähköposti ja 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).

⁽¹⁹⁸⁾ 18 U.S.C. § 1030. Tietokonepetoksista ja -väärinkäytöksistä annetun lain (Computer Fraud and Abuse Act) mukaan henkilö voi nostaa kanteen henkilöä vastaan tahallisesti luvattomasta tietoihin pääsystä (tai luvallisen pääsyn rajojen ylittämisestä) saadakseen tietoja jostain finanssilaitoksesta, Yhdysvaltojen hallituksen tietokonejärjestelmästä tai muusta tietystä tietokoneesta, ja tietyissä olosuhteissa myös yksittäistä valtion virkamiestä vastaan.

⁽¹⁹⁹⁾ 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”.

⁽²⁰⁰⁾ 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 hankkiakseen tai luovuttaakseen suojattuja taloudellisia tietoja säännösten vastaisesti. Viranomaisten pääsy suojattuihin taloudellisiin tietoihin on yleensä kielletty, ellei tietojen luovuttamisen ehtona ole laillista haastetta tai etsintä lupaa, tai ellei tietyin rajoituksin esitetä kirjallista pyyntöä ja henkilö, jonka tietoja haetaan, saa ilmoituksen tällaisesta pyynnöstä.

⁽²⁰¹⁾ 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.

⁽²⁰²⁾ Unionin tuomioistuin on tunnustanut, että lainvalvonta on oikeutettu poliittinen tavoite. Ks. yhdistetyt asiat C-293/12 ja C-594/12, Digital Rights Ireland ym., ECLI:EU:C:2014:238, 42 kohta. Ks. myös Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohta ja Euroopan ihmisoikeustuomioistuimen tuomio asiassa Weber ja Saravia v. Saksa, hakemus nro 54934/00, 104 kohta.

- (141) Komissio katsoo, että tämä täyttää direktiivin 95/46/EY 25 artiklan vaatimukset, kun sitä tulkitaan ottaen huomioon Euroopan unionin perusoikeuskirja, kuten Euroopan unionin tuomioistuin on selvittänyt erityisesti asiassa Schrems antamassaan tuomiossa.

5. TIETOSUOJAVIRANOMAISTEN TOIMET JA TIEDOT KOMISSIOILLE

- (142) Asiassa Schrems antamassaan tuomiossa unionin tuomioistuin selvensi, että komissiolla ei ole toimivaltaa rajoittaa direktiivin 95/46/EY 28 artiklaan perustuvia tietosuojaviranomaisten toimivaltuuksia (mukaan lukien keskeyttää tiedonsiirrot), jos jokin henkilö kyseiseen säännökseen perustuvaa vaatimusta esittäessään asettaa kyseenalaiseksi sen, onko komission tietosuojan tason riittävyttä koskeva päätös yksityisyyden suojaa ja tietosuojaa koskevan perusoikeuden mukainen ⁽²⁰³⁾.
- (143) Jotta Privacy Shield -järjestelyn toimintaa voidaan valvoa tehokkaasti, jäsenvaltioiden olisi ilmoitettava komissiolle tietosuojaviranomaisten toteuttamista asiaankuuluvista toimista.
- (144) Unionin tuomioistuin katsoi lisäksi, että direktiivin 95/46/EY 25 artiklan 6 kohdan toisen alakohdan mukaisesti jäsenvaltioiden ja niiden elinten on toteutettava tarvittavat toimenpiteet noudattaakseen unionin toimielinten säädöksiä, sillä toimenpiteitä koskee pääsääntöisesti lainmukaisuusolettama, ja niillä on näin ollen oikeusvaikutuksia niin kauan kuin niitä ei ole peruutettu, kumottu kumoamiskanteen johdosta tai todettu pätemättömiksi ennakkoratkaisupyynnön tai lainvastaisuusväitteen seurauksena. Näin ollen direktiivin 95/46/EY 25 artiklan 6 kohdan mukainen tietosuojan tason riittävyttä koskeva komission päätös sitoo kaikkia jäsenvaltioiden elimiä, joille se on osoitettu, mukaan lukien niiden riippumattomat valvontaviranomaiset ⁽²⁰⁴⁾. Jos tällainen viranomainen on vastaanottanut valituksen, jossa asetetaan kyseenalaiseksi se, onko tietosuojan tason riittävyttä koskeva komission päätös yksityisyyden suojaa ja tietosuojaa koskevan perusoikeuden suojan mukainen, ja katsoo, että esitetyt perusteet ovat perusteltuja, kansallisessa lainsäädännössä on säädettävä oikeussuojakeinoista, joiden avulla viranomainen voi esittää perusteensa kansallisessa tuomioistuimessa, ja jos asiasta on epäilyksiä, tuomioistuimen on lykättävä asian käsittelyä ja pyydyttävä unionin tuomioistuimelta ennakkoratkaisua ⁽²⁰⁵⁾.

6. TIETOSUOJAN RIITTÄVÄN TASON SÄÄNNÖLLINEN UUELLEENTARKASTELU

- (145) Ottaen huomioon, että Yhdysvaltojen oikeusjärjestyksen tarjoama tietosuojan taso saattaa muuttua, komissio tarkastelee tämän päätöksen hyväksymisen jälkeen säännöllisin väliajoin, onko EU:n ja Yhdysvaltojen välisellä Privacy Shield -järjestelyllä taatun tietosuojan tason riittävyttä koskevat toteamukset edelleen tosiasiallisesti ja oikeudellisesti perusteltuja. Tällainen tarkastelu on joka tapauksessa tehtävä, kun komissio saa tietoja, jotka aiheuttavat perusteltuja epäilyksiä tältä osin ⁽²⁰⁶⁾.
- (146) Sen vuoksi komissio seuraa jatkuvasti EU:n ja Yhdysvaltojen välisellä Privacy Shield -järjestelyllä luotuja henkilötietojen siirron yleisiä puitteita, samoin kuin sitä, noudattavatko Yhdysvaltojen viranomaiset tämän päätöksen liitteenä oleviin asiakirjoihin sisältyviä lausumia ja sitoumuksia. Tämän prosessin helpottamiseksi Yhdysvallat on sitoutunut ilmoittamaan komissiolle olennaisista muutoksista Yhdysvaltojen lainsäädännössä siltä osin kuin muutokset liittyvät Privacy Shield -järjestelyn kannalta merkityksellisiin tietosuojakysymyksiin ja sellaisiin rajoituksiin ja suojoitimiin, jotka koskevat viranomaisten pääsyä henkilötietoihin. Lisäksi tämä päätös on vuotuisen yhteisen uudelleentarkastelun kohteena. Tarkastelu kattaa kaikki näkökohdat, jotka liittyvät EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toimintaan, mukaan luettuna kansallisen turvallisuuden ja lainvalvonnan nimissä tehdyt poikkeukset järjestelyn periaatteista. Koska tietosuojan tason riittävyyden toteamiseen voi vaikuttaa myös unionin oikeuden kehitys, komissio arvioi Privacy Shield -järjestelyn tarjoaman suojan tasoa yleisen tietosuoja-asetuksen soveltamisen alkamisen jälkeen.
- (147) Liitteissä I, II ja VI mainitun vuotuisen yhteisen uudelleentarkastelun toteuttamiseksi komissio tapaa kauppaministeriön ja liittovaltion kauppakomission edustajat sekä tarvittaessa edustajia muista ministeriöistä ja virastoista, jotka osallistuvat Privacy Shield -järjestelyjen täytäntöönpanoon, ja kansallista turvallisuutta koskevissa asioissa ODN:n ja muiden tiedusteluyhteisön toimijoiden edustajat sekä oikeusasiamiehen. Kokous on avoin EU:n tietosuojaviranomaisille ja 29 artiklan mukaisen tietosuojatyöryhmän edustajille.

⁽²⁰³⁾ Schrems, 40 kohta ja sitä seuraavat kohdat, 101–103 kohta.

⁽²⁰⁴⁾ Schrems, 51, 52 ja 62 kohta.

⁽²⁰⁵⁾ Schrems, 65 kohta.

⁽²⁰⁶⁾ Schrems, 76 kohta.

- (148) Komissio pyytää vuotuisen yhteisen tarkastelun yhteydessä, että kauppaministeriö toimittaa kattavat tiedot kaikista EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toimintaan liittyvistä asiaankuuluvista näkökohdista, kuten tietosuojaviranomaisten kauppaministeriölle siirtämistä asioista ja viran puolesta suoritettujen, periaatteiden noudattamista koskevien tarkastelujen tuloksista. Komissio pyytää myös selvityksiä mahdollisista kysymyksistä tai asioista, jotka koskevat EU:n ja Yhdysvaltojen välistä Privacy Shield -järjestelyä ja sen toimintaa ja johtuvat saatavilla olevista tiedoista, mukaan lukien USA FREEDOM Act -laissa sallitut avoimuusraportit sekä Yhdysvaltojen tiedusteluviranomaisten, kansallisten tietosuojaviranomaisten ja yksityisyyden suojaa käsittelevien ryhmien julkiset raportit sekä tiedotusvälineissä esitetyt tiedot tai muut mahdolliset lähteet. Komission tehtävän helpottamiseksi tältä osin jäsenvaltioiden olisi ilmoitettava komissiolle tapauksista, joissa niiden elinten toimilla, jotka vastaavat järjestelyn periaatteiden noudattamisesta Yhdysvalloissa, ei pystytty varmistamaan periaatteiden noudattamista, ja havainnoista, joiden mukaan kansallisesta turvallisuudesta tai rikosten ehkäisemisestä, tutkimisesta, paljastamisesta tai syytetoimista vastaavien Yhdysvaltojen viranomaisten toimet eivät takaa vaadittavaa suojatasoa.
- (149) Komissio laatii vuotuisen yhteisen uudelleentarkastelun perusteella julkisen raportin, joka toimitetaan Euroopan parlamentille ja neuvostolle.

7. TIETOSUOJAN TASON RIITTÄVYYTTÄ KOSKEVAN PÄÄTÖKSEN SOVELTAMISEN KESKEYTTÄMINEN

- (150) Jos tarkastusten tai muiden käytettävissä olevien tietojen perusteella komissio katsoo, että Privacy Shield -järjestelyn tarjoaman suojan taso ei enää olennaisesti vastaa unionissa tarjottavaa tasoa tai että on olemassa selviä viitteitä siitä, että järjestelyn periaatteiden tehokas noudattaminen Yhdysvalloissa ei ole enää varmistettu, tai että kansallisesta turvallisuudesta tai rikosten ehkäisemisestä, tutkimisesta, paljastamisesta tai syytetoimista vastaavien Yhdysvaltojen viranomaisten toimet eivät takaa vaadittavaa suojatasoa, se ilmoittaa asiasta kauppaministeriölle ja pyytää asianmukaisten toimenpiteiden toteuttamista, joilla voitaisiin tietyn, kohtuullisen määräajan kuluessa puuttua ripeästi tapauksiin, joissa järjestelyn periaatteita ei mahdollisesti noudateta. Jos Yhdysvaltojen viranomaiset eivät määräajan umpeutumisen jälkeen osoita riittävällä tavalla, että EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely takaa edelleen periaatteiden tehokkaan noudattamisen ja riittävän suojan, komissio aloittaa menettelyn tämän päätöksen soveltamisen keskeyttämiseksi osittain tai kokonaan tai päätöksen kumoamiseksi ⁽²⁰⁷⁾. Vaihtoehtoisesti komissio voi tehdä ehdotuksen tämän päätöksen muuttamisesta, esimerkiksi rajoittamalla tietosuojan tason riittävyyttä koskevan toteamuksen soveltamisalan vain sellaisiin tiedonsiirtoihin, joihin sovelletaan lisäedellytyksiä.
- (151) Komissio aloittaa keskeyttämis- tai kumoamismenettelyn erityisesti silloin kun
- a) on viitteitä siitä, että Yhdysvaltojen viranomaiset eivät noudata tämän päätöksen liitteenä oleviin asiakirjoihin sisältyviä lausumia ja sitoumuksia, mukaan lukien ne edellytykset ja rajoitukset, jotka koskevat Yhdysvaltojen viranomaisten pääsyä Privacy Shield -järjestelyn puitteissa siirrettyihin henkilötietoihin lainvalvonnan, kansallisen turvallisuuden ja muun yleisen edun nimissä;
 - b) EU:n rekisteröityjen valitukset jätetään todellisuudessa käsittelemättä; tässä yhteydessä komissio ottaa huomioon kaikki olosuhteet, joilla on vaikutusta EU:n rekisteröityjen mahdollisuuteen käyttää oikeuksiaan, erityisesti oman varmennuksen antaneiden yhdysvaltalaisyriyten vapaaehtoinen sitoumus tehdä yhteistyötä tietosuojaviranomaisten kanssa ja noudattaa heidän neuvojaan; tai
 - c) oikeusasiamies ei anna viipymättä asianmukaisia vastauksia EU:n rekisteröityjen pyyntöihin.
- (152) Komissio harkitsee myös menettelyn aloittamista tarkoituksenaan muuttaa tätä päätöstä, keskeyttää sen soveltaminen tai kumota se, jos Yhdysvaltojen kauppaministeriö tai muut järjestelyn täytäntöönpanoon osallistuvat ministeriöt tai virastot tai, kun on kyse kansallista turvallisuutta koskevista asioista, Yhdysvaltojen tiedusteluyhteisön edustajat tai oikeusasiamies eivät EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toimintaa koskevan vuotuisen yhteisen uudelleentarkastelun yhteydessä tai muuten toimita tietoja tai selvennyksiä, joita tarvitaan arvioitaessa, onko järjestelyn periaatteita noudatettu, ovatko valitusten käsittelymenettelyt

⁽²⁰⁷⁾ Yleisen tietosuoja-asetuksen soveltamisen alkamispäivästä komissio käyttää toimivaltaansa hyväksyä asianmukaisesti perustelluissa erittäin kiireellisissä tapauksissa täytäntöönpanosäädöksen, jolla keskeytetään välittömästi tämän päätöksen soveltaminen, ilman säädöksen toimittamista ennakoon asianomaiselle komiteamenettelyn mukaiselle komitealle. Säädös on voimassa enintään kuuden kuukauden ajan.

tehokkaita tai onko vaadittu tietosuojaan taso alentunut Yhdysvaltojen tiedusteluviranomaisten toimien johdosta, erityisesti sen seurauksena, että henkilötietojen keruuta ja/tai niihin pääsyä ei ole rajoitettu siihen, mikä on ehdottoman välttämätöntä ja oikeasuhteista. Tältä osin komissio ottaa huomioon, missä määrin asianomaiset tiedot voidaan saada muista lähteistä, mukaan lukien sellaiset oman varmennuksen antaneiden yhdysvaltalaisyriyten raportit, jotka on sallittu USA FREEDOM Act -laissa.

- (153) Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä on julkaissut lausuntonsa EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman suojan tasosta ⁽²⁰⁸⁾. Lausunto on otettu huomioon tämän päätöksen valmistelussa.
- (154) Euroopan parlamentti on antanut päätöslauselman transatlanttisista tietovirroista ⁽²⁰⁹⁾.
- (155) Tässä päätöksessä säädetty toimenpiteet ovat direktiivin 95/46/EY 31 artiklan 1 kohdalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

1. Komissio katsoo direktiivin 95/46/EY 25 artiklan 2 kohdan soveltamiseksi, että Yhdysvallat takaa riittävän suojan henkilötiedoille, jotka siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa unionista Yhdysvalloissa oleville organisaatioille.
2. EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely muodostuu Yhdysvaltojen kauppaministeriön 7 päivänä heinäkuuta 2016 antamista järjestelyn periaatteista, jotka on esitetty liitteessä II, ja virallisista lausumista ja sitoumuksista, jotka sisältyvät liitteissä I ja III–VII lueteltuihin asiakirjoihin.
3. Edellä olevan 1 kohdan soveltamiseksi henkilötietoja siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa silloin, kun ne siirretään unionista sellaisille Yhdysvalloissa oleville organisaatioille, jotka on sisällytetty Yhdysvaltojen kauppaministeriön liitteessä II esitettyjen järjestelyn periaatteiden I ja III jakson mukaisesti ylläpitämään ja julkisesti saataville asettamaan Privacy Shield -luetteloon.

2 artikla

Tämä päätös ei vaikuta henkilötietojen käsittelyä jäsenvaltioissa koskevien direktiivin 95/46/EY säännösten, erityisesti 4 artiklan, soveltamiseen, lukuun ottamatta 25 artiklan 1 kohtaa.

3 artikla

Kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät toimivaltuuksiaan direktiivin 95/46/EY 28 artiklan 3 kohdan mukaisesti keskeyttääkseen sellaiselle Yhdysvalloissa sijaitsevalle organisaatiolle suunnatut tietovirrat tai kieltääkseen ne lopullisesti, joka on sisällytetty Privacy Shield -luetteloon liitteessä II esitettyjen järjestelyn periaatteiden I ja III jakson mukaisesti yksilöiden suojelemiseksi henkilötietojen käsittelyssä, asianomaisen jäsenvaltion on ilmoitettava siitä komissiolle viipymättä.

4 artikla

1. Komissio seuraa jatkuvasti EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toimintaa arvioidakseen, varmistaako Yhdysvallat edelleen järjestelyn puitteissa unionista Yhdysvalloissa sijaitseville organisaatioille siirrettyjen henkilötietojen suojan riittävän tason.

⁽²⁰⁸⁾ Lausunto 01/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojaan tason riittävyyttä koskevasta päätösluonnoksesta, annettu 13.4.2016.

⁽²⁰⁹⁾ Euroopan parlamentin 26. toukokuuta 2016 antama päätöslauselma transatlanttisista tietovirroista (2016/2727(RSP)).

2. Jäsenvaltiot ja komissio ilmoittavat toisilleen tapauksista, joissa näyttää siltä, että Yhdysvaltojen valtiolliset elimet, joilla on lakisääteiset valtuudet toteuttaa täytäntöönpanotoimia liitteessä II vahvistettujen järjestelyn periaatteiden noudattamiseksi, eivät ota käyttöön tehokkaita havainto- ja valvontamekanismeja, joiden avulla voidaan havaita 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 ehdottoman välttämätöntä ja/tai tällaista oikeuteen puuttumista vastaan ei ole tehokasta oikeussuojaa.

4. Yhden vuoden kuluessa siitä päivästä, jona tämä päätös annetaan tiedoksi jäsenvaltioille, ja vuosittain sen jälkeen komissio arvioi 1 artiklan 1 kohdassa esitetyn päätelmän kaikkien saatavilla olevien tietojen perusteella, mukaan lukien liitteissä I, II ja VI mainitut tiedot, jotka on saatu osana vuotuista yhteistä tarkastelua.

5. Komissio raportoi kaikista asiaankuuluvista havainnoista direktiivin 95/46/EY 31 artiklan nojalla perustetulle komitealle.

6. Komissio esittää luonnoksen toimenpiteistä direktiivin 95/46/EY 31 artiklan 2 kohdassa tarkoitetun menettelyn mukaisesti tämän päätöksen soveltamisen keskeyttämiseksi tai päätöksen muuttamiseksi tai kumoamiseksi taikka sen soveltamisalan rajoittamiseksi muun muassa silloin, kun on viitteitä siitä, että

- Yhdysvaltojen viranomaiset eivät noudata tämän päätöksen liitteenä oleviin asiakirjoihin sisältyviä lausumia ja sitoumuksia, mukaan lukien edellytykset ja rajoitukset, jotka koskevat Yhdysvaltojen viranomaisten pääsyä EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa siirrettyihin henkilötietoihin lainvalvonnan, kansallisen turvallisuuden ja muun yleisen edun nimissä;
- EU:n rekisteröityjen valitukset jätetään todellisuudessa järjestelmällisesti käsittelemättä; tai
- oikeusasiamies on järjestelmällisesti laiminlyönyt liitteessä III olevan 4 kohdan e alakohdassa edellytettyjen oikea-aikaisten ja asianmukaisten vastausten antamisen EU:n rekisteröidyille.

Komissio esittää luonnoksen toimenpiteistä myös silloin, jos EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toiminnan varmistamiseen osallistuvien elinten yhteistyön puute estää komissiota arvioimasta vaikutuksia 1 artiklan 1 kohdassa esitettyyn päätelmään.

5 artikla

Jäsenvaltioiden on toteutettava kaikki tämän päätöksen noudattamisen edellyttämät toimenpiteet.

6 artikla

Tämä päätös on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä 12 päivänä heinäkuuta 2016.

Komission puolesta
Věra JOUROVÁ
Komission jäsen

LIITE I

Kirje Yhdysvaltojen kauppaministeriltä Penny Pritzkeriltä

7. heinäkuuta 2016

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

Arvoisa komissaari Jourová

Yhdysvaltojen puolesta minulla on kunnia toimittaa ohessa EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä koskeva asiakirja-aineisto. Materiaali on tulosta hedelmällisistä keskusteluista, joita työryhmämme ovat käyneet kahden vuoden ajan. Tämä paketti sekä muut tiedot, jotka ovat Euroopan komission saatavilla julkisista lähteistä, tarjoavat komissiolle erittäin vankan perustan, jonka pohjalta se voi tehdä uudet tietosuojan riittävyttä koskevat johtopäätöksensä ⁽¹⁾.

Meillä molemmilla on syytä olla ylpeitä järjestelyyn tehdyistä parannuksista. Privacy Shield -järjestely perustuu periaatteisiin, joilla on vahva ja yksimielinen tuki Atlantin molemmiin puolin. Olemme parantaneet periaatteiden toimintaa entisestään. Yhteistyömme ansiosta meillä on todellinen mahdollisuus parantaa yksityisyyden suojaa kaikkialla maailmassa.

Privacy Shield -paketti sisältää yksityisyyden suojaa koskevat periaatteet sekä liitteessä 1 olevan kirjeen, jonka on laatinut kauppaministeriön kansainvälisen kaupan osasto (International Trade Administration, ITA). Kyseinen osasto hallinnoi Privacy Shield -ohjelmaa. Kirjeessä selostetaan kauppaministeriön antamia sitoumuksia, joilla pyritään varmistamaan Privacy Shield -järjestelyn tehokas toiminta. Pakettiin sisältyy myös liite 2. Siinä selostetaan kauppaministeriön sitoumuksia, jotka koskevat Privacy Shield -järjestelyyn kuuluvaa välimiesmenettelyä.

Olen kehottanut henkilöstöäni kohdentamaan Privacy Shield -järjestelyyn kaikki tarvittavat resurssit hankkeen panemiseksi täytöntöön ripeästi ja täysimääräisesti ja sen varmistamiseksi, että liitteissä 1 ja 2 annetut sitoumukset täytetään oikea-aikaisesti.

Privacy Shield -paketti sisältää myös seuraavat muiden yhdysvaltalaisten virastojen toimittamat asiakirjat:

- liittovaltion kauppakomission (Federal Trade Commission, FTC) kirje, jossa selostetaan, kuinka kauppakomissio valvoo Privacy Shield -järjestelyn noudattamista;
- liikenneministeriön kirje, jossa selostetaan, kuinka liikenneministeriö valvoo Privacy Shield -järjestelyn noudattamista;
- kaksi kansallisen tiedusteluviraston johtajan (Office of the Director of National Intelligence, jäljempänä 'ODNI') laatimaa kirjettä suojoitusta ja rajoituksista, joita sovelletaan Yhdysvaltojen kansallisiin turvallisuusviranomaisiin;
- ulkoministeriön kirje ja sen oheismuistio, jossa selostetaan ulkoministeriön sitoumusta perustaa uusi tietosuojasta vastaavan oikeusasiamiehen virka. Oikeusasiamiehelle voidaan esittää kysymyksiä, jotka koskevat Yhdysvaltojen signaalitiedustelukäytäntöjä;
- sekä oikeusministeriön kirje suojoitusta ja rajoituksista, jotka koskevat Yhdysvaltojen viranomaisten pääsyä tietoihin lainvalvonnan ja yleisen edun nimissä.

Voitte olla vakuuttuneita siitä, että Yhdysvallat ottaa nämä sitoumukset vakavasti.

⁽¹⁾ Jos komission päätöstä, joka koskee EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan riittävyttä, sovelletaan myös Islantiin, Liechtensteiniin ja Norjaan, Privacy Shield -paketti kattaa paitsi Euroopan unionin jäsenvaltiot myös nämä kolme maata.

Privacy Shield -paketti toimitetaan kokonaisuudessaan julkaistavaksi Yhdysvaltojen virallisessa lehdessä (Federal Register) 30 päivän kuluessa siitä, kun tietosuojan riittävyyttä koskeva lopullinen päätös on tehty.

Odotamme innokkaasti yhteistyötä kanssanne pannessamme Privacy Shield -järjestelyä täytäntöön ja käynnistäessämme yhdessä tämän prosessin seuraavan vaiheen.

Kunnioittavasti
Penny Pritzker

Liite 1

Kansainvälisestä kaupasta vastaavan vt. alivaltiosihteerin Ken Hyattin kirje

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

Arvoisa komissaari Jourová

Kansainvälisen kaupan osaston puolesta olen iloinen voidessani tehdä selkoa siitä, miten EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely parantaa henkilötietojen suojaa ja millaisia sitoumuksia kauppaministeriö on tehnyt varmistaakseen, että Privacy Shield -järjestely toimii tuloksellisesti. Se, että tämä historiallinen järjestely 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 ongelmien sattuessa heillä on käytössään oikeussuojakeinoja. Sen tuoma varmuus auttaa transatlanttista taloutta kasvamaan, sillä sen avulla varmistetaan, että tuhannet eurooppalaiset ja amerikkalaiset yritykset voivat edelleen investoida ja käydä kauppaa yli rajojen. Privacy Shield -järjestely on tulosta yli kahden vuoden kovista ponnisteluista ja yhteistyöstä Euroopan komission kollegoiden kanssa. Odotamme innolla mahdollisuutta jatkaa työskentelyä komission kanssa sen varmistamiseksi, että Privacy Shield toimii tarkoitetulla tavalla.

Olemme tehneet komission kanssa työtä kehittääksemme Privacy Shield -järjestelyn, jotta Yhdysvaltoihin sijoittautuneilla organisaatioilla on mahdollisuus täyttää EU:n lainsäädännön mukaiset tietosuojan riittävyttä koskevat vaatimukset. Uusi järjestely tarjoaa useita merkittäviä hyötyjä sekä yksityishenkilöille että yrityksille. Ensinnäkin se on merkittävä yksityisyyden suojan kokonaisuus, joka turvaa EU:n kansalaisten tietoja. Järjestely edellyttää siihen osallistuvilta yhdysvaltalaisilta organisaatioilta seuraavaa: niiden on laadittava järjestelyn kanssa sopusoinnussa olevat tietosuojaperiaatteet; niiden on annettava sitoumus Privacy Shield -järjestelyn periaatteiden noudattamisesta, ja sitoumuksen on oltava julkinen niin, että siitä tulee Yhdysvaltojen lain mukaan täytäntöönpanokelpoinen; 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 liittovaltion kauppakomission (U.S. Federal Trade Commission, FTC), liikenneministeriön (Department of Transportation, DOT) tai muun lainvalvontaviraston toimivallan alaisia. Toiseksi Privacy Shield -järjestelyn ansiosta tuhannet yritykset Yhdysvalloissa ja eurooppalaisten yritysten tytäryhtiöt Yhdysvalloissa voivat saada henkilötietoja Euroopan unionista. Näin edistetään tietovirtoja, jotka tukevat transatlanttista kauppaa. Transatlanttiset taloussuhteet ovat jo nyt maailman suurimmat. Niiden osuus maailman taloustuotannosta on puolet, ja tavara- ja palveluvaihdon määrä on lähes biljoona dollaria. Taloussuhteilla pidetään yllä miljoonia työpaikkoja Atlantin molemmin puolin. Yrityksiä, joille transatlanttiset tietovirrat ovat tärkeitä, on kaikilla teollisuuden aloilla, ja niiden joukossa on suuria Fortune 500 -yrityksiä sekä monia pk-yrityksiä. Transatlanttisten tietovirtojen avulla yhdysvaltalaiset organisaatiot voivat käsitellä tietoja, joita ne tarvitsevat voidakseen tarjota tavaroita, palveluja ja työtilaisuuksia EU:n kansalaisille. Privacy Shield -järjestelyllä edistetään yhteisiä tietosuojaperiaatteita ja kurotaan umpeen eroja, jotka vallitsevat EU:n ja Yhdysvaltojen oikeudellisten lähestymistapojen välillä. Samalla edistetään sekä Euroopan että Yhdysvaltojen kaupallisia ja taloudellisia tavoitteita.

Vaikka yrityksen päätös liittyä oman varmennuksensa myötä järjestelyyn on vapaaehtoinen, sääntönä on, että kun yritys on julkisesti sitoutunut noudattamaan Privacy Shield -järjestelyä, sitoumus on Yhdysvaltojen lainsäädännön mukaan täytäntöönpanokelpoinen ja täytäntöönpanon toimittaa joko liittovaltion kauppakomissio tai Yhdysvaltojen liikenneministeriö sen mukaan, mikä viranomainen on toimivaltainen Privacy Shield -järjestelyyn sitoutuneen organisaation suhteen.

Privacy Shield -järjestelyn periaatteisiin tehdyt parannukset

Neuvottelujen tuloksena saavutettu Privacy Shield -järjestely vahvistaa yksityisyyden suojaa seuraavasti:

- Järjestelyn ilmoitusperiaatteen mukaisesti vaaditaan, että henkilöille annetaan lisätietoa. Tähän kuuluu ilmoitus siitä, että organisaatio osallistuu Privacy Shield -järjestelyyn ja että henkilöillä on oikeus tutustua henkilötietoihinsa, samoin kuin tieto siitä, mikä elin toimii riippumattomana riitojenratkaisuelimenä.
- Privacy Shield -järjestelyssä vahvistetaan sellaisten henkilötietojen suojaa, jotka järjestelyyn osallistuva organisaatio siirtää rekisterinpitäjänä toimivalle kolmannelle osapuolelle. Näissä tapauksissa osapuolten on tehtävä sopimus, jonka mukaan 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 Privacy Shield -järjestelyn periaatteita.

- Privacy Shield -järjestelyssä parannetaan sellaisten henkilötietojen suojaa, jotka järjestelyyn osallistuva organisaatio siirtää edustajanaan toimivalle kolmannelle osapuolelle. Privacy Shield -järjestelyyn osallistuvan organisaation on toteutettava seuraavat toimet: sen on varmistettava kohtuullisin ja asianmukaisin toimin, että edustaja käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa Privacy Shield -periaatteiden mukaisia organisaation velvoitteita; havaitessaan luvaton tiedonkäsitelyä sen on ryhdyttävä kohtuullisiin ja asianmukaisiin toimiin kyseisen tiedonkäsitelyn lopettamiseksi ja tilanteen korjaamiseksi; organisaation on pyynnöstä annettava kauppaministeriölle yhteenveto tai keskeiset osat sisältävä jäljennös yksityisyyden suojaa koskevista määräyksistä, jotka sisältyvät edustajan kanssa tehtyyn sopimukseen.
- Privacy Shield -periaatteiden mukaan järjestelyyn osallistuva organisaatio on vastuussa sellaisten henkilötietojen käsittelystä, jotka se vastaanottaa järjestelyn yhteydessä ja sittemmin siirtää edustajanaan toimivalle kolmannelle osapuolelle. Lisäksi Privacy Shield -järjestelyyn osallistuva organisaatio on järjestelyn periaatteiden mukaan korvausvelvollinen, jos sen edustaja käsittelee kyseisiä henkilötietoja tavalla, joka ei ole järjestelyn periaatteiden mukainen, ellei organisaatio osoita, että se ei ole vastuussa tapahtumasta, joka johti syntyneeseen vahinkoon.
- Privacy Shield -järjestelyssä tehdään selväksi, että järjestelyyn osallistuvien organisaatioiden on rajoitettava henkilötietojen käsittely tietoihin, jotka ovat tarpeellisia tiedonkäsitelyn tarkoituksen kannalta.
- Privacy Shield -järjestelyssä noudatettavien vaatimusten mukaan järjestelyyn osallistuvan organisaation on vuosittain vahvistettava kauppaministeriölle sitoutumisensa siihen, että se soveltaa järjestelyn periaatteita tietoihin, jotka se on vastaanottanut järjestelyyn osallistumisensa aikana ja jotka se päättää säilyttää itsellään irtautuessaan järjestelystä.
- Järjestelyssä noudatettavien vaatimusten mukaan organisaation on järjestettävä riippumaton muutoksenhakumekanismi ilman, että tästä aiheutuu kuluja henkilöille.
- Privacy Shield -järjestelyssä vaaditaan, että organisaatioiden ja niiden valitsemien riippumattomien muutoksenhakumekanismien on vastattava nopeasti järjestelyä koskeviin kauppaministeriön tiedusteluihin ja tietopyyntöihin.
- Privacy Shield -järjestelyssä vaaditaan, että organisaatiot vastaavat viipymättä valituksiin, jotka EU:n jäsenvaltioiden viranomaiset ovat toimittaneet kauppaministeriön kautta ja jotka koskevat järjestelyn periaatteiden noudattamista.
- Privacy Shield -järjestelyssä vaaditaan, että jos järjestelyyn osallistuvalla organisaatiolla osoitetaan sääntöjen rikkomukseen perustuva tuomioistuimen tai liittovaltion kauppakomission määräys, organisaatio julkistaa kaikki Privacy Shield -järjestelyä koskevat osat sellaisista sääntöjen noudattamista koskevista kertomuksista tai arviointikertomuksista, jotka on toimitettu liittovaltion kauppakomissiolle.

Kauppaministeriön toteuttama Privacy Shield -järjestelyn hallinto ja valvonta

Kauppaministeriö vahvistaa uudelleen sitoumuksensa siitä, että se pitää yllä ja yleisön saatavilla virallista luetteloa, jäljempänä 'Privacy Shield -luettelo', yhdysvaltalaisista organisaatioista, jotka ovat toimittaneet oman varmennuksensa kauppaministeriölle ja vahvistaneet sitoumuksensa järjestelyn periaatteiden noudattamisesta. Kauppaministeriö pitää Privacy Shield -luettelon ajan tasalla siten, että se poistaa siitä organisaatiot, jotka vetäytyvät siitä vapaaehtoisesti, jotka jättävät tekemättä kauppaministeriön menettelytapojen mukaisen vuotuisen uudelleenvarmennuksen tai joiden havaitaan jatkuvasti rikkovan järjestelyn periaatteita. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa myös sellaisista yhdysvaltalaisista organisaatioista, jotka ovat aiemmin antaneet oman varmennuksensa kauppaministeriölle mutta jotka on sittemmin poistettu Privacy Shield -luettelosta, mukaan lukien organisaatiot, jotka on poistettu niiden jatkuvasti rikottua järjestelyn periaatteita. Kauppaministeriö mainitsee aina perusteen, jonka vuoksi organisaatio on poistettu luettelosta.

Lisäksi kauppaministeriö sitoutuu vahvistamaan Privacy Shield -järjestelyn hallintoa ja valvontaa. Erityisesti kauppaministeriö toteuttaa seuraavat toimet:

Kauppaministeriö sisällyttää enemmän tietoa Privacy Shield -järjestelyn verkkosivustolle:

- Privacy Shield -luetteloa pidetään yllä, samoin kuin luetteloa organisaatioista, jotka ovat aiemmin esittäneet oman varmennuksensa järjestelyn periaatteiden noudattamisesta mutta jotka eivät enää ole oikeutettuja Privacy Shield -järjestelyn etuihin.
- Näkyvästi esillä olevalla selostuksella tehdään selväksi, että yksikään organisaatio, joka on poistettu Privacy Shield -luettelosta, ei enää voi hyötyä järjestelyn eduista mutta että organisaation on kuitenkin edelleen sovellettava järjestelyn periaatteita henkilötietoihin, jotka se on saanut osallistumisensa aikana, ja että tämä velvoite kestää niin kauan kuin se säilyttää kyseisiä tietoja.
- Lisäksi esillä on linkki liittovaltion kauppakomission verkkosivustolla olevaan luetteloon, joka koskee Privacy Shield -järjestelyyn liittyviä, liittovaltion kauppakomissiossa käsiteltyjä asioita.

Kauppaministeriö tarkastaa, että oman varmennuksen vaatimukset täyttyvät:

- Ennen kuin kauppaministeriö vahvistaa organisaation oman varmennuksen (tai vuotuisen uudelleenvarmennuksen) ja lisää organisaation Privacy Shield -luetteloon, kauppaministeriö varmistaa, että organisaatio on
 - toimittanut edellytetyt yhteystietonsa,
 - kuvannut, kuinka organisaatio käsittelee EU:sta saatavia henkilötietoja,
 - selostanut, mitä henkilötietoja sen oma varmennus kattaa,
- jos organisaatiolla on julkiset verkkosivut, ilmoittanut verkko-osoitteen, jossa sen tietosuojaperiaatteet ovat saatavilla ja katsottavissa, tai jos julkisia verkkosivuja ei ole, ilmoittanut, missä yleisö voi tutustua kyseisiin periaatteisiin,
- sisällyttänyt tietosuojaperiaatteisiinsa ilmoituksen siitä, että se noudattaa järjestelyn periaatteita, ja jos tietosuoja-periaatteet ovat saatavilla verkossa, sisällyttänyt niihin linkin kauppaministeriön Privacy Shield -järjestelyä koskevalle verkkosivustolle,
- ilmoittanut, millä erityisellä lakisäätöisellä elimellä (joka on lueteltu järjestelyn periaatteissa tai niiden tulevassa liitteessä) on toimivalta käsitellä organisaatiosta tehty valitukset, jotka koskevat mahdollisia sopimattomia tai vilpillisiä käytäntöjä ja yksityisyyttä koskevien lakien ja asetusten rikkomuksia,
- siinä tapauksessa, että organisaatio on päättänyt täyttää muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen a kohdan i ja iii alakohdan vaatimukset sitoumuksella, jonka mukaan se tekee yhteistyötä asiaankuuluvien EU:n tietosuojaviranomaisten kanssa, ilmoittanut aikomuksestaan tehdä yhteistyötä tietosuojaviranomaisten kanssa Privacy Shield -järjestelyssä vireille tulleiden valitusten tutkimisessa ja ratkaisemisessa ja erityisesti aikomuksestaan vastata tietosuojaviranomaisten kysymyksiin, kun EU:n rekisteröidyt ovat esittäneet valituksensa suoraan maansa kansalliselle tietosuojaviranomaiselle,
- ilmoittanut kaikki yksityisyydensuojaohjelmat, joihin organisaatio osallistuu,
- ilmoittanut, millä menetelmällä tarkastetaan, että järjestelyn periaatteiden noudattaminen on varmistettu (esim. tarkastus yrityksen sisällä, kolmannen osapuolen tekemä tarkastus),
- ilmoittanut sekä omassa varmennuksessaan että tietosuojaperiaatteissaan, mikä riippumaton muutoksenhakumekanismi on käytettävissä valitusten tutkimiseen ja ratkaisemiseen,
- sisällyttänyt tietosuojaperiaatteisiin – siinä tapauksessa että ne ovat saatavilla verkossa – linkin sen riippumattoman muutoksenhakumekanismiin verkkosivustoon, joka on käytettävissä ratkaisematta olevien valitusten tutkimiseen, tai linkin lomakkeeseen, jota käyttäen kyseiselle mekanismille voi toimittaa valituksen,
- jos organisaatio on ilmoittanut aikovansa vastaanottaa EU:sta henkilöstötietoja ja käyttää niitä työsuhteidensa yhteydessä, toteuttanut seuraavat toimet: ilmoittanut sitoutuvansa yhteistyöhön tietosuojaviranomaisten kanssa ja noudattavansa näiden määräyksiä siinä tarkoituksessa, että valituksiin, jotka koskevat organisaation toimia henkilöstötietojen osalta, saadaa ratkaisut; toimittanut kauppaministeriölle jäljennöksen organisaation henkilöstöä koskevista tietosuojaperiaateista; sekä ilmoittanut, missä henkilöstö, jota asia koskee, voi tutustua organisaation tietosuojaperiaatteisiin.
- Kauppaministeriö tarkastaa yhdessä riippumattomien muutoksenhakumekanismien kanssa, että organisaatiot ovat tosiasiaassa rekisteröityneet – jos tällainen rekisteröinti vaaditaan – mekanismeissa, jotka ne ovat ilmoittaneet toimittamisensa omista varmennuksista.

Kauppaministeriö pyrkii seuraamaan tarkemmin organisaatioita, jotka on poistettu Privacy Shield -luettelosta:

- Kauppaministeriö ilmoittaa organisaatioille, jotka on poistettu Privacy Shield -luettelosta järjestelyn periaatteiden jatkuvan rikkomisen vuoksi, että niillä ei ole oikeutta säilyttää Privacy Shield -järjestelyssä vastaanotettuja tietoja.
- Kauppaministeriö lähettää kyselylomakkeet organisaatioille, joiden omat varmennukset raukeavat tai jotka ovat vapaaehtoisesti vetäytyneet Privacy Shield -järjestelystä, sen tarkistamiseksi, aikooko organisaatio palauttaa tai hävittää Privacy Shield -järjestelyn puitteissa saamansa henkilötiedot vai aikovatko ne jatkaa yksityisyyden suojaa koskevien periaatteiden soveltamista kyseisiin henkilötietoihin, ja jos henkilötiedot aiotaan säilyttää, kuka organisaatiossa toimii yhteyspisteenä järjestelyyn liittyvissä kysymyksissä.

Kauppaministeriö etsii organisaatioita, jotka totuudenvastaisesti väittävät osallistuvansa järjestelyyn, ja puuttuu näihin tapauksiin:

- Kauppaministeriö tarkistaa sellaisten organisaatioiden tietosuojaperiaatteet, jotka ovat aiemmin osallistuneet Privacy Shield -järjestelyyn mutta jotka on poistettu Privacy Shield -luettelosta, ja pyrkii näin havaitsemaan osallistumista koskevia totuudenvastaisia väittämiä.
- Kun organisaatio a) vetäytyy Privacy Shield -järjestelystä tai b) jättää toimittamatta uudelleenvarmennuksen, jossa se olisi todennut, että se edelleen noudattaa järjestelyn periaatteita, tai c) kun se poistetaan Privacy Shield -järjestelystä varsinkin ”sen jatkuvasti rikottua järjestelyn periaatteita”, kauppaministeriö tarkastaa jatkuvasti viran puolesta, että organisaatio on poistanut kaikista julkistamistaan tietosuojaperiaatteista kaikki Privacy Shield -järjestelyä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuu edelleen aktiivisesti Privacy Shield -järjestelyyn ja että sillä on oikeus hyödyntää sen etuja. Kun kauppaministeriö havaitsee, että tällaisia viittauksia ei ole poistettu, se antaa organisaatiolle varoituksen, jossa kauppaministeriö toteaa, että jos organisaatio jatkaa väitteitään osallistumisestaan Privacy Shield -järjestelyyn, kauppaministeriö siirtää tarvittaessa asian toimivaltaisen viraston käsiteltäväksi mahdollisia lainvalvontatoimia varten. Jos organisaatio ei poista viittauksia eikä toimita omaa varmennusta siitä, että se noudattaa Privacy Shield -järjestelyn periaatteita, kauppaministeriö siirtää asian viran puolesta liittovaltion kauppakomissiolle, liikenneministeriölle tai muulle toimivaltaiselle lainvalvontavirastolle tai soveltuissa tapauksissa ryhtyy toimiin valvoakseen Privacy Shield -varmennusmerkin käyttöä.
- Kauppaministeriö toteuttaa muita toimia, joilla pyritään havaitsemaan totuudenvastaisia väitteitä osallistumisesta Privacy Shield -järjestelyyn ja paljastamaan Privacy Shield -varmennusmerkin epäasianmukainen käyttö. Näitä toimia ovat esimerkiksi sellaisia verkkosivuja koskevat internethaut, joissa Privacy Shield -varmennusmerkkiä esiintyy tai joissa olevissa organisaation tietosuojaperiaatteissa viitataan Privacy Shield -järjestelyyn.
- Tarkkaillessaan viran puolesta tilanteita, joissa esitetään totuudenvastaisia väitteitä osallistumisesta Privacy Shield -järjestelyyn ja joissa on kyse Privacy Shield -varmennusmerkin epäasianmukaisesta käytöstä, kauppaministeriö puuttuu viipymättä kaikkiin havaitsemiinsa tapauksiin ja muun muassa toimittaa aiemmin kuvatulla tavalla varoituksia organisaatioille, jotka antavat virheellistä tietoa osallistumisestaan.
- Kauppaministeriö toteuttaa muita asianmukaisia korjaavia toimia ja muun muassa ryhtyy sen käytettävissä oleviin oikeudellisiin toimenpiteisiin sekä siirtää asioita liittovaltion kauppakomission, liikenneministeriön tai muun toimivaltaisen lainvalvontaviraston käsiteltäväksi.
- Kauppaministeriö käsittelee ripeästi sille toimitetut valitukset, jotka koskevat totuudenvastaisia väitteitä osallistumisesta järjestelyyn, ja puuttuu viipymättä kyseisiin tapauksiin.

Kauppaministeriö tarkastelee organisaatioiden tietosuojaperiaatteita havaitakseen paremmin totuudenvastaisia väitteitä osallistumisesta Privacy Shield -järjestelyyn ja puuttuakseen niihin tehokkaammin. Erityisesti kauppaministeriö tarkastaa sellaisten organisaatioiden tietosuojaperiaatteet, joiden oma varmennus on rauennut siitä syystä, että ne eivät ole antaneet uudelleenvarmennusta järjestelyn periaatteiden noudattamisesta. Kauppaministeriö tekee tällaisia tutkimuksia sen tarkastamiseksi, onko organisaatio poistanut kaikista julkistamistaan tietosuojaperiaatteista kaikki Privacy Shield -järjestelyä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuu edelleen aktiivisesti Privacy Shield -järjestelyyn. Näiden tarkastusten tuloksena kauppaministeriö saattaa havaita organisaatioita, jotka eivät ole poistaneet kyseisiä viittauksia. Ministeriö toimittaa niille ministeriön päälakimiehen toimiston (Office of General Counsel) laatiman kirjeen, jossa varoitetaan mahdollisista lainvalvontatoimista, ellei viittauksia poisteta. Kauppaministeriö huolehtii seurannasta sen varmistamiseksi, että organisaatiot joko poistavat sopimattomat viittaukset tai antavat uudelleenvarmennuksen järjestelyn periaatteiden noudattamisesta. Lisäksi kauppaministeriö pyrkii havaitsemaan organisaatioita, jotka eivät ole koskaan osallistuneet Privacy Shield -järjestelyyn mutta jotka esittävät totuudenvastaisia väitteitä osallistumisestaan, ja toteuttaa näiden organisaatioiden osalta samanlaisia korjaavia toimenpiteitä kuin edellä on selostettu.

Kauppaministeriö tarkastelee määräajoin viran puolesta periaatteiden noudattamista ja arvioi ohjelmaa:

- Kauppaministeriö valvoo jatkuvasti periaatteiden noudattamista, muun muassa lähettämällä osallistuville organisaatioille yksityiskohtaisia kyselylomakkeita. Tällä tavoin pyritään tunnistamaan aihealueita, jotka saattavat edellyttää jatkotoimia. Periaatteiden noudattamista tarkastellaan varsinkin seuraavissa tapauksissa: a) kauppaministeriö on vastaanottanut organisaatiota koskevia yksilöityjä valituksia, jotka liittyvät järjestelyn periaatteiden noudattamiseen, eivätkä valitukset ole aiheettomia, b) organisaatio ei anna tyydyttävää vastausta Privacy Shield -järjestelyä koskevaan kauppaministeriön tietopyyntöön tai c) on uskottavaa näyttöä siitä, että organisaatio ei noudata Privacy Shield -järjestelyssä antamia sitoumuksia. Kauppaministeriön on tarvittaessa kuultava toimivaltaista tietosuojaviranomaista periaatteiden noudattamisen tarkastelusta.
- Kauppaministeriö arvioi säännöllisesti Privacy Shield -järjestelyn hallintoa ja valvontaa sen varmistamiseksi, että seurannalla voidaan asianmukaisesti puuttua esiin nouseviin uusiin kysymyksiin.

Kauppaministeriö on lisännyt Privacy Shield -järjestelyn hallinnon ja valvonnan voimavaroja ja muun muassa kaksinker-
taistanut tähän toimintoon osallistuvan henkilöstön määrän. Kauppaministeriö osoittaa vastaisuudessaakin riittävästi voimavaroja tähän toimintoon, jotta ohjelman tuloksellinen seuranta ja hallinnointi voidaan varmistaa.

Kauppaministeriö räätälöi Privacy Shield -järjestelyn verkkosivuston eri kohdeyleisöille:

Kauppaministeriö muotoilee Privacy Shield -järjestelyn verkkosivuston niin, että se keskittyy kolmeen kohdeyleisöön: EU:n kansalaiset, EU:n yritykset ja Yhdysvaltojen yritykset. 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 Privacy Shield -järjestelyn 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 omaa Privacy Shield -varmennusta. EU:n yritysten on sivuston avulla helpompi tarkastaa, 1) onko organisaatio oikeutettu Privacy Shield -järjestelyyn etuihin, 2) minkä tyyppisiä tietoja organisaation oma Privacy Shield -varmennus kattaa, 3) millaisia tietosuojaperiaatteita sovelletaan varmennuksen kattamiin tietoihin sekä 4) millä menetelmällä organisaatio varmistaa, että se noudattaa järjestelyn periaatteita.

Kauppaministeriö lisää yhteistyötään tietosuojaviranomaisten kanssa:

Jotta yhteistyölle tietosuojaviranomaisten kanssa olisi paremmat edellytykset, kauppaministeriö perustaa erityisen yhteyspisteen, joka toimii linkkinä tietosuojaviranomaisten suuntaan. Jos tietosuojaviranomainen katsoo, että 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. Yhteyspisteelle ilmoitetaan myös organisaatioista, jotka väittävät totuudenvastaisesti osallistuvansa Privacy Shield -järjestelyyn, vaikka eivät ole koskaan toimittaneet omaa varmennusta järjestelyn periaatteiden noudattamisesta. Yhteyspiste myös avustaa tietosuojaviranomaisia, jotka etsivät tietoja tietyn organisaation omasta varmennuksesta tai aiemmasta osallistumisesta ohjelmaan, sekä vastaa tietosuojaviranomaisten tiedusteluihin, jotka koskevat tiettyjen Privacy Shield -järjestelyn vaatimusten täytäntöönpanoa. Yhteyspisteen perustamisen lisäksi kauppaministeriö toimittaa tietosuojaviranomaisille Privacy Shield -järjestelyä koskevaa materiaalia, jonka tietosuojaviranomaiset voivat sisällyttää omille verkkosivustoilleen ja näin lisätä järjestelyn läpinäkyvyyttä EU:n kansalaisten ja EU:n yritysten näkökulmasta. Privacy Shield -järjestelyä ja siihen liittyviä oikeuksia ja velvollisuuksia koskevan tiedon lisääntyessä pitäisi olla helpompaa tunnistaa aiheeseen liittyvät ongelmat sitä mukaa kun ne syntyvät ja sitten ratkaista ne asianmukaisesti.

Kauppaministeriö edistää periaatteiden rikkomuksia koskevien valitusten ratkaisemista:

Tietosuojaviranomaisten kauppaministeriön käsiteltäväksi saattamat valitukset, joiden mukaan Privacy Shield -järjestelyyn osallistuva organisaatio ei noudata järjestelyn periaatteita, saapuvat kauppaministeriölle yhteyspisteen kautta. Kauppaministeriö pyrkii parhaansa mukaan edistämään sitä, että valitukseen saadaan ratkaisu Privacy Shield -järjestelyyn osallistuvan organisaation kanssa. Kauppaministeriö antaa tietosuojaviranomaiselle selonteon asian edistymisestä 90 päivän kuluessa valituksen vastaanottamisesta. Jotta valituksen tekeminen olisi helpompaa, kauppaministeriö laatii sitä varten vakiolomakkeen, jonka tietosuojaviranomaiset voivat toimittaa yhteyspisteelle. Yhteyspiste pitää kirjaa kaikista valituksista, jotka kauppaministeriö on vastaanottanut tietosuojaviranomaisilta, ja ministeriö antaa myöhemmin selostettavassa vuotuisessa tarkastelussa kertomuksen, jossa kunakin vuonna vastaanotettuja valituksia analysoidaan yhtenä kokonaisuutena.

Kauppaministeriö perustaa välimiesmenettelyn ja valitsee välimiehet yhteistyössä komission kanssa:

Kauppaministeriö täyttää liitteen I mukaiset sitoumuksensa ja julkaisee menettelytavat sen jälkeen, kun niistä on saavutettu yhteisymmärrys.

Privacy Shield -järjestelyn toimivuutta tarkastellaan yhteisen mekanismin avulla:

Kauppaministeriö, liittovaltion kauppakomissio ja tarvittaessa muut virastot pitävät komission, asiasta kiinnostuneiden tietosuojaviranomaisten ja 29 artiklan mukaisen tietosuojatyöryhmän edustajien kanssa vuotuisia kokouksia, joissa kauppaministeriö selostaa Privacy Shield -järjestelyn kulloistakin tilannetta. Vuotuisissa kokouksissa keskustellaan ajankohtaisista kysymyksistä, jotka liittyvät Privacy Shield -järjestelyn toimintaan, täytäntöönpanoon ja valvontaan, mukaan lukien tietosuojaviranomaisilta kauppaministeriölle siirretyt asiat sekä viran puolesta tehtyjen, periaatteiden noudattamista koskevien tarkastelujen tulokset. Vuotuisissa kokouksissa voidaan keskustella myös lainsäädännön merkityksellisistä muutoksista. Ensimmäisessä vuotuisessa tarkastelussa ja tarvittaessa myöhemmissä tarkasteluissa keskustellaan myös muista aiheista, kuten automaattisista päätöksistä, sekä siitä, millaisia yhtäläisyyksiä ja eroja EU:n ja Yhdysvaltojen lähestymistapojen välillä on.

Lainsäädännön muutokset:

Kauppaministeriö pyrkii kohtuullisin toimin antamaan komissiolle tietoja merkittävistä muutoksista Yhdysvaltojen laeissa siltä osin kuin muutokset liittyvät Privacy Shield -järjestelyn kannalta merkityksellisiin tietosuojakysymyksiin ja sellaisiin rajoituksiin ja suojatoimiin, jotka koskevat Yhdysvaltojen viranomaisten pääsyä henkilötietoihin ja näiden tietojen myöhempää käyttöä.

Kansallista turvallisuutta koskeva poikkeus:

Kansallisen tiedusteluviraston päälakimies, Robert Litt, on toimittanut kauppaministeriön henkilökunnan jäsenille Justin Antonipillaille ja Ted Deanille osoittamansa kaksi kirjettä. Kirjeiden aiheena ovat rajoitukset, joita kansallisen turvallisuuden vuoksi sovelletaan Privacy Shield -järjestelyn periaatteiden noudattamiseen. Kirjeet on toimitettu edelleen teille. Kirjeissä käsitellään laajasti muun muassa Yhdysvaltojen signaalitiedusteluun liittyviä toimintaperiaatteita, suojatoimia ja rajoituksia. Lisäksi kirjeissä on kuvattu läpinäkyvyyttä, jota tiedusteluyhteisö harjoittaa näissä kysymyksissä. Komission parhaillaan arvioidessa Privacy Shield -järjestelyä kirjeissä annetut tiedot tuottavat varmuutta, jonka perusteella on mahdollista päätellä, että Privacy Shield -järjestely toimii asianmukaisesti ja että sen periaatteita noudatetaan. Ymmärrämme, että voitte tuoda Privacy Shield -järjestelyn tulevilla vuotuisissa tarkasteluissa keskustelun kohteeksi tietoja, jotka tiedusteluyhteisö on julkistanut, sekä muita tietoja ja että näitä tietoja voidaan hyödyntää kyseisissä tarkasteluissa.

Privacy Shield -järjestelyn periaatteiden ja sen yhteydessä toimittujen kirjeiden ja tietojen, muun muassa Privacy Shield -järjestelyn hallintoa ja valvontaa koskevien kauppaministeriön sitoumusten perusteella meidän olettamuksemme on, että komissio tekee päätelmän, jonka mukaan EU:n ja Yhdysvaltojen Privacy Shield -järjestely tuottaa EU:n lainsäädännön edellyttämän riittävän suojan ja tietosiirrot EU:sta Privacy Shield -järjestelyyn osallistuville organisaatioille jatkuvat.

Kunnioittavasti

Ken Hyatt

Liite 2

Välimiesmenettelyä koskeva malli

LIITE I

Liitteessä I esitetään ehdot, joiden mukaisesti Privacy Shield -järjestelyyn osallistuvat organisaatiot ovat velvollisia osallistumaan välimiesmenettelyyn muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaisesti. Sitovaa välitysmahdollisuutta, jota jäljempänä selostetaan, sovelletaan vaatimuksiin, jotka koskevat EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn soveltamisalaan kuuluvia tietoja ja joihin ei ole saatu ratkaisua. Tämän vaihtoehdon tarkoituksena on tarjota nopea, riippumaton ja oikeudenmukainen mekanismi ratkaisun saamiseksi sellaisiin väitettyihin järjestelyn periaatteiden rikkomustapauksiin, joita ei ole kyetty ratkaisemaan muilla mahdollisilla Privacy Shield -järjestelyn mekanismeilla. Henkilöllä on oikeus valita, turvautuuko hän välitysmenettelyyn.

A. Soveltamisala

Välimiesmenettely on henkilön käytettävissä sellaisten vaatimusten osalta, jotka ovat jääneet vaille ratkaisua. Välimiesmenettelyn avulla voidaan saada vastaus kysymykseen, onko Privacy Shield -järjestelyyn osallistuva organisaatio rikkonut järjestelyn velvoitteita kyseisen henkilön osalta ja onko kyseinen rikkomus edelleen täysin tai osittain korjaamatta. Välimiesmenettelyä voidaan käyttää ainoastaan tähän tarkoitukseen. Välimiesmenettelyä ei voida hyödyntää esimerkiksi asioissa, jotka liittyvät järjestelyn periaatteista myönnettäviin poikkeuksiin ⁽¹⁾ tai Privacy Shield -järjestelyn tarjoaman suojan riittävyyttä koskeviin väitteisiin.

B. Käytettävissä olevat korjaavat toimenpiteet

Välimiesmenettelyssä Privacy Shield -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. Välimiespaneelilla ei ole toimivaltuuksia määrätä muita korjaavia toimenpiteitä. Kun välimiespaneeli harkitsee, mitä korjaavia toimenpiteitä se määrää, sen on otettava huomioon muut korjaavat toimenpiteet, joita on jo määrätty muissa Privacy Shield -järjestelyn mekanismeissa. Vahingonkorvauksia, kustannusten korvauksia, palkkioita tai muita korjaavia toimenpiteitä ei voida määrätä. Molemmat osapuolet vastaavat itse asianajajiensa palkkioista.

C. Toimet, jotka on tehtävä ennen välimiesmenettelyä

Henkilön, joka on päättänyt turvautua välimiesmenettelyyn, on ennen menettelyn vireillepanoa 1) otettava väitetty järjestelyn periaatteiden rikkomus esille suoraan organisaation kanssa ja annettava organisaatiolle tilaisuus ratkaista asia aikataulussa, jota selostetaan järjestelyn periaatteiden III osan 11 kohdan d alakohdan i alakohdassa; 2) hyödynnettävä järjestelyn periaatteiden mukaista riippumatonta muutoksenhakumekanismia, josta ei aiheudu kuluja henkilölle; ja 3) otettava asia tietosuojaviranomaisen välityksellä esille kauppaministeriön kanssa ja annettava kauppaministeriölle tilaisuus ratkaista asia parhaansa mukaan aikataulussa, jota selostetaan kauppaministeriön kansainvälisen kaupan osaston kirjeessä. Tästä ei aiheudu kuluja henkilölle.

Välimiesmenettelyä ei voida käyttää, jos järjestelyn periaatteiden rikkomus, josta henkilö esittää väitteen, 1) on aiemmin ollut sitovan välimiesmenettelyn kohteena, 2) on ratkaistu tuomioistuimen lopullisella päätöksellä oikeudenkäynnissä, jonka asianosainen henkilö on ollut tai 3) on aiemmin ratkaistu osapuolten välisellä sopimuksella. Menettelyyn ei myöskään voida turvautua, jos 1) EU:n tietosuojaviranomainen on toimivaltainen järjestelyn periaatteiden III osan 5 tai 9 kohdan mukaisesti tai 2) EU:n tietosuojaviranomainen on toimivaltainen ratkaisemaan väitettyä rikkomusta 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 rikkomuksen nojalla hyvitystä toisella foorumilla. Jos ei-rahallinen kompensatio ei kuitenkaan täysin riitä korjaamaan väitettyä rikkomusta, henkilön turvautuminen välimiesmenettelyyn ei estä häntä esittämästä normaaliin tapaan vahingonkorvausvaadetta tuomioistuimessa.

⁽¹⁾ Privacy Shield -järjestelyn periaatteiden I.5 kohta.

E. Asian siirtäminen tuomioistuimeen ja täytäntöönpano

Henkilöt ja Privacy Shield -järjestelyyn osallistuvat organisaatiot voivat hakea muutosta välimiespaneelin päätökseen tuomioistuimelta sekä vaatia tuomioistuimessa päätöksen täytäntöönpanoa yhdysvaltalaisesta välimiesmenettelystä annetun liittovaltion lain (Federal Arbitration Act) nojalla ⁽¹⁾. Asia on pantava vireille liittovaltion piirituomioistuimessa, jonka alueelliseen toimivaltaan Privacy Shield -järjestelyyn osallistuvan organisaation ensisijainen liiketoimipaikka kuuluu.

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

F. Välimiespaneeli

Asianosaisten on valittava välimiehet luettelosta, jota käsitellään jäljempänä.

Yhdysvaltojen kauppaministeriö ja Euroopan komissio laativat sovellettavan lainsäädännön mukaisesti luettelon vähintään 20 välimiehestä, jotka valitaan riippumattomuuden, nuhteettomuuden ja asiantuntemuksen perusteella. Tässä yhteydessä sovelletaan seuraavaa:

Seuraavia sääntöjä sovelletaan välimiehiin:

- 1) Välimiehet ovat luettelossa kolmen vuoden ajan, jollei poikkeuksellisista olosuhteista tai perustellusta syystä muuta johdu, ja toimikautta voidaan yhden kerran jatkaa vielä kolmella vuodella.
- 2) Välimiehet eivät saa ottaa ohjeita menettelyn asianosaisilta, Privacy Shield -järjestelyyn osallistuvalla organisaatiolla, Yhdysvalloilta, EU:lta, EU:n jäsenvaltiolta, muulta viranomaiselta, valtiolliselta elimeltä tai lainvalvontaviranomaiselta, eivätkä he saa olla etu yhteydessä mainittuihin tahoihin.
- 3) Välimiehillä on oltava lupa lakimiehen ammatin harjoittamiseen Yhdysvalloissa, ja heidän on oltava Yhdysvaltojen yksityisyyden suojaa koskevan lainsäädännön asiantuntijoita, joilla on asiantuntemusta myös EU:n tietosuojalainsäädännöstä.

G. Välimiesmenettelyyn sovellettavat säännöt

Kuuden kuukauden kuluessa siitä kun tietosuojan riittävyttä koskeva päätös on annettu, kauppaministeriö ja Euroopan komissio sopivat sovellettavan lainsäädännön mukaisesti, että jokin olemassa oleva, vakiintunut yhdysvaltalainen välimiesmenettelysäännöstö (kuten AAA- tai JAMS-säännöstö) valitaan Privacy Shield -paneelin menettelytapasäännöiksi. 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 rikkomuksesta sekä henkilön valinnan mukaisesti todisteeksi esitettäviä asiakirjoja ja muuta todistusaineistoa ja/tai vaatimukseen sovellettavaa lakia koskevia näkemyksiä.

⁽¹⁾ 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. Sama §. 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, jolle se toteaa, 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 siitä johtuvat riidat, 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 §.

2. Laaditaan menettelyt sen varmistamiseksi, että yhteen rikkomukseen, josta henkilö esittää väitteitä, ei sovelleta kaksia 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 EU:n tietosuojaviranomainen voi EU:n kansalaisen pyynnöstä avustaa ilmoituksen valmistelussa. Tämä avustaminen voi liittyä vain ilmoitukseen, sillä EU:n 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 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, jolle toisin ole sovittu asianosaisten kesken.

H. Kustannukset

Välimiesten olisi kohtuullisin toimenpitein pyrittävä minimoimaan välimiesmenettelyyn liittyviä kustannuksia ja palkkioita.

Kauppaministeriö edistää sovellettavan lainsäädännön mukaisesti ja Euroopan komissiota kuultuaan sellaisen rahaston perustamista, johon Privacy Shield -järjestelyyn osallistuvien organisaatioiden on suoritettava vuotuinen maksu. Maksu perustuu osittain organisaation kokoon. Rahastosta katetaan välitysmenettelyjen kustannukset, muun muassa välimiesten palkkiot vahvistettavaan enimmäismäärään saakka. Rahastoa hallinnoi kolmas osapuoli, joka raportoi säännöllisesti rahaston toiminnasta. Kauppaministeriö ja Euroopan komissio arvioivat rahaston toimintaa vuotuisen tarkastelun yhteydessä. Tällöin arvioidaan esimerkiksi, onko tarvetta mukauttaa rahastoon tehtäviä maksuja ja välimiesten palkkioiden ylärajoja, ja tarkastellaan muun muassa välimiesmenettelyjen lukumäärää, kustannuksia ja kestoja. Kauppaministeriöllä ja Euroopan komissiolla on yhteisymmärrys siitä, että Privacy Shield -järjestelyyn osallistuville organisaatioille ei pidä asettaa liiallista taloudellista raskautta. Asianajajien palkkiot eivät kuulu tämän säännöksen soveltamisalaan, eikä niitä kateta tämän säännöksen nojalla perustetusta rahastosta.

LIITE II

YHDYSVALTOJEN KAUPPAMINISTERIÖN HYVÄKSYMÄT EU:N JA YHDYSVALTOJEN PRIVACY SHIELD -JÄRJESTELYN PERIAATTEET**I. YLEISKATSAUS**

1. Vaikka Yhdysvallat ja Euroopan unioni ovat yhtä mieltä tavoitteesta, jonka mukaan yksityisyyden suoja on vahvistettava, Yhdysvaltojen lähestymistapa yksityisyyteen on erilainen kuin Euroopan unionin. Yhdysvalloissa käytetään alakohtaista lähestymistapaa, jossa yhdistyvät lainsäädäntö, sääntely ja itsesääntely. Kun kyseiset erot otetaan huomioon ja jotta Yhdysvalloissa toimivien organisaatioiden käyttöön saadaan luotettava mekanismi, jolla voidaan siirtää henkilötietoja Euroopan unionista Yhdysvaltoihin, ja jotta EU:n rekisteröidyt samalla edelleenkin hyötyvät tehokkaista turvakeista ja suojaustoimista, joihin heillä EU:n lainsäädännön mukaan on oikeus silloin kun heidän EU:n ulkopuolisiin maihin siirrettyjä henkilötietojaan käsitellään, kauppaministeriö vahvistaa nämä Privacy Shield -periaatteet, jotka sisältävät myös täydentävät periaatteet (yhdessä 'järjestelyn periaatteet'). Ministeriö hyväksyy periaatteet sen toimivallan nojalla, joka sille laissa on annettu kansainvälisen kaupan kasvattamista, edistämistä ja kehittämistä varten (ks. Yhdysvaltojen lakikodifikaation kaupankäyntiä koskevassa 15 osastossa oleva kauppaministeriön toimivaltaa ja tehtäviä koskeva 1512 § – 15 U.S.C. § 1512). Järjestelyn periaatteet on laadittu yhdessä Euroopan komission sekä elinkeinoelämän ja muiden sidosryhmien kanssa Yhdysvaltojen ja Euroopan unionin välisen kaupankäynnin helpottamiseksi. Ne on tarkoitettu yksinomaan sellaisten yhdysvaltalaisen organisaatioiden käyttöön, jotka saavat henkilötietoja Euroopan unionista ja jotka noudattavat järjestelyn periaatteita täyttääkseen Privacy Shield -järjestelyn osallistumiselle asetetut vaatimukset ja siten hyötyäkseen Euroopan komission tietosuojan riittävyyttä koskevasta päätöksestä⁽¹⁾. Järjestelyn periaatteilla ei ole vaikutusta sellaisten kansallisten säädösten soveltamiseen, jotka on annettu direktiivin 95/46/EY, jäljempänä 'direktiivi', täytäntöönpanemiseksi ja joita sovelletaan henkilötietojen käsittelyyn jäsenvaltioissa. Järjestelyn periaatteilla ei myöskään rajoiteta yksityisyyttä koskevia velvoitteita, joita muutoin sovelletaan Yhdysvaltojen lainsäädännön mukaisesti.
2. Jotta organisaatio voi tukeutua Privacy Shield -järjestelyyn tehdessään henkilötietojen siirtoja EU:sta, sen on annettava oma varmennus kauppaministeriölle (tai kauppaministeriön nimeämälle taholle). Vaikka organisaatiot näin ollen liittyvät Privacy Shield -järjestelyyn täysin vapaaehtoisesti, järjestelyn periaatteiden noudattaminen on pakollista: organisaatioiden, jotka antavat oman varmennuksen kauppaministeriölle ja julkisesti ilmoittavat sitoutuvansa noudattamaan järjestelyn periaatteita, on noudatettava periaatteita täysimääräisesti. Jotta organisaatio voi liittyä Privacy Shield -järjestelyyn, sen on täytettävä seuraavat vaatimukset: a) sen on oltava liittovaltion kaupakomission, 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; d) sekä pantava ne täysimääräisesti täytäntöön. Jos organisaatio rikkoo järjestelyn periaatteita, siihen voidaan kohdistaa lainvalvontatoimia liittovaltion kaupakomissiosta annetun lain (Federal Trade Commission Act) 5 §:n nojalla (15 U.S.C. § 45(a)). Säännöksessä kielletään kaupankäynnissä toteutettavat tai kaupankäyntiin vaikuttavat sopimattomat ja vilpilliset toimet. Lainvalvontatoimiin voidaan ryhtyä myös muiden sellaisten lakien tai säädösten nojalla, joissa kielletään tuollaiset toimet.
3. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa, jäljempänä 'Privacy Shield -luettelo', yhdysvaltalaisista organisaatioista, jotka ovat toimittaneet oman varmennuksensa kauppaministeriölle ja vahvistaneet sitoumuksensa järjestelyn periaatteiden noudattamisesta. Organisaatio voi hyödyntää Privacy Shield -järjestelyn etuja siitä päivästä lähtien, jona kauppaministeriö merkitsee organisaation Privacy Shield -luetteloon. Kauppaministeriö poistaa organisaation Privacy Shield -luettelosta, jos organisaatio vetäytyy Privacy Shield -järjestelystä vapaaehtoisesti tai jos se jättää toimittamatta kauppaministeriölle vuotuisen uudelleenvarmennuksensa. Kun organisaatio poistetaan Privacy Shield -luettelosta, se ei voi enää hyödyntää Euroopan komission tietosuojan riittävyyttä koskevaa päätöstä saadakseen henkilötietoja EU:sta. Organisaation on jatkettava järjestelyn periaatteiden soveltamista henkilötietoihin, jotka se on saanut sinä aikana, kun se on osallistunut Privacy Shield -järjestelyyn, ja sen on annettava kauppaministeriölle tästä sitoumus vuosittain niin kauan kuin se säilyttää kyseisiä tietoja. Muussa tapauksessa sen on palautettava tai hävitettävä tiedot tai tarjottava suoja tiedoille jollakin toisella hyväksyttävällä keinolla. Kauppaministeriö poistaa Privacy Shield -luettelosta myös organisaatiot, jotka ovat jatkuvasti jättäneet noudattamatta järjestelyn periaatteita. Näillä organisaatioilla ei ole oikeutta hyödyntää Privacy Shield -järjestelyn etuja, ja niiden on palautettava tai hävitettävä henkilötiedot, jotka ne saivat Privacy Shield -järjestelyssä.
4. Kauppaministeriö pitää yllä ja yleisön saatavilla virallista luetteloa myös sellaisista yhdysvaltalaisista organisaatioista, jotka ovat aiemmin antaneet oman varmennuksensa kauppaministeriölle mutta jotka on sittemmin poistettu Privacy Shield -luettelosta. Kauppaministeriö esittää näiden organisaatioiden osalta selkeän varoitustekstin seuraavista seikoista: nämä organisaatiot eivät osallistu Privacy Shield -järjestelyyn; Privacy Shield -luettelosta poistaminen merkitsee, että kyseiset organisaatiot eivät voi väittää noudattavansa Privacy Shield -periaatteita ja että niiden on

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

vältettävä kaikkia lausuntoja tai harhaanjohtavia käytäntöjä, joista voisi ymmärtää, että ne osallistuvat Privacy Shield -järjestelyyn; tällaisilla organisaatioilla ei ole enää oikeutta hyödyntää Euroopan komission tietosuojan riittävyyttä koskevaa päätöstä, jonka avulla nämä järjestöt voisivat saada henkilötietoja EU:sta. Liittovaltion kauppakomissio, liikenneministeriö tai jokin muu lainvalvontaviranomainen voi kohdistaa lainvalvontatoimenpiteitä organisaatioon, joka jatkaa väitteitään osallistumisestaan Privacy Shield -järjestelyyn tai antaa joitain muita järjestelyyn liittyviä vääriä tietoja sen jälkeen kun organisaatio on poistettu Privacy Shield -luettelosta.

5. Järjestelyn periaatteiden noudattamista voidaan rajoittaa seuraavasti: a) siinä määrin kuin on tarpeellista kansallisen turvallisuuden, julkisen edun tai lainvalvonnan vaatimusten vuoksi; b) lailla, hallituksen antamalla asetuksella tai tuomioistuimen päätöksellä, jonka seurauksena syntyy ristiriitaisia velvoitteita tai jossa annetaan nimenomainen lupa tiettyyn toimintaan, jos organisaatio voi tällaista lupaa käyttäessään osoittaa, että organisaatio poikkeaa järjestelyn periaatteista vain siinä määrin kuin on tarpeellista, jotta lupaan liittyvä ensisijainen ja perusteltu intressi voi toteutua; tai c) jos direktiivissä tai jäsenvaltion lainsäädännössä sallitaan poikkeus ja tällaisia poikkeuksia sovelletaan vertailukelpoisissa olosuhteissa. Järjestelyn periaatteiden tavoitteena on parantaa yksityisyyden suojaa. Organisaatioiden tulisi toimia tämän tavoitteen kanssa yhdenmukaisesti ja pyrkiä panemaan nämä periaatteet täytäntöön täysimääräisesti ja läpinäkyvästi. Niiden tulisi muun muassa selostaa tietosuojaperiaatteissaan, jos periaatteista poiketaan säännönmukaisesti 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 siitä syystä että tavoitteena on parantaa yksityisyyden suojaa – valitsevan mahdollisuuksien mukaan korkeatasoisemman suojan.
6. Organisaatioiden on sovellettava järjestelyn periaatteita kaikkiin Privacy Shield -järjestelyä hyödyntäen siirrettyihin henkilötietoihin sen jälkeen kun organisaatiot ovat liittyneet Privacy Shield -järjestelyyn. Jos organisaatio on päättänyt hyödyntää Privacy Shield -järjestelyn 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.
7. Yhdysvaltojen lainsäädäntöä sovelletaan kysymyksiin, jotka liittyvät Privacy Shield -järjestelyn periaatteiden ja järjestelyyn kuuluvien organisaatioiden tietosuojaperiaatteiden tulkintaan ja noudattamiseen. Poikkeuksena ovat organisaatiot, jotka ovat sitoutuneet yhteistyöhön Euroopan tietosuojaviranomaisten kanssa. Ellei toisin mainita, sovelletaan kaikkia periaatteisiin kuuluvia asianmukaisia sääntöjä.
8. Määritelmät:
 - a. 'Henkilötiedoilla' tarkoitetaan jossakin muodossa rekisteröityjä tunnistetun tai tunnistettavan henkilön tietoja, joihin sovelletaan direktiiviä 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 periaatteet tulevat voimaan päivänä, jona Euroopan komissio on antanut lopullisen päätöksensä tietosuojan riittävyydestä.

II. JÄRJESTELYN PERIAATTEET

1. Ilmoitusperiaate

- a. Organisaation on ilmoitettava henkilöille
 - i. osallistumisestaan Privacy Shield -järjestelyyn ja annettava heille linkki Privacy Shield -luetteloon tai kyseisen luettelon verkko-osoite,
 - ii. siitä, minkä tyyppisiä henkilötietoja on kerätty, sekä tarvittaessa organisaatioon kuuluvista yksiköistä tai tytäryhtiöistä, jotka myös noudattavat järjestelyn periaatteita,

- iii. sitoumuksestaan soveltaa järjestelyn periaatteita kaikkiin henkilötietoihin, jotka organisaatio saa EU:sta Privacy Shield -järjestelyä hyödyntäen,
 - iv. tarkoituksista, joihin se kerää ja käyttää henkilötietoja,
 - v. siitä, mitkä ovat 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. siitä, minkä tyyppisille kolmansille osapuolille se luovuttaa henkilötietoja ja keitä nämä kolmannet osapuolet ovat, sekä tarkoituksesta, jonka vuoksi se luovuttaa tietoja niille,
 - vii. heidän oikeudestaan tutustua henkilötietoihinsa,
 - viii. valinnanmahdollisuuksista ja välineistä, jotka organisaatio tarjoaa henkilöille sitä tarkoitusta varten, että 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 välimiesmenettelyn käsiteltäväksi,
 - xii. vaatimuksesta, jonka mukaan henkilötietoja on luovutettava lainmukaisen, julkisen viranomaisen esittämän pyynnön nojalla muun muassa kansalliseen turvallisuuteen tai lainvalvontaan liittyvien vaatimusten täyttämiseksi, ja
 - xiii. organisaation vastuusta tapauksissa, joissa tietoja on siirretty edelleen kolmansille osapuolille.
- b. Yllämainittu ilmoitus on annettava siten, että käytetty kieli on selkeää ja että ilmoitus on 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 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 sittemmin antaneet suostumuksensa. Henkilöille on tarjottava valinnanvapauden käyttämistä varten mekanismeja, joka 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 tiettyä tehtävää (tai tehtäviä) organisaation puolesta ja sen ohjeiden mukaisesti. Organisaation on kuitenkin aina tehtävä sopimus edustajan kanssa.
- c. Arkaluonteisten tietojen osalta (esim. henkilötiedot, jotka koskevat henkilön terveydentilaa, rotua tai etnistä alkuperää, poliittista kantaa, uskonnollista tai eettistä vakaumusta, kuulumista ammattiliittoon tai sukupuolielämää) henkilöiden on annettava organisaatiolle myönteinen ja 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 sittemmin 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. Organisaation on myös tehtävä sopimus rekisterinpitäjänä toimivan kolmannen osapuolen kanssa. 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 tietosuoja, jonka taso vastaa Privacy Shield -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 tietosuoja kuin Privacy Shield -järjestelyn periaatteet edellyttävät; iii) sen on varmistettava kohtuullisin ja asianmukaisin toimin, että edustaja käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa Privacy Shield -periaatteiden mukaisia organisaation velvoitteita; iv) sen on vaadittava edustajaa ilmoittamaan organisaatiolle, jos edustaja toteaa, ettei se enää kykene tarjoamaan tietosuojaa, joka vastaa Privacy Shield -periaatteita; v) havaitessaan luvaton tiedonkäsittelyä, mukaan lukien iv kohdassa mainittu tilanne, sen on ryhdyttävä kohtuullisiin ja asianmukaisiin toimiin kyseisen tiedonkäsittelyn lopettamiseksi ja tilanteen korjaamiseksi; ja vi) sen on pyynnöstä annettava kauppaministeriölle yhteenvedo 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⁽¹⁾. Tapa, jolla organisaatio käsittelee henkilötietoja, ei saa olla yhteensopimaton sen käyttötarkoituksen kanssa, johon tiedot on kerätty tai johon henkilö on sittemmin 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 selvitettävissä⁽²⁾, ainoastaan niin kauan kuin se on tarpeen tietojenkäsittelyn 5a 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 järjestelyn muita periaatteita ja määräyksiä. Organisaatioiden olisi toteutettava kohtuulliset ja asianmukaiset toimenpiteet tämän säännöksen noudattamiseksi.

6. Tietoihin pääsyä koskeva periaate

- a. Henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja 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 verrattuna henkilön tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa tai jos muun kuin kyseisen henkilön oikeuksia loukattaisiin.

⁽¹⁾ 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 kohtuullinen henkilö voi odottaa tiedon keruulta ko. tilanteessa.

⁽²⁾ 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 tunnistamisen viemä aika ja kustannus ja tietojenkäsittelyhetkellä käytettävissä oleva teknologia), tällöin henkilöllisyys on tässä yhteydessä "selvitettävissä".

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 vähintään kuuluttava seuraavaa:
- helposti käytettävissä olevat riippumattomat muutoksenhakumekanismit, joissa jokaisen henkilön valitukset ja häntä koskevat riidat tutkitaan ja ratkaistaan järjestelyn periaatteita noudattaen ripeästi ilman, että henkilölle aiheutuu kuluja, ja joissa määrätään maksettavaksi vahingonkorvauksia, jos tästä on säädetty sovellettavassa laissa tai yksityissektorin luomissa normeissa;
 - 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
 - organisaatioille asetettava velvollisuus korjata puutteet, jotka johtuvat siitä, että ne eivät ole noudattaneet järjestelyn periaatteita, vaikka ovat ilmoittaneet noudattavansa niitä, 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 järjestelyä koskeviin kauppaministeriön tiedusteluihin ja tietopyyntöihin. 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 valitusten käsittelyä ja niihin annettavia ratkaisuja.
- 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 lähetetään edelleen, Privacy Shield -järjestelyyn osallistuva organisaatio on vastuussa sellaisten henkilötietojen käsittelystä, jotka se on vastaanottanut Privacy Shield -järjestelyssä ja sittemmin siirtänyt sen edustajana toimivalle kolmannelle osapuolelle. Privacy Shield -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 organisaatiolla annetaan sääntöjen rikkomukseen perustuva tuomioistuimen tai liittovaltion kauppakomission määräys, organisaation on julkistettava luottamuksellisuusvaatimusten rajoissa kaikki Privacy Shield -järjestelyä koskevat osat sellaisista sääntöjen noudattamista koskevista kertomuksista tai arviointikertomuksista, jotka on toimitettu liittovaltion kauppakomissiolle. Kauppaministeriö on perustanut tietosuojaviranomaisille erityisen yhteyspisteen. Tietosuojaviranomaiset voivat sen kautta tuoda esiin Privacy Shield -järjestelyyn osallistuviin organisaatioihin liittyviä ongelmia, jotka koskevat järjestelyn periaatteiden noudattamista. Liittovaltion kauppakomissio asettaa etusijalle sellaiset järjestelyn periaatteiden noudattamatta jättämisestä koskevat asiat, jotka kauppaministeriö ja EU:n jäsenvaltioiden viranomaiset ovat siirtäneet sen käsiteltäväksi. Liittovaltion kauppakomissio antaa 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 tietojen käsittely
- on rekisteröidyn tai muun henkilön elintärkeiden etujen mukaista;
 - on tarpeen oikeudellisen vaatimuksen laitimiseksi tai siihen vastaamiseksi;
 - on tarpeen lääketieteellisen hoidon antamiseksi tai diagnoosin tekemiseksi;
 - 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, ja vapautus, joka direktiivissä annetaan journalistiselle materiaalille, 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 yhdysvaltalaisien henkilöiden ja organisaatioiden toimien osalta.
- b. Privacy Shield -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 Privacy Shield -järjestelyn periaatteiden mukaan vastuussa, jos ne toisen organisaation puolesta pelkästään siirtävät, reitittävät, välittävät tai varastoivat tietoja. Privacy Shield -järjestelyn periaatteissa ei luoda toissijaista vastuuta. Tämä vastaa direktiivin sääntelyä. 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 tiedonsaantiperiaatteen mukaisesti.
- b. Julkisissa osakeyhtiöissä ja harvainyhtiöissä, myös Privacy Shield -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 Privacy Shield -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 lakisääteisten tai yleisen edun mukaisten vaatimusten täyttämiseksi, sekä lisäksi olosuhteissa, joissa Privacy Shield -järjestelyn periaatteiden soveltaminen vaikuttaisi haitallisesti organisaation oikeutettuihin etuihin. Oikeutettuja etuja ovat muun muassa sen valvominen, että organisaatiot noudattavat lainmukaisia velvoitteita ja että niiden tilinpäätökset on laadittu sääntöjen mukaisesti, samoin kuin luottamussellisuus, 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 Euroopan unionin tietosuojaviranomaisten kanssa, jäljempänä kuvatulla tavalla. EU:sta henkilötietoja vastaanottavien yhdysvaltalaisien organisaatioiden on Privacy Shield -järjestelyssä 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 kauppatieteiden ministeriölle osoittamassaan Privacy Shield -järjestelyn 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 Privacy Shield -järjestelyssä tehtyjä valituksia ja
 - iii. noudattaa kaikkia tietosuojaviranomaisten antamia ohjeita, joissa todetaan, että organisaation on Privacy Shield -järjestelyn periaatteiden noudattamiseksi toteutettava erityistoimia. Näihin kuuluvat korjaavat toimet ja korvaukset niiden henkilöiden hyväksi, joihin periaatteiden noudattamatta jättäminen on vaikuttanut. Organisaatio myös antaa tietosuojaviranomaisille kirjallisen vahvistuksen kyseisten toimien toteuttamisesta.
- c. Tietosuojaviranomaisten paneelin toiminta
- i. Tiedotuksesta ja neuvonnasta muodostuva tietosuojaviranomaisten yhteistyö järjestetään seuraavasti:
 1. Neuvonnasta vastaa Euroopan unionin tasolla perustettava epävirallinen tietosuojaviranomaisten paneeli, joka muun muassa auttaa yhtenäisen ja johdonmukaisen lähestymistavan varmistamisessa.
 2. Paneeli antaa yhdysvaltalaisille organisaatioille lausuntonsa yksityishenkilöiden tekemistä, ratkaistavina olevista valituksista, jotka koskevat EU:sta Privacy Shield -järjestelyn mukaisesti siirrettyjen henkilötietojen käsittelyä. Näillä ohjeilla on tarkoitus varmistaa, että Privacy Shield -järjestelyn periaatteita sovelletaan asianmukaisesti. Ohjeissa selostetaan myös asianosaisten (asianosaisten) hyväksi tehtävät korjaavat toimet, joita tietosuojaviranomaiset pitävät asianmukaisina.
 3. Paneeli antaa lausuntonsa tapauksista, joita organisaatiot ovat siirtäneet sen käsiteltäväksi, ja/tai valituksista, jotka koskevat tietosuojaviranomaisten kanssa Privacy Shield -järjestelyssä 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 lausuntonsa 60 päivän kuluessa valituksen tai sille siirretyn tapauksen vastaanottamisesta ja mahdollisuuksien mukaan lyhyemmässä ajassa.
 5. Paneeli julkistaa vastaanottamiensa valitusten käsittelyn tulokset, jos katsoo 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 ohjeiden 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 koskevista asioista, tai että se pitää yhteistyösopimusta vakavan sopimusrikkomuksen vuoksi mitättömänä. Jälkimmäisessä tapauksessa paneeli ilmoittaa mitättömyydestä kauppatieteiden ministeriölle, jotta Privacy Shield -luetteloa voidaan muuttaa tarvittavalla tavalla. Jos sitoumusta tietosuojaviranomaisten kanssa tehtävästä yhteistyöstä tai Privacy Shield -järjestelyn periaatteita ei noudateta, liittovaltion kauppakomissiosta annetun lain 5 §:n tai muun vastaavan lain säännöksen nojalla voidaan nostaa vilpillistä menettelyä koskeva kanne.
- d. Jos organisaatio haluaa, että sen Privacy Shield -järjestelyyn 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, ja organisaatioilta voidaan tämän lisäksi veloittaa tarpeelliset käännöskulut, joita aiheutuu, kun paneeli käsittelee sille siirrettyjä asioita ja organisaatiota vastaan tehtyjä valituksia. Vuosimaksu on enintään 500 Yhdysvaltojen dollaria, ja se on pienempi pienemmille yrityksille.

6. Oma varmennus

- a. Organisaatio voi alkaa hyödyntää Privacy Shield -järjestelyyn liittyviä etuja siitä päivästä lähtien, jona kauppaministeriö on – todettuaan että organisaation oma varmennus on täydellinen – merkinnyt oman varmennuksen Privacy Shield -luetteloon.
- b. Tehdäkseen oman varmennuksensa Privacy Shield -järjestelyssä organisaation on toimitettava kauppaministeriölle tätä koskeva asiakirja, jonka on allekirjoittanut järjestelyyn liittyvää organisaatiota edustava toimihenkilö ja joka sisältää vähintään seuraavat tiedot:
- organisaation nimi, postiosoite, sähköpostiosoite sekä puhelin- ja faksinumerot,
 - kuvaus organisaation toiminnoista, jotka liittyvät EU:sta saataviin henkilötietoihin ja
 - kuvaus tällaisia henkilötietoja koskevista organisaation tietosuojaperiaatteista. Kuvauksessa annetaan muun muassa seuraavat tiedot:
 - 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,
 - milloin tietosuojaperiaatteet on pantu täytäntöön,
 - mikä on yhteysosoite asioissa, jotka koskevat valitusten käsittelyä, tietoihin tutustumista koskevia pyyntöjä sekä kaikkia muita Privacy Shield -järjestelyyn liittyviä kysymyksiä,
 - millä erityisellä lakisääteisellä elimellä (joka on lueteltu 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 rikkomuksia,
 - kaikkien sellaisten yksityisyydensuojaohjelmien nimet, joihin organisaatio osallistuu,
 - millä menetelmällä tarkastetaan, että järjestelyn periaatteiden noudattaminen on varmistettu (esimerkiksi tarkastus yrityksen sisällä, kolmannen osapuolen tekemä tarkastus; ks. tarkastamista koskeva täydentävä periaate) ja
 - riippumaton muutoksenhakumekanismi, jota voidaan käyttää ratkaisematta olevien valitusten tutkimiseen.
- c. Jos organisaatio haluaa, että sen Privacy Shield -järjestelyyn liittyvät edut kattavat myös henkilöstötiedot, jotka on siirretty EU:sta käytettäväksi työsuhteiden yhteydessä, tämä on mahdollista, jos lakisääteisellä elimellä, joka on lueteltu järjestelyn periaatteissa tai niiden tulevassa liitteessä, on toimivalta käsitellä organisaatiota vastaan esitetyt vaateet, jotka koskevat henkilöstötietojen käsittelyä. Lisäksi organisaation on todettava tämä omassa varmennuksessaan ja ilmoitettava, että se sitoutuu tekemään yhteistyötä EU:n toimivaltais(t)en viranomais(t)en 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.
- d. Kauppaministeriö pitää yllä Privacy Shield -luetteloa organisaatioista, jotka ovat toimittaneet täydellisen oman varmennuksen ja jotka niin ollen saavat hyödykseen Privacy Shield -järjestelyn edut. Kauppaministeriö päivittää listaa vuosittain annettavilla uudelleenvarmennuksilla sekä ilmoituksilla, jotka on saatu riitojenratkaisua ja täytäntöönpanoa koskevien täydentävien periaatteiden mukaisesti. Oma varmennus on annettava uudelleen vähintään kerran vuodessa. Jos organisaatio ei uusi omaa varmennustaan, se poistetaan Privacy Shield -luettelosta eikä sille enää myönnetä järjestelyn etuja. Sekä Privacy Shield -luettelo että organisaatioiden omat varmennukset julkistetaan. Kaikkien organisaatioiden, jotka kauppaministeriö on merkinnyt Privacy Shield -luetteloon, on mainittava myös julkaistuissa tietosuojaperiaatteissaan, että ne noudattavat Privacy Shield

-järjestelyn periaatteita. Jos organisaation tietosuojaperiaatteet ovat saatavilla verkossa, niissä on oltava linkki kauppaministeriön Privacy Shield -verkkosivustolle sekä linkki sellaisen riippumattoman muutoksenhakumekanismin verkkosivustoon tai valituslomakkeeseen, joka voi tutkia ratkaisematta olevat valitukset.

- e. Yksityisyyden suojaa koskevia periaatteita sovelletaan välittömästi varmennuksen jälkeen. Privacy Shield -järjestelyn periaatteet vaikuttavat liikesuhteisiin, joita organisaatioilla on kolmansien osapuolten kanssa. Organisaatiot, jotka antavat oman varmennuksensa Privacy Shield -järjestelyssä kahden ensimmäisen kuukauden kuluessa järjestelyn voimaantulopäivästä, saattavat olemassa olevat liikesuhteensa kolmansien osapuolten kanssa niin pian kuin mahdollista tietojen edelleen siirtämiseen liittyvää vastuuvastuuta koskevan periaatteen mukaisiksi. Tämä toimenpide on joka tapauksessa tehtävä yhdeksän kuukauden kuluessa päivästä, jona organisaatio antoi varmennuksensa Privacy Shield -järjestelyyn. Kun organisaatiot kyseisen siirtymäkauden aikana siirtävät tietoja kolmannelle osapuolelle, niiden on i) sovellettava ilmoitus- ja valintaperiaatteita ja ii) jos henkilötietoja siirretään edustajana toimivalle kolmannelle osapuolelle, niiden on varmistettava, että edustajalla on velvollisuus järjestää vähintään Privacy Shield -järjestelyn periaatteiden mukainen tietosuoja.
- f. Organisaation on sovellettava Privacy Shield -järjestelyn periaatteita kaikkiin henkilötietoihin, jotka organisaatio saa EU:sta järjestelyä hyödyntäen. Sitoutumista Privacy Shield -järjestelyn periaatteiden noudattamiseen ei rajoiteta ajallisesti niiden henkilötietojen osalta, jotka organisaatio on saanut ollessaan oikeutettu Privacy Shield -järjestelyn etuihin. Sitoutuminen merkitsee sitä, että organisaatio soveltaa järjestelyn periaatteita tällaisiin tietoihin niin kauan kuin organisaatio tallentaa, käyttää tai luovuttaa tietoja, vaikka se olisi myöhemmin mistä tahansa syystä jättäytynyt Privacy Shield -järjestelyn ulkopuolelle. Organisaation, joka vetäytyy Privacy Shield -järjestelystä mutta joka haluaa säilyttää tällaiset tiedot, on vahvistettava kauppaministeriölle vuosittain sitoumuksensa, jonka mukaan se jatkaa periaatteiden soveltamista tietoihin tai antaa tiedoille "riittävän" suojan muiden hyväksytyjen keinojen avulla (esimerkiksi käyttämällä sopimusta, joka vastaa täysin Euroopan komission hyväksymissä vakiosopimuslausekkeissa olevia ehtoja). Muussa tapauksessa sen on palautettava tai hävitettävä tiedot. Organisaation, joka vetäytyy Privacy Shield -järjestelystä, on poistettava kaikista tietosuojaperiaatteistaan kaikki Privacy Shield -järjestelyä koskevat viittaukset, joista voisi päätellä, että organisaatio osallistuisi edelleen aktiivisesti Privacy Shield -järjestelyyn ja että se olisi oikeutettu järjestelyn etuihin.
- g. Organisaation, joka lakkaa olemasta erillinen oikeussubjekti sulautumisen tai yritystoston seurauksena, on ilmoitettava tästä kauppaministeriölle etukäteen. Ilmoitukseen on sisällyttävä tieto myös siitä, onko organisaation haltuun ottava yksikkö tai sulautumisessa muodostuva yksikkö i) yritystoston tai sulautumiseen sovellettavan lain nojalla ilman eri toimenpiteitä edelleen sidoksissa Privacy Shield -järjestelyn periaatteisiin vai ii) haluaako se antaa oman varmennuksensa Privacy Shield -järjestelyn periaatteiden noudattamisesta tai toteuttaa muita suojaustoimenpiteitä, kuten solmia kirjallisen sopimuksen, jossa taataan Privacy Shield -järjestelyn periaatteiden noudattaminen. Siinä tapauksessa, että kumpikaan vaihtoehtoista i) tai ii) ei sovellu, kaikki Privacy Shield -järjestelyn kautta saadut tiedot on viipymättä hävitettävä.
- h. Kun organisaatio vetäytyy Privacy Shield -järjestelystä, sen on – olipa syy mikä tahansa – poistettava kaikki maininnat, joista voisi päätellä, että organisaatio osallistuu edelleen Privacy Shield -järjestelyyn tai että se on oikeutettu järjestelyn etuihin. Jos EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn varmennusmerkki on käytössä, myös se on poistettava. Jos organisaatio antaa yleisölle vääriä tietoja Privacy Shield -järjestelyn periaatteiden noudattamisesta, liittovaltion kauppakomissio 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 Privacy Shield -järjestelyn 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. Itsearviointimenetelmällä tehdyn tarkastuksen tuloksena on voitava todeta, että organisaation julkistetut tietosuojaperiaatteet, jotka koskevat EU:sta saatuja henkilötietoja, ovat täsmällisiä, kattavia, näkyvällä paikalla olevia, täysimääräisesti täytäntöönpanettavia ja helposti tutustuttavissa olevia. Tarkastuksessa on myös todettava seuraavat seikat: organisaation tietosuojaperiaatteet ovat Privacy Shield -järjestelyn periaatteiden mukaisia; henkilöille annetaan tieto kaikista yrityksen sisäisistä valitusten käsittelymekanismeista ja riippumattomista mekanismeista, joille henkilöt voivat tehdä valituksia; organisaatio on ottanut käyttöön menettelyt, joiden avulla työntekijöitä koulutetaan panemaan tietosuojaperiaatteet täytäntöön 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, joka todentaa itsearviointin. 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, arvioinnin tuloksista on käytävä ilmi, että EU:n alueelta saatuja henkilötietoja koskevat tietosuojaperiaatteet ovat Privacy Shield -järjestelyn periaatteiden mukaisia, että tietosuojaperiaatteita noudatetaan ja että henkilöille kerrotaan valitusmenettelyistä. Arvioinnissa voidaan hyödyntää tarpeen mukaan muun muassa tarkastusta, satunnaisotantaan perustuvia tarkistuksia, "houkutuslintuja" tai teknisiä apuvälineitä. Arvioinnin tekijän tai organisaation toimihenkilön tai muun valtuutetun edustajan on vähintään kerran vuodessa allekirjoitettava lausunto, joka todentaa, että ulkopuolisen tekemä periaatteiden noudattamista koskeva arviointi on saatettu menestyksellisesti loppuun. Lausunnon on pyynnöstä oltava henkilöiden saatavilla, tai sen on oltava käytettävissä periaatteiden noudattamista koskevan tutkinnan tai valitusmenettelyn yhteydessä.
- e. Organisaatioiden on dokumentoitava Privacy Shield -järjestelyn 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. Privacy Shield -järjestelyn periaatteiden mukaan tiedonsaanti on keskeistä yksityisyyden suojassa. Henkilö voi sen perusteella erityisesti tarkistaa häntä itseään koskevan tiedon paikkansapitävyyden. Tiedonsaantiperiaatteella tarkoitetaan, että yksilöillä on oikeus
1. saada organisaatiolta vahvistus siitä, käsittelee se heitä koskevia henkilötietoja (⁽¹⁾);
 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 halutaan. 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 kanssa henkilö on ollut tekemisissä tai minkä luonteista tietoa pyyntö koskee tai mikä on tiedon käyttötarkoitus.
- iii. Tiedonsaantiperiaatteen perimmäisen luonteen mukaisesti organisaatioiden olisi aina vilpittömästi pyrittävä antamaan tiedot. Jos esimerkiksi tietyt tiedot on suojattava ja ne voidaan helposti erottaa muista pyynnön koskemista henkilötiedoista, organisaation on erotettava suojattu tieto ja annettava muu tieto henkilön saataville. Jos organisaatio päättää, että pääsyä tietoihin on jossain tapauksessa rajoitettava, päätös on perusteltava tietoja pyytävälle henkilölle ja tälle on ilmoitettava, mistä tai keneltä saa asiasta lisätietoja.

b. Tiedonsaannista 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 verrattuna henkilön tietosuojaan kohdistuviin riskeihin kyseisessä tapauksessa. Kustannukset ja tietojen antamisesta aiheutuvat rasitteet ovat tärkeitä tekijöitä, ja ne olisi otettava huomioon, mutta niiden perusteella ei päätetä, onko tiedon antaminen kohtuullista.

(¹) Organisaation olisi vastattava henkilön kysymyksiin, jotka koskevat tiedonkäsittelyn tarkoitusta, käsiteltyjen henkilötietojen luokkia sekä henkilötietojen vastaanottajia tai vastaanottajien luokkia.

- ii. Jos henkilötietoa esimerkiksi käytetään yksityishenkilöä koskevan tärkeän päätöksen tekemiseen (esimerkiksi jos myönnetään tai päätetään olla myöntämättä jotain merkittävää, kuten vakuutus, laina tai työpaikka), organisaation on annettava tiedot, vaikka tietojen hankkiminen olisi suhteellisen vaikeaa tai kallista. Tämä on myös muiden näissä täydentävissä periaatteissa olevien sääntöjen mukaista. Vaikka pyydytetyt henkilötiedot eivät olisi arkaluonteisia ja vaikka niiden perusteella ei tehtäisi päätöksiä, joilla on merkittävä vaikutus henkilöön, mutta tiedot ovat helposti saatavilla ja niiden toimittaminen halpaa, organisaation on myönnettävä pääsy näihin tietoihin.

c. Luottamukselliset kaupalliset tiedot

- i. Luottamuksellinen kaupallinen tieto on organisaation suojelemaa tietoa, jonka julkaiseminen auttaisi 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.
- 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 mahdollisten syiden, joiden vuoksi pääsy voidaan rajoittaa, on oltava erityisiä. Organisaatio voi – kuten myös direktiivissä säädetään – kieltäytyä luovuttamasta tietoja, jos tietojen luovuttaminen todennäköisesti vaarantaa 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 se haittaa 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 tai työntekijän tekemän valituksen käsittelyä tai työntekijän seuraajan valintaa koskevaa suunnittelua ja yritysten uudelleenorganisointia tai
 - 5. tietojen luovuttaminen haittaa luottamuksellisuutta, 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. Henkilöille on esitettävä syyt, joiden perusteella pääsy tietoihin rajoitetaan, ja mainittava yhteyspiste, jossa voi esittää lisäkysymyksiä.

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 nähtäväkseen henkilötietonsa. Organisaatio voi periä maksun, joka ei saa olla liiallinen.
- ii. Maksun periminen saattaa olla perusteltua esimerkiksi silloin, kun tietopyynnöt ovat ilmeisen kohtuuttomia erityisesti toistuvuutensa takia.
- iii. Tiedonsaantia ei voida estää kustannussyihin vetoamalla, jos rekisteröity tarjoutuu maksamaan kustannukset.

g. Toistuvat tai tarpeettomat tietopyynnot

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 tietopyynnot

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

i. Vastaamisaika

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

9. Henkilöstötiedot

a. Privacy Shield -järjestelyn kattavuus

- i. Kun EU:ssa toimiva organisaatio siirtää (entistä tai nykyistä) henkilöstöään koskevia, työsuhteen yhteydessä kerättyjä henkilötietoja emoyhtiölle tai organisaatioon sidoksissa olevalle yhtiölle tai riippumattomalle palvelujen tarjoajalle, joka sijaitsee Yhdysvalloissa ja joka osallistuu Privacy Shield -järjestelyyn, tiedon siirtoon sovelletaan järjestelyn periaatteita. Näissä tapauksissa tietojen keräämiseen ja niiden käsittelyyn ennen siirtoa sovelletaan kyseisen EU-maan kansallista lainsäädäntöä, ja kaikkia tämän lainsäädännön mukaisia ehtoja ja rajoituksia, jotka koskevat tietojen siirtoa, on noudatettava.
- ii. Privacy Shield -järjestelyn periaatteita sovelletaan vain silloin kun siirretään tai annetaan käyttöön yksittäinen henkilötieto, jonka perusteella henkilö tunnistetaan tai on tunnistettavissa. Yhteenlaskettuihin työtekijätietoihin 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 Privacy Shield -järjestelyssä, 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 henkilötietojen käyttöä, esitetään tietyt 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 vaarantuisi.

c. Tiedonsaantiperiaatteen soveltaminen

Täydentävässä tiedonsaantiperiaatteessa selostetaan syitä, joiden perusteella voidaan kieltäytyä luovuttamasta pyydettyjä henkilöstötietoja tai rajoittaa niiden saantia. Euroopan unionin työnantajien on luonnollisesti noudatettava paikallisia säädöksiä ja varmistettava, että Euroopan unioniin sijoittautuneet työntekijät saavat tietoja kotimaansa lainsäädännön mukaisesti huolimatta siitä, missä tietoja käsitellään ja säilytetään. Privacy Shield -järjestelyn periaatteet edellyttävät, että tällaista tietoa Yhdysvalloissa käsittelevä organisaatio tekee asiassa yhteistyötä ja luovuttaa tiedot joko suoraan tai eurooppalaisen työnantajan kautta.

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 rikkomuksesta 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 käännyttävä 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 Privacy Shield -järjestelyn rikkomukseen. Tämä on tehokkain tapa soveltaa usein päällekkäisiä oikeuksia ja velvollisuuksia, jotka johtuvat paikallisista työlaeista, työsuopimuksista ja tietosuojasäädöksistä.
- ii. Privacy Shield -järjestelyyn osallistuvan yhdysvaltalaisen organisaation, joka käyttää Euroopan unionista toimitettua henkilöstötietoa ja haluaa kyseisten tiedonsiirtojen kuuluvan Privacy Shield -järjestelyn piiriin, olisi tämän vuoksi sitouduttava tekemään yhteistyötä toimivaltaisten Euroopan unionin viranomaisten kanssa näiden tekemissä tutkimuksissa ja noudattamaan kyseisten viranomaisten näissä tapauksissa antamia ohjeita.

e. Tietojen edelleen siirtämiseen liittyvää vastuuvuolisuutta koskeva periaate

Vähäistä työntekijämäärää koskeva, Privacy Shield -järjestelyssä toteutettava henkilötietojen siirto rekisterinpitäjälle voidaan toteuttaa tiedonsaantiperiaatetta soveltamatta ja ilman että rekisterinpitäjänä toimivan kolmannen osapuolen kanssa tehdään sopimusta, vaikka tätä muutoin vaadittaisiin tietojen edelleen siirtämiseen liittyvää vastuuvuolisuutta koskevan periaatteen mukaan, jos kyse on Privacy Shield -järjestelyyn osallistuvan organisaation satunnaisesta henkilöstöön liittyvästä operatiivisesta toimesta, jossa tietoja käytetään esimerkiksi lentolipun tai hotellihuoneen varaamiseen tai vakuutusluoajan järjestämiseen, ja jos Privacy Shield -järjestelyyn osallistuva organisaatio on noudattanut ilmoitus- ja valintaperiaatetta.

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 Privacy Shield -järjestelyyn.

- ii. Eurooppalaisen rekisterinpitäjän on tehtävä sopimus aina, kun tietoja siirretään pelkästään käsittelytarkoituksessa riippumatta siitä, käsitelläänkö tiedot EU:ssa vai sen ulkopuolella, ja siitä, osallistuuko tietojen käsittelijä Privacy Shield -järjestelyyn. Sopimuksen tavoitteena 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. Henkilötietojen käsittelijä ymmärtää, onko edelleen siirtäminen sallittua, ja

3. ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää antamaan vastauksia henkilöille, jotka toteuttavat järjestelyn periaatteiden mukaisia oikeuksiaan.

- iii. Koska Privacy Shield -järjestelyyn osallistuvat takaavat riittävän tietosuojan, siihen kuuluvien organisaatioiden kanssa tehtävät, pelkkää tietojenkäsittelyä koskevat sopimukset eivät edellytä ennakkolupaa (tai EU:n jäsenvaltio myöntää tällaisen luvan automaattisesti). Ennakkolupa tarvitaan sitä vastoin sopimuksiin, joissa tietojen vastaanottajat eivät osallistu Privacy Shield -järjestelyyn tai eivät muutoin takaa riittävää tietosuoja.

b. Siirrot samaan ryhmään kuuluvien yritysten tai yksiköiden välillä

Kun henkilötietoja siirretään kahden sellaisen rekisterinpitäjän välillä, jotka kuuluvat samaan yritysryhmään, tietojen edelleen siirtämiseen liittyvää vastuuvollisuutta 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 Privacy Shield -järjestelyn periaatteiden mukaisena. Kun tällaisia siirtoja tehdään, Privacy Shield -organisaatio on edelleen vastuussa järjestelyn periaatteiden noudattamisesta.

c. Siirrot rekisterinpitäjien välillä

Kun siirtoja tehdään rekisterinpitäjien välillä, vastaanottavan rekisterinpitäjän ei tarvitse olla Privacy Shield -järjestelyyn osallistuva organisaatio eikä sillä tarvitse olla riippumatonta muutoksenhakumekanismeja. Privacy Shield -järjestelyyn kuuluvan organisaation on tehtävä sopimus tietojen vastaanottavan, rekisterinpitäjänä toimivan kolmannen osapuolen kanssa. Sopimuksessa on määrättävä, että kolmannen osapuolen on järjestettävä tietosuoja, jonka taso vastaa Privacy Shield -järjestelyn tasoa, mutta siinä ei tarvitse määrätä, että kolmas osapuoli osallistuu Privacy Shield -järjestelyyn tai että sillä on riippumaton muutoksenhakumekanismi. Kolmannen osapuolen on kuitenkin asetettava käyttöön vastaava muutoksenhakumekanismi.

11. Riitojenratkaisu ja täytäntöönpano

- a. Muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteessa määrätään vaatimuksista, jotka koskevat Privacy Shield -järjestelyn 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 yksityisellä sektorilla kehitettyjä yksityisyydensuojaohjelmia, joissa Privacy Shield -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 Euroopan unionin 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 kauppakomissiosta annetun lain 5 §:n ja muiden samanlaisia säännöksiä sisältävien lakien ja asetusten nojalla (kauppakomissiosta annetun lain 5 §:ssä kielletään sopimattomat ja vilpilliset toimet).

- c. Jotta varmistettaisiin, että organisaatiot noudattavat Privacy Shield -järjestelyssä antamia sitoumuksia, ja jotta tuettaisiin ohjelman hallinnointia, organisaatioiden ja riippumattomia muutoksenhakumekanismeja hallinnoivien elinten on kauppamasteriön pyynnöstä annettava tietoja, jotka liittyvät Privacy Shield -järjestelyyn. 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. Kuluttajia 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 aiemmillä hyvillä tuloksilla. Kuten muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteissa edellytetään, muutoksenhaun on oltava henkilöiden helposti käytettävissä ja maksutonta. Riitojenratkaisuelinten olisi tutkittava kaikki valitukset paitsi ne, jotka ovat ilmeisen perusteettomia. Tämä ei estä sitä, että organisaatio, 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. Ehdolla ei kuitenkaan pitäisi heikentää organisaation sitoumusta tutkia asianmukaiset valitukset. Lisäksi muutoksenhakumekanismia hallinnoivien elinten olisi annettava henkilöille täydelliset ja helposti saatavilla olevat tiedot siitä, miten riitojenratkaisumenettely etenee sen jälkeen kun valitus on tehty. Näiden tietojen joukossa olisi oltava ilmoitus mekanismin yksityisyydensuojakäytännöistä Privacy Shield -järjestelyn periaatteiden mukaisesti. Jotta valitusten käsittelyyn sovellettavaa menettelyä voitaisiin helpottaa, muutoksenhakumekanismia hallinnoivien elinten olisi tehtävä yhteistyötä sellaisten välineiden kehittämiseksi kuten esimerkiksi vakiomuotoinen valituslomake.
- ii. Riippumattomia muutoksenhakumekanismeja hallinnoivien elinten on sisällytettävä julkisille internetsivuilleen tietoja Privacy Shield -järjestelyn periaatteista ja palveluista, joita ne järjestelyssä tuottavat. Näihin tietoihin on sisällyttävä: 1) tiedot Privacy Shield -järjestelyn vaatimuksista, joiden mukaan on järjestettävä riippumaton muutoksenhakumekanismi, tai linkki tällaisiin vaatimuksiin; 2) linkki kauppaministeriön Privacy Shield -verkkosivulle; 3) tieto siitä, että elimen Privacy Shield -järjestelyn yhteydessä tuottamat riitojenratkaisupalvelut ovat henkilöille maksuttomia; 4) kuvaus siitä, kuinka Privacy Shield -järjestelyyn liittyvä valitus voidaan jättää käsiteltäväksi; 5) aikataulu, jonka mukaisesti Privacy Shield -järjestelyyn liittyvä valitus käsitellään; 6) ja kuvaus siitä, millaiset korjaavat toimet ovat mahdollisia.
- iii. Riippumattomia muutoksenhakumekanismeja hallinnoivien elinten on julkaistava vuosittain kertomus, jossa esitetään niiden riitojenratkaisupalveluja koskevat tilastot. Luvut esitetään yhteenlaskettuina kokonaissummoina. Vuosikertomukseen on sisällyttävä 1) kertomusvuoden aikana saatujen Privacy Shield -järjestelyyn liittyvien valitusten yhteismäärä, 2) saatujen valitusten lajit, 3) riitojenratkaisuun liittyvät laatuksymykset, kuten valitusten käsittelyajan pituus ja 4) valitusten tulokset, erityisesti määrättyjen korjaavien toimenpiteiden 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 Privacy Shield -järjestelyyn osallistuva organisaatio rikkonut järjestelyn velvoitteitaan kyseisen henkilön osalta ja onko kyseinen rikkomus edelleen täysin tai osittain korjaamatta. Välimiesmenettelyä voidaan käyttää ainoastaan tähän tarkoitukseen. Välimiesmenettelyä ei voida hyödyntää esimerkiksi asioissa, jotka liittyvät järjestelyn periaatteista myönnettäviin poikkeuksiin⁽¹⁾ tai Privacy Shield -järjestelyn tarjoaman suojan riittävyyttä koskeviin väitteisiin. Välimiesmenettelyssä Privacy Shield -paneelilla, joka koostuu yhdestä tai kolmesta välimiehestä sen mukaan kuin osapuolet sopivat, on toimivalta määrätä yksilökohtaisesta, ei-rahallisesta kompensatiosta, joka on tarpeen yksityisyyden suojaa koskevien periaatteiden noudattamatta jättämisen korjaamiseksi ja joka koskee ainoastaan kyseistä henkilöä. Tällaisia kompensatioita ovat henkilön mahdollisuus tutustua tietoihinsa sekä hänen tietojensa korjaaminen, hävittäminen tai palauttaminen. Henkilöt ja Privacy Shield -järjestelyyn osallistuvat organisaatiot voivat hakea muutosta tuomioistuimelta välimiespaneelin päätökseen ja vaatia tuomioistuimessa sen täytäntöönpanoa Yhdysvaltojen lainsäädännössä olevan välimiesmenettelystä annetun liittovaltion lain (Federal Arbitration Act) nojalla.

⁽¹⁾ Privacy Shield -järjestelyn periaatteiden I.5 kohta.

e. Korjaavat toimenpiteet ja seuraamukset

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 esittänyttä 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 rikkomuksen vakavuutta. Seuraamukseksi olisi tietyissä olosuhteissa määrättävä sekä se, että järjestelyn periaatteiden noudattamatta jättäminen julkaistaan, että se, että tiedot hävitetään⁽¹⁾. Muita seuraamuksia voivat olla merkin käyttöoikeuden keskeyttäminen tai peruuttaminen, järjestelyn periaatteiden noudattamatta jättämisestä henkilölle aiheutuneen vahingon korvaaminen ja kielto määräys. Yksityisellä sektorilla toimivien riitojen ratkaisusta tai itsesääntelystä vastaavien elinten on ilmoitettava tapauksen mukaan tuomioistuimelle tai asiassa toimivaltaiselle valtiolliselle elimelle sellaiset tapaukset, joissa Privacy Shield -järjestelyyn osallistuva organisaatio ei noudata niiden päätöksiä, sekä ilmoitettava niistä kauppaministeriölle.

f. Liittovaltion kauppakomission toiminta

Liittovaltion kauppakomissio on sitoutunut asettamaan tarkastelussaan etusijalle tapaukset, jotka se on vastaanottanut i) yksityisyyden suojan itsesääntelystä vastaavilta elimiltä ja muilta riippumattomilta riitojen ratkaisuelimiltä, 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 aihetta 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 rikkomuksessa on kyse totuudenvastaisista väitteistä, joiden mukaan organisaatiot noudattavat Privacy Shield -järjestelyn periaatteita tai osallistuvat järjestelyyn, vaikka ne eivät enää ole Privacy Shield -luettelossa tai eivät ole koskaan toimittaneet omaa varmennustaan kauppaministeriölle. Liittovaltion kauppakomissio voi hakea siviilioikeudellista seuraamusta hallinnollisen kielto määräyksen rikkomisesta, ja se voi nostaa siviili- tai rikosjutun liittovaltion tuomioistuimen päätöksen noudattamatta jättämisestä. Liittovaltion kauppakomissio ilmoittaa kauppaministeriölle kaikista tällaisista toimistaan. Kauppaministeriö kehottaa muita valtiollisia elimiä ilmoittamaan sille, mitkä ovat lopulliset johtopäätökset oikeudenkäynneissä tai muissa menettelyissä, jotka koskevat Privacy Shield -järjestelyn periaatteiden noudattamista.

g. Jatkuva järjestelyn periaatteiden noudattamatta jättäminen

- i. Jos organisaatio jättää jatkuvasti noudattamatta Privacy Shield -järjestelyn periaatteita, se menettää oikeutensa järjestelyn etuihin. Kauppaministeriö poistaa Privacy Shield -luettelosta organisaatiot, jotka ovat jatkuvasti jättäneet noudattamatta järjestelyn periaatteita, ja niiden on palautettava tai hävitettävä henkilötiedot, jotka ne ovat vastaanottaneet Privacy Shield -järjestelyn avulla.
- ii. Periaatteiden rikkominen on jatkuva, jos organisaatio, joka on toimittanut kauppaministeriölle oman varmennuksensa, kieltäytyy noudattamasta yksityisyyden suojan itsesääntelystä vastaavan elimen, riippumattoman riitojenratkaisuelimen tai valtiollisen elimen lopullista päätöstä tai jos tällainen elin on todennut organisaation toistuvasti rikkoneen järjestelmän periaatteita siinä määrin, että sen oma ilmoitus periaatteiden noudattamisesta ei enää ole uskottava. Organisaation on näissä tapauksissa viivytyksettä ilmoitettava kauppaministeriölle asiasta. 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 jättävän jatkuvasti noudattamatta järjestelyn periaatteita.
- iii. Kauppaministeriö poistaa organisaation Privacy Shield -luettelosta sellaisen ilmoituksen seurauksena, jonka mukaan organisaatio jättää jatkuvasti noudattamatta järjestelyn periaatteita, tulipa ilmoitus organisaatiolta itseltään, yksityisyyden suojan itsesääntelyä harjoittavalta elimeltä tai muulta riippumattomasta riitojenratkaisua harjoittavalta elimeltä tai valtiolliselta elimeltä. Rikkoneelle organisaatiolle kuitenkin annetaan 30 päivän

⁽¹⁾ Riitojenratkaisuelimet voivat harkita, missä tapauksissa seuraamuksia käytetään. Kyseisten tietojen arkaluonteisuus on yksi tekijöistä, jotka on otettava huomioon päätettäessä, vaaditaanko tietojen hävittämistä. Huomioon on otettava myös se, onko organisaatio kerätessään, käyttäessään tai luovuttaessaan tietoa rikkonut järjestelyn periaatteita räikeästi.

määräaika, jonka aikana sillä on tilaisuus antaa vastaus. Kauppaministeriön ylläpitämästä Privacy Shield -luettelosta käyvät näin ollen selvästi ilmi organisaatiot, jotka ovat oikeutettuja järjestelyn etuihin, ja organisaatiot, jotka eivät enää ole oikeutettuja kyseisiin etuihin.

- iv. Jos organisaatio hakee osallistumisoikeutta itsesääntelyelimessä voidakseen uudestaan osallistua Privacy Shield -järjestelyyn, sen on toimitettava kyseiselle elimelle täydelliset tiedot aiemmasta osallistumisestaan Privacy Shield -järjestelyyn.

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 rekisteröidyllä on oltava mahdollisuus kieltää häntä itseään koskevien tietojen käyttäminen suoramarkkinointiin milloin tahansa. Tällöin on kuitenkin noudatettava organisaation asettamia kohtuullisia aikarajoja, jotka antavat organisaatiolle riittävästi aikaa kiellon täytäntöönpanoon. Organisaatio voi myös edellyttää riittävästi tietoja, jotta se voi varmistua tietojenkäsittelyn kieltämistä vaativan henkilöllisyydestä. Yhdysvalloissa tämän vaihtoehdon voi valita käyttämällä keskitettyä kiello-ohjelmaa, esimerkiksi suoramarkkinointiyhdistyksen Direct Marketing Association's Mail Preference Service -palvelua. Kyseiseen palveluun osallistuvien organisaatioiden olisi tiedotettava tällaisesta mahdollisuudesta kuluttajille siltä varalta, että nämä eivät halua saada mainoksia. 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. Lentomatikustajien 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. Direktiivin 26 artiklan mukaan henkilötietoja voidaan siirtää "sellaiseen kolmanteen maahan, jossa ei taata 25 artiklan 2 kohdassa tarkoitettua tietosuojan riittävää tasoa", jos i) se on tarpeen kuluttajan pyytämien palvelujen tarjoamiseksi tai sopimuksen, kuten kanta-asiakassopimuksen ehtojen täyttämiseksi tai ii) jos kuluttaja on selkeästi antanut siihen suostumuksensa. Privacy Shield -järjestelyssä mukana olevat yhdysvaltalaiset organisaatiot antavat riittävän henkilötietojen suojan, ja ne saavat siten ottaa vastaan EU:sta siirrettyjä tietoja täyttämättä näitä ehtoja tai muita ehtoja, joista säädetään direktiivin 26 artiklassa. Koska Privacy Shield -järjestelyssä 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 Privacy Shield -järjestelyn periaatteiden soveltaminen

EU:n jäsenvaltioiden lainsäädäntöä sovelletaan henkilötietojen keruuseen ja kaikkeen tietojenkäsittelyyn, joka toteutetaan ennen tietojen siirtämistä Yhdysvaltoihin. Privacy Shield -järjestelyn periaatteita sovelletaan, kun tiedot on siirretty Yhdysvaltoihin. Farmaseuttiseen tutkimukseen ja muihin tarkoituksiin käytettävistä tiedoista olisi tarvittaessa poistettava viittaukset henkilöihin.

b. Tulevaisuudessa tehtävä tieteellinen tutkimus

- i. Farmaseuttisissa ja lääkeaineita koskevista tutkimuksista saadut henkilötiedot ovat usein arvokkaita tulevaisuudessa tehtävälle tieteelliselle tutkimukselle. Jos yhtä tutkimusta varten kerättyjä henkilötietoja siirretään yhdysvaltalaiselle organisaatiolle, joka osallistuu Privacy Shield -järjestelyyn, 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 koskevista tutkimuksista, 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

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

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 kuulavalta, joka on hoitanut kyseistä henkilöä tutkimuksen aikana, taikka tutkimuksen teettäneeltä organisaatiolta.

f. Tuotteen turvallisuuden ja tehon seuranta

Lääkkeitä ja lääkintälaitteita valmistavan yrityksen ei tarvitse soveltaa ilmoitusvelvollisuuteen, valintamahdollisuuteen, tietojen edelleen siirtoa koskevaan vastuuvollisuuteen eikä tiedonsaantiin liittyviä Privacy Shield -järjestelyn periaatteita toteuttaessaan seuranta, 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

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. Tällä tavoin koodatun tiedon siirto EU:sta Yhdysvaltoihin ei ole sellainen henkilötietojen siirto, johon sovelletaan Privacy Shield -järjestelyn periaatteita.

15. Julkisten rekistereiden tiedot ja yleisesti saatavilla olevat tiedot

- a. Organisaation on sovellettava yleisesti saatavilla oleviin henkilötietoihin Privacy Shield -järjestelyn 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 saatua tietoa, 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 Privacy Shield -järjestelyn periaatteiden vastaisesti, jotta se tai muut voisivat hyötyä tässä selostetuista poikkeuksista, organisaatio menettää järjestelyn mukaiset 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, Privacy Shield -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 Privacy Shield -järjestelyyn osallistuvat organisaatiot ovat julkaisseet näissä raporteissa, voidaan yhdessä niiden tietojen kanssa, jotka tiedusteluyhteisö on julkaissut, sekä yhdessä muiden tietojen kanssa hyödyntää tehtäessä vuotuista yhteistä tarkastelua Privacy Shield -järjestelyn 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

Välimiesmenettelyä koskeva malli

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

A. Soveltamisala

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

B. Korjaavat toimenpiteet, jotka voidaan määrätä

Välimiesmenettelyssä Privacy Shield -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. Välimiespaneelilla ei ole toimivaltuuksia määrätä muita korjaavia toimenpiteitä. Kun välimiespaneeli harkitsee, mitä korjaavia toimenpiteitä se määrää, sen on otettava huomioon muut korjaavat toimenpiteet, joita on jo määrätty muissa Privacy Shield -järjestelyn 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 rikkomus esille suoraan organisaation kanssa ja annettava organisaatiolle tilaisuus ratkaista asia aikataulussa, jota selostetaan järjestelyn periaatteiden III osan 11 kohdan d alakohdan i alakohdassa; 2) hyödynnettävä järjestelyn periaatteiden mukaista riippumatonta muutoksenhakumekanismia, josta ei aiheudu kuluja henkilölle; ja 3) otettava asia tietosuojaviranomaisen välityksellä esille kauppaministeriön kanssa ja annettava kauppaministeriölle tilaisuus ratkaista asia parhaansa mukaan aikataulussa, jota selostetaan kauppaministeriön kansainvälisen kaupan osaston kirjeessä. Tästä ei aiheudu kuluja henkilölle.

Välimiesmenettelyä ei voida käyttää, jos asia, joka koskee samaa henkilön väittämää järjestelyn periaatteiden rikkomusta, 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. Menettelyyn ei myöskään voida turvautua, jos 1) EU:n tietosuojaviranomainen on toimivaltainen järjestelyn periaatteiden III osan 5 tai 9 kohdan mukaisesti tai 2) se on toimivaltainen ratkaisemaan väitettyä rikkomusta 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 rikkomuksen nojalla hyvitystä toisella foorumilla. Jos ei-rahallinen kompensatio ei kuitenkaan täysin riitä korjaamaan väitettyä rikkomusta, henkilön turvautuminen välimiesmenettelyyn ei estä häntä esittämästä normaaliin tapaan vahingonkorvausvaadetta tuomioistuimessa.

⁽¹⁾ Privacy Shield -järjestelyn periaatteiden I.5 kohta.

E. Asian siirtäminen tuomioistuimeen ja täytäntöönpano

Henkilöt ja Privacy Shield -järjestelyyn osallistuvat organisaatiot voivat hakea muutosta tuomioistuimelta välimiespaneelin päätökseen ja vaatia sen täytäntöönpanoa Yhdysvaltojen lainsäädännössä olevan välimiesmenettelystä annetun liittovaltion lain ⁽¹⁾ (Federal Arbitration Act) nojalla. Asia on pantava vireille liittovaltion piirituomioistuimessa, jonka alueelliseen toimivaltaan Privacy Shield -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 luettelosta, jota käsitellään jäljempänä.

Yhdysvaltojen kauppaministeriö ja Euroopan komissio laativat sovellettavan lainsäädännön mukaisesti luettelon vähintään 20 välimiehestä, jotka valitaan riippumattomuuden, nuhteettomuuden ja asiantuntemuksen perusteella. Tässä menettelyssä sovelletaan seuraavaa:

Seuraavia sääntöjä sovelletaan välimiehiin:

- 1) Välimiehet ovat luettelossa kolmen vuoden ajan, jollei poikkeuksellisista olosuhteista tai perustellusta syystä muuta johdu, ja toimikautta voidaan yhden kerran jatkaa vielä kolmella vuodella;
- 2) Välimiehet eivät saa ottaa ohjeita menettelyn asianosaisilta, Privacy Shield -järjestelyyn osallistuvalla organisaatiolta, Yhdysvalloilta, EU:lta, EU:n jäsenvaltiolta, muulta viranomaiselta, valtiolliselta elimeltä tai lainvalvontaviranomaiselta, eivätkä he saa olla etuyhteydessä mainittuihin tahoihin; ja
- 3) välimiehillä on oltava lupa lakimiehen ammatin harjoittamiseen Yhdysvalloissa, ja heidän on oltava Yhdysvaltojen yksityisyyden suojaa koskevan lainsäädännön asiantuntijoita, joilla on asiantuntemusta myös EU:n tietosuojalainsäädännöstä.

G. Välimiesmenettelyyn sovellettavat säännöt

Kuuden kuukauden kuluessa siitä kun tietosuojan riittävyttä koskeva päätös on annettu, kauppaministeriö ja Euroopan komissio sopivat sovellettavan lainsäädännön mukaisesti, että jokin olemassa oleva, vakiintunut yhdysvaltalainen välimiesmenettelysäännöstö (kuten AAA- tai JAMS-säännöt) valitaan Privacy Shield -paneelin menettelytapasäännöiksi. 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 rikkomuksesta sekä henkilön valinnan mukaisesti todisteena esitettäviä asiakirjoja ja muuta todistusaineistoa ja/tai vaatimukseen sovellettavaa lakia koskevia näkemyksiä.

⁽¹⁾ 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. Sama §. 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, jolle se totea, 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 sen seurauksena syntyvät riidat, 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 välimiesmenettelyyn 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 §.

2. Laaditaan menettelyt sen varmistamiseksi, että yhteen rikkomukseen, josta henkilö esittää väitteitä, ei sovelleta kaksia 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 EU:n tietosuojaviranomainen voi EU:n kansalaisen pyynnöstä avustaa ilmoituksen valmistelussa. Tämä avustaminen voi liittyä vain ilmoitukseen, sillä EU:n 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 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, jolle toisin ole sovittu asianosaisten kesken.

H. Kustannukset

Välimiesten olisi kohtuullisin toimenpitein pyrittävä minimoimaan välimiesmenettelyyn liittyviä kustannuksia ja palkkioita.

Kauppaministeriö edistää sovellettavan lainsäädännön mukaisesti ja Euroopan komissiota kuultuaan sellaisen rahaston perustamista, johon Privacy Shield -järjestelyyn osallistuvien organisaatioiden on suoritettava vuotuinen maksu. Maksu perustuu osittain organisaation kokoon. Rahastosta katetaan välitysmenettelyjen kustannukset, muun muassa välimiesten palkkiot vahvistettavaan enimmäismäärään saakka. Rahastoa hallinnoi kolmas osapuoli, joka raportoi säännöllisesti rahaston toiminnasta. Kauppaministeriö ja Euroopan komissio arvioivat rahaston toimintaa vuotuisen tarkastelun yhteydessä. Tällöin arvioidaan esimerkiksi, onko tarvetta mukauttaa rahastoon tehtäviä maksuja ja välimiesten palkkioiden ylärajoja, ja tarkastellaan muun muassa välimiesmenettelyjen lukumäärää, kustannuksia ja kestoja. Kauppaministeriöllä ja Euroopan komissiolla on yhteisymmärrys siitä, että Privacy Shield -järjestelyyn osallistuville organisaatioille ei pidä asettaa liiallista taloudellista raskautta. Asianajajien palkkiot eivät kuulu tämän säännöksen soveltamisalaan, eikä niitä kateta tämän säännöksen nojalla perustetusta rahastosta.

LIITE III

Kirje Yhdysvaltojen ulkoministeriltä John Kerryltä

7. heinäkuuta 2016

Arvoisa komissaari Jourová

Olen iloinen siitä, että olemme saavuttaneet yhteisymmärryksen Euroopan unionin ja Yhdysvaltojen Privacy Shield -järjestelystä, johon sisällytetään oikeusasiamiesmekanismi. Tämän tietosuojasta vastaavan oikeusasiamiehen välityksellä EU:n alueella toimivat viranomaiset voivat toimittaa EU:n kansalaisten puolesta kysymyksiä, jotka koskevat Yhdysvaltojen signaalitiedustelukäytäntöjä.

Presidentti Barack Obama ilmoitti 17. tammikuuta 2014 merkittävistä tiedustelualan uudistuksista, jotka sisältyvät presidentin määräykseen 28 (Presidential Policy Directive, PPD-28). PPD-28:n nojalla olen nimennyt ulkoministeriön alivaltiosihteerin Catherine A. Novellin yhteyspisteeksi, jonka kautta ulkomaiset hallitukset voivat esittää Yhdysvalloille tämän signaalitiedustelutoimintaa koskevia kysymyksiä. Novelli toimii samalla myös tietotekniikkaan liittyvän kansainvälisen diplomatian johtavana koordinaattorina. Yhteyspistetehtävän lisäksi olen liitteessä A selostettujen ehtojen mukaisesti perustanut Privacy Shield -järjestelyyn oikeusasiamiesmekanismin ja määrännyt alivaltiosihteerin Novellin oikeusasiamiehen tehtävään. Liitteessä A selostettuja ehtoja on päivitetty 22. helmikuuta 2016 päivätyn kirjeeni jälkeen. Alivaltiosihteerin Novelli on riippumaton Yhdysvaltojen tiedusteluyhteisöstä, ja hän raportoi suoraan minulle.

Olen määrännyt, että henkilöstöni osoittaa tälle uudelle oikeusasiamiesmekanismille voimavarat, jotka sen täytäntöönpanemiseen tarvitaan, ja olen vakuuttunut siitä, että vastaamme mekanismin avulla tehokkaasti EU:n kansalaisten huolenaiheisiin.

Kunnioittavasti

John F. Kerry

Liite A

EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn signaalitiedustelua koskeva oikeusasiamiesmekanismi

EU:n ja Yhdysvaltojen Privacy Shield -järjestely on tärkeä, ja sitä silmällä pitäen tässä muistiossa selostetaan menettelyt, joiden mukaisesti pannaan täytäntöön presidentin määräyksen 28 (PPD-28) mukainen signaalitiedustelua koskeva mekanismi ⁽¹⁾.

Presidentti Obama piti 17. tammikuuta 2014 puheen, jossa ilmoitettiin tärkeistä tiedustelualan uudistuksista. Puheessaan presidentti huomautti, että "ponnistelumme auttavat suojaamaan ei ainoastaan omaa kansakuntaamme vaan myös ystäviämme ja liittolaisiamme. Ponnistelumme ovat tuloksellisia vain jos tavalliset kansalaiset muissa maissa luottavat siihen, että Yhdysvallat kunnioittaa myös heidän yksityisyyttään". Presidentti Obama ilmoitti antavansa uuden presidentin määräyksen, PPD-28:n, "määrätäksään tarkasti, mitä me teemme ja mitä me emme tee, kun kyse on meidän ulkomaille suuntautuvasta tarkkailutoiminnastamme."

PPD-28:n 4 § d kohdassa määrätään ulkoministeri nimeämään tietotekniikkaan liittyvän kansainvälisen diplomatian johtava koordinaattori. Tämä "toimii yhteyspisteenä, jonka kautta ulkomaiset hallitukset voivat esittää Yhdysvalloille sen signaalitiedustelutoimintaa koskevia kysymyksiä." Tammikuusta 2015 lähtien alivaltiosihteeri C. Novelli on toiminut johtavana koordinaattorina.

Tässä muistiossa kuvataan uutta mekanismia, jota johtava koordinaattori soveltaa. Mekanismin avulla helpotetaan sellaisten kysymysten ja niihin annettavien vastausten käsittelyä, jotka liittyvät EU:sta Yhdysvaltoihin toimitettuihin tietoihin ja jotka koskevat kansallisen turvallisuuden perusteella tietoihin myönnettävää pääsyä. Tietojen toimittaminen perustuu Privacy Shield -järjestelyyn, vakiosopimuslausekkeisiin, yrityksiä koskeviin sitoviin sääntöihin, poikkeuksiin ⁽²⁾ tai mahdollisiin tuleviin poikkeuksiin ⁽³⁾, ja tiedot toimitetaan vakiintuneita reittejä pitkin Yhdysvaltojen lainsäädännön ja toimintaperiaatteiden nojalla.

- 1. Privacy Shield -järjestelyn oikeusasiamies.** Johtava koordinaattori toimii Privacy Shield -järjestelyn oikeusasiamiehenä. Hän nimeää muita ulkoministeriön virkamiehiä, jotka tarvittaessa auttavat häntä täyttämään tässä muistiossa selostetut velvollisuudet. (Jäljempänä koordinaattoria ja kaikkia muita virkamiehiä, jotka hoitavat oikeusasiamiestehtäviä, kutsutaan 'oikeusasiamieheksi'.) Oikeusasiamies toimii läheisessä yhteistyössä muiden ministeriöiden ja virastojen asianomaisten virkamiesten kanssa, jotka ovat vastuussa kysymysten käsittelystä Yhdysvaltojen sovellettavien lakien ja toimintaperiaatteiden mukaisesti. Oikeusasiamies on riippumaton tiedustelu-yhteisöstä. Oikeusasiamies raportoi suoraan ulkoministerille. Tämä varmistaa, että oikeusasiamies suorittaa tehtävänsä puolueettomasti ja ettei mikään vaikuta epäasianmukaisesti oikeusasiamiehen antamiin vastauksiin.
- 2. Tehokas koordinointi.** Oikeusasiamies hyödyntää ja koordinoi tuloksellisesti jäljempänä selostettavia valvontaelimiä varmistaakseen, että hänellä on tarvittavat tiedot niiden vastauksien laatimiseksi, jotka hän antaa kansalaisten

⁽¹⁾ Jos komission päätöstä, joka koskee EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan riittävyyttä, sovelletaan myös Islantiin, Liechtensteiniin ja Norjaan, Privacy Shield -paketti kattaa paitsi Euroopan unionin myös nämä kolme maata. Sen vuoksi viittaukset EU:hun ja sen jäsenvaltioihin tarkoittavat myös Islantia, Liechtensteiniä ja Norjaa.

⁽²⁾ 'Poikkeuksella' tarkoitetaan tässä yhteydessä kaupallista tietojen siirtoa tai siirtoa, joka toteutetaan sillä ehdolla, että a) rekisteröity on yksiselitteisesti antanut suostumuksensa suunniteltuun siirtoon tai b) siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöön panemiseksi tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä tai c) siirto on tarpeen sellaisen sopimuksen solmimiseksi tai täyttämiseksi, joka on tehty rekisterinpitäjän ja kolmannen osapuolen välillä rekisteröidyn edun nimissä, tai d) siirto on tarpeen tai sitä edellytetään laissa tärkeän yleisen edun turvaamiseksi tai oikeusvaateen laatimiseksi, esittämiseksi tai kiistämiseksi tai e) siirto on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi tai f) siirto tehdään rekisteristä, joka on lakien ja asetusten mukaisesti yleisön tai kenen tahansa sellaisen henkilön käytettävissä, joka voi esittää tiedonsaannille oikeutetun perusteen, siltä osin kuin rekisterin käytön lailliset ehdot täyttyvät kussakin yksittäisessä tapauksessa.

⁽³⁾ 'Mahdollinen tuleva poikkeus' tarkoittaa tässä yhteydessä kaupallista tietojen siirtoa tai siirtoa, joka toteutetaan yhdellä seuraavista ehdoista sillä edellytyksellä, että ehto on laillinen peruste henkilötietojen siirtämiselle EU:sta Yhdysvaltoihin: a) rekisteröity on antanut nimenomaisen suostumuksensa ehdotettuun siirtoon sen jälkeen, kun hänelle on ilmoitettu, että tällaiset siirrot voivat aiheuttaa rekisteröidylle riskejä tietosuojan tason riittävyyttä koskevan päätöksen ja asianmukaisten suojatoimien puuttumisen vuoksi tai b) siirto on tarpeen rekisteröidyn tai muiden henkilöiden elintärkeiden etujen suojaamiseksi, jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan tai c) kun on kyse siirrosta kolmanteen maahan tai kansainväliselle järjestölle eikä mikään muu poikkeus tai mahdollinen tuleva poikkeus sovellu, ainoastaan jos siirto ei ole toistuva, koskee vain vähäistä määrää rekisteröityjä, on tarpeen rekisterinpitäjän pakottavien oikeutettujen etujen toteuttamiseksi eivätkä rekisteröidyn edut tai oikeudet ja vapaudet syrjäytä kyseisiä rekisterinpitäjän etuja ja rekisterinpitäjä on arvioinut kaikkia tiedonsiirtoon liittyviä seikkoja ja tämän arvioinnin perusteella esittänyt asianmukaiset takeet, joilla varmistetaan henkilötietojen suojaa.

valituksia käsittelevän EU:n elimen kysymyksiin. Jos kysymys koskee sitä, onko tarkkailu Yhdysvaltojen lainsäädännön mukaista, oikeusasiamiehellä on mahdollisuus tehdä yhteistyötä sellaisen riippumattoman valvontaelimen kanssa, jolla on tutkintavaltuudet asiassa.

- a. Oikeusasiamies tekee tiivistä yhteistyötä muiden Yhdysvaltojen hallituksen virkamiesten, mukaan lukien riippumattomien valvontaelinten kanssa sen varmistamiseksi, että esitetyt kysymykset käsitellään ja niihin vastataan sovellettavien lakien ja toimintaperiaatteiden mukaisesti. Erityisesti oikeusasiamies koordinoi tiiviisti kansallisen turvallisuusviraston johtajan (ODNI) ja oikeusministeriön kanssa ja tarvittaessa muiden Yhdysvaltojen kansalliseen turvallisuuteen liittyviä tehtäviä hoitavien ministeriöiden ja virastojen kanssa, samoin kuin virastojen valvontaviranomaisten, tiedonvapautta parantavaan lakiin liittyviä tehtäviä hoitavien virkamiesten ja kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavien virkamiesten kanssa.
- b. Yhdysvaltojen hallitus luottaa siihen, että mekanismit, joilla ministeriöt ja virastot koordinoivat ja valvovat kansalliseen turvallisuuteen liittyviä asioita, auttavat oikeusasiamiestä vastaamaan 4 kohdan e alakohdassa tarkoitettulla tavalla kysymyksiin, jotka on esitetty 3 kohdan b alakohdan nojalla.
- c. Oikeusasiamies voi saattaa yksityisyyden suojaa koskevia kysymyksiä yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan, jäljempänä 'valvontalautakunta', käsiteltäväksi.

3. Kysymysten esittäminen

- a. Pyyntö toimitetaan ensin jäsenvaltioiden valvontaviranomaisille, jolla on toimivalta valvoa kansallisia turvallisuuspalveluja ja/tai viranomaisten suorittamaa henkilötietojen käsittelyä. Kysymyksen toimittaa oikeusasiamiehelle EU:n keskitetty elin, jäljempänä yhteisesti 'kansalaisten valituksia käsittelevä EU:n elin'.
- b. Kansalaisten valituksia käsittelevä EU:n elin varmistaa, että kysymys on täydellinen, ja toteuttaa tätä varten seuraavat toimet:
 - i) tarkastaa kansalaisen henkilöllisyyden sekä sen, että henkilö toimii omissa nimissään eikä valtion elimen tai hallitustenvälisen järjestön edustajana;
 - ii) varmistaa, että kysymys esitetään kirjallisesti ja että se sisältää seuraavat tiedot:
 - kaikki tiedot, joihin kysymys perustuu;
 - mitä tietoa tai hyvitystä pyydetään;
 - minkä Yhdysvaltojen hallituksen elimen, jos minkään, uskotaan olevan osallisena asiassa;
 - millä muilla toimenpiteillä on pyritty saamaan kyseiset tiedot tai hyvitys ja mikä tulos niillä on saavutettu;
 - iii) varmistaa, että kysymys koskee tietoja, joiden osalta on perusteltua syytä uskoa, että ne on siirretty EU:sta Yhdysvaltoihin Privacy Shield -järjestelyn, vakiosopimuslausekkeen, yrityksiä koskevien sitovien sääntöjen, poikkeusten tai mahdollisten tulevien poikkeusten nojalla;
 - iv) varmistaa alustavasti, että kysymys ei ole aiheeton eikä sitä ole tehty vilpillisessä mielessä.
- c. Se, että kysymys olisi täydellinen oikeusasiamiehen tämän muistion mukaista jatkokäsittelyä varten, ei edellytä, että kysymyksessä osoitettaisiin Yhdysvaltojen hallinnon tosiasiasa saaneen kysymyksen esittävän henkilön tiedot käyttöönsä signaalitiedustelun avulla.

4. Sitoumus, joka koskee viestintää kansalaisten valituksia käsittelevän EU:n elimen kanssa.

- a. Kun oikeusasiamies vastaanottaa kysymyksen kansalaisten valituksia käsittelevältä EU:n elimeltä, hän toimittaa elimelle vahvistuksen kysymyksen vastaanottamisesta.
- b. Oikeusasiamies tekee alustavan tarkastelun varmistaakseen, että kysymys on täydellinen 3 kohdan b alakohdassa edellytetyllä tavalla. Jos oikeusasiamies havaitsee, että kysymys ei ole täydellinen tai että oikeusasiamies tarvitsee siitä lisätietoja, hän pyrkii käsittelemään ja ratkaisemaan nämä ongelmat kysymyksen toimittaneen, kansalaisten valituksia käsittelevän EU:n elimen kanssa.

- c. Jos oikeusasiamies tarvitsee lisätietoja kysymyksestä sen asianmukaisen käsittelyn helpottamiseksi tai jos kysymyksen alun perin esittäneen henkilön olisi ryhdyttävä johonkin erityiseen toimeen asiassa, oikeusasiamies antaa tästä tiedon kysymyksen toimittaneelle, kansalaisten valituksia käsittelevälle EU:n elimelle.
- d. Oikeusasiamies seuraa, miten kysymysten käsittely etenee, ja antaa aiheesta tarvittaessa ajantasaisia selvityksiä kansalaisten valituksia käsittelevälle EU:n elimelle.
- e. Kun kysymys on täydellinen 3 kohdassa kuvatulla tavalla, oikeusasiamies antaa kysymyksen toimittaneelle, kansalaisten valituksia käsittelevälle EU:n elimelle viipymättä asianmukaisen vastauksen ja noudattaa tällöin edelleen tietojen suojaamiseen liittyviä velvoitteita sovellettavien lakien ja toimintaperiaatteiden mukaisesti. Oikeusasiamies antaa kysymyksen toimittaneelle, kansalaisten valituksia käsittelevälle EU:n elimelle vastauksen, jossa se vahvistaa seuraavaa: i) valitus on tutkittu asianmukaisesti, ja ii) tietojenkäsittelyssä on noudatettu Yhdysvaltojen lainsäädäntöä, toimeenpanoasetuksia, presidentin määräyksiä ja virastojen toimintaperiaatteita, joissa on säädetty ODNI:n kirjeessä kuvatuista rajoituksista ja suojatoimista; siinä tapauksessa, että mainittuja säännöksiä ei ole noudatettu, vahvistetaan, että sääntöjenvastaisuudet on korjattu. Oikeusasiamies ei vahvista eikä kiistä, onko henkilö ollut tarkkailun kohteena, eikä ilmoita, mitä nimenomaista korjaavaa toimenpidettä asiassa on sovellettu. Kuten jäljempänä 5 kohdassa selostetaan, tiedonvapautta parantavaan lakiin perustuvat kysymykset käsitellään kyseisen säädöksen ja sovellettavien asetusten mukaisesti.
- f. Oikeusasiamies on suoraan yhteydessä kansalaisten valituksia käsittelevän EU:n elimen kanssa, ja tämä elin puolestaan vastaa yhteydenpidosta kysymyksen esittäneen henkilön kanssa. Jos suorat yhteydet ovat osa jotain jäljempänä kuvattua, selvitysten perustana olevaa prosessia, nämä yhteydet tapahtuvat voimassa olevien menettelytapojen mukaisesti.
- g. Tämän muistion sitoumuksia ei sovelleta yleisluonteisiin väitteisiin, joiden mukaan EU:n ja Yhdysvaltojen Privacy Shield -järjestely on ristiriidassa Euroopan unionin tietosuojavaatimusten kanssa. Tässä muistiossa esitetyt sitoumukset perustuvat Euroopan komission ja Yhdysvaltojen hallituksen yhteiselle käsitykselle, jonka mukaan tässä mekanismissa annettujen sitoumusten soveltamisalan seurauksena voi syntyä resurssipula, myöskin tiedonvapautta parantavaan lakiin perustuvien kysymysten vuoksi. Jos oikeusasiamiehen tehtävien hoitaminen vaatii kohtuuttomasti resursseja ja tämä muodostaa esteen kyseisten sitoumusten täyttämiseksi, Yhdysvaltojen hallitus neuvottelee Euroopan komission kanssa siitä, mitä muutoksia olisi tehtävä tilanteen korjaamiseksi.
5. **Tietopyynnöt.** Pyyntö tutustua Yhdysvaltojen hallituksen asiakirjoihin voidaan esittää ja käsitellä tiedonvapautta parantavan lain, jäljempänä 'FOIA-laki', nojalla.
- a. FOIA-lain nojalla kuka tahansa – riippumatta henkilön kansallisuudesta – voi pyytää mahdollisuutta tutustua liittovaltion virastoissa oleviin asiakirjoihin. Tämä säädös on sisällytetty Yhdysvaltojen lakikodifikaatioon (5 U.S.C. § 552). FOIA-laki ja FOIAa koskevat lisätiedot ovat saatavilla osoitteissa www.foia.gov ja <http://www.justice.gov/oip/foia-resources>. Kullakin virastolla on johtava FOIA-virkailija, ja kukin virasto antaa julkisella verkkosivustollaan tietoa siitä, kuinka FOIA-pyyntö toimitetaan virastolle. Virastoilla on menettelytapoja toistensa kuulemisesta sellaisten FOIA-pyyntöjen osalta, jotka koskevat toisessa virastossa olevia asiakirjoja.
- b. Seuraavassa joitakin esimerkkejä FOIA-toiminnoista:
- i) ODNI on perustanut ODNI-FOIA-portaalin: <http://www.dni.gov/index.php/about-this-site/foia>. Portaaliin annetaan tietoa siitä, miten pyyntö esitetään ja miten olemassa olevan pyynnön tilanne tarkistetaan, sekä siitä, kuinka päästä tutustumaan tietoon, jonka ODNI on asettanut saataville ja julkaissut FOIA-lain nojalla. ODNI-FOIA -portaaliin on linkkejä muiden tiedusteluyhteisön toimijoiden FOIA-sivustoihin: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>
- ii) Oikeusministeriön tiedotuspolitiikasta vastaava toimisto tarjoaa kattavaa FOIA-tietoa: <http://www.justice.gov/oip>. Sivustolla ei ainoastaan anneta tietoa siitä, miten FOIA-pyyntö toimitetaan oikeusministeriölle, vaan siellä annetaan opastusta myös Yhdysvaltojen hallinnolle FOIA-vaatimusten tulkinnasta ja soveltamisesta.

- c. FOIA-laissa luetellaan tietty määrä poikkeuksia, jotka koskevat pääsyä hallituksen asiakirjoihin. Näihin kuuluvat rajoitukset, jotka koskevat pääsyä kansalliseen turvallisuuteen liittyviin turvallisuusluokiteltuihin tietoihin, kolmansien osapuolten henkilötietoihin sekä lainvalvonnassa tehtyjen tutkimusten tietoihin. Rajoitukset vastaavat sitä, mitä kukin EU:n jäsenvaltio on säätänyt omista tiedonsaantia koskevissa laeissaan. Rajoituksia sovelletaan samalla tavalla yhdysvaltalaisiin ja ei-yhdysvaltalaisiin henkilöihin.
- d. Jos tietojen luovuttamisesta FOIA-lain nojalla syntyy riitaa, asiassa voidaan tehdä hallinnollinen muutoksenhaku, minkä jälkeen muutosta voidaan hakea liittovaltion tuomioistuimessa. Tuomioistuin käsittelee asian kokonaan uudestaan päättäessään, oliko tietojen antamatta jättäminen asianmukaista (5 U.S.C. § 552 (a)(4)(B)), ja se voi velvoittaa hallituksen antamaan tiedot. Joissakin tapauksissa tuomioistuin on kumonnut hallituksen väitteet siitä, että tiedot olisi salattava turvallisuusluokituksen vuoksi. Vaikka rahamääräisiä vahingonkorvauksia ei voida määrätä, tuomioistuin voi määrätä asianajajan palkkiot korvattavaksi.
6. **Lisätoimia koskevat pyynnöt.** Pyyntö, jossa väitetään, että lakia on rikottu tai että on syyllistytty muuhun väärinkäyttöön, siirretään sellaisen Yhdysvaltojen hallinnon elimen käsiteltäväksi, jolla on toimivaltuudet tutkia asia ja puuttua sääntöjenvastaaisuuksiin siten kuin jäljempänä selostetaan. Tällaisia elimiä ovat esimerkiksi riippumattomat valvontaelimet.
- a. Virastojen valvontaviranomaisten riippumattomuus perustuu lakiin. Heillä on laajat valtuudet tehdä ohjelmia koskevia tutkimuksia, tarkastuksia ja arviointoja. Toimivaltuuksiin kuuluu myös petosten ja väärinkäytösten tai lainrikkomusten tutkiminen. Valvontaviranomaiset voivat suositella korjaavia toimia.
- i) Virastojen valvontaviranomaisista annetussa laissa (The Inspector General Act 1978), sellaisena kuin se on muutettuna, luotiin oikeudellinen perusta valvontaviranomaisten toiminnalle. Valvontaviranomaiset ovat riippumattomia ja puolueettomia yksiköitä, joita on useimmissa virastoissa. Valvontaviranomaisten tehtävänä on torjua tuhlailevaa varainkäyttöä, petoksia ja väärinkäytöksiä virastojensa ohjelmissa ja toiminnoissa. Tässä tarkoituksessa kunkin valvontaviranomaisen velvollisuutena on tehdä virastonsa ohjelmia ja toimintoja koskevia tarkastuksia ja tutkimuksia. Lisäksi valvontaviranomaiset edistävät sellaisia toimia koskevaa johtamista ja koordinoitua, joilla pyritään lisäämään viraston ohjelmien ja toimintojen taloudellisuutta, tehokkuutta ja tuloksellisuutta sekä ehkäisemään ja havaitsemaan niissä tapahtuvia petoksia ja väärinkäytöksiä. Valvontaviranomaiset antavat suosituksia toimintaperiaatteista, jotka koskevat kyseisiä toimia.
- ii) Tiedusteluyhteisön kaikilla toimijoilla on oma valvontaviranomaisen toimistonsa (Office of the Inspector General), jonka vastuulla on valvoa muun muassa ulkomaantiedustelutoimintaa. Joitakin valvontaviranomaisen kertomuksia, jotka koskevat tiedustelutoimintaa, on julkistettu.
- iii) Seuraavassa joitakin esimerkkejä valvontaviranomaisista:
- Tiedusteluyhteisön valvontaviranomaisen toimisto perustettiin tiedustelutoiminnan talousarviota koskevan vuoden 2010 lain (Intelligence Authorization Act of Fiscal Year 2010 – <http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf>) 405 §:n nojalla. Tiedusteluyhteisön valvontaviranomaisen tehtävänä on suorittaa koko tiedusteluyhteisön laajuisia tarkastuksia, tutkimuksia ja arviointoja, joiden avulla pyritään havaitsemaan tiedusteluyhteisön tehtävät läpileikkaavia järjestelmäriskkejä, haavoittuvuuksia ja heikkouksia ja puuttumaan näihin ongelmiin ja siten parantamaan koko tiedusteluyhteisön taloudellisuutta ja tehokkuutta. Tiedusteluyhteisön valvontaviranomaisella on valtuudet tutkia ODNIn tai tiedusteluyhteisön tiedusteluohjelmiin ja -toimintoihin liittyviä valituksia tai tietoja, jotka koskevat väitettyjä lakien, sääntöjen tai asetusten rikkomuksia tai tuhlailevaa varainkäyttöä, petoksia tai vallan väärinkäyttöä tai kansanterveydelle ja yleiselle turvallisuudelle aiheutuvaa merkittävää tai erityistä vaaraa. Tietoa siitä, miten tiedusteluyhteisön valvontaviranomaiseen otetaan suoraan yhteyttä ilmoituksen tekemiseksi, on seuraavassa osoitteessa: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>
 - Yhdysvaltojen oikeusministeriön valvontaviranomaisen toimisto (<https://www.justice.gov>) on lailla perustettu riippumaton yksikkö. Sen tehtävänä on paljastaa ja torjua tuhlailevaa varainkäyttöä, petoksia, väärinkäytöksiä ja virkavelvollisuuksien rikkomuksia, jotka ovat tapahtuneet oikeusministeriön ohjelmissa tai joihin ministeriön henkilökunta on syyllistynyt. Samoin valvontaviranomaisen tehtävänä on edistää ministeriön ohjelmien taloudellisuutta ja tehokkuutta. Valvontaviranomainen tutkii ministeriön henkilökunnan väitetyt siviili- ja rikosoikeudellisten lakien rikkomukset ja tarkastaa myös ministeriön ohjelmia. Valvontaviranomainen on toimivaltainen tutkimaan kaikki virkavelvollisuuksien rikkomuksia koskevat valitukset, jotka on tehty oikeusministeriön työntekijöitä vastaan. Toimivalta koskee seuraavia elimiä: Yhdysvaltojen liittovaltion poliisi (Federal Bureau of Investigation), Yhdysvaltojen huumevirasto (Drug Enforcement Administration), Yhdysvaltojen liittovaltion vankeinhoitolaitos (Federal Bureau of Prisons), Yhdysvaltojen liittovaltion seriffinvirasto (U.S. Marshals Service), Yhdysvaltojen alkoholi-, tupakka-, ampuma-ase- ja räjähdeseasioita hoitava viranomainen (Bureau of Alcohol, Tobacco, Firearms, and Explosives), Yhdysvaltojen liittovaltion syyttäjäviranomaisten toimistot (United States Attorneys Offices) sekä oikeusministeriön muiden osastojen tai toimistojen työntekijät. Tästä on yksi poikkeus: ministeriön virkavastuutoimisto (Office of Professional Responsibility) tutkii syytökset, joiden mukaan ministeriön palveluksessa oleva syyttäjä tai lainvalvontahenkilökuntaan kuuluva olisi syyllistynyt virkavelvollisuuksien rikkomukseen käyttäessään ministeriön syyttäjälle kuuluvia toimivaltuuksia esitutkinnassa, syyttämässä tai

lainopillisessa neuvonnassa. Lisäksi terrorisminvastaisen USA Patriot Act -lain (vahvistettu 26.10.2001) 1001 §:ssä määrätään valvontaviranomaisia tutkimaan tietoja ja valituksia, joiden mukaan oikeusministeriön työntekijät ovat rikkoneet kansalaisoikeuksia ja -vapauksia. Valvontaviranomainen pitää yllä julkista verkkosivustoa (<https://www.oig.justice.gov>), jonka kautta voi myös jättää valituksen (<https://www.oig.justice.gov/hotline/index.htm>).

b. Myös Yhdysvaltojen hallinnon toimistoilla ja yksiköillä, jotka vastaavat yksityisyyttä ja kansalaisvapauksia koskevista asioista, on omat velvollisuutensa näissä asioissa. Seuraavassa tästä joitakin esimerkkejä:

- i) Syyskuun 11. päivän komission suosituksia täytäntöönpanevan lain (Implementing Recommendations of the 9/11 Commission Act of 2007; Yhdysvaltojen lakikodifikaation kohta 42 U.S.C. § 2000-ee1) 803 §:ssä perustetaan joihinkin ministeriöihin ja virastoihin (mukaan lukien ulkoasiainministeriö, oikeusministeriö ja ODNI) yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaavien virkamiesten virat. Lain 803 §:n mukaan yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaavat virkamiehet ovat toimipaikkojensa pääneuvonantajia, joiden tehtävänä on muun muassa varmistaa, että kyseisen ministeriön, viraston tai tiedusteluyhteisön toimijan menettelyt ovat asianmukaisia, jotta sellaisilta henkilöiltä tulevat valitukset, jotka väittävät, että kyseinen ministeriö, virasto tai toimija on rikkonut heidän yksityisyyden suojaansa tai kansalaisvapauksiaan, käsitellään asianmukaisesti.
- ii) ODNI:n kansalaisvapauksien suojasta vastaava virkamies johtaa ODNI:n kansalaisvapauksista ja yksityisyyden suojasta vastaavaa toimistoa (ODNI Civil Liberties and Privacy Office). Kyseinen virka perustettiin vuoden 1948 kansallista turvallisuutta koskevalla lailla, sellaisena kuin se on muutettuna. ODNI:n kansalaisvapauksista ja yksityisyyden suojasta vastaavan toimiston tehtäviin kuuluu sen varmistaminen, että tiedusteluyhteisön toimijoiden toimintaperiaatteisiin ja menettelytapoihin on sisällytetty riittävät kansalaisvapauksia ja yksityisyyttä koskevat suojatoimet. Toimisto tutkii myös valituksia, joissa väitetään, että ODNI:n ohjelmissa ja toiminnoissa rikotaan kansalaisvapauksia ja yksityisyyttä. ODNI:n kansalaisvapauksista ja yksityisyyden suojasta vastaava toimisto tarjoaa yleisölle tietoa verkkosivustollaan, jolla annetaan myös ohjeet valituksen tekemisestä (www.dni.gov/clpo). Jos toimisto vastaanottaa yksityisyyden ja kansalaisvapauksien loukkaamista koskevan valituksen, joka koskee tiedusteluyhteisön ohjelmia ja toimintoja, se koordinoi muiden tiedusteluyhteisön toimijoiden kanssa, miten tiedusteluyhteisön olisi jatkokäsiteltävä kyseistä valitusta. On huomattava, että myös kansallisella turvallisuusvirastolla (NSA) on kansalaisvapauksista ja yksityisyyden suojasta vastaava toimisto. Sen tehtävistä on tietoa toimiston verkkosivustolla (https://www.nsa.gov/civil_liberties/). Jos esiin tulee tietoja, jotka osoittavat, että jokin virasto ei noudata yksityisyyden suojaa koskevia vaatimuksia (esimerkiksi PPD-28:n 4 §:ssä olevia vaatimuksia), virastot hyödyntävät tällöin vaatimusten noudattamista varmistavia mekanismejaan, joiden avulla tilanne tarkistetaan ja ongelma korjataan. Virastojen edellytetään ilmoittavan ODNI:lle tapauksista, joissa PPD-28:n vaatimuksia ei ole noudatettu.
- iii) Oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaava toimisto auttaa kyseisestä toiminta-alueesta vastaavaa ministeriön johtavaa virkamiestä täyttämään tehtävänsä ja velvollisuutensa. Toimiston tärkein tehtävä on turvata Yhdysvaltojen kansalaisten yksityisyyttä ja kansalaisvapauksia tarkastamalla, valvomalla ja koordinoimalla ministeriön toimintoja, jotka liittyvät yksityisyyden suojaan. Toimistolle kuuluvat seuraavat tehtävät: se antaa oikeudellista neuvontaa ja opastusta ministeriön yksiköille; se varmistaa, että ministeriö noudattaa yksityisyyden suojan vaatimuksia, mukaan luettuna yksityisyyden suojaa koskeva vuoden 1974 Privacy Act -laki sekä sähköistä hallintoa koskevan vuoden 2002 E-Government Act -lain ja liittovaltion tietoturvan hallintaa koskevan Security Management Act -lain yksityisyssännökset, samoin kuin näiden lakien täytäntöönpanon edistämiseksi annetut hallinnolliset määräykset; se kehittää ja toteuttaa ministeriön yksityisyyden suojaa koskevaa koulutusta; se avustaa yksityisyyden ja kansalaisvapauksien suojasta vastaavaa ministeriön johtavaa virkamiestä ministeriön tietosuojapolitiikan kehittämisessä; se valmistelee yksityisyyden suojaan liittyvää raportointia Yhdysvaltojen presidentille ja kongressille; ja tarkastaa ministeriön tietojenkäsittelykäytäntöjä sen varmistamiseksi, että ne ovat yhdenmukaiset yksityisyyden ja kansalaisvapauksien suojelun kanssa. Oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaava toimisto antaa yleisölle tietoa tehtävistään osoitteessa <http://www.justice.gov/opcl>
- iv) Yhdysvaltojen lain (42 U.S.C. § 2000ee ja sitä seuraavat pykälät) mukaan valvontalautakunnan on jatkuvasti seurattava i) ministeriöiden, virastojen ja toimeenpanovallan toimijoiden toimintaperiaatteita ja menettelytapoja, jotka koskevat toimia kansakunnan suojelemiseksi terrorismilta, sekä kyseisten toimintaperiaatteiden ja menettelytapojen täytäntöönpanoa sen varmistamiseksi, että yksityisyyden ja kansalaisvapauksien suoja toteutuu, ja ii) muita toimeenpanovallan toimia, jotka koskevat kansakunnan suojelemista terrorismilta, sen selvittämiseksi, suojellaanko toimien yhteydessä yksityisyyttä ja kansalaisvapauksia asianmukaisesti ja ovatko toimet yksityisyyttä ja kansalaisvapauksia koskevien lakien, asetusten ja toimintaperiaatteiden mukaisia. Valvontalautakunta myös käy läpi yksityisyyteen ja kansalaisvapauksiin liittyviä tehtäviä hoitavilta virkamiehiltä vastaanottamia raportteja sekä antaa kyseisille virkamiehille tarvittaessa näiden toimintaa koskevia suosituksia. Syyskuun 11. päivän komission suosituksia täytäntöönpanevan lain 803 §:ssä säädetään, että kahdeksan liittovaltion viraston (joihin kuuluvat muun muassa puolustusministeriö, sisäisestä turvallisuudesta vastaava ministeriö, kansallinen tiedusteluvirasto ja Yhdysvaltojen keskustiedustelupalvelu) sekä valvontalautakunnan määräämien muiden virastojen yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaavien virkamiesten on toimitettava säännöllisiä raportteja valvontalautakunnalle. Raporteissa on muun muassa selostettava kyseisen viraston vastaanottamien, väitettyjä rikkomuksia koskevien valitusten määrä, luonne ja

niihin annetut ratkaisut. Valvontalautakunnan toimivaltuuksista annetussa laissa säädetään, että valvontalautakunta vastaanottaa kyseiset raportit ja että sen on tarvittaessa annettava yksityisyyteen ja kansalaisvapauksiin liittyvistä asioista vastaaville virkamiehille näiden tehtäviä koskevia suosituksia.

LIITE IV

Liittovaltion kauppakomission puheenjohtajan Edith Ramirezin kirje

7. heinäkuuta 2016

SÄHKÖPOSTITSE

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

Arvoisa komissaari Jourová

Yhdysvaltojen liittovaltion kauppakomissio kiittää mahdollisuudesta kertoa toimista, joilla se valvoo EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toteutumista. Me uskomme, että Privacy Shield -järjestely on erittäin tärkeä pyrkinessämme helpottamaan yksityisyyttä suojelevaa kaupankäyntiä yhä verkostoituneemmassa maailmassa. Järjestelyn avulla yritykset voivat tehdä merkittäviä liiketoimia globaalissa taloudessa samaan aikaan kun EU:n kuluttajien yksityisyyden suoja säilyy korkeatasoisena. Liittovaltion kauppakomissio on pitkään pyrkinyt suojelemaan yksityisyyttä kansainvälisissä yhteyksissä ja tekee uuden järjestelyn valvonnasta keskeisen painopisteensä. Jäljempänä kuvaamme liittovaltion kauppakomission tähän asti toteuttamia voimaperäisiä yksityisyydensuojatoimia, siltä osin kuin on ollut kyse alkuperäisen safe harbor -ohjelman valvonnasta. Selostamme myös lähestymistapaamme uuden järjestelyn valvonnassa.

Liittovaltion kauppakomissio ilmaisi julkisesti sitoumuksensa safe harbor -ohjelman valvontaan ensimmäisen kerran vuonna 2000. Tuolloin silloinen liittovaltion kauppakomission puheenjohtaja Robert Pitofsky lähetti Euroopan komissiolle kirjeen, jossa hän selosti liittovaltion kauppakomission sitoumusta valvoa tarmokkaasti safe harbor -ohjelman yksityisyydensuojaperiaatteiden toteutumista. Liittovaltion kauppakomissio on vaalinut sitoumistaan tekemällä lähes 40 lainvalvontatointia ja lukuisia lisätutkimuksia sekä tekemällä yhteistyötä yksittäisten Euroopan tietosuojaviranomaisten kanssa kysymyksissä, jotka ovat kiinnostaneet molempia tahoja.

Sen jälkeen kun Euroopan komissio oli marraskuussa 2013 esittänyt huolensa safe harbor -ohjelman hallinnosta ja valvonnasta, me ja Yhdysvaltojen kauppaministeriö aloitimme Euroopan komission virkamiesten kanssa neuvottelut siitä, kuinka safe harbor -ohjelmaa voitaisiin vahvistaa. Samaan aikaan kun nämä keskustelut olivat vireillä, Euroopan unionin tuomioistuimien antoi 6. lokakuuta 2015 päätöksensä Schrems-asiassa ja muun muassa mitätöi Euroopan komission päätöksen, joka koski safe harbor -ohjelman tietosuojan riittävyyttä. Tämän päätöksen jälkeen jatkoimme tiivistä työtä kauppaministeriön ja Euroopan komission kanssa vahvistaaksemme EU:n alueella asuville henkilöille annettavaa yksityisyyden suojaa. Privacy Shield -järjestely on näiden neuvottelujen tulos. Liittovaltion kauppakomissio sitoutuu uuden järjestelyn tarmokkaaseen valvontaan samalla tavalla kuin aiemmin safe harbor -ohjelman valvontaan. Tässä kirjeessä dokumentoidaan tämä sitoumus.

Erityisesti vahvistamme sitoumuksemme neljällä keskeisellä alueella: 1) annamme etusijan valitusten käsittelemiselle ja tutkimuksille; 2) puutumme totuudenvastaisiin tai vilpillisiin väitteisiin, jotka koskevat osallistumista Privacy Shield -järjestelyyn; 3) jatkamme määräysten noudattamisen valvontaa; ja 4) vahvistamme yhteyksiä ja valvontayhteistyötä Euroopan tietosuojaviranomaisten kanssa. Jäljempänä annamme tarkat tiedot kustakin sitoumuksesta ja selostamme liittovaltion kauppakomission tehtäviä kuluttajien yksityisyyden suojelussa ja safe harbor -ohjelman valvonnassa sekä valotamme Yhdysvaltojen yksityisyydensuojakysymyksiä myös yleisemmin ⁽¹⁾.

I. TAUSTA**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

⁽¹⁾ Annamme lisätietoja Yhdysvaltojen liittovaltion ja osavaltioiden yksityisyysslaeista liitteessä A. Lisäksi yhteenvedo meidän viimeaikaisista yksityisyyden suojan ja tietoturvan liittyvistä lainvalvontatoimistamme on saatavilla liittovaltion kauppakomission verkkosivustolla <https://www.ftc.gov/reports/privacy-data-security-update-2015>

valvoo useiden lakien noudattamista suojellakseen kuluttajia koskevan tiedon yksityisyyttä ja turvallisuutta. Liittovaltion kauppakomissio valvoo liittovaltion kauppakomissiosta annetun lain noudattamista. Siinä kielletään kaupankäynnissä toteutettavat tai kaupankäyntiin vaikuttavat ”sopimattomat” ja ”vilpilliset” toimet tai käytännöt ⁽¹⁾. Lausuma, laiminlyönti tai käytäntö on vilpillinen, jos se on olennainen ja johtaa kuluttajia virheellisesti kuvittelemaan, että heidän toimintansa on järkevää tietyssä tilanteessa ⁽²⁾. Toimi tai käytäntö on sopimaton, jos se aiheuttaa tai todennäköisesti aiheuttaa merkittäviä haittoja, jotka eivät ole kohtuudella kuluttajien vältettävissä ja joiden vastapainoksi kuluttajille tai kilpailutilanteelle ei koidu yhtä suuria hyötyjä ⁽³⁾. Liittovaltion kauppakomissio valvoo myös kohdennettuja lakeja, joilla suojataan terveyteen ja luottoihin sekä muihin rahoitusasioihin liittyviä tietoja sekä verkossa olevaa lapsia koskevaa tietoa. Liittovaltion kauppakomissio on antanut asetuksia kaikkien näiden kohdennettujen lakien täytäntöönpanemiseksi.

Liittovaltion kauppakomission toimivalta, joka perustuu liittovaltion kauppakomissiosta annettuun lakiin, koskee ”kaupankäynnissä toteutettavia tai kaupankäyntiin vaikuttavia” toimia. Kauppakomissiolla ei ole toimivaltaa rikosoikeudellisessa lainvalvonnassa 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, vakuutustoimintaa ja telepalveluyritysten tavanomaisia tiedonsiirtopalveluja. Kauppakomission toimivaltuudet eivät myöskään koske useimpia voittoa tavoittelemattomia yhteisöjä, mutta ne koskevat valehyväntekeväisyyttä harjoittavia tai muita yhteisöjä, jotka väittävät olevansa voittoa tavoittelemattomia mutta jotka todellisuudessa 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 ⁽⁴⁾. Joissakin tapauksissa liittovaltion kauppakomission toimivaltuudet ovat rinnakkaisia jonkin toisen lainvalvontaviranomaisen toimivaltuuksien kanssa.

Yhteytemme liittovaltion ja osavaltioiden viranomaisiin ovat vankat, ja teemme tiivistä yhteistyötä koordinoiaksemme tutkimuksia ja siirtääksemme tarvittaessa asioita asianomaisten tahojen käsiteltäväksi.

Yksityisyyden suojelussa lainvalvonta on liittovaltion kauppakomission lähestymistavan keskiössä. Tähän päivään mennessä liittovaltion kauppakomissio on pannut vireille yli 500 asiaa suojellakseen yksityisyyttä ja kuluttajatietojen turvallisuutta. Asioissa on ollut kyse sekä verkossa olevasta että muusta tiedosta, ja lainvalvontatoimet ovat koskeneet sekä suuria että pieniä yrityksiä. Syyt asioiden vireille panemiseen ovat olleet seuraavia: yritys ei ole hävittänyt arkaluonteista kuluttajatietoa asianmukaisesti; yritys ei ole säilyttänyt kuluttajan henkilötietoja turvallisesti; yritys on jäljittänyt kuluttajia verkossa vilpillisessä tarkoituksessa, lähettänyt heille roskapostia ja asentanut vakoiluohjelmia tai muita haittaohjelmia kuluttajien tietokoneisiin; ja yritys on rikkonut puhelinmyynnin älä soita -sääntöä tai muita sääntöjä sekä kerännyt ja levittänyt mobiililaitteita koskevaa kuluttajatietoa epäasianmukaisesti. Liittovaltion kauppakomission lainvalvontatoimet, koskivatpa ne fyysistä tai digitaalista maailmaa, tekevät selväksi yrityksille, että niiden on suojeltava kuluttajien yksityisyyttä.

Liittovaltion kauppakomissio on myös edistänyt useita toimintaperiaatealoitteita, joiden tavoitteena on ollut parantaa kuluttajien yksityisyyden suojaa ja joista on ollut hyötyä kauppakomission lainvalvontatyössä. Kauppakomissio on järjestänyt seminaareja ja julkaissut raportteja, joissa on suositeltu parhaita käytäntöjä. Tavoitteet ovat olleet seuraavia: parantaa yksityisyyttä mobiiliympäristössä; lisätä datavälitysalan läpinäkyvyyttä; maksimoida suurien tietomäärien edut ja samalla pienentää niihin liittyviä riskejä, erityisesti sellaisten kuluttajien osalta, jotka ovat pienituloisia ja joille tarjotut palvelut ovat puutteellisia; sekä tuoda esiin muun muassa kasvotunnistuksen ja esineiden internetin vaikutukset yksityisyyden suojaan ja tietoturvaan.

Liittovaltion kauppakomissio järjestää myös kuluttajien ja yritysten koulutusta ja pyrkii näin tehostamaan lainvalvontaan ja toimintaperiaatteiden kehittämiseen liittyvien aloitteidensa vaikutusta. Kauppakomissio on hyödyntänyt useita välineitä – julkaisuja, verkkosovelluksia, seminaareja ja sosiaalista mediaa – tuodakseen yleisön saataville koulutusmateriaalia monista aiheista kuten mobiilisovelluksista, lasten yksityisyydestä ja tietoturvallisuudesta. Viimeksi kauppakomissio on käynnistänyt lähde liikkeelle turvallisesti -aloitteen. Siinä annetaan uusia ohjeita yrityksille niiden kokemusten pohjalta, jotka on saatu kauppakomission tietoturvallisuustapauksista. Aloitteen yhteydessä on myös pidetty joukko seminaareja eri puolilla maata. Kauppakomissio on lisäksi ollut pitkään johtava tekijä koulutuksissa, joissa kuluttajille annetaan tietoa tietokoneturvallisuuden peruskysymyksistä. Viime vuonna meidän OnGuard-verkkosivustollamme ja sen espanjan-kielisellä vastineella, Alera en Línealla, vierailtiin yli 5 miljoonaa kertaa.

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

Privacy Shield -järjestely on osa laajempaa Yhdysvalloissa noudatettavaa yksityisyyden suojaa, josta EU:n kuluttajat hyötyvät monin tavoin.

⁽¹⁾ 15 U.S.C. § 45(a).

⁽²⁾ Ks. liittovaltion kauppakomission toimintaperiaatelausunto, joka koskee vilpillistä menettelyä ja joka on liitteenä asiassa *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), saatavilla osoitteessa <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>

⁽³⁾ Ks. 15 U.S.C § 45(n); liittovaltion kauppakomission toimintaperiaatelausunto, joka koskee sopimatonta menettelyä ja joka on liitteenä asiassa *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), saatavilla osoitteessa <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>

⁽⁴⁾ Ks. asia *California Dental Ass'n v. Liittovaltion kauppakomissio*, 526 U.S. 756 (1999).

Liittovaltion kauppakomissiosta annetussa laissa oleva sopimattomien tai vilpillisten toimien ja käytäntöjen kielto ei rajoitu siihen, että sillä suojellaan yhdysvaltalaisia kuluttajia yhdysvaltalaisilta yrityksiltä, sillä kielto kattaa käytännöt, jotka 1) aiheuttavat tai todennäköisesti aiheuttavat kohtuullisesti ennustettavissa olevia vahinkoja Yhdysvalloissa tai joihin 2) liittyy olennaista toimintaa Yhdysvalloissa. Lisäksi samat hyvitysmenetelmät, esimerkiksi vahingonkorvaus, ovat kauppakomission käytössä sekä ulkomaisten että kotimaisten kuluttajien suojaamiseksi.

Kauppakomission lainvalvontatyö hyödyttää tosiaankin tuntuvasti sekä yhdysvaltalaisia että ulkomaisia kuluttajia. Esimerkiksi liittovaltion kauppakomissiosta annetun lain 5 §:ään liittyvät lainvalvontatoimet ovat suojanneet samalla tavalla sekä yhdysvaltaisten että ulkomaisten kuluttajan yksityisyyttä. Asiassa, joka pantiin vireille Accusearch-nimistä datavälittäjää vastaan, kauppakomissio väitti, että yhtiön toiminta, jossa se myi luottamuksellisia puhelutietoja kolmansille osapuolille ilmoittamatta asiasta kuluttajille tai hankkimatta näiden hyväksyntää, oli liittovaltion kauppakomissiosta annetun lain 5 §:n vastainen sopimaton käytäntö. Accusearch myi tietoja, jotka koskivat sekä yhdysvaltalaisia että ulkomaisia kuluttajia⁽¹⁾. Tuomioistuimien antoi Accusearchille määräyksen, jossa se kielsi yhtiötä muun muassa markkinoimasta tai myymästä kuluttajien henkilötietoja ilman näiden kirjallista lupaa, ellei kyseisiä tietoja ollut saatu laillisesti julkisista lähteistä. Tuomioistuimien määräsi yhtiön palauttamaan saamaansa hyötyä lähes 200 000 Yhdysvaltojen dollaria⁽²⁾.

Kauppakomission TRUSTe:n kanssa saavuttama sovinto on toinen esimerkki. Se varmistaa, että kuluttajat, mukaan lukien Euroopan unionin kuluttajat, voivat luottaa lausumiin, joita maailmanlaajuinen itsesääntelyorganisaatio antaa tekemistään kotimaisten ja ulkomaisten verkkopalveluiden tarkastuksista ja varmennuksista⁽³⁾. On tärkeää huomata, että meidän TRUSTe:hen kohdistuneilla toimillamme lujitettiin yksityisyyteen liittyvää itsesääntelyjärjestelmää yleisemminkin, sillä niillä varmistettiin sellaisten yksiköiden vastuuvollisuus, joilla on tärkeä asema itsesääntelyjärjestelmissä, myös rajat ylittävissä yksityisyydensuojajärjestelmissä.

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

C. Safe harbor -järjestelmän valvonta

Osana yksityisyyden suojan ja tietoturvallisuuden valvonnan ohjelmaansa liittovaltion kauppakomissio on pyrkinyt suojaamaan EU:n kuluttajia myös lainvalvontatoimilla, jotka koskevat safe harbor -ohjelman rikkomuksia. Liittovaltion kauppakomissio on pannut vireille 39 safe harbor -ohjelmaan liittyvää lainvalvontaintoa: 36 väitettyä virheellistä väitettä, jotka koskivat varmennusta, ja kolme tapausta (Googlea, Facebookia ja Myspacea vastaan), joissa oli kysymys safe harbor -ohjelman yksityisyydensuojaperiaatteiden rikkomuksesta⁽⁴⁾. Nämä tapaukset osoittavat varmennusten täytäntöönpanokelpoisuuden ja periaatteiden rikkomisen seuraukset. Googlelle, Facebookille ja Myspacelle annetuissa 20-vuotuisissa suostumusmääräyksissä vaaditaan, että yhtiöt toteuttavat laajamittaisia yksityisyydensuojaohjelmia. Kyseiset ohjelmat on suunniteltava siten, että niillä voidaan kohtuullisella tavalla hallita nykyisten ja uusien tuotteiden ja palveluiden kehittämiseen ja hallinnoimiseen liittyviä yksityisyyssriskejä sekä suojata henkilötietojen yksityisyyttä ja luottamuksellisuutta. Määräyksissä edellytetyissä kattavissa yksityisyydensuojaohjelmissa on määriteltävä olennaiset odotettavissa olevat riskit ja selostettava valvontamenetelmät, joilla riskejä hallitaan. Yhtiöiden on myös järjestettävä yksityisyydensuojaohjelmiansa jatkuva, riippumaton arviointi, jonka tulokset on toimitettava liittovaltion kauppakomissiolle. Määräyksissä kielletään kyseisiä yhtiöitä myös antamasta harhaanjohtavia tietoja tietosuojakäytännöistään ja osallistumisestaan yksityisyydensuoja- tai tietoturvajärjestelyihin. Kieltoa sovellettaisiin näiden yhtiöiden toimiin ja käytäntöihin myös uudessa Privacy Shield -järjestelyssä. Liittovaltion kauppakomissio voi valvoa näiden määräysten noudattamista hakemalla siviilioikeudellisten seuraamusten määräämistä. Google itse asiassa maksoi ennätyskelliset

⁽¹⁾ Ks. Kanadan yksityisyysskomissaarin toimisto, Kanadan yksityisyydensuojalain (PIPEDA) nojalla Accusearch, Inc.:ä (joka harjoittaa liiketoimintaa nimellä Abika.com) vastaan tehty valitus, osoitteessa https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Kanadan tietosuojavaltuutetun toimisto toimitti *amicus curiae* -kirjelmän pyytäen liittovaltion kauppakomissiota ryhtymään toimiin sekä teki oman tutkimuksensa, jossa tultiin siihen tulokseen, että Accusearchin käytännöt rikkoivat myös Kanadan lakia.

⁽²⁾ Ks. Liittovaltion kauppakomissio v. Accusearch, Inc., No. 06CV015D (Wyomingin piirituomioistuimien, 20.12.2007), aff'd 570 F.3d 1187 (10. Cir. 2009).

⁽³⁾ Ks. asia True Ultimate Standards Everywhere, Inc., No. C-4512 (Liittovaltion kauppakomissio, 12.3.2015) (päätos ja määräys), saatavilla osoitteessa <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>

⁽⁴⁾ Ks. asia Google, Inc., No. C-4336 (Liittovaltion kauppakomissio, 13.10.2011) (päätos ja määräys), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; asia Facebook, Inc., No. C-4365 (Liittovaltion kauppakomissio, 27.7.2012) (päätos ja määräys), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; asia Myspace LLC, No. C-4369 (Liittovaltion kauppakomissio, 30.8.2012) (päätos ja määräys), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>

22,5 miljoonan Yhdysvaltojen dollarin siviilioikeudelliset seuraamukset vuonna 2012 saadaksesen päätökseen kauppakomission määräyksen rikkomista koskeneiden väitteiden käsittelyn. Niinpä näillä liittovaltion kauppakomission hankkimilla määräyksillä suojellaan maailmanlaajuisesti yli miljardia kuluttajaa, joista sadat miljoonat asuvat Euroopassa.

Liittovaltion kauppakomission valvontatoimissa on keskitytty myös totuudenvastaisiin, vilpillisiin tai harhaanjohtaviin väitteisiin, jotka koskevat osallistumista safe harbor -ohjelmaan. Kauppakomissio ottaa nämä väitteet vakavasti. Esimerkiksi asiassa liittovaltion kauppakomissio v. Karnani kauppakomissio ryhtyi vuonna 2011 toimiin yhdysvaltalaisesta verkkokauppiasta vastaan. Kauppakomissio väitti, että verkkokauppias ja hänen yhtiönsä saivat brittiläiset kuluttajat uskomaan, että yhtiö oli sijoittautunut Yhdistyneeseen kuningaskuntaan. Kauppias oli muun muassa käyttänyt .uk -verkkotunnusta ja esittänyt hinnat Britannian valuutassa ja tehnyt viittauksia Yhdistyneen kuningaskunnan postijärjestelmään⁽¹⁾. Kun kuluttajat vastaanottivat tuotteet, he totesivat kuitenkin, että oli peritty odottamattomia tuontitulleja, takuut eivät olleet voimassa Yhdistyneessä kuningaskunnassa ja kauppahinnan palauttamisesta perittiin kuluja. Liittovaltion kauppakomissio syytti vastaajia myös siitä, että he olivat harhautaneet kuluttajia osallistumisestaan safe harbor -ohjelmaan. On huomionarvoista, että kaikki uhriksi joutuneet kuluttajat olivat Yhdistyneestä kuningaskunnasta.

Monet muista hoitamistamme tapauksista, jotka koskivat safe harbor -ohjelman valvontaa, liittyivät organisaatioihin, jotka olivat liittyneet safe harbor -ohjelmaan ja sittemmin laiminlyöneet vuotuisen varmennuksensa mutta jotka edelleen kuitenkin väittivät olevansa ohjelman jäseniä. Kuten jäljempänä selostetaan, liittovaltion kauppakomissio sitoutuu puuttumaan myös sellaisiin totuudenvastaisiin väitteisiin, jotka koskevat osallistumista Privacy Shield -järjestelyyn. Tämä strateginen lainvalvontatoiminta täydentää kauppaministeriön entistä voimallisempia toimia, joilla tarkastetaan varmennuksia ja uudelleenvarmennuksia koskevien ohjelman vaatimusten noudattamista, joilla valvotaan periaatteiden noudattamista, myös järjestelyn osallistujille lähetettävien kyselylomakkeiden avulla, ja joilla pyritään havaitsemaan totuudenvastaiset väitteet osallistumisesta järjestelyyn ja järjestelyn varmennusmerkin väärinkäyttö⁽²⁾.

II. ETUSIJAN ANTAMINEN VALITUSTEN KÄSITTELEMISELLE JA TUTKIMUKSET

Samalla tavalla kuin safe harbor -ohjelmassa, liittovaltion kauppakomissio antaa myös Privacy Shield -järjestelyssä etusijan EU:n jäsenvaltioista toimitettaville valituksille. Annamme etusijan myös valituksille, jotka koskevat Privacy Shield -järjestelyn itsesääntelyä koskevien suuntaviivojen noudattamatta jättämistä ja jotka yksityisyyden suojan itsesääntelystä vastaavat elimet ja muut riippumattomat riitojen ratkaisuelimet ovat siirtäneet kauppakomission käsiteltäviksi.

Jotta valitusten toimittaminen EU:n jäsenvaltioista olisi järjestelyssä helpompaa, liittovaltion kauppakomissio laatii parhaillaan vakioitua valitusten toimitusprosessia ja antaa EU:n jäsenvaltioille opastusta siitä, millaista tietoa kauppakomissio voisi parhaiten hyödyntää valitusten käsittelyssä. Osana tätä työtä liittovaltion kauppakomissio nimeää virastostaan yhteyspisteen EU:n jäsenvaltioilta tulevia valituksia varten. Tämä on erittäin hyödyllistä silloin kun valituksen toimittava viranomainen on tutkinut väitetyn rikkomuksen alustavasti ja pystyy tekemään liittovaltion kauppakomission kanssa yhteistyötä tutkimuksen aikana.

Kun liittovaltion kauppakomissio vastaanottaa valituksen EU:n jäsenvaltiolta tai itsesääntelyorganisaatiolta, se voi ryhtyä useampaankin toimenpiteeseen asian hoitamiseksi. Me voimme esimerkiksi tarkastaa yrityksen tietosuojaperiaatteet, hankkia lisätietoja suoraan yritykseltä tai kolmansilta osapuolilta, tehdä seurantatyötä yhdessä valituksen toimittaneen viranomaisen kanssa, arvioida, noudattaako rikkomus jotain kaavaa tai koskeeko se suurta määrää kuluttajia, päätellä, koskeeko valitus asioita, jotka kuuluvat kauppaministeriön toimialueeseen, arvioida, olisiko kuluttajien ja yritysten kouluttamisesta hyötyä ja tarvittaessa panna vireille lainvalvontamenettely.

Liittovaltion kauppakomissio sitoutuu myös tietojen vaihtamiseen valituksia toimittaneiden valvontaviranomaisten kanssa ja muun muassa tiedottamaan valitusten käsittelyn vaiheesta noudattaen luottamuksellisuutta koskevia lakeja ja rajoituksia. Sikäli kuin vastaanotettujen valitusten määrä ja laatu sallivat, annetaan myös valituksia koskeva arvio, joka sisältää muuan muassa kuvauksen keskeisistä asiaan liittyvistä kysymyksistä ja liittovaltion kauppakomission toimivaltansa rajoissa vireille panemista lakien rikkomusta koskevista toimista. 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

⁽¹⁾ Ks. Liittovaltion kauppakomissio v. Karnani, No. 2:09-cv-05276 (Kalifornian piirituomioistuimien 20.5.2011) (vahvistettu lopullinen määräys), saatavilla osoitteessa <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; ks. myös Lesley Fair, FTC Business Center Blog, Around the World in Shady Ways, <https://www.ftc.gov/blog/2011/06/around-world-shady-ways> (9.6.2011).

⁽²⁾ Ks. kansainvälisen kaupan osastossa toimivan kansainvälisestä kaupasta vastaavan vt. alivaltiosihteeri Ken Hyattin kirje oikeus-, kuluttaja- ja tasa-arvoasioista vastaavalle komissaarille Věra Jourovälle.

pyytää tietoa valituksen käsittelyvaiheesta siinä tarkoituksessa, että se voi 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 lainvalvonnassa. 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, joiden kieltämät menettelyt ovat olennaisilta osiltaan samanlaisia kuin liittovaltion kauppakomission valvomien lakien kieltämät menettelyt ⁽¹⁾. 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 ⁽²⁾.

Sen lisäksi että liittovaltion kauppakomissio asettaa etusijalle Privacy Shield -järjestelyyn liittyvät valitukset, jotka se vastaanottaa EU:n jäsenvaltioilta ja järjestelyyn kuuluvilta yksityisyyden suojan itsesääntelyorganisaatioilta ⁽³⁾, se sitoutuu tarvittaessa tutkimaan järjestelyn rikkomuksia omasta aloitteestaan erilaisia välineitä käyttäen.

Liittovaltion kauppakomissio on reilusti yli kymmenen vuoden ajan noudattanut määrätietoista tutkimusohjelmaa, jonka kohteena ovat olleet kaupallisia organisaatioita koskevat yksityisyydensuoja- ja tietoturva-asiat. Kauppakomissio on osana näitä tutkimuksia selvittänyt rutiinimaisesti, onko tutkimuksen kohteena oleva yksikkö esittänyt safe harbor -ohjelmaa koskevia lausumia. Jos se on esittänyt niitä ja tutkimuksessa on tullut ilmi, että safe harbor -ohjelman yksityisyydensuoja-periaatteita on ilmeisesti rikottu, liittovaltion kauppakomissio on ottanut ohjelman rikkomusvälttämisen osaksi lainvalvontatoimiaan. Me jatkamme tätä ennakoivaa lähestymistapaa uudessa järjestelyssä. On tärkeää huomata, että liittovaltion kauppakomissio tekee huomattavasti useampia tutkimuksia kuin lopulta tulee julki lainvalvontatoimina. Monet tutkimukset lopetetaan, koska tutkijat eivät havaitse, että lakia olisi ilmeisesti rikottu. Koska liittovaltion kauppakomission tutkimukset eivät ole julkisia ja ne ovat luottamuksellisia, tutkimuksen lopettamista ei useinkaan julkaista.

Lähes 40 safe harbor -ohjelmaan liittyvää lainvalvontainta, jotka liittovaltion kauppakomissio on pannut vireille, osoittavat, että kauppakomissio on sitoutunut valvomaan ennakoivasti rajat ylittävien yksityisyydensuojaohjelmien noudattamista. Kauppakomissio tutkii mahdollisia Privacy Shield -järjestelyn rikkomuksia osana säännöllisiä yksityisyydensuoja- ja tietoturvatutkimuksia.

III. PUUTTUMINEN TOTUUDENVASTAISIIIN TAI VILPILLISIIN VÄITTEISIIN OSALLISTUMISESTA PRIVACY SHIELD -JÄRJESTELYYN

Kuten edellä on selostettu, liittovaltion kauppakomissio ryhtyy toimiin sellaisia yksiköitä vastaan, jotka esittävät virheellisiä lausumia osallistumisestaan järjestelyyn. Kauppakomissio antaa etusijan kauppaministeriöstä tuleville valituksille, joissa ministeriö on todennut, että organisaatio väittää perusteettomasti osallistuvansa järjestelyyn tai käyttävä luvatta jotain järjestelyn varmennusmerkkiä.

Lisäksi on todettava, että jos organisaatio sitoutuu noudattamaan Privacy Shield -järjestelyn periaatteita tietosuojaperiaatteissaan, se, että organisaatio ei rekisteröidy kauppaministeriössä tai että se laiminlyö rekisteröinnin voimassa pitämisen, ei sinänsä itsestään selvästi vapauta organisaatiota lainvalvontatoimilta, joihin liittovaltion kauppakomissio ryhtyy organisaation antamien sitoumusten vuoksi.

⁽¹⁾ 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(j)(3). Kilpailulakien valvonta ei kuulu näiden valtuuksien soveltamisalaan.

⁽²⁾ Esimerkiksi varainhoitovuosina 2012–2015 liittovaltion kauppakomissio käytti verkkoturvallisuuslain mukaisia valtuuksiaan jakamalla tietoa vastauksena lähes 60:een ulkomaiselta virastolta tulleeneseen pyyntöön ja tekemällä lähes 60 siviilioikeudellista tutkimuspyyntöä (tämä vastaa hallinnollista haastetta, administrative subpoena) avustaakseen 25 ulkomaisessa tutkimuksessa.

⁽³⁾ Vaikka liittovaltion kauppakomissio ei ratkaise eikä sovitele yksittäisiä kuluttajien tekemiä valituksia, se vahvistaa antavansa etusijan Privacy Shield -järjestelyä 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 tutkimuskohteita. EU:n alueella asuvat henkilöt voivat jättää valituksen liittovaltion kauppakomissiolle käyttämällä samaa valitusjärjestelmää kuin Yhdysvaltojen kansalaiset, osoitteessa www.ftc.gov/complaint. EU:n alueella asuvien henkilöiden kannalta saattaa olla hyödyllisintä jättää yksittäiset Privacy Shield -järjestelyä koskevat valitukset oman jäsenvaltionsa tietosuojaviranomaiselle tai vaihtoehtoiselle riitojenratkaisuelimelle.

IV. MÄÄRÄYSTEN NOUDATTAMISEN VALVONTA

Liittovaltion kauppakomissio vahvistaa myös sitoumuksensa, jonka mukaan se valvoo lainvalvontamääräysten noudattamista varmistaakseen Privacy Shield -järjestelyn noudattamisen.

Me valvomme järjestelyn noudattamista siten, että tuleviin kauppakomission määräyksiin, jotka koskevat Privacy Shield -järjestelyä, sisällytetään erilaisia soveltuvia kieltoehtoja. Silloin kun liittovaltion kauppakomission lainvalvontatoimet perustuvat Privacy Shield -järjestelyä tai muita yksityisyydensuojaohjelmia koskeviin virheellisiin lausumiin, määräyksessä kielletään esittämästä näitä lausumia.

Liittovaltion kauppakomission tapaukset, jotka liittyvät alkuperäisen safe harbor -ohjelman valvontaan, ovat valaisevia. Tapauksia, joissa oli väitetty totuudenvastaisesti tai vilpillisesti, että organisaatiolla oli safe harbor -varmennus, oli 36. Kaikissa näitä tapauksia koskevista määräyksistä kielletään vastaajaa esittämästä virheellisiä lausuntoja osallistumisestaan safe harbor -ohjelmaan tai muuhun yksityisyydensuoja- tai tietoturvaohjelmaan ja vaaditaan vastaajaa toimittamaan liittovaltion kauppakomissiolle määräyksen noudattamisen todentava raportti. Tapauksissa, joissa oli kyse safe harbor -ohjelman yksityisyydensuojaperiaatteiden rikkomuksesta, yrityksiä pyydettiin panemaan täytäntöön kattavat yksityisyydensuojaohjelmat ja hankkimaan riippumattomalta kolmannelta osapuolelta arvio kyseisistä ohjelmista joka toinen vuosi 20 vuoden ajan ja toimittamaan arviot liittovaltion kauppakomissiolle.

Jos liittovaltion kauppakomission hallinnollisia määräyksiä rikotaan, voidaan siviilioikeudellisina seuraamuksina määrätä enintään 16 000 Yhdysvaltojen dollaria rikkomusta kohti tai, jos rikkomus jatkuu, 16 000 dollaria päivää kohti ⁽¹⁾. 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 safe harbor -ohjelman määräyksiä noudatetaan, kuten se tekee kaikkien määräystensä osalta. Liittovaltion kauppakomissio ottaa yksityisyyden suojaan ja tietoturvallisuuteen liittyvien määräystensä valvonnan vakavasti ja panee tarvittaessa kanteita vireille määräysten noudattamisen varmistamiseksi. Kuten edellä on todettu, esimerkiksi Google maksoi 22,5 miljoonaa Yhdysvaltojen dollaria siviilioikeudellisina seuraamuksina saadakseen päätökseen sellaisten väitteiden käsittelyn, joiden mukaan se oli rikkonut liittovaltion kauppakomission määräyksiä. On tärkeää huomata, että liittovaltion kauppakomission määräyksellä suojellaan kaikkia yrityksen kanssa asioivia kuluttajia ympäri maailman eikä pelkästään valituksen jättäneitä kuluttajia.

Lopuksi on todettava, että liittovaltion kauppakomissio pitää verkossa yllä luetteloa yrityksistä, joille on annettu määräys joko safe harbor -ohjelman tai uuden Privacy Shield -järjestelyn valvonnan yhteydessä ⁽²⁾. Lisäksi Privacy Shield -järjestelyn periaatteet edellyttävät nyt, että jos järjestelyyn osallistuvalla organisaatiolla annetaan periaatteiden rikkomukseen perustuva tuomioistuimen tai liittovaltion kauppakomission määräys, organisaation on julkistettava luottamuksellisuutta koskevien lakien ja asetusten rajoissa kaikki järjestelyyn liittyvät osat sellaisista sääntöjen noudattamista koskevista kertomuksista tai arviointikertomuksista, jotka on toimitettu liittovaltion kauppakomissiolle.

V. YHTEYDET EUROOPAN TIETOSUOJAVIRANOMAIISIIN JA VALVONTAYHTEISTYÖ NIIDEN KANSSA

Liittovaltion kauppakomissio katsoo, että Euroopan tietosuojaviranomaisilla on merkittävä tehtävä varmistettaessa Privacy Shield -järjestelyn periaatteiden noudattamista, ja kauppakomissio haluaa lisätä keskinäistä konsultointia ja lainvalvontayhteistyötä. Sen lisäksi että liittovaltion kauppakomissio kuulee Euroopan tietosuojaviranomaisia, kun se käsittelee näiden toimittamia yksittäisiä valituksia, kauppakomissio sitoutuu osallistumaan säännöllisiin kokouksiin 29 artiklan työryhmän edustajien kanssa keskustellakseen yleisesti, kuinka järjestelyä koskevaa lainvalvontayhteistyötä voitaisiin parantaa. Lisäksi liittovaltion kauppakomissio osallistuu kauppaministeriön, Euroopan komission ja 29 artiklan työryhmän edustajien ohella järjestelyn 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. Erityisesti on mainittava, että liittovaltion kauppakomissio käynnisti yhdessä Euroopan unionista ja eri puolilta maailmaa tulevien lainvalvontakumppaniensa kanssa viime vuonna hälytysjärjestelmän jakaakseen tutkimuksia koskevaa tietoa ja edistääkseen lainvalvonnan koordinaatiota. Hälytysjärjestelmä on toteutettu maailmanlaajuisessa yksityisyyden suojaa koskevan valvonnan verkostossa (Global Privacy Enforcement Network, jäljempänä 'GPEN'). GPEN-hälytysjärjestelmä voisi olla erityisen hyödyllinen Privacy Shield -järjestelyssä. Liittovaltion kauppakomissio ja Euroopan tietosuojaviranomaiset voisivat hyödyntää sitä Privacy Shield -järjestelyyn liittyvien ja muiden tutkimusten koordinoimisessa. Sitä voitaisiin myös pitää ensimmäisenä vaiheena tiedon jakamisessa, jotta kuluttajien yksityisyyttä suojattaisiin koordinoitusti ja entistä tehokkaammin. Odotamme innolla, että voimme jatkaa

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

⁽²⁾ Ks. Liittovaltion kauppakomissio, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251

yhteistyötä asianomaisten EU:n viranomaisten kanssa, jotta GPEN-hälytysjärjestelmä saataisiin käyttöön laajemmin ja jotta voisimme kehittää muitakin välineitä parantaaksemme lainvalvontayhteistyötä yksityisyydensuojatapauksissa, myös Privacy Shield -järjestelyn osalta.

Liittovaltion kauppakomissio vahvistaa mielihyvin sitoumuksensa valvoa uuden Privacy Shield -järjestelyn noudattamista. Odotamme innolla myös sitä, että yhteistyömme EU:n kollegojen kanssa jatkuu ja että suojellemme yhdessä kuluttajien yksityisyyttä Atlantin molemmin puolin.

Kunnioittavasti

Edith Ramirez

Puheenjohtaja

Liite A

Taustaa EU:n ja Yhdysvaltojen Privacy Shield -järjestelylle: Yhdysvaltojen yksityisyydensuoja- ja tietoturva ympäristö pääpiirteittäin

Suoja, joka annetaan EU:n ja Yhdysvaltojen Privacy Shield -järjestelyssä, on osa laajempaa yksityisyydensuojaa, jonka Yhdysvaltojen oikeudellinen järjestelmä kokonaisuutena tarjoaa. Ensinnäkin Yhdysvaltojen liittovaltion kauppakomissio toteuttaa määrätietoista yksityisyydensuoja- ja tietosuojaohjelmia, jota se soveltaa yhdysvaltalaisiin kauppakäytäntöihin, ja suojelee näin kuluttajia ympäri maailmaa. Toiseksi on todettava, että kuluttajien yksityisyyden suojaa ja tietoturvaa koskeva ympäristö on kehittynyt Yhdysvalloissa huomattavasti vuoden 2000 jälkeen, kun alkuperäinen EU:n ja Yhdysvaltojen safe harbor -ohjelma hyväksyttiin. Tuon hetken jälkeen on säädetty monia liittovaltion ja osavaltioiden lakeja, jotka koskevat yksityisyyden suojaa ja tietoturvaa. Myös julkisoikeudellisten ja yksityisoikeudellisten kanteiden määrä, joilla on pyritty yksityisyyden suojaan liittyvien oikeuksien toteuttamiseen, on lisääntynyt huomattavasti. Yhdysvaltojen laissa oleva kuluttajien yksityisyyttä ja tietoturvaa koskeva suoja, jota sovelletaan kaupallisiin tietojenkäsittelykäytäntöihin, on laaja-alainen, ja se täydentää suojaa, joka EU:n alueella asuville henkilöille annetaan uudessa järjestelyssä.

I. LIITTOVALTION KAUPPAKOMISSION YLEINEN YKSITYISYYDEN SUOJAA JA TIETOTURVAA KOSKEVA LAINVALVONTA-OHJELMA

Liittovaltion kauppakomissio on Yhdysvaltojen johtava kuluttajansuojavirasto, joka keskittyy kaupan alan yksityisyydensuojajaksymyksiin. Liittovaltion kauppakomissiolla on toimivaltuudet nostaa syytteitä sellaisten sopimattomien ja vilpillisten toimien ja käytäntöjen vuoksi, jotka rikkovat kuluttajien yksityisyyttä. Sillä on toimivalta valvoa myös kohdennettumia yksityisyyden lakeja, jotka suojaavat tiettyjä talous- ja terveystietoja, lapsia koskevia tietoja ja tietyissä asiakasvalintaa koskevista päätöksistä käytettyjä tietoja.

Liittovaltion kauppakomissiolla on vertaansa vailla oleva kokemus kuluttajien yksityisyyden suojan valvonnasta. Liittovaltion kauppakomissio on lainvalvontatoimissaan puuttunut lainvastaisiin käytäntöihin sekä verkossa että sen ulkopuolella. Liittovaltion kauppakomissio on lainvalvontatarkoituksissa esimerkiksi nostanut kanteita tunnettuja yhtiöitä, kuten Googlea, Facebookia, Twitteriä, Microsoftia, Wyndhamia, Oraclea, HTC:ta ja Snapchatia vastaan, mutta myös vähemmän tunnettuja yhtiöitä vastaan. Liittovaltion kauppakomissio on nostanut kanteita yrityksiä vastaan seuraavien epäilyjen perusteilla: yritys on lähettänyt kuluttajille roskapostia tai asentanut vakoiluohjelmia tietokoneisiin, laiminlyönyt kuluttajien henkilötietojen turvallisen säilyttämisen, jäljittänyt kuluttajia verkossa vilpillisessä tarkoituksessa, rikkonut lasten yksityisyyttä, kerännyt kuluttajien mobiililaitteita koskevaa tietoa lainvastaisesti ja laiminlyönyt sellaisten internetiin yhdistettyjen laitteiden tietoturvan, joissa on säilytetty henkilötietoja. Lainvalvontatoimien seurauksena annetuissa määräyksissä on tyypillisesti asetettu yritys liittovaltion kauppakomission jatkuvaan valvontaan 20 vuoden ajaksi, kielletty lain rikkominen vastedes ja asetettu yritykselle merkittävät rahamääräiset seuraamukset määräysten rikkomisesta ⁽¹⁾. On tärkeää huomata, että liittovaltion kauppakomission määräykset eivät suojele vain henkilöitä, jotka ovat ehkä tehneet valituksen ongelmasta, vaan ne suojelevat kaikkia kuluttajia, jotka ovat vastaisuudessa tekemisissä yrityksen kanssa. Rajat ylittävistä tilanteista on todettava, että liittovaltion kauppakomissiolla on toimivaltuudet suojella kaikkia maailman kuluttajia sellaisilta käytännöiltä, jotka toteutetaan Yhdysvalloissa ⁽²⁾.

Tähän mennessä liittovaltion kauppakomissio on nostanut kanteita yli 130 roskaposti- ja vakoiluohjelmatapauksessa, yli 120:ssä soittokiellon rikkomistapauksessa, yli 100 tapauksessa, jotka liittyvät luottokelpoisuusraportointia koskevaan Fair Credit Reporting Act -lakiin, lähes 60 tietoturvasuosiassa, yli 50:ssä yleistä yksityisyyden suojaa koskevassa tapauksessa, lähes 30 tapauksessa, jotka liittyvät rahoitusalan tietoturvasta annettuun Gramm-Leach-Bliley Act -lakiin, ja yli 20 tapauksessa, jotka liittyvät lasten yksityisyyden suojasta internetissä annetun COPPA-lain valvontaan ⁽³⁾. Näiden lainvalvontatoimien lisäksi liittovaltion kauppakomissio on myös toimittanut ja julkaissut varoituskirjeitä ⁽⁴⁾.

⁽¹⁾ Yritykselle, joka rikkoo liittovaltion kauppakomission määräystä, määrätään enintään 16 000 Yhdysvaltojen dollarin suuruinen siviilioikeudellinen seuraamus rikkomukselta tai, jos rikkomus jatkuu, 16 000 Yhdysvaltojen dollarin seuraamus päivältä. Ks. 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

⁽²⁾ Kongressi on nimenomaisesti vahvistanut liittovaltion kauppakomission toimivaltuuden ryhtyä oikeudellisiin toimenpiteisiin (mukaan lukien vahingonkorvauksen vaatiminen) kaikissa ulkomaankauppaan liittyvissä toiminnaissa ja käytännöissä, jos nämä 1) aiheuttavat tai todennäköisesti aiheuttavat Yhdysvalloissa vahinkoja, joiden syntymistä voidaan kohtuudella odottaa, tai jos 2) niihin liittyy olennaisia toimintaa Yhdysvalloissa. Ks. 15 U.S.C. § 45(a)(4).

⁽³⁾ Joissakin kauppakomission yksityisyyden suojaa ja tietosuojaa koskevista tapauksista väitetään, että yritys on harjoittanut sekä vilpillisiä että sopimattomia käytäntöjä. Näissä tapauksissa on myös toisinaan kyse useiden lakien väitetyistä rikkomuksista (kuten Fair Credit Reporting Act -laki, Gramm-Leach-Bliley Act -laki ja COPPA-laki).

⁽⁴⁾ Ks. esimerkiksi liittovaltion kauppakomission lehdistötiedote, jossa selostetaan varoitusta mahdollisesta COPPA-rikkomuksesta (Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations, 22. joulukuuta 2014), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa>; liittovaltion kauppakomission lehdistötiedote, jossa selostetaan varoitusta mahdollisesta tietojenvälittäjän yksityisyyden rikkomuksesta (Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations, 7. toukokuuta 2013), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations>; liittovaltion kauppakomission lehdistötiedote, jossa selostetaan varoitusta mahdollisesta luottokelpoisuusraportointia koskevasta rikkomuksesta (Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act, 3. huhtikuuta 2013), saatavilla osoitteessa <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may>

Osana vankkaa yksityisyyden suojaan liittyvää lainvalvontaan liittovaltion kauppakomissio on säännöllisesti tutkinut myös mahdollisia safe harbor -ohjelman rikkomuksia. Safe harbor -ohjelman hyväksymisen jälkeen liittovaltion kauppakomissio on tehnyt lukuisia oma-aloitteisia tutkimuksia, jotka koskevat ohjelman noudattamista, ja se on nostanut ohjelman rikkomisen vuoksi 39 kannetta yhdysvaltalaisia yrityksiä vastaan. Liittovaltion kauppakomissio jatkaa tätä ennakoivaa lähestymistapaa, ja uuden järjestelyn valvonnasta tulee yksi sen painopisteistä.

II. LIITTOVALTION JA OSAVALTIOIDEN TOIMET KULUTTAJIEN YKSITYISYYDEN SUOJAAMISEKSI

Safe harbor -ohjelman täytäntöönpanosta annetussa yleiskatsauksessa, joka on safe harbor -ohjelman tietosuojan riittävyttä koskevan Euroopan komission päätöksen liitteenä, annetaan tiivistelmä monista liittovaltion ja osavaltioiden laeista, jotka olivat voimassa, kun safe harbor -ohjelma hyväksyttiin vuonna 2000 ⁽¹⁾. Noihin aikoihin monissa liittovaltion laeissa – liittovaltion kauppakomissiosta annetun lain 5 §:n lisäksi – säädettiin henkilötietojen keräämisestä ja käyttämisestä kaupallisiin tarkoituksiin. Nämä lait koskivat johdollista viestintää (Cable Communications Policy Act), ajokortin haltijoiden henkilötietoja (Driver's Privacy Protection Act), sähköisen viestinnän tietosuojaa (Electronic Communications Privacy Act), sähköisiä maksunsiirtoja (Electronic Funds Transfer Act), luottokelpoisuusraportointia (Fair Credit Reporting Act), rahoitusalan tietoturva (Gramm-Leach-Bliley Act), taloudellisen yksityisyyden suojaa (Right to Financial Privacy Act), puhelinviestintää (Telephone Consumer Protection Act) sekä videofilmien vuokrausta ja ostoa (Video Privacy Protection Act). Myös monilla osavaltioilla oli vastaavaa lainsäädäntöä näillä aloilla.

Vuoden 2000 jälkeen sekä liittovaltion että osavaltioiden tasolla on edelleen parannettu kuluttajien yksityisyyden suojaa ⁽²⁾. Liittovaltiotasolla liittovaltion kauppakomissio on esimerkiksi muuttanut COPPA-sääntöjä vuonna 2013 antaakseen lasten henkilötiedoille tietyissä kohdin lisäsuojaa. Liittovaltion kauppakomissio on myös hyväksynyt kaksi sääntöä, joilla pannaan täytäntöön Gramm-Leach-Bliley Act -lakia, nimittäin yksityisyyssäännön (Privacy Rule) ja suojatoimisäännön (Safeguards Rule). Nämä säännöt edellyttävät, että rahoituslaitokset ⁽³⁾ julkistavat tiedonjakamiskäytäntönsä ja panevat täytäntöön kattavan tietoturvaohjelman suojatakseen kuluttajatietoja ⁽⁴⁾. Vastaavasti luottokelpoisuusraportointia koskevassa vuoden 2003 laissa (Fair and Accurate Credit Transactions Act, jäljempänä 'FACTA-laki') täydennetään pitkäaikaisia Yhdysvaltojen luottolakeja ja asetetaan tiettyjen arkaluonteisten taloudellisten tietojen peittämistä, jakamista ja hävittämistä koskevia vaatimuksia. Liittovaltion kauppakomissio on julkistanut joukon sääntöjä FACTA-lain täytäntöönpanemiseksi. Säännöt koskevat muun muassa seuraavia seikkoja: kuluttajien oikeus saada maksuton vuotuinen lainakertomus; vaatimukset, jotka asetetaan kuluttajia koskevien kertomusten turvalliselle hävittämiseksi; kuluttajien oikeus määrätä, että hänelle ei lähetetä tiettyjä luotto- ja vakuutusarvioita; kuluttajien oikeus määrätä, että tytäryhtiö ei saa käyttää kuluttajaa koskevia tietoja tuotteidensa ja palveluidensa markkinoinnissa; ja vaatimukset, joiden mukaan rahoituslaitosten ja luotonantajien on toteutettava ohjelmia henkilöllisyysvarkauksien havaitsemiseksi ja torjumiseksi ⁽⁵⁾. Lisäksi säännöt, joilla on pantu täytäntöön sairausvakuutusta koskevaa The Health Insurance Portability and Accountability Act -lakia, on tarkistettu vuonna 2013. Tällöin on lisätty suojatoimia, jotka koskevat henkilöiden terveystietojen yksityisyyttä ja turvaa ⁽⁶⁾. Myös säännöt, joissa suojellaan kuluttajia ei-toivotulta puhelinmyynniltä, automaattisilta soittoilta ja roskapostilta, ovat tulleet voimaan. Kongressi on myös säätänyt lakeja, jotka vaativat tiettyjä terveystietoja kerääviä yhtiöitä antamaan kuluttajille ilmoituksen, jos tietojen käytössä todetaan rikkomus ⁽⁷⁾.

Myös osavaltiot ovat säätäneet hyvin aktiivisesti yksityisyyden suojaan ja tietoturvaan liittyviä lakeja. Vuoden 2000 jälkeen 47 osavaltiota sekä Columbian piirikunta, Guam, Puerto Rico ja Yhdysvaltojen Neitsytsaaret ovat säätäneet lakeja,

⁽¹⁾ Ks. Yhdysvaltojen kauppaministeriö, safe harbor -ohjelman täytäntöönpanosta annettu yleiskatsaus, saatavilla osoitteessa https://build.export.gov/main/safeharbor/eu/eg_main_018481

⁽²⁾ Laajempi tiivistelmä Yhdysvalloissa annettavasta oikeusturvasta yksityisyyden suojaan liittyvissä asioissa on saatavilla teoksessa Daniel J. Solove & Paul Schwartz, Information Privacy Law (5. painos 2015).

⁽³⁾ Rahoituslaitokset määrittävät Gramm-Leach-Bliley Act -laissa hyvin väljästi, jotta määritelmän alaan kuuluisivat kaikki yritykset, joiden toiminnassa rahoitustuotteilla tai -palveluilla on "huomattava merkitys". Näihin kuuluvat esimerkiksi sekkejä rahaksi vaihtavat yritykset, lyhytaikaisia lainoja myöntävät yritykset, kiinteistölainavälittäjät, lainantajat, jotka eivät ole pankkeja, irtaimen tai kiinteän omaisuuden arvioijat ja ammattimaiset veroneuvojat.

⁽⁴⁾ Finanssipalveluiden kuluttajasuojasta annetussa vuoden 2010 laissa (Consumer Financial Protection Act, lyhennetään 'CFPA', julkaistu nimikkeellä Title X of Pub. L. 111-203, 124 Stat. 1955, annettu 21. heinäkuuta 2010, tunnetaan myös nimellä "Dodd-Frank Wall Street Reform and Consumer Protection Act") useimmat liittovaltion kauppakomission säädösvaltuudet, jotka sille annettiin Gramm-Leach-Bliley Act -laissa, siirrettiin finanssipalveluiden kuluttajasuojavirastolle (Consumer Financial Protection Bureau, jäljempänä 'CFPB'). Liittovaltion kauppakomission Gramm-Leach-Bliley Act -laissa annetut lainvalvontavaltuudet säilyivät, samoin kuin säädösvaltuudet Safeguards Rule -säännön osalta ja rajoitetut säädösvaltuudet Privacy Rule -säännön osalta (koskien autokauppiaita).

⁽⁵⁾ Finanssipalveluiden kuluttajasuojalain mukaisesti liittovaltion kauppakomissio jakaa Fair Credit Reporting Act -lain valvontaan liittyvät tehtävänsä CFPB:n kanssa, mutta säädösvaltuudet siirtyivät suurelta osin CFPB:lle (poikkeuksena varkauksien tunnistamiseen liittyvät Red Flags -sääntö ja tietojen hävittämiseen liittyvä Disposal Rule -sääntö).

⁽⁶⁾ Ks. liittovaltion lakikodifikaatio 45 C.F.R. osat 160, 162, 164.

⁽⁷⁾ Ks. esimerkiksi talouden elvyttämiseen liittyvä American Recovery & Reinvestment Act -laki vuodelta 2009 (Pub. L. No. 111-5, 123 Stat. 115 (2009)) ja tähän liittyvät asetukset, 45 C.F.R. §§ 164.404–164.414; 16 C.F.R. pt. 318.

joissa vaaditaan yrityksiä ilmoittamaan henkilöille näiden henkilötietoja koskevista tietoturvarikkomuksista ⁽¹⁾. Ainakin 32 osavaltiota ja Puerto Rico ovat säätäneet lakeja, joissa asetetaan henkilötietojen tuhoamista tai hävittämistä koskevia vaatimuksia ⁽²⁾. Jotkin osavaltiot ovat säätäneet myös yleisiä tietoturvalakeja. Lisäksi Kalifornia on säätänyt eräitä yksityisyyden suojaa koskevia lakeja, muun muassa lain, jossa vaaditaan yrityksiltä tietosuojaperiaatteiden laatimista ja jäljittämisen kieltokäytäntöjen ("Do Not Track") julkistamista ⁽³⁾, lain, jossa vaaditaan tietojen välittäjiltä suurempaa läpinäkyvyyttä ("Shine the Light") ⁽⁴⁾, sekä lain, jossa edellytetään alaikäisten käyttöön poistonäppäintä tietynlaisten sosiaalisen median tietojen pois pyyhkimiseksi ⁽⁵⁾. Näiden lakien ja muiden oikeusperustojen nojalla liittovaltion ja osavaltioiden hallinnot ovat määränneet huomattavia sakkoja yrityksille, jotka ovat laiminlyöneet kuluttajien henkilötietojen yksityisyyden suojan ja tietoturvan ⁽⁶⁾.

Myös yksityisten tahojen nostamat oikeusjutut ovat johtaneet voitollisiin tuomioihin ja sovintoratkaisuihin, jotka lisäävät kuluttajien yksityisyyden suojaa ja tietoturvaa. Esimerkiksi vuonna 2015 Target sitoutui maksamaan 10 miljoonaa Yhdysvaltojen dollaria osana sellaisten asiakkaiden kanssa tehtyä sovintoratkaisua, jotka väittivät, että heidän henkilökohtaiset taloustietonsa olivat vaarantuneet laajamittaisen tietoturvarikkomuksen seurauksena. Vuonna 2013 AOL sitoutui maksamaan 5 miljoonaa dollaria sovintoratkaisussa, joka tehtiin ryhmäkanteen saamiseksi päätökseen. Asiassa väitettiin, että kun satojentuhansien AOL:n jäsenten hakukysymystietoja oli luovutettu, tietojen tekeminen tunnistamattomiksi oli ollut riittämätöntä. Liittovaltion tuomioistuimien vahvisti lisäksi, että Netflix oli velvollinen maksamaan 9 miljoonaa dollaria asiassa, jossa väitettiin, että yhtiö oli säilyttänyt vuokraushistoriatietoja vuoden 1988 Video Privacy Protection Act -lain vastaisesti. Liittovaltion tuomioistuimet Kaliforniassa vahvistivat kaksi erillistä sovintoratkaisua, joissa asianosaisena oli Facebook. Toinen sovinto oli raha-arvoltaan 20 miljoonaa dollaria ja toinen 9,5 miljoonaa dollaria, ja oikeudenkäynnin kohteena olevat asiat liittyivät yhtiön käyttäjäasiakkaiden henkilötietojen keräämiseen, käyttämiseen ja jakamiseen. Lisäksi vuonna 2008 Kalifornian osavaltion tuomioistuin vahvisti 20 miljoonan dollarin sovintoratkaisun LensCraftersin kanssa asiassa, jossa oli kyse kuluttajien terveystietojen lainvastaisesta luovuttamisesta.

Kuten tämä tiivistelmä osoittaa, Yhdysvalloissa annetaan kuluttajien yksityisyydelle ja tietoturvalle kaiken kaikkiaan huomattavan tehokasta oikeussuojaa. Uusi Privacy Shield -järjestely, jolla varmistetaan mielekkäät suojatoimet EU:n alueella asuville henkilöille, on osa tätä laajempaa kokonaisuutta, jossa kuluttajien yksityisyyden suoja ja tietoturva ovat jatkossakin tärkeä painopiste.

⁽¹⁾ Ks. esimerkiksi National Conference of State Legislatures ("NCSL"), State Security Breach Notification Laws (4. tammikuuta 2016), saatavilla osoitteessa <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

⁽²⁾ NCSL, Data Disposal Laws (12.1.2016), saatavilla osoitteessa <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>

⁽³⁾ Ks. Kalifornian yrityksiä ja ammatteja koskeva laki, Cal. Bus. & Professional Code §§ 22575–22579.

⁽⁴⁾ Ks. Kalifornian siviililaki, Cal. Civ. Code §§ 1798.80–1798.84.

⁽⁵⁾ Ks. Kalifornian yrityksiä ja ammatteja koskeva laki, Cal. Bus. & Professional Code §§ 22580–22582.

⁽⁶⁾ Ks. yksityisyyden suojaa koskeva artikkeli Jay Cline, U.S. Takes the Gold in Doling Out Privacy Fines, Computerworld (17. helmikuuta 2014), saatavilla osoitteessa http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17&pageNumber=1

LIITE V

Yhdysvaltojen liikenneministerin Anthony Foxxin kirje

19. helmikuuta 2016

Komissaari Věra Jourová
Euroopan komissio
Rue de la Loi / Wetstraat 200
1049 Bryssel
Belgia

Viite: EU:n ja Yhdysvaltojen Privacy Shield -järjestely

Arvoisa komissaari Jourová

Yhdysvaltojen liikenneministeriö kiittää mahdollisuudesta selostaa tehtäviään, jotka liittyvät Privacy Shield -järjestelyn valvontaan. Privacy Shield -järjestely 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 safe harbor -ohjelman toteutumista kirjeessä, jonka se toimitti Euroopan komissiolle yli 15 vuotta sitten. Liikenneministeriö vakuutti kirjeessä, että se valvoisi tarmokkaasti safe harbor -ohjelman toteutumista. Liikenneministeriö pitää edelleen kiinni tästä sitoumuksestaan ja dokumentoi sen tässä kirjeessä.

Liikenneministeriö uudistaa sitoumuksensa erityisesti seuraavilla keskeisillä alueilla: 1) etusijan antaminen väitettyjen Privacy Shield -järjestelyn rikkomusten tutkimuksille; 2) asianmukaisten lainvalvontatoimien kohdistaminen yksiköihin, jotka esittävät totuudenvastaisia tai vilpillisiä väitteitä Privacy Shield -järjestelyn varmennuksista; ja 3) Privacy Shield -järjestelyn rikkomuksia koskevien määräysten valvonta ja julkistaminen. Annamme tietoa kustakin sitoumuksesta ja tarvittaessa taustoitamme liikenneministeriön tehtäviä kuluttajien yksityisyyden suojaamisessa ja Privacy Shield -järjestelyn valvonnassa.

I. TAUSTA

A. Liikenneministeriön toimivalta, joka liittyy yksityisyyden suojaamiseen

Ministeriö on vahvasti sitoutunut varmistamaan kuluttajien lentoyhtiöille ja lipunkirjoittajille antamien tietojen yksityisyyttä. Liikenneministeriön valtuudet tällä osa-alueella vahvistetaan Yhdysvaltojen laissa, ks. 49 U.S.C § 41712. Kyseisessä lainkohdassa lentoliikenteen harjoittajia ja lipunkirjoittajia kielletään käyttämästä lentokuljetusten myynnissä sopimatonta tai vilpillistä menettelyä tai sopimatonta kilpailumenettelyä, joka aiheuttaa tai todennäköisesti aiheuttaa vahinkoa kuluttajalle. Lainkohta vastaa liittovaltion kauppakomissiosta annetun lain 5 §:ää (15 U.S.C. § 45). Tulkintamme sopimatonta tai vilpillistä menettelyä koskevasta laista on se, että se kieltää lentoyhtiötä ja lipunkirjoittajaa 1) rikkomasta tietosuojaperiaatteitaan tai 2) keräämästä tai luovuttamasta yksityistä tietoa tavalla, joka on yleisen järjestyksen vastainen tai moraaliton tai aiheuttaa kuluttajalle merkittävää vahinkoa ilman että se olisi perusteltua minkään tasapainottavan edun vuoksi. Tulkitsemme lisäksi 41712 §:ää siten, että se kieltää lentoliikenteen harjoittajaa ja lipunkirjoittajaa 1) rikkomasta liikenneministeriön vahvistamia määräyksiä, joissa tietyt yksityisyyden suojaan liittyvät käytännöt todetaan sopimattomiksi tai vilpillisiksi tai 2) rikkomasta lakia lasten yksityisyyden suojasta internetissä (Children's Online Privacy Protection Act, jäljempänä 'COPPA-laki') tai liittovaltion kauppakomission määräyksiä, joilla COPPA-lakia pannaan täytäntöön. 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 Privacy Shield -järjestelyn periaatteita, ministeriöllä on oikeus käyttää 41712 §:n mukaisia toimivaltuuksia varmistaakseen, että periaatteita noudatetaan. Jos siis matkustaja antaa tietoja Privacy Shield -järjestelyn periaatteita noudattamaan sitoutuneelle lentoliikenteen harjoittajalle tai lipunkirjoittajalle ja jos lentoliikenteen harjoittaja tai lipunkirjoittaja ei noudata kyseisiä periaatteita, kyseessä on 41712 §:n rikkomus.

B. Lainvalvontakäytännöt

Ilmailualan lainvalvonnasta ja oikeudellisista menettelyistä vastaava ministeriön yksikkö (Office of Aviation Enforcement and Proceedings, jäljempänä 'valvontayksikkö') tutkii 41712 §:n soveltamisalaan kuuluvia tapauksia ja toimii niissä syyttäjänä. Se valvoo 41712 §:ssä säädettyä sopimattomien ja vilpillisten käytäntöjen kieltoa pääasiassa neuvottelujen avulla, valmistelemalla kieltomääräyksiä (cease and desist order) ja laatimalla siviilioikeudellisia seuraamuksia (civil penalty) koskevia päätösluonnoksia. Tiedot mahdollisista rikkomuksista tulevat yksikölle paljolti valituksista, joita yksikkö vastaanottaa yksityishenkilöiltä, matkatoimistoilta, lentoyhtiöiltä ja yhdysvaltalaisilta ja ulkomaisilta viranomaisilta. Kuluttajat voivat käyttää liikenneministeriön verkkosivustoa tehdäkseen yksityisyyden suojaan koskevan valituksen lentoyhtiötä tai lipunkirjoittajaa vastaan ⁽¹⁾.

Jos asiassa ei saavuteta kohtuullista ja asianmukaista sovintoa, valvontayksiköllä on toimivaltuudet panna vireille lainvalvontamenettely. Menettelyyn kuuluu istunto, jossa esitetään todisteita ja jota johtaa liikenneministeriön hallinto-lainkäytöstä vastaava tuomari. Tuomarilla on valtuudet antaa kieltomääräyksiä ja määrätä siviilioikeudellisia seuraamuksia. Seurauksena 41712 §:n rikkomisesta voi olla kieltomääräyksen antaminen ja enintään 27 500 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 valvontayksikön tutkimusten tuloksena ja joka hyödyttää suoraan kuluttajia (esimerkiksi siten, että heille maksetaan rahaa tai annetaan arvoseleitä) sen sijaan että rikkoja maksaisi vastaavan määrän rahamääräisinä seuraamuksina Yhdysvaltojen hallitukselle. Tätä on tapahtunut aiemmin ja voi sopivissa olosuhteissa tapahtua myös Privacy Shield -järjestelyn 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 kieltoa lentoliikennepalvelujen harjoittamisessa tai myynissä 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.

Liikenneministeriö valvoo myös, että lentoyhtiöt noudattavat ei-yhdysvaltalaisia kuluttajia koskevia kohdennettuja lakeja (esimerkiksi COPPA-lakia). 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. Yhdysvaltalaisien 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. Jos yhdysvaltalaiset tai ulkomaiset lentoyhtiöt, jotka harjoittavat toimintaa Yhdysvalloissa, rikkovat COPPA-lakia, liikenneministeriöllä on toimivalta ryhtyä lainvalvontatoimiin.

II. PRIVACY SHIELD -JÄRJESTELYN VALVONTA

Jos lentoyhtiö tai lipunkirjoittaja päättää osallistua Privacy Shield -järjestelyyn ja liikenneministeriö vastaanottaa valituksen, jossa väitetään, että lentoyhtiö tai lipunkirjoittaja on rikkonut järjestelyä, ministeriö toteuttaa määrätietoisesti seuraavat toimet valvoakseen järjestelyn noudattamista.

⁽¹⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>

A. Etusijan antaminen rikkomusväitteiden tutkinnalle

Liikenneministeriön valvontayksikkö tutkii jokaisen valituksen, jossa väitetään, että Privacy Shield -järjestelyä on rikottu (myös Euroopan tietosuojaviranomaisilta vastaanotetut valitukset), ja ryhtyy lainvalvontatoimiin, jos ilmenee, että rikkomuksesta on näyttöä. Lisäksi valvontayksikkö tekee yhteistyötä liittovaltion kauppakomission ja kauppaministeriön kanssa ja antaa etusijan sellaisten väitteiden tutkimiselle, joiden mukaan sääntelyn alaiset yksiköt eivät noudata Privacy Shield -järjestelyssä antamiaan yksityisyyden suojaa koskevia sitoumuksia.

Kun valvontayksikölle esitetään väite, jonka mukaan Privacy Shield -järjestelyä on rikottu, yksikkö 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, liittyykö rikkomuksiin jokin kaava 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 Privacy Shield -järjestelyn rikkomuksista, se koordinoi asiaa liittovaltion kauppakomission kanssa. Ministeriö ilmoittaa liittovaltion kauppakomissiolle ja kauppaministeriölle myös Privacy Shield -järjestelyä koskevien lainvalvontatoimien tuloksista.

B. Puuttuminen totuudenvastaisiin tai vilpillisiin väitteisiin osallistumisesta järjestelyyn

Liikenneministeriö sitoutuu jatkossakin tutkimaan Privacy Shield -järjestelyn rikkomuksia, muun muassa totuudenvastaisia tai vilpillisiä väitteitä osallistumisesta Privacy Shield -järjestelyyn. Ministeriö antaa etusijan kauppaministeriöstä tuleville valituksille, joissa ministeriö on todennut, että organisaatio väittää perusteettomasti osallistuvansa Privacy Shield -järjestelyyn tai käyttää luvatta järjestelyn varmennusmerkkiä.

Lisäksi on todettava, että jos organisaatio sitoutuu tietosuojaperiaatteissaan noudattamaan Privacy Shield -järjestelyn materiaalisia periaatteita, se, että organisaatio ei rekisteröidy kauppaministeriössä tai että se laiminlyö rekisteröinnin voimassa pitämisen, ei sinänsä itsestään selvästi vapauta organisaatioita lainvalvontatoimilta, joihin liikenneministeriö ryhtyy, jotta organisaatio noudattaisi järjestelyä koskevia sitoumuksiaan.

C. Privacy Shield -järjestelyn rikkomuksiin liittyvien lainvalvontamääräysten seuranta ja julkistaminen

Liikenneministeriön valvontayksikkö sitoutuu myös jatkossa – kun tämä on tarpeen Privacy Shield -järjestelyn noudattamisen varmistamiseksi – seuraamaan, että lainvalvontatarkoituksessa annettuja määräyksiä noudatetaan. Varsinkin siinä tapauksessa, että yksikkö antaa määräyksen, jonka mukaan lentoyhtiön tai lipunkirjoittajan on lopetettava Privacy Shield -järjestelyn ja 41712 §:n rikkomus ja pidätyttävä siitä myös tulevaisuudessa, yksikkö valvoo, että kyseinen toimija noudattaa kieltomääräystä. Yksikkö pitää lisäksi huolen siitä, että Privacy Shield -järjestelyyn liittyvissä asioissa annetut määräykset ovat saatavilla sen verkkosivustolla.

Odotamme innolla, että Privacy Shield -järjestelyä 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

Anthony R. Foxx

Liikenneministeri

LIITE VI

Kansallisen tiedusteluviraston päälakimiehen Robert Littin kirje

22. helmikuuta 2016

Justin S. Antonipillai
Neuvonantaja
Yhdysvaltojen kauppaministeriö
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Toinen apulaisvaltiosihteeri
Kauppaministeriön kansainvälisen kaupan osasto
1401 Constitution Ave., NW
Washington, DC 20230

Arvoisa Justin Antonipillai ja arvoisa Ted Dean

Viimeisten kahden ja puolen vuoden aikana Yhdysvallat on EU:n ja Yhdysvaltojen Privacy Shield -järjestelyä koskeissa neuvotteluissa antanut huomattavan määrän tietoa siitä, miten Yhdysvaltojen tiedusteluyhteisön signaalitiedustelu toimii. Tähän on sisällynyt tietoa kyseisiä toimintoja koskevasta oikeudellisesta kehyksestä, monikerroksisesta valvonnasta ja suuresta läpinäkyvyydestä sekä ylipäänsä yksityisyyden ja kansalaisvapauksien suojelusta. Näillä tiedoilla on pyritty avustamaan Euroopan komissiota sen päättäessä, ovatko suojatoimet riittäviä siltä osin kuin ne liittyvät Privacy Shield -järjestelyn periaatteisiin sovellettavaan kansallista turvallisuutta koskevaan poikkeukseen. Tässä asiakirjassa esitetään tiivistelmä annetuista tiedoista.

I. PPD-28 JA YHDYSVALTOJEN SIGNAALITIEDUSTELUTOIMINNAN TOTEUTTAMINEN

Yhdysvaltojen tiedusteluyhteisö kerää ulkomaantiedustelutietoja tarkoin hallitulla tavalla. Tällöin Yhdysvaltojen lakeja noudatetaan tarkasti, toiminnan valvonnassa on useita kerroksia ja toiminnassa keskitytään tärkeisiin ulkomaantiedustelutietoihin ja kansallisen turvallisuuden painopisteisiin. Yhdysvaltojen signaalitiedusteluaineiston keruuta säätelevät monet lait ja toimintaperiaatteet. Näitä ovat muun muassa seuraavat: Yhdysvaltojen perustuslaki, ulkomaantiedustelun valvontaa koskeva laki (Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 ja sitä seuraavat pykälät, jäljempänä 'FISA-laki'), toimeenpanoasetus 12333 ja sen täytäntöönpanosta annetut säännöt, presidentin ohjeet sekä useat menettelytavat ja ohjeet, joita ulkomaantiedustelun valvonnasta vastaava tuomioistuin (FISA Court, jäljempänä 'FISC-tuomioistuin') ja oikeusministeriö ovat hyväksyneet ja joissa vahvistetuilla täydentävillä säännöillä rajoitetaan ulkomaantiedustelutiedon keräämistä, säilyttämistä, käyttöä ja levittämistä ⁽¹⁾.

a. Yleiskatsaus PPD-28:aan

Presidentti Obama piti tammikuussa 2014 puheen, jossa hän hahmotteli tiettyjä uudistuksia Yhdysvaltojen signaalitiedustelutoimintaan, ja antoi tätä toimintaa koskevan presidentin määräyksen 28 (PPD-28) ⁽²⁾. Presidentti korosti, että Yhdysvaltojen signaalitiedustelutoiminta turvaa ei vain omaa maatamme ja omaa vapauttamme vaan myös muita maita ja niiden vapautta, mukaan lukien EU:n jäsenvaltioita, jotka nojautuvat Yhdysvaltojen tiedusteluelimien hankkimiin tietoihin omien kansalaistensa suojelemiseksi.

PPD-28:ssa vahvistetaan joukko periaatteita ja vaatimuksia, joita sovelletaan kaikkeen Yhdysvaltojen signaalitiedustelutoimintaan ja kaikkiin ihmisiin riippumatta heidän kansallisuudestaan tai asuinpaikastaan. Erityisesti siinä asetetaan tiettyjä vaatimuksia menettelytavoille, joita sovelletaan Yhdysvaltojen signaalitiedustelun avulla hankittujen, ei-yhdysvaltalaisia henkilöitä koskevien henkilötietojen keräämiseen, säilyttämiseen ja levittämiseen. Näitä vaatimuksia selostetaan tarkemmin jäljempänä, mutta tiivistettynä ne ovat seuraavat:

— PPD-28:ssa toistetaan se, että Yhdysvallat kerää signaalitiedustelutietoa ainoastaan laissa, toimeenpanoasetuksessa tai muussa presidentin määräyksessä annetun luvan mukaisesti.

⁽¹⁾ Lisätietoja Yhdysvaltojen ulkomaantiedustelutoiminnasta on julkisesti saatavilla IC on the Record -nimisellä verkkosivustolla (www.icontherecord.tumblr.com). Kyseessä on kansallisen tiedusteluviraston julkinen verkkosivusto, jolla pyritään lisäämään hallituksen tiedustelutoiminnan läpinäkyvyyttä.

⁽²⁾ Saatavilla osoitteessa <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

- PPD-28:ssa vahvistetaan menettelytavat sen varmistamiseksi, että signaalitiedustelua toteutetaan vain oikeutetun ja luvallisen kansallisen turvallisuuspyrkimyksen edistämiseksi.
- PPD-28:ssa edellytetään myös, että kun tietojen keräämistä signaalitiedustelun avulla suunnitellaan, yksityisyyteen ja kansalaisvapauksiin liittyvien seikkojen huomioon ottaminen on olennainen osa suunnittelua. Yhdysvallat ei varsinkaan kerää tiedustelutietoja tukahduttaakseen tai vaikeuttaakseen arvostelun tai eriävien mielipiteiden ilmaisemista tai saattaakseen ihmisiä huonompaan asemaan näiden etnisen alkuperän, rodun, sukupuolen, sukupuolisen suuntautumisen tai uskonnon perusteella tai hankkiakseen yhdysvaltalaisille yrityksille ja elinkeinoelämän aloille kaupallista kilpailuetua.
- PPD-28:ssa määrätään, että signaalitiedustelun on oltava niin räätälöityä kuin mahdollista ja että valikoimatonta signaalitiedustelutiedon keruuta voidaan käyttää vain erikseen lueteltuihin tarkoituksiin.
- PPD-28:ssa määrätään, että tiedusteluyhteisön on otettava käyttöön menettelytapa, joilla pyritään kohtuullisella tavalla minimoimaan signaalitiedustelun tuloksena kerättyjen henkilötietojen levitystä ja säilytystä ja joilla varsinkin laajennetaan eräät Yhdysvaltojen kansalaisten henkilötiedoille annetut suojatoimet koskemaan myös ei-yhdysvaltaisten henkilöiden henkilötietoja.
- Virastojen menettelytavat, joilla PPD-28 pannaan täytäntöön, on hyväksytty ja julkaistu.

On selvää, että tässä selostettuja menettelytapoja ja suojatoimia sovelletaan Privacy Shield -järjestelyyn. Kun tietoa on siirretty yhdysvaltalaisille yrityksille Privacy Shield -järjestelyssä tai missä tahansa muussa järjestelyssä, Yhdysvaltojen tiedusteluelimet voivat pyytää tuota tietoa yrityksiltä vain jos pyyntö on FISA-lain mukainen tai jos sen perustana on jokin kansallista turvallisuutta koskevasta kirjeestä (National Security Letter) säädetty laki (näitä lakeja selostetaan jäljempänä) ⁽¹⁾. Vahvistamatta tai kieltämättä tiedotusvälineissä esiintynyttä tietoa, jonka mukaan Yhdysvaltojen tiedusteluyhteisö keräisi Yhdysvaltoihin lähetettävää tietoa transatlanttisista kaapeista, todetaan lisäksi, että jos kyseistä tiedonkeruuta tapahtuisi, se tehtäisiin noudattaen tässä selostettuja rajoituksia ja suojatoimia, mukaan lukien PPD-28:n vaatimuksia.

b. Tiedonkeruun rajoitukset

PPD-28:ssa esitetään useita tärkeitä yleisperiaatteita, jotka koskevat tietojen keruuta signaalitiedustelussa:

- Signaalitiedustelutiedon keruun on perustuttava säädökseen tai presidentin hyväksyntään, ja se on toteutettava Yhdysvaltojen perustuslain ja lainsäädännön mukaisesti.
- Yksityisyyden suojan ja kansalaisvapauksien on oltava olennainen osa signaalitiedustelutoiminnan suunnittelua.
- Signaalitiedustelutietoja kerätään ainoastaan silloin, kun siihen on pätevä ulkomaantiedusteluun tai vastatiedusteluun liittyvä peruste.
- Yhdysvallat ei kerää signaalitiedustelutietoja tukahduttaakseen tai vaikeuttaakseen arvostelun tai eriävien mielipiteiden ilmaisemista.
- Yhdysvallat ei kerää signaalitiedustelutietoja saattaakseen ihmisiä huonompaan asemaan näiden etnisen alkuperän, rodun, sukupuolen, sukupuolisen suuntautumisen tai uskonnon perusteella.
- Yhdysvallat ei kerää signaalitiedustelutietoja hankkiakseen yhdysvaltalaisille yrityksille ja elinkeinoelämän aloille kaupallista kilpailuetua.
- Yhdysvaltojen signaalitiedustelun on *aina* oltava niin räätälöityä kuin mahdollista, ja siinä on otettava huomioon muiden tietolähteiden saatavuus. Tämä tarkoittaa muun muassa sitä, että signaalitiedustelutiedon keruu on aina kun mahdollista kohdennettua eikä valikoimatonta.

Vaativuudesta, jonka mukaan signaalitiedustelun on oltava niin räätälöityä kuin mahdollista, sovelletaan paitsi tapaan, jolla signaalitiedustelutietoa kerätään, myös itse tietoon, jota kerätään. Esimerkiksi kun tiedusteluyhteisö päättää, kerätäänkö

⁽¹⁾ Lainvalvonta- tai sääntelyvirastot voivat Yhdysvalloissa pyytää yrityksiltä tietoja tutkintatarkoituksiin muiden rikosoikeudellisten, siviilioikeudellisten tai sääntelyyn liittyvien valtuuksien nojalla, mutta nämä valtuudet eivät kuulu tämän asiakirjan soveltamisalaan, joka rajoittuu kansallista turvallisuutta koskeviin valtuuksiin.

signaalitiedustelutietoa, sen on otettava huomioon, onko muuta tietoa saatavilla, mukaan lukien diplomaattitieto ja julkinen tieto, ja sen on mahdollisuuksien mukaan annettava etusija näille muille tiedonhankintatavoille. Lisäksi tiedusteluyhteisön toimijoiden toimintaperiaatteisiin olisi sisällyttävä vaatimus, jonka mukaan keruu olisi mahdollisuuksien mukaan kohdennettava erityisiin ulkomaisiin tiedustelukohteisiin tai -aiheisiin erottelukijöiden avulla (esimerkiksi erityiset viestintävälineet, valintakriteerit ja tunnisteet).

On tärkeää nähdä komissiolle toimitetut tiedot kokonaisuutena. Päätöksiä siitä, mikä on "mahdollista" tai "käytännössä mahdollista", ei jätetä yksittäisten henkilöiden harkinnan varaan, vaan niihin sovelletaan toimintaperiaatteita, jotka virastot ovat vahvistaneet PPD-28:n nojalla ja jotka on julkistettu, sekä muita virastojen selostamia prosesseja⁽¹⁾. Kuten PPD-28:ssa todetaan, signaalitiedustelutiedon valikoimattomalla keruulla tarkoitetaan keruuta, joka tehdään teknisten tai operationaalisten syiden vuoksi käyttämättä erottelukijöitä (esimerkiksi erityisiä tunnisteita tai valintakriteerejä). Tältä osin PPD-28:ssa todetaan, että tiedusteluyhteisön toimijoiden on kerättävä valikoimatonta signaalitiedustelutietoa tietyissä olosuhteissa tunnistaakseen uusia tai syntymässä olevia uhkia ja hankkiakseen muuta elintärkeää kansalliseen turvallisuuteen liittyvää tietoa, joka on usein kätkettynä modernien maailmanlaajuisten yhteyksien suureen ja monimutkaiseen järjestelmään. Siinä todetaan myös, että valikoimaton signaalitiedustelutiedon kerääminen aiheuttaa yksityisyyden suojaan ja kansalaisvapauksiin liittyviä pulmia. Näin ollen PPD-28:ssa ohjataan tiedusteluyhteisö asettamaan etusijalle ratkaisuja, jotka mahdollistaisivat signaalitiedustelutiedon kohdennetun keruun valikoimattoman sijaan. Tiedusteluyhteisön toimijoiden olisi sen vuoksi tehtävä pikemminkin kohdennettuja kuin valikoimattomia signaalitiedusteluja aina, kun se on käytännössä mahdollista⁽²⁾. Näillä periaatteilla varmistetaan, että valikoimatonta tiedonkeruuta koskeva poikkeus ei kumoa pääsääntöä.

Käsite "kohtuus" on Yhdysvaltojen lainsäädännön keskeinen periaate. Kohtuusvaatimus tarkoittaa sitä, että tiedusteluyhteisön toimijoiden ei tarvitse ottaa käyttöön mitä tahansa teoriassa mahdollista toimenpidettä vaan että niiden on tasapainotettava oikeutetut yksityisyyden ja kansalaisvapauksien suojelun intressit signaalitiedustelutoiminnan käytännön vaatimusten kanssa. Myös tämän asian osalta virastot ovat vahvistaneet toimintaperiaatteita, ja niillä voidaan saada varmuutta siitä, että ilmaisu "kohtuullisella tavalla minimoidaan signaalitiedustelun tuloksena kerättyjen henkilötietojen levitystä ja säilytystä" ei heikennä yleisen säännön soveltamista.

PPD-28:ssa säädetään myös, että valikoimatonta signaalitiedustelutiedon keruuta voidaan käyttää ainoastaan kuuteen erityiseen tarkoitukseen: ulkovaltojen tiettyjen toimintojen havaitsemiseen ja torjuntaan; terrorismin torjuntaan; aseiden leviämisen estämiseen; kyberturvallisuuden vahvistamiseen; Yhdysvaltojen tai sen liittolaisten asevoimiin kohdistuvien uhkien havaitsemiseen ja torjuntaan; ja kansainvälisen rikollisuuden uhkien torjumiseen, mukaan luettuina pyrkimykset seuraamusten välttämiseen. Presidenttiä avustava kansallisen turvallisuuden neuvonantaja tarkastaa vuosittain kansallisen tiedusteluviraston johtajaa kuultuaan käyttötarkoitukset, joiden perusteella on sallittua kerätä valikoimatonta signaalitiedustelutietoa, ja arvioi, olisiko käyttötarkoituksiin tehtävä muutoksia. Kansallisen tiedusteluviraston johtaja julkistaa tämän luettelon niin laajasti kuin kansallinen turvallisuus huomioon ottaen on mahdollista. Tämän myötä valikoimattoman signaalitiedustelutiedon käyttöä rajoitetaan merkittävästi ja läpinäkyvästi.

Lisäksi tiedusteluyhteisön toimijat, jotka panevat täytäntöön PPD-28:aa, ovat vahvistaneet olemassa olevia analyyttisiä menetelmiä ja standardeja, jotka koskevat arvioimattomaan signaalitiedustelutietoon liittyviä tiedustelukysymyksiä⁽³⁾. Kun analyytikot laativat tiedustelukysymyksiä ja muita hakusanoja ja -tekniikoita, heidän on varmistettava, että niiden avulla tunnistettava tiedustelutieto on merkittävää pätevän ulkomaantiedustelu- tai lainvalvontatehtävän kannalta. Tässä tarkoituksessa tiedusteluyhteisön toimijoiden on kohdistettava henkilöitä koskevat tiedustelukysymykset sellaisiin signaalitiedustelutiedon lajeihin, joilla voidaan täyttää ulkomaantiedusteluun tai lainvalvontaan liittyvä tiedontarve, jotta kyseisen tiedontarpeen kannalta tarpeettomia henkilötietoja ei käytettäisi.

On tärkeää tähdentää, että Yhdysvaltojen tiedusteluyhteisön signaalitiedustelulla suorittama mahdollinen valikoimaton internetviestinnän tiedonkeruu kohdistuu vain pieneen osaan internetiä. Kuten edellä selostetaan, kohdennettujen pyyntöjen käytöllä lisäksi varmistetaan, että vain tiedot, joilla on mahdollisesti tiedusteluarvoa, tulevat analyytikoiden tutkittaviksi. Näillä rajoituksilla pyritään suojaamaan kaikkien henkilöiden yksityisyyttä ja kansalaisvapauksia riippumatta heidän kansalaisuudestaan tai asuinpaikastaan.

⁽¹⁾ Saatavilla osoitteessa www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Näillä menettelyillä toteutetaan tässä kirjeessä käsitellyt kohdentamis- ja räätälöintikäsitteet tavalla, joka vaihtelee tiedusteluyhteisön toimijasta toiseen.

⁽²⁾ Yhtenä esimerkkinä voidaan mainita kansallisen turvallisuusviraston menettelytapaohjeet, jotka on annettu PPD-28:n täytäntöönpanemiseksi. Menettelytapaohjeissa määrätään, että tiedonkeruu toteutetaan mahdollisuuksien mukaan käyttämällä yhtä tai useampaa valintakriteeriä, joiden avulla tiedonkeruu pyritään kohdistamaan erityisiin ulkomaantiedustelun kohteisiin (esimerkiksi johonkin tunnettuun kansainväliseen terroristiin tai terroristiryhmään) tai erityisiin ulkomaantiedustelun aiheisiin (esimerkiksi ulkomaisen vallan tai sen asiamiesten toteuttamaan joukkotuhoukseiden levittämiseen).

⁽³⁾ Saatavilla osoitteessa http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf

Yhdysvalloilla on pitkälle kehitettyjä menettelytapoja sen varmistamiseksi, että signaalitiedustelua toteutetaan ainoastaan kansalliseen turvallisuuteen liittyvien asianmukaisten tavoitteiden edistämiseksi. Presidentti vahvistaa ulkomaanti-edusteluun liittyvät kansakunnan ensisijaiset painopisteet vuosittain laajamittaisen ja virallisen virastojen välisen menettelyn jälkeen. Kansallisen tiedusteluviraston johtajan tehtävänä on muotoilla näistä tiedustelun painopisteistä kansallisia tiedusteluprioriteetteja koskeva kehys (National Intelligence Priorities Framework, jäljempänä 'tiedustelukehys'). PPD-28:ssa on lujitettu ja parannettu virastojen välistä menettelyä sen varmistamiseksi, että korkean tason päätöksentekijät käsittelevät ja hyväksyvät kaikki tiedusteluyhteisön tiedustelupainopisteet. Tiedusteluyhteisön määräyksessä nro 204 (Intelligence Community Directive, ICD 204) ⁽¹⁾ annetaan tarkempia ohjeita tiedustelukehyksestä, ja määräystä päivitettiin tammikuussa 2015 PPD-28:n vaatimusten sisällyttämiseksi siihen. Vaikka tiedustelukehys on luokiteltu salaiseksi, Yhdysvaltojen ulkomaanti-edustelun erityisiä painopisteitä käsitellään vuosittain kansallisen tiedusteluviraston johtajan laatimassa, ei-salaisessa koko maailman kattavassa uhka-arviossa (Worldwide Threat Assessment), joka on saatavilla myös ODN:n verkkosivustolla.

Tiedustelukehyksen painopistealueet esitetään melko yleisellä tasolla. Painopisteisiin sisältyy sellaisia aiheita kuin tiettyjen ulkomaisten vihollisten pyrkimykset hankkia ydinaseita ja ballistisia ohjuksia, huumausainekartellien rappioittavat vaikutukset ja ihmisoikeusrikkomukset tietyissä maissa. Lisäksi ne koskevat kaikkia tiedustelutoimia, eivät ainoastaan signaalitiedustelua. Organisaatio, joka on vastuussa siitä, että tiedustelukehys otetaan huomioon varsinaisessa signaaliti-edustelussa, on kansallinen signaalitiedustelukomitea (National Signals Intelligence Committee, SIGCOM). Se toimii kansallisen turvallisuusviraston piirissä. Kansallisen turvallisuusviraston johtaja on nimetty signaalitiedustelun toiminnalliseksi johtajaksi toimeenpanoasetuksessa 12333, ja hänen vastuullaan on valvoa ja koordinoida koko tiedusteluyhteisön signaalitiedustelua. Häntä valvovat tässä tehtävässä puolustusministeriö ja kansallisen tiedusteluviraston johtaja. Signaalitiedustelukomiteassa on edustajia kaikista tiedusteluyhteisön toimijoista, ja kun Yhdysvallat on pannut PPD-28:n täytäntöön täysimääräisesti, siinä on täysi edustus myös muista ministeriöistä ja virastoista, joilla on valvottavanaan signaalitiedustelun toimintaperiaatteisiin liittyviä intressejä.

Kaikki Yhdysvaltojen ministeriöt ja virastot, jotka hyödyntävät ulkomaanti-edustelutietoja, toimittavat tietojen keruuta koskevat pyyntönsä signaalitiedustelukomitealle. Signaalitiedustelukomitea tutkii pyynnöt, varmistaa, että ne ovat tiedustelukehyksen mukaisia, ja asettaa ne etusijajärjestykseen muun muassa seuraavilla perusteilla:

- Voiko signaalitiedustelun avulla saada hyödyllistä tietoa kyseisessä tapauksessa, vai onko olemassa parempia ja kustannustehokkaampia tietolähteitä, joilla tietotarve voidaan tyydyttää, kuten kuviin tai julkisiin lähteisiin perustuvat tiedot?
- Kuinka merkittävä tämä tietotarve on? Jos tavoite on korkealla sijalla tiedustelukehyksessä, se on useimmiten korkealla sijalla myös signaalitiedustelun painopisteissä.
- Millaista signaalitiedustelua voitaisiin käyttää?
- Onko tiedonkeruu mahdollisimman räätälöityä? Onko ajankäytöllisiä, maantieteellisiä tai muita rajoituksia?

Yhdysvaltojen signaalitiedusteluun liittyvät vaatimukset edellyttävät, että prosessissa kiinnitetään nimenomaista huomiota myös muihin tekijöihin, joita ovat seuraavat:

- Onko tiedonkeruun kohde tai keräämiseen käytetty menetelmä erityisen arkaluonteinen? Jos on, korkean tason päätöksentekijöiden on käsiteltävä asia.
- Aiheutuuko tiedonkeruusta perusteetonta riskiä yksityisyyden suojalle ja kansalaisvapauksille kohteen kansalaisuudesta riippumatta?
- Onko tarpeen lisätä tiedon levittämistä ja säilyttämistä koskevia suojatoimia yksityisyyden tai kansallisten turvallisuusetujen suojelemiseksi?

Menettelyn lopuksi signaalitiedustelukomitean vahvistama tiedustelupyynnöjen ensisijaisuusjärjestys toimitetaan kansallisen turvallisuusviraston koulutetulle henkilökunnalle, joka määrittää erityiset valintakriteerit, kuten puhelinnumerot tai sähköpostiosoitteet. Olettamuksena on, että niitä käyttämällä kyetään keräämään pyyntöjen ensisijaisuusjärjestystä vastaavia ulkomaanti-edustelutietoja. Kaikki valintakriteerit on tarkistettava ja hyväksyttävä ennen kuin ne syötetään kansallisen turvallisuusviraston tiedonkeruujärjestelmiin. Silloinkin se, kerätäänkö tietoja ja milloin niitä itse asiassa kerätään, riippuu kuitenkin osin muista seikoista kuten siitä, onko tietojen keräämiseen riittävästi resursseja.

⁽¹⁾ Saatavilla osoitteessa <http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>

Menettelyn avulla varmistetaan, että Yhdysvaltojen signaalitiedustelun kohteet vastaavat perusteltuja ja merkittäviä ulkomaantiedustelutiedon tarpeita. Ja kun tiedonkeruu toteutetaan FISA-lain nojalla, kansallisen turvallisuusviraston ja muiden virastojen on luonnollisesti noudatettava FISC-tuomioistuimen vahvistamia lisärajoituksia. Lyhyesti sanottuna kansallinen turvallisuusvirasto ja muut Yhdysvaltojen tiedusteluvirastot eivät päätä yksin mitä tietoja ne keräävät.

Tällä menettelyllä varmistetaan kaiken kaikkiaan, että korkean tason päätöksentekijät, jotka pystyvät parhaiten määrittämään Yhdysvaltojen ulkomaantiedustelun tietotarpeet, vahvistavat kaikki tiedustelutoiminnan painopisteet ja että kyseiset päätöksentekijät ottavat huomioon paitsi kyseisen tiedonkeruun mahdollisen arvon myös siihen liittyvät riskit, mukaan lukien riskit, jotka koskevat yksityisyyden suojaa, kansallisia taloudellisia etuja ja ulkosuhteita.

Sen tiedon osalta, joka siirretään Yhdysvaltoihin Privacy Shield -järjestelyssä, on todettava, että vaikka Yhdysvallat ei voi vahvistaa eikä kieltää, hyödyntääkö se joitakin nimenomaisia tiedustelumetodeja tai -operaatioita, PPD-28:n vaatimuksia sovelletaan kaikkiin Yhdysvaltojen toteuttamiin signaalitiedusteluoperaatioihin riippumatta kerättävän tiedon lajista tai lähteestä. Lisäksi olipa signaalitiedustelutiedon keruun luvallinen tarkoitus mikä hyvänsä, mukaan lukien ulkosuhteiden hoito tai kansallinen turvallisuus, rajoituksia ja suojatoimia sovelletaan kyseiseen keruuseen.

Yllä selostetut menettelyt osoittavat, että on selkeästi sitouduttu estämään mielivaltainen ja kohdentamaton signaalitiedustelutietojen keruu ja noudattamaan – hallituksemme korkeimmalta tasolta lähtien – kohtuuseriaa. PPD-28:ssa ja sen täytäntöönpanemiseksi annetuissa virastojen menettelytavoissa esitetään selkeämmin, mitä nykyisiä ja uusia rajoituksia sovelletaan tarkoituksiin, joihin Yhdysvallat kerää ja käyttää signaalitiedustelutietoja. Kyseisiä tarkoituksia myös kuvaillaan täsmällisemmin. Tämä antaa varmuuden siitä, että signaalitiedustelutoimintaa harjoitetaan nyt ja vastaisuudessa ainoastaan ulkomaantiedustelun oikeutettujen tavoitteiden edistämiseksi.

c. Tietojen säilyttämistä ja levittämistä koskevat rajoitukset

PPD-28:n 4 §:ssä vaaditaan, että jokaiseen tiedusteluyhteisön toimijaan sovelletaan nimenomaisia, tietojen säilyttämistä ja levittämistä koskevia rajoituksia, jotka koskevat signaalitiedustelussa hankittuja ei-yhdysvaltalaisen henkilöiden henkilötietoja ja jotka vastaavat Yhdysvaltojen kansalaisten henkilötietoja koskevia rajoituksia. Nämä säännöt on sisällytetty kaikkien tiedusteluyhteisön toimijoiden menettelytapoihin, jotka on vahvistettu helmikuussa 2015 ja jotka ovat julkisesti saatavilla. Jotta henkilötietoja voitaisiin säilyttää ja levittää ulkomaantiedustelutietona, niiden on täytettävä seuraavat edellytykset: niiden täytyy liittyä luvalliseen tiedustelutiedon tarpeeseen sen mukaan kuin edellä selostetussa tiedustelukehysprosessissa määritellään; on voitava kohtuudella olettaa, että ne ovat todisteita rikoksesta; tai niiden on täytettävä jokin muu vaatimus, jonka perusteella yhdysvaltalaisen henkilöiden henkilötietoja voidaan säilyttää toimeenpanoasetuksen 12333 2.3 §:n mukaisesti.

Tietoja, joiden osalta kyseiset edellytykset eivät täyty, ei saa säilyttää pidempään kuin viiden vuoden ajan, ellei kansallisen tiedusteluviraston johtaja nimenomaisesti päättää, että säilyttämisen jatkaminen on Yhdysvaltojen kansallisten turvallisuussetujen mukaista. Niinpä tiedusteluyhteisön toimijoiden on hävitettävä ei-yhdysvaltalaisen henkilön signaalitiedustelussa kerätyt tiedot viiden vuoden kuluessa keräämisestä, ellei esimerkiksi todeta, että tiedot ovat merkittäviä luvallisen ulkomaantiedustelun tietotarpeen kannalta, tai ellei kansallisen tiedusteluviraston johtaja – kuultuaan ODN:n kansalaisvapauksien suojasta vastaavan neuvonantajan samoin kuin yksityisyyden suojaan ja kansalaisvapauksiin liittyviä tehtäviä hoitavien viraston virkamiesten näkemykset – totea, että säilyttämisen jatkaminen on kansallisten turvallisuussetujen mukaista.

Lisäksi virastojen kaikkiin toimintaperiaatteisiin, joilla pannaan PPD-28:aa täytäntöön, sisältyy nykyisin nimenomainen vaatimus, jonka mukaan henkilötietoja ei saa levittää yksinomaan sillä perusteella, että kyseessä on ei-yhdysvaltalainen henkilö. ODN on antanut kaikille tiedusteluyhteisön toimijoille määräyksen, jonka mukaan tämä vaatimus on otettava huomioon⁽¹⁾. Tiedusteluyhteisön henkilöstön on erityisesti otettava huomioon ei-yhdysvaltalaisen henkilöiden yksityisyyden suojan tarve laatiessaan ja levittäessään tiedusteluraportteja. Varsinkaan signaalitiedustelutietoa, joka koskee ulkomaalaisen henkilön rutiinitoimintoja, ei pidettäisi ulkomaantiedustelutietona ainoastaan siitä syystä, että kyse on ulkomaalaisesta. Niin ollen kyseistä tietoa ei voida levittää eikä säilyttää pysyvästi, ellei tieto muuten ole merkityksellistä luvallisen ulkomaantiedustelun tiedontarpeen kannalta. Tämä on merkittävä rajoitus, ja sen avulla saadaan ratkaisu Euroopan komission esiin tuomaan ongelmaan, joka koskee ulkomaantiedustelun käsitteen laajuutta sellaisena kuin se määritellään toimeenpanoasetuksessa 12333.

⁽¹⁾ Tiedusteluyhteisön määräys 203, saatavilla osoitteessa <http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf>

d. Säännösten noudattamisen valvonta

Ulkomaantiedustelua koskeva Yhdysvaltojen valvontajärjestelmä on tiukka ja monitasoinen. Sen avulla varmistetaan sovellettavien lakien ja menettelytapojen noudattaminen, mukaan lukien PPD-28:ssa vahvistetut säännöt, jotka koskevat ei-yhdysvaltalaisia henkilöitä koskevien signaalitiedustelutietojen keräämistä, säilyttämistä ja levittämistä. Valvontajärjestelmään kuuluu seuraavaa:

- Tiedusteluyhteisön palveluksessa on satoja henkilöitä, joiden tehtävänä on valvonta. Yksin kansallisessa turvallisuusvirastossa on 300 ihmistä, jotka valvovat sääntöjen noudattamista, ja myös muilla toimijoilla on valvontatoimistoja. Lisäksi Yhdysvaltojen oikeusministeriö valvoo tiedustelutoimintaa laaja-alaisesti, ja valvontaa harjoittaa myös puolustusministeriö.
- Kaikilla tiedusteluyhteisön toimijoilla on oma valvontaviranomaisen toimistonsa (Office of the Inspector General), jonka vastuulla on valvoa muun muassa ulkomaantiedustelutoimintaa. Valvontaviranomaisten riippumattomuus perustuu lakiin. Niillä on laajat valtuudet tehdä ohjelmia koskevia tutkimuksia, tarkastuksia ja arviointoja, ja niiden toimivaltuuksiin kuuluu myös petosten ja väärinkäytösten tai lain rikkomusten tutkiminen. Valvontaviranomaiset voivat suositella korjaavia toimia. Vaikka valvontaviranomaisten suositukset eivät ole sitovia, niiden tarkastuskertomukset julkistetaan usein ja joka tapauksessa annetaan tiedoksi kongressille. Tämä koskee myös seurantakertomuksia, kun aiemmissa kertomuksissa on suositeltu korjaavia toimia mutta niitä ei ole vielä saatu päätökseen. Kongressi on niin ollen tietoinen kaikista säännösten noudattamatta jättämisistä ja voi painostaa korjaavien toimien toteuttamiseen muun muassa talousarviovaltuuksiensa avulla. Joitakin valvontaviranomaisten kertomuksia, jotka koskevat tiedustelutoimintaa, on julkistettu ⁽¹⁾.
- ODNin kansalaisvapauksista ja yksityisyyden suojasta vastaavan toimiston tehtävänä on varmistaa, että tiedusteluyhteisön toimintatavat edistävät kansallista turvallisuutta mutta samalla suojelevat kansalaisvapauksia ja oikeutta yksityisyyteen ⁽²⁾. Muilla tiedusteluyhteisön toimijoilla on omat yksityisyyden suojasta vastaavat virkamiehensä.
- Yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaava lautakunta (Privacy and Civil Liberties Oversight Board, jäljempänä 'valvontalautakunta') on riippumaton elin, joka on perustettu lailla, ja sen tehtävänä on analysoida ja tarkastaa terrorismin vastaisia ohjelmia ja toimintaperiaatteita ja muun muassa signaalitiedustelun hyödyntämistä sen varmistamiseksi, että kyseisissä toimita suojataan yksityisyyttä ja kansalaisvapauksia riittävästi. Valvontalautakunta on julkaissut useita tiedustelutoimintaa koskevia kertomuksia.
- Kuten jäljempänä tarkemmin selostetaan, FISC-tuomioistuin, joka koostuu riippumattomista liittovaltion tuomareista, valvoo, että kaikissa FISA-lain nojalla toteutettavissa signaalitiedustelutietojen keruutoiminnoissa noudatetaan säännöksiä.
- Lopuksi on todettava, että Yhdysvaltojen kongressilla, erityisesti edustajainhuoneen ja senaatin tiedustelu- ja oikeusasioiden valiokunnilla, on merkittäviä valvontavelvoitteita, jotka liittyvät kaikkeen Yhdysvaltojen harjoittamaan ulkomaantiedusteluun, myös signaalitiedusteluun.

Näiden virallisten valvontamekanismien lisäksi tiedusteluyhteisöllä on käytössä useita mekanismeja sen varmistamiseksi, että yhteisö noudattaa edellä selostettuja tiedustelutietojen keräämistä koskevia rajoituksia. Esimerkiksi:

- Ministeriöiden virkamiesten on vahvistettava signaalitiedustelun tiedontarpeensa vuosittain.
- Kansallinen turvallisuusvirasto pitää silmällä signaalitiedustelun tavoitteita koko keruuprosessin ajan voidakseen varmistua, että niiden avulla todellakin saadaan arvokasta ulkomaantiedustelutietoa, joka vastaa painopisteitä, ja jos jonkin tavoitteen osalta niin ei ole, tavoitteen mukainen tiedonkeruu lopetetaan. Muilla menettelytavoilla varmistetaan, että valintakriteerit tarkistetaan säännöllisesti.

⁽¹⁾ Ks. esimerkiksi oikeusministeriön valvontaviranomaisen laatima FBI:tä koskeva kertomus (A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008, syyskuu 2012), saatavilla osoitteessa <https://oig.justice.gov/reports/2016/o1601a.pdf>

⁽²⁾ Ks. www.dni.gov/clpo

- Presidentti Obaman nimittämän riippumattoman tarkasteluryhmän suosituksesta kansallisen tiedusteluviraston johtaja on luonut uuden seurantamekanismin. Sen avulla seurataan sellaisen signaalitiedustelutiedon keräämistä ja levittämistä, joka on erityisen arkaluonteista joko kohteen luonteen tai keräämistävän vuoksi. Tavoitteena on varmistaa, että tiedonkeruu on korkean tason päätöksentekijöiden linjausten mukaista.
- Lopuksi on todettava, että ODNI tarkistaa vuosittain tiedusteluyhteisön resurssien jaon ja arvioi, vastaako se tiedusteluhyksessä olevia painopisteitä ja tiedustelutoiminnan tehtävää kokonaisuutena. Tässä tarkistuksessa arvioidaan kaikenlaisen tiedustelutiedon, mukaan lukien signaalitiedustelun keräämisen merkitys, ja katsotaan sekä menneisyyttä (onko tiedusteluyhteisö onnistunut saavuttamaan tavoitteensa?) että tulevaisuutta (mitkä tiedusteluyhteisön tarpeet ovat tästä eteenpäin?). Näin varmistetaan, että signaalitiedustelun resursseilla palvellaan tärkeimpiä kansallisia painopisteitä.

Kuten tästä kattavasta yleiskatsauksesta ilmenee, tiedusteluyhteisö ei päätä yksinään, mitä keskusteluja se kuuntelee. Se ei myöskään yritä kerätä kaikkea mahdollista tietoa, eikä se toimi vapaasti ilman valvontaa. Se keskittyy toimissaan painopisteisiin, jotka päätöksentekijät ovat asettaneet, ja sen toimet määräytyvät prosessissa, johon koko hallinto osallistuu ja jota valvovat kansallinen turvallisuusvirasto, ODNI, oikeusministeriö ja puolustusministeriö.

PPD-28:ssa on myös useita muita säännöksiä, joilla varmistetaan, että signaalitiedustelussa kerättyjä henkilötietoja suojataan kohteen kansalaisuudesta riippumatta. PPD-28:ssa säädetään esimerkiksi tietoturvallisuudesta, pääsystä tietoihin ja laadunvarmistuksesta, minkä tavoitteena on suojella signaalitiedustelun avulla hankittuja henkilötietoja. Siinä määrätään pakollisesta koulutuksesta, jolla varmistetaan, että tiedusteluyhteisön työntekijät ymmärtävät velvollisuutensa suojella henkilötietoja kohteen kansalaisuudesta riippumatta. PPD-28:ssa säädetään myös lisämekanismeista, joilla vahvistetaan valvontaa ja varmistetaan sääntöjen noudattamista. Näihin kuuluvat säännölliset tarkastukset ja arvioinnit, joita valvonnasta ja sääntöjen noudattamisen varmistamisesta vastaavat virkamiehet tekevät ja jotka koskevat signaalitiedustelun avulla saatujen henkilötietojen suojaa. Näissä tarkastuksissa on myös arvioitava, noudattavatko virastot tällaisten tietojen suojaamiseksi vahvistettuja menettelyjä.

Lisäksi PPD-28:ssa säädetään, että sääntöjen rikkomukseen liittyvät tapaukset, jotka ovat merkittäviä ja joihin liittyy ei-yhdysvaltalaisia henkilöitä, käsitellään korkealla hallinnon tasolla. Jos ilmi tulee merkittävä rikkomustapaus, joka koskee signaalitiedustelussa kerättyjä henkilötietoja, koskivatpa ne ketä tahansa henkilöä, asiasta on – sen lisäksi mitä jo olemassa olevat raportointivaatimukset edellyttävät – raportoitava viipymättä kansallisen turvallisuusviraston johtajalle. Jos tapaus liittyy ei-yhdysvaltalaisen henkilön henkilötietoihin, kansallisen tiedusteluviraston johtajan on ulkoministeriä ja asianomaisen tiedusteluyhteisön toimijan johtajaa kuultuaan päätettävä, olisiko asiasta ilmoitettava asianomaiselle ulkovaltojen hallitukselle, tällöin kuitenkin suojellen lähteitä, menetelmiä ja yhdysvaltalaista henkilöstöä. Lisäksi ulkoministeri on – siten kuin PPD-28:ssa määrätään – nimennyt korkean virkamiehen, alivaltiosihteeri Catherine Novellin, toimimaan ulkomaisten hallitusten yhteyspisteenä siltä varalta, että nämä tahtovat tuoda esiin Yhdysvaltojen signaalitiedustelussa havaitsemiaan ongelmia. Sitoumus käsitellä asioita korkealla tasolla on esimerkki toimista, joita Yhdysvaltojen hallitus on viime vuosina toteuttanut vahvistaakseen luottamusta siihen, että sekä yhdysvaltalaiset että ei-yhdysvaltalaiset henkilöiden henkilötietoja suojataan monilukuisilla ja -kerroksisilla menettelyillä.

e. Yhteenveto

Yhdysvaltojen menettelyissä, joissa kerätään, säilytetään ja levitetään ulkomaantiedustelussa hankittua tietoa, suojataan kaikkia henkilötietoja tehokkaasti kohteen kansalaisuudesta riippumatta. Kyseisissä menettelyissä varmistetaan erityisesti seuraavat seikat: tiedusteluyhteisömme keskittyy kansallista turvallisuutta suojaavissa toimissaan asioihin, jotka ovat luvallisia lakien, toimeenpanoasetusten ja presidentin määräysten mukaisesti; tiedusteluyhteisö suojaa tietoja luvattomalta pääsylvä, käytöltä ja luovuttamiselta; tiedusteluyhteisön toiminta on monikerroksisen arvioinnin ja valvonnan kohteena, ja muun muassa kongressin valvontavaliokunnat valvovat sitä. PPD-28 ja sen täytäntöönpanemiseksi annetut menettelytavat ovat osoitus pyrkimyksistämme laajentaa tiettyjen minimointiperiaatteiden ja muiden merkittävien tietosuojaperiaatteiden soveltaminen kaikkien henkilöiden henkilötietoihin heidän kansalaisuudestaan riippumatta. Yhdysvaltojen signaalitiedustelun avulla kerättyihin henkilötietoihin sovelletaan Yhdysvaltojen laeissa ja presidentin määräyksissä olevia periaatteita ja vaatimuksia, mukaan lukien PPD-28:ssa olevat suojatoimet. Näillä periaatteilla ja vaatimuksilla varmistetaan, että kaikkia henkilöitä kohdellaan ihmisarvoisesti ja kunnioittavasti riippumatta heidän kansalaisuudestaan tai asuinpaikastaan, ja tunnustetaan, että kaikilla henkilöillä on perusteltu tarve yksityisyyden suojaan heidän henkilötietojensa käsittelyn yhteydessä.

II. FISA-LAIN (FOREIGN INTELLIGENCE SURVEILLANCE ACT) 702 §

FISA-lain ⁽¹⁾ 702 §:n mukainen tiedonkeruu ei ole ”laajamittaista ja kohdentamatonta”, vaan se kohdennetaan tarkasti siten, että kerätään ulkomaantiedustelutietoja yksilöllisesti tunnistetuista, perustelluista kohteista. Kyseinen tiedonkeruu on säädetty laissa luvalleiseksi yksiselitteisesti ja nimenomaisesti. Tiedonkeruuseen kohdistuu sekä riippumatonta oikeudellista valvontaa että merkittävää toimeenpanohaaran ja kongressin toteuttamaa valvontaa ja arviointia. Tätä 702 §:n mukaista tiedonkeruuta pidetään signaalitiedusteluna, ja PPD-28:n vaatimuksia sovelletaan siihen ⁽²⁾.

FISA-lain 702 §:n mukainen tiedonkeruu on yksi arvokkaimmista tietolähteistä, ja se suojaa sekä Yhdysvaltoja että sen eurooppalaisia kumppaneita. Kattavat tiedot 702 §:ään perustuvasta toiminnasta ja toiminnan valvonnasta ovat julkisesti saatavilla. Monia ohjelmaan liittyviä tuomioistuimille tehtyjä hakemuksia, tuomioistuinten päätöksiä ja valvontaraportteja on luokiteltu ei-salaisiksi ja julkistettu ODN:n julkisilla verkkosivuilla osoitteessa www.icontherecord.tumblr.com. Lisäksi valvontalautakunta on analysoinut 702 §:ää laaja-alaisesti raportissaan, joka on saatavilla osoitteessa <https://www.pclob.gov/library/702-Report.pdf> ⁽³⁾.

FISA-lain 702 § hyväksyttiin osana kyseisen lain muuttamisesta vuonna 2008 annettua lakia ⁽⁴⁾, laajan kongressissa käydyn julkisen keskustelun jälkeen. FISA-laissa säädetään, että ulkomaantiedustelutiedon hankkiminen kohdistamalla tiedustelu Yhdysvaltojen ulkopuolella olevaan ei-yhdysvaltalaiseen henkilöön on luvallista ja että yhdysvaltalaiset sähköisiä viestintäpalveluja tarjoavat yritykset voidaan pakottaa avustamaan tässä. FISA-lain 702 §:ssä annetaan oikeusministerille ja kansallisen tiedusteluviraston johtajalle eli kahdelle ministeritason virkamiehelle, jotka presidentti nimittää ja joiden nimityksen senaatti vahvistaa, valtuudet toimittaa vuotuinen sertifiointi FISC-tuomioistuimelle ⁽⁵⁾. Näissä sertifiointeissa määritetään kerättävän ulkomaantiedustelutiedon erityiset lajit, kuten tiedot, jotka liittyvät terrorismin torjuntaan tai joukkotuhoaseisiin. Tiedon lajien on oltava niitä, jotka FISA-lain määritelmien mukaan kuuluvat ulkomaantiedustelun alaan ⁽⁶⁾. Kuten valvontalautakunta on todennut, näiden määritelmien vuoksi ulkomaalaisista ei voida kerätä tietoa rajattomasti ⁽⁷⁾.

Sertifiointeihin on myös sisällytettävä ns. kohdentamis- ja minimointimenettelyt, jotka FISC-tuomioistuimen on tarkastettava ja hyväksyttävä ⁽⁸⁾. Kohdentamismenettelyjen tavoitteena on sen varmistaminen, että keruu toteutetaan ainoastaan siten kuin laki sallii ja että keruu kuuluu sertifiointien alaan. Minimointimenettelyjen tavoitteena on rajoittaa Yhdysvaltojen kansalaisia koskevien tietojen hankkimista, levittämistä ja säilyttämistä, mutta menettelyihin kuuluu myös säännöksiä, joilla annetaan merkittävä suojaa ei-yhdysvaltalaisia henkilöitä koskeville tiedoille, kuten jäljempänä selostetaan. Kuten edellä on todettu, PPD-28:ssa presidentti lisäksi määräsi, että tiedusteluyhteisön on annettava lisäsuojaa ei-yhdysvaltaisten henkilöiden henkilötiedoille, ja tätä suojaa sovelletaan tietoihin, jotka on kerätty 702 §:n nojalla.

Kun tuomioistuin on hyväksynyt kohdentamis- ja minimointimenetelmät, 702 §:n mukainen tiedonkeruu ei enää ole valikoimatonta tai kohdentamatonta, vaan se kohdentuu pelkästään tiettyihin henkilöihin, joista on päätetty kerätä tietoja. Tämän on todennut myös valvontalautakunta ⁽⁹⁾. Keruu on kohdennettu yksittäisten valintakriteerien (kuten

⁽¹⁾ 50 U.S.C. § 1881a.

⁽²⁾ Yhdysvaltojen laki voi saada tietojen hankkimiseen liittyvän tuomioistuimen määräyksen myös muiden FISA-lain säännösten nojalla, ja tämä koskee myös Privacy Shield -järjestelyssä siirrettyjä tietoja. Ks. 50 U.S.C. § 1801 ja sitä seuraavat pykälät. FISA-lain I osastossa säädetään sähköisen tarkkailun ja III osastossa koti- tai paikanetsinnän luvallisuudesta. Kummassakin osastossa edellytetään tuomioistuimen määräystä (paitsi hätätilanteissa) ja vaaditaan aina, että on oltava perusteltua syytä olettaa kohteen olevan vieras valta tai vieraan vallan asiamies. FISA-lain IV osastossa säädetään, että on luvallista käyttää lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiä (pen registers, trap and trace devices) ulkomaantiedusteluun, vastatiedusteluun tai terrorismin torjumiseen liittyvissä luvallisissa tutkimuksissa. Järjestelmien käyttämiseen tarvitaan tuomioistuimen määräys (paitsi hätätilanteissa). FISA-lain V osastossa säädetään, että FBI voi saada haltuunsa liiketoimintatiedot, joilla on merkitystä ulkomaantiedusteluun, vastatiedusteluun tai terrorismin torjumiseen liittyvissä luvallisissa tutkimuksissa. Tietojen hankkimiseen tarvitaan tuomioistuimen määräys (paitsi hätätilanteissa). Kuten jäljempänä selostetaan, terrorismin vastaisessa USA FREEDOM Act -laissa nimenomaisesti kielletään FISA-lakiin perustuvien teleliikennettä ja liiketoimintatietoja koskevien tuomioistuinten määräysten käyttö tietojen valikoimattomaan keräämiseen ja USA FREEDOM Act -laissa säädetään ”erityistä valintakriteeriä” koskevasta vaatimuksesta sen varmistamiseksi, että mainittuja valtuuksia käytetään kohdennetusti.

⁽³⁾ 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, 2. heinäkuuta 2014, jäljempänä ”valvontalautakunnan kertomus”).

⁽⁴⁾ Ks. julkisoikeudellisia säädöksiä koskeva Pub. L. No. 110-261, 122 Stat. 2436 (2008).

⁽⁵⁾ Ks. 50 U.S.C. § 1881a(a) ja (b).

⁽⁶⁾ Ks. sama laki § 1801(e).

⁽⁷⁾ Ks. valvontalautakunnan kertomuksen sivu 99.

⁽⁸⁾ Ks. 50 U.S.C. § 1881a(d) ja (e).

⁽⁹⁾ Ks. valvontalautakunnan kertomuksen sivu 111.

sähköpostiosoitteiden tai puhelinnumerojen) avulla. Valintakriteerit ovat sellaisia, että Yhdysvaltojen tiedusteluhenkilöstön päätelmien mukaan niitä todennäköisesti käytetään sen tyyppisten ulkomaantiedustelutietojen viestintään, jotka tuomioistuimelle toimitettu sertifiointi kattaa ⁽¹⁾. Syyt, joiden vuoksi henkilö on valittu tiedustelun kohteeksi, on dokumentoitava, ja oikeusministeriö tarkastaa jälkepäin jokaista valintakriteeriä koskevan dokumentaation ⁽²⁾. Yhdysvaltojen hallitus on julkistanut tietoja, joista ilmenee, että vuonna 2014 tiedustelua kohdistettiin 702 §:n nojalla noin 90 000 henkilöön. Tämä on minimaalinen osuus koko maailman yli 3 miljardista internetin käyttäjästä ⁽³⁾.

FISA-lain 702 §:n nojalla kerättäviin tietoihin sovelletaan tuomioistuimen hyväksymiä minimointimenettelyjä, joiden avulla annetaan suojaa sekä yhdysvaltalaisille että ei-yhdysvaltalaisille henkilöille ja jotka on julkistettu ⁽⁴⁾. Esimerkkinä voidaan todeta, että viestintä, joka on hankittu 702 §:n nojalla, koskipa se yhdysvaltalaisista tai ei-yhdysvaltalaisista henkilöä, säilytetään tietokannoissa, joihin pääsyä valvotaan tarkasti. Tietokantoja voi tutkia ainoastaan tiedusteluhenkilöstö, joka on saanut yksityisyyden suojelemiseksi vahvistettuja minimointimenettelyitä koskevan koulutuksen ja jolle on nimenomaisesti annettu pääsy tietoihin siinä tarkoituksessa, että se voi hoitaa luvallisia tehtäviään ⁽⁵⁾. Tietoja voidaan käyttää vain ulkomaantiedustelussa saatujen tietojen tunnistamiseen tai todisteena rikoksesta ⁽⁶⁾. PPD-28:n mukaan tietoja voidaan levittää ainoastaan jos on kyse perustellusta ulkomaantiedusteluun tai lainvalvontaan liittyvästä käyttötarkoituksesta. Pelkästään se, että yksi viestinnän osapuoli ei ole Yhdysvaltojen kansalainen, ei riitä ⁽⁷⁾. Minimointimenettelyssä ja PPD-28:ssa asetetaan rajat myös sille, kuinka kauan 702 §:n nojalla saatuja tietoja voidaan säilyttää ⁽⁸⁾.

FISA-lain 702 §:n valvonta on laajaa, ja kaikki valtiovaltamme kolme haaraa osallistuvat siihen. Virastoilla, jotka panevat lakia täytäntöön, on monitasoisia sisäisen valvonnan menettelyitä, mukaan lukien riippumattoman valvontaviranomaisen valvonta. Niillä on myös teknisiä kontroleja, jotka koskevat pääsyä tietoihin. Oikeusministeriö ja kansallinen tiedusteluvirasto arvioivat ja tutkivat tarkasti 702 §:n hyödyntämistä sen tarkastamiseksi, että säännöksiä noudatetaan. Virastojen on myös oma-aloitteisesti raportoitava mahdollisista tapauksista, joissa säännöksiä ei ole noudatettu. Tapaukset tutkitaan, ja kaikki säännösten rikkomukset ilmoitetaan FISC-tuomioistuimelle, presidentin tiedusteluvalvontakomitealle (President's Intelligence Oversight Board) ja kongressille, ja puutteet korjataan tarpeen mukaan ⁽⁹⁾. Tähän mennessä ei ole esiintynyt tapauksia, joissa olisi tahallisesti yritetty rikkoa lakia tai kiertää lakisääteisiä vaatimuksia ⁽¹⁰⁾.

FISC-tuomioistuimella on merkittävä rooli 702 §:n täytäntöönpanossa. Tuomioistuin koostuu riippumattomista liittovaltion tuomareista, joiden toimikausi FISC-tuomioistuimessa kestää seitsemän vuotta mutta joilla – kuten kaikilla liittovaltion tuomareilla – on elinikäinen oikeus pysyä tuomarin virassaan. Kuten edellä on todettu, tuomioistuimen on käytävä läpi vuotuiset sertifiointit ja kohdentamis- ja minimointimenettelyt sen selvittämiseksi, ovatko ne lain mukaisia. Lisäksi kuten edellä on todettu, havaitessaan rikkomustapauksia hallinnon on välittömästi ilmoitettava niistä tuomioistuimelle ⁽¹¹⁾. Useita tuomioistuimen päätöksiä on luokiteltu ei-salaisiksi ja julkistettu, ja niistä käy ilmi, kuinka poikkeuksellisen laadukasta tuomioistuimen lainkäyttö on ja kuinka poikkeuksellisen riippumaton se on käsitellessään rikkomustapauksia.

Tuomioistuimen menettelyjen vaativuutta on kuvattu sen entisen puheenjohtajan kongressille lähettämässä kirjeessä, joka on julkistettu ⁽¹²⁾. Jäljempänä selostettavan USA FREEDOM Act -lain myötä tuomioistuimella on nyt nimenomainen toimivalta nimittää ulkopuolinen lakimies toimimaan riippumattomana asianajajana ja puolustamaan yksityisyyden suojaa tapauksissa, joissa esiintyy uusia tai merkittäviä oikeudellisia kysymyksiä ⁽¹³⁾. Se, että maan riippumaton tuomioistuinlaitos osallistuu näin tiiviisti ulkomaantiedusteluun liittyviin toimintoihin, joiden kohteena olevat henkilöt eivät ole maan kansalaisia eivätkä asu sen alueella, on epätavallista ellei tavatonta. Tämä antaa varmuutta siitä, että 702 §:n mukainen tiedonkeruu tapahtuu sitä säätelevien lakien mukaisesti.

⁽¹⁾ Kuten edellinen alaviite.

⁽²⁾ Ks. valvontalautakunnan kertomuksen sivu 8; 50 U.S.C. § 1881a(l); ks. myös kansallisen turvallisuusviraston kansalaisvapauksista ja yksityisyyden suojasta vastaavan toimiston johtajan kertomus viraston FISA-lain 702 §:n soveltamisesta, sivu 4 (NSA Director of Civil Liberties and Privacy Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702), saatavilla osoitteessa <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>

⁽³⁾ Kansallisen tiedusteluviraston johtajan avoimuusraportti vuodelta 2014, saatavilla osoitteessa http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014

⁽⁴⁾ Minimointimenettelyt ovat saatavilla seuraavissa osoitteissa: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf>; <http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf>; ja <http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf>

⁽⁵⁾ Ks. kansallisen turvallisuusviraston kansalaisvapauksista ja yksityisyyden suojasta vastaavan toimiston johtajan kertomus viraston FISA-lain 702 §:n soveltamisesta, kertomuksen sivu 4.

⁽⁶⁾ Ks. esimerkiksi kansallisen turvallisuusviraston kertomus minimointimenettelyistä, sivu 6, linkki alaviitteessä 23.

⁽⁷⁾ Tiedusteluyhteisön PPD-28 -menettelyt ovat saatavilla osoitteessa <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>

⁽⁸⁾ Ks. kansallisen turvallisuusviraston minimointimenettelyt; PPD-28:n 4 §.

⁽⁹⁾ Ks. 50 U.S.C. § 1881(l); ks. myös valvontalautakunnan kertomuksen sivut 66–76.

⁽¹⁰⁾ Ks. oikeusministerin ja kansallisen tiedusteluviraston johtajan puolivuositilain laatima arvio FISA-lain 702 §:n noudattamisesta, sivut 2 ja 3 (Semiannual Assessment of Compliance with Procedures and Guidelines Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence), saatavilla osoitteessa <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>

⁽¹¹⁾ FISC-tuomioistuimen työjärjestyksen sääntö nro 13 (Foreign Intelligence Surveillance Court Rules of Procedures), saatavilla osoitteessa <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>

⁽¹²⁾ Reggie B. Waltonin kirje Patrick J. Leahylle, päiväty 29. heinäkuuta 2013, saatavilla osoitteessa <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>

⁽¹³⁾ Ks. USA FREEDOM Act -lain 401 §, julkisoikeudellisia säädöksiä koskeva P.L. 114-23.

Kongressi harjoittaa valvontaa laissa edellytettujen, tiedustelu- ja oikeusasioiden valiokunnille toimitettavien kertomusten avulla sekä lukuisten tilannekatsausten ja kuulemisten avulla. Näihin kuuluvat seuraavat kertomukset: oikeusministerin puolivuositilannekatsaus, jossa selostetaan 702 §:n hyödyntämistä ja kaikkia rikkomustapauksia ⁽¹⁾; erillinen oikeusministerin ja kansallisen tiedusteluviraston johtajan puolivuositilannekatsaus, jossa selostetaan kohdennus- ja minimointimenettelyitä, mukaan lukien sellaisten menettelyiden noudattaminen, joilla pyritään varmistamaan, että tiedonkeruu tapahtuu perustellun ulkomaantiedusteluun liittyvän syyn vuoksi ⁽²⁾; sekä tiedusteluyhteisön toimijoiden johtajien vuotuinen kertomus, johon sisältyvän vakuutuksen mukaan 702 §:n nojalla toteutettava tiedonkeruu tuottaa edelleen ulkomaantiedustelutietoa ⁽³⁾.

Lyhyesti sanottuna 702 §:n nojalla toteutettava tiedonkeruu on laissa sallittua, siihen kohdistuu monitasoista valvontaa (arviointeja, tuomioistuinvalvontaa ja yleistä valvontaa) ja – kuten FISC-tuomioistuin on todennut hiljattain julkaisussaan kannassaan – sitä ”ei toteuteta valikoimattomasti ja kohdentamattomasti” vaan ”[...] erillisillä kohdennuspäätöksillä, jotka koskevat yksittäisiä (viestintään käytettäviä) välineitä” ⁽⁴⁾.

III. USA FREEDOM ACT -LAKI

Terrorismin vastaisella USA FREEDOM Act -lailla, joka vahvistettiin kesäkuussa 2015, muutettiin huomattavasti tarkkailuun ja muuhun kansalliseen turvallisuuteen liittyviä valtuuksia Yhdysvalloissa. Lailla lisättiin näiden valtuuksien käyttöön ja FISC-tuomioistuimen päätöksiin liittyvää läpinäkyvyyttä, kuten jäljempänä selostetaan ⁽⁵⁾. Lailla varmistetaan, että tiedustelusta ja lainvalvonnasta vastaavilla ammattihenkilöillä on toimivaltuudet, jotka he tarvitsevat kansakunnan suojelemiseksi, samalla kun varmistetaan myös, että henkilöiden yksityiselämää suojataan asianmukaisella tavalla näitä toimivaltuuksia käytettäessä. Lailla parannetaan yksityisyyden ja kansalaisvapauksien suojaa ja lisätään läpinäkyvyyttä.

Laissa kielletään valikoimattoman tiedon kerääminen sekä yhdysvaltalaisista että ei-yhdysvaltalaisista henkilöistä FISA-lain nojalla tai käyttämällä kansallista turvallisuutta koskevia kirjeitä (National Security Letters). Viimeksi mainitut ovat eräänlaisia hallinnollisia haasteita (subpoena), joiden käytöstä säädetään laissa ⁽⁶⁾. Laissa asetettu kiello käsittää erityisesti puhelinliikenteen metadatan, joka koskee Yhdysvalloissa olevien ja Yhdysvaltojen ulkopuolella olevien henkilöiden välisiä puheluita, ja kattaisi myös näillä toimivaltuuksilla kerättyjä Privacy Shield -järjestelyn tietoja. Laissa edellytetään, että hallitus käyttää näitä tietojen haun mahdollistavia toimivaltuuksiaan ainoastaan ns. erityisen valintakriteerin pohjalta. Termillä tarkoitetaan kriteeriä, joka liittyy erityisesti johonkin henkilöön, pankkitiliin, osoitteeseen tai henkilökohtaiseen laitteeseen siten, että haettavan tiedon alaa rajataan niin paljon kuin on kohtuudella mahdollista ⁽⁷⁾. Näin varmistetaan entistä paremmin, että tietojen kerääminen tiedustelutarkoituksiin on täsmällisesti kohdennettua.

Laissa on tehty merkittäviä muutoksia myös FISC-tuomioistuimessa käytäviin oikeudenkäynteihin. Näillä muutoksilla sekä lisätään läpinäkyvyyttä että annetaan lisätakeita yksityisyyden suojasta. Kuten edellä on todettu, laissa säädettiin mahdollisuudesta perustaa pysyvä paneeli, joka koostuu turvallisuusselvityksen läpäisseistä lakimiehistä. Heillä on oltava asiantuntemusta kysymyksissä, jotka liittyvät yksityisyyden suojaan ja kansalaisvapauksiin, tiedustelutiedon keräämiseen, viestintäteknologiaan tai muihin merkittäviin aloihin, ja heidät voidaan nimittää toimimaan oikeudessa asiantuntijoina (*amicus curiae*) asioissa, joissa tulee esille merkittäviä tai uusia laintulkintoja. Nämä lakimiehet voivat esittää oikeudellisia argumentteja, joilla edistetään yksilöiden yksityisyyden ja kansalaisvapauksien suojaa, ja he saavat käyttöönsä kaikki tiedot, myös turvallisuusluokitellut tiedot, jotka tuomioistuin katsoo heidän tarvitsevan tehtävänsä hoitamiseksi ⁽⁸⁾.

Laissa myös lisätään entisestään ennennäkemätöntä läpinäkyvyyttä, jota Yhdysvaltojen hallitus on noudattanut tiedustelukysymyksissä, ja vaaditaan, että kansallisen tiedusteluviraston johtaja oikeusministeriä kuultuaan joko luokittelee ei-salaiseksi kaikki FISC-tuomioistuimen tai FISCR-muutoksenhakutuomioistuimen päätökset, määräykset tai lausunnot, joihin liittyy merkittävää norminmuodostusta tai laintulkintaa, tai julkaisee niistä ei-salaisen tiivistelmän.

⁽¹⁾ Ks. 50 U.S.C. § 1881f.

⁽²⁾ Ks. saman lain § 1881a(l)(1).

⁽³⁾ Ks. saman lain § 1881a(l)(3). Jotkin näistä kertomuksista ovat salaisia.

⁽⁴⁾ FISC-tuomioistuimen muistiolausunto ja määräys, sivu 26 (FISC 2014, Mem. Opinion and Order), saatavilla osoitteessa <http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>

⁽⁵⁾ Ks. USA FREEDOM Act of 2015, julkisoikeudellisia säädöksiä koskeva Pub. L. No. 114-23, § 401, 129 Stat. 268.

⁽⁶⁾ Ks. saman lain §§ 103, 201, 501. Kansallista turvallisuutta koskevista kirjeistä säädetään useissa laeissa, joissa annetaan FBI:lle valtuudet saada tietyn tyyppisten yritysten lainakertomuksissa, kirjanpidoissa ja sähköisissä tilausasiakas- ja liiketapahtumarekistereissä olevia tietoja. Kirjeitä voidaan hyödyntää ainoastaan kansainvälisen terrorismin tai salaisen tiedustelutoiminnan torjumiseksi. Ks. 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. On tavallista, että FBI käyttää kansallista turvallisuutta koskevia kirjeitä kerätäksään erittäin tärkeää ei-sisällöllistä tietoa terrorismin torjuntaan tai vastatiedusteluun liittyvien tutkimusten alkuvaiheissa. Kyseistä tietoa voisi olla esimerkiksi sellaisen tilinavaajan henkilöllisyys, jolla saattaa olla yhteyksiä jonkin terroristiryhmän, kuten Isisin, asiamehiin. Kansallista turvallisuutta koskevan kirjeen vastaanottaja voi vastustaa kirjeessä esitettyjä vaatimuksia viemällä asian tuomioistuimen käsiteltäväksi. Ks. 18 U.S.C. § 3511.

⁽⁷⁾ Ks. sama.

⁽⁸⁾ Ks. saman lain § 401.

Lisäksi laissa säädetään laajamittaisesta tietojen julkistamisesta, joka liittyy FISA-lakiin perustuvaan tiedonkeruuseen ja kansallista turvallisuutta koskevien kirjeiden perusteella tehtyihin tietopyyntöihin. Yhdysvaltojen hallituksen on annettava vuosittain kongressille ja julkisuuteen tieto muun muassa seuraavista seikoista: haettujen ja saatujen FISA-määräysten ja -sertifiointien lukumäärä; arvio siitä, kuinka monta yhdysvaltalaisista ja ei-yhdysvaltalaisista henkilöä on ollut tarkkailun kohteena; sekä *amicus curiae* -nimitysten määrä ⁽¹⁾. Lisäksi laissa edellytetään hallituksen raportoivan julkisuuteen myös siitä, kuinka monta tietopyyntöä kohdistettiin yhdysvaltalaisiin ja ei-yhdysvaltalaisiin henkilöihin kansallista turvallisuutta koskevien kirjeiden perusteella ⁽²⁾.

Yrityksiä koskevasta läpinäkyvyydestä on todettava, että laissa tarjotaan yrityksille monia vaihtoehtoisia tapoja, joilla he voivat raportoida julkisuuteen FISA-määräysten ja hallitukselta saamiensa määräysten ja kansallista turvallisuutta koskevien kirjeiden yhteismäärän, samoin kuin niiden asiakastilien määrän, joita kyseiset määräykset ovat koskeneet ⁽³⁾. Useat yritykset ovat jo antaneet kyseiset tiedot, ja niistä on paljastunut, että niiden asiakkaiden määrä, joiden tietoja on pyydetty, on vähäinen.

Nämä yritysten avoimuusraportit osoittavat, että Yhdysvaltojen tiedusteluelinten pyynnot koskevat vain minimaalista osaa tiedoista. Erään suuryrityksen hiljattaisessa avoimuusraportissa esimerkiksi kävi ilmi, että sen saamat kansalliseen turvallisuuteen liittyvät pyynnot (FISA-lakiin tai kansallista turvallisuutta koskevaan kirjeeseen perustuvat) koskivat vähempää kuin 20 000:tä asiakastiliä, kun sen tilausasiakasmäärä oli vähintään 400 miljoonaa. Toisin sanoen kaikki Yhdysvaltojen kansalliseen turvallisuuteen liittyvät pyynnot, joista tämä yritys raportoi, koskivat vähempää kuin 0,005:tä prosenttia sen tilausasiakkaista. Vaikka kaikki kyseiset pyynnot olisivat koskeneet safe harbor -ohjelman tietoja, mitä ne tietenkään eivät koskeneet, on selvää, että pyynnot olivat kohdennettuja ja laajuudeltaan asianmukaisia ja että ne eivät olleet valikoimattomia eivätkä kohdentamattomia.

Lopuksi on todettava, että vaikka säädökset, joissa on säädetty mahdollisuudesta antaa kansallista turvallisuutta koskeva kirje, ovat jo rajoittaneet tilanteita, joissa tällaisen kirjeen vastaanottajaa voidaan kieltää kertomasta siitä, USA FREEDOM Act -laissa säädettiin edelleen, että ilmaisukiellon tarvetta on tarkistettava säännöllisesti. Samoin laissa edellytettiin, että kirjeen vastaanottajalle on ilmoitettava, kun tilanne ei enää vaadi ilmaisukiellon noudattamista. Laissa myöskin koottiin yhteen kaikki menettelyt, joiden avulla kirjeen vastaanottaja voi vastustaa ilmaisukieltoa ⁽⁴⁾.

Yhteenvedona voidaan todeta, että USA FREEDOM Act -laissa säädetyt merkittävät muutokset Yhdysvaltojen tiedustelutoimivaltuuksiin ovat selvä näyttö laajakantoisista toimista, joita Yhdysvallat on toteuttanut asettaakseen henkilötietojen, yksityisyyden ja kansalaisvapauksien suojan sekä läpinäkyvyyden etualalle kaikissa Yhdysvaltojen tiedustelukäytännöissä.

IV. LÄPINÄKYVYYS

Sen läpinäkyvyyden lisäksi, jota Yhdysvaltojen tiedusteluyhteisöltä edellytetään USA FREEDOM Act -laissa, yhteisö toimittaa julkisuuteen paljon muutakin tietoa ja antaa näin vahvan esimerkin läpinäkyvyydestä tiedustelutoiminnassa. Tiedusteluyhteisö on julkaissut monia toimintaperiaatteita, menettelytapoja, FISC-tuomioistuinten päätöksiä ja muuta ei-salaiseksi luokiteltua aineistoa ja osoittanut näin poikkeuksellista läpinäkyvyyttä. Lisäksi tiedusteluyhteisö on lisännyt olennaisesti sellaisten tilastotietojen julkistamista, jotka kuvaavat, kuinka hallitus käyttää kansallista turvallisuutta koskevaan tiedonkeruuseen liittyviä toimivaltuuksiaan. Tiedusteluyhteisö julkaisi 22. huhtikuuta 2015 toisen vuotuisen raporttinsa, jossa esiteltiin tilastoja siitä, kuinka usein hallitus käytti näitä merkittäviä toimivaltuuksiaan. Lisäksi ODNI on julkaissut verkkosivustollaan ja IC On the Record -verkkosivustolla joukon konkreettisia läpinäkyvyyssperiaatteita ⁽⁵⁾, samoin kuin täytäntöönpanosuunnitelman ⁽⁶⁾, jonka mukaisesti periaatteet muutetaan konkreettisiksi, mitattaviksi toimiksi. Kansallisen tiedusteluviraston johtaja määräsi lokakuussa 2015, että jokaisen tiedusteluelimen on nimettävä läpinäkyvyydestä vastaava virkamies, joka edistää läpinäkyvyyttä ja johtaa läpinäkyvyyssaloitteita viraston toimialalla ⁽⁷⁾. Läpinäkyvyydestä vastaava virkamies tekee tiivistä yhteistyötä kunkin tiedusteluelimen yksityisyyden suojasta ja kansalaisvapauksista vastaavan virkamiehen kanssa varmistaakseen, että läpinäkyvyys, yksityisyyden suoja ja kansalaisvapaudet pysyvät ensisijaisina tavoitteina.

⁽¹⁾ Ks. saman lain § 602.

⁽²⁾ Ks. sama.

⁽³⁾ Ks. saman lain § 603.

⁽⁴⁾ Ks. saman lain §§ 502(f)–503.

⁽⁵⁾ Saatavilla osoitteessa <http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>

⁽⁶⁾ Saatavilla osoitteessa <http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>

⁽⁷⁾ Ks. sama.

Esimerkkinä läpinäkyvyystoimista on mainittava, että kansallisen turvallisuusviraston yksityisyyden ja kansalaisvapauksien suojasta vastaava johtava virkamies on antanut useita ei-salaisia raportteja viime vuosien aikana, muun muassa raportit toimista, jotka perustuvat 702 §:ään, toimeenpanoasetukseen 12333 ja USA FREEDOM Act -lakiin⁽¹⁾. Lisäksi tiedusteluyhteisö toimii tiiviissä yhteistyössä valvontalautakunnan, kongressin ja Yhdysvaltojen yksityisyyden suojaa edistävän yhteisön kanssa parantaakseen Yhdysvaltojen tiedustelutoiminnan läpinäkyvyyttä milloin mahdollista ja ottaen huomioon tarpeen suojella arkaluonteisia tiedustelulähteitä ja -menetelmiä. Kaiken kaikkiaan Yhdysvaltojen tiedustelutoiminnot ovat yhtä läpinäkyviä elleivät läpinäkyvämpiä kuin minkään muun maan tiedustelutoiminnot koko maailmassa. Kun otetaan huomioon tarve suojella arkaluonteisia tiedustelulähteitä ja -menetelmiä, läpinäkyvyys on niin suurta kuin mahdollista.

Yhdysvaltojen tiedustelupalvelutoiminnan laajamittaisesta läpinäkyvyydestä voidaan esittää seuraava yhteenveto:

- Tiedusteluyhteisö on julkaissut verkossa tuhansia sivuja tuomioistuimen päätöksiä ja tiedusteluelimien menettelytapoja ja antanut näin yleiskuvan tiedustelutoimintamme erityisistä menetelmistä ja vaatimuksista. Olemme julkaisseet raportteja myös siitä, kuinka tiedusteluelimet ovat noudattaneet niihin kohdistuvia rajoituksia.
- Tiedusteluelinten korkea-arvoiset virkamiehet puhuvat usein julkisesti organisaatioidensa tehtävistä ja toiminnoista ja muun muassa kuvailevat järjestelmiä, joilla sääntöjen noudattaminen varmistetaan, ja suojatoimia, joita organisaation toimintaan sovelletaan.
- Tiedusteluyhteisö julkaisi monia muita tiedustelutoimintaa koskevia asiakirjoja tiedonvapautta parantavan FOIA-lain nojalla.
- Presidentti antoi määräyksen PPD-28, jossa selostetaan julkisesti tiedustelutoimintamme sovellettavia lisärajoituksia, ja ODNI on julkaissut kaksi raporttia näiden rajoitusten täytäntöönpanosta.
- Laissa edellytetään nyt tiedusteluyhteisön julkaisevan merkittäviä oikeudellisia päätöksiä, joita FISC-tuomioistuin on antanut, tai niiden tiivistelmiä.
- Hallituksen edellytetään raportoivan vuosittain, missä määrin se on hyödyntänyt tiettyä kansalliseen turvallisuuteen liittyviä toimivaltuuksia, ja myös yrityksillä on lupa raportoida tästä asiasta.
- Valvontalautakunta on julkistanut useita yksityiskohtaisia raportteja tiedustelutoiminnasta ja aikoo tehdä niin jatkossakin.
- Tiedusteluyhteisö antaa kongressin valvontavaliokunnille runsaasti salaista tietoa.
- Kansallisen tiedusteluviraston johtaja on vahvistanut tiedusteluyhteisön toimintaa koskevat läpinäkyvyysperiaatteet.

Merkittävä läpinäkyvyys jatkuu tulevaisuudessakin. Kaikki julkiset tiedot ovat luonnollisesti kauppaministeriön ja Euroopan komission saatavilla. Privacy Shield -järjestelyn täytäntöönpanoa koskeva kauppaministeriön ja Euroopan komission vuotuinen tarkastelu antaa Euroopan komissiolle tilaisuuden keskustella kaikista kysymyksistä, jotka ovat nousseet esiin minkä tahansa uuden julkistetun tiedon myötä, sekä kaikista muistakin Privacy Shield -järjestelyä ja sen toimintaa koskevista asioista. Käsityksemme mukaan ministeriö voi harkintansa mukaan pyytää muiden virastojen ja muun muassa tiedusteluyhteisön edustajia osallistumaan tähän tarkasteluun. Tämä keskusteluväylä on luonnollisesti käytettävissä sen mekanismin lisäksi, joka PPD-28:ssa on säädetty EU:n jäsenvaltioiden käytettäväksi ja jolla nämä voivat tuoda esiin tarkkailuun liittyviä ongelmia nimetyn ulkoministeriön virkamiehen kanssa.

V. OIKEUSSUOJAKEINOT

Yhdysvaltojen lainsäädännössä säädetään useista oikeussuojakeinoista, joita henkilöt voivat käyttää, jos he joutuvat lainvastaisen sähköisen tarkkailun kohteeksi kansalliseen turvallisuuteen liittyvän syyn vuoksi. FISA-lain mukaan oikeus hakea hyvitystä yhdysvaltalaisessa tuomioistuimessa ei rajoitu Yhdysvaltojen kansalaisiin. Henkilö, jolla on asiavaltuus esillä olevassa asiassa, voi saada oikeussuojaa lainvastaisen sähköisen tarkkailun vuoksi FISA-lain nojalla. FISA-laki

⁽¹⁾ Saatavilla osoitteessa https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf

esimerkiksi antaa henkilölle, joka on joutunut lainvastaisen sähköisen tarkkailun kohteeksi, oikeuden haastaa Yhdysvaltojen hallituksen virkamiehiä vastaamaan omasta puolestaan vahingonkorvausvaatimukseen, joka voi käsittää muun muassa rankaisevan vahingonkorvauksen ja korvauksen asianajajan kuluista. Ks. 50 U.S.C. § 1810. Henkilöt, joilla on asiavaltuus esillä olevassa asiassa, voivat panna vireille myös siviilioikeudellisen kanteen Yhdysvaltojen hallitusta vastaan saadakseen vahingonkorvausta, mukaan lukien korvauksen asianajajan kuluista, jos heitä koskevaa tietoa, joka on hankittu sähköisen FISA-tarkkailun avulla, on laittomasti ja tieteen tahtoon käytetty tai luovutettu. Ks. 18 U.S.C. § 2712. Jos hallitus on hankkinut henkilöä koskevaa tietoa tai johtanut sitä sähköisen FISA-tarkkailun avulla ja hallitus aikoo käyttää tietoa tai luovuttaa sen kyseisen henkilön vahingoksi oikeudellisessa tai hallinnollisessa prosessissa Yhdysvalloissa, hallituksen on ilmoitettava aikomuksestaan etukäteen tuomioistuimelle ja kyseiselle henkilölle, joka katsoessaan joutuneensa rikkomuksen kohteeksi voi tämän jälkeen kiistää tarkkailun laillisuuden ja vaatia tiedon hävittämistä. Ks. 50 U.S.C. § 1806. Lopuksi FISA-laissa säädetään myös rikosoikeudellisista seuraamuksista henkilöille, jotka osallistuvat tahallisesti lainvastaiseen sähköiseen tarkkailuun lain toimeenpanon varjolla tai jotka tahallisesti käyttävät tai luovuttavat lainvastaisella tarkkailulla hankittua tietoa. Ks. 50 U.S.C. § 1809.

EU:n kansalaisilla on muitakin keinoja saada oikeussuojaa sellaisia hallituksen virkamiehiä vastaan, jotka ovat hallituksen puolesta lainvastaisesti hankkineet henkilötietoja tai käyttäneet niitä, myös silloin kun nämä ovat näin toimiessaan rikkoneet lakia väitettyjen kansalliseen turvallisuuteen liittyvien tarkoituksien vuoksi. Tietokonepetoksista ja -väärinkäytöksistä annetussa laissa (Computer Fraud and Abuse Act) kielletään tahallinen luvaton tunkeutuminen (tai luvallisen pääsyn rajojen ylittäminen) siinä tarkoituksessa, että hankittaisiin tietoja rahoituslaitokselta, Yhdysvaltojen hallituksen tietokonejärjestelmästä tai tietokoneesta, johon on tunkeuduttu internetin kautta. Laissa kielletään myös kiristys- tai petostarkoituksessa tehty uhkaus vahingoittaa suojattua tietokonetta. Ks. 18 U.S.C. § 1030. Jokainen henkilö, olipa tämän kansalaisuus mikä tahansa, joka kärsii vahinkoa tai menetyksiä tämän lain rikkomuksen seurauksena, voi haastaa lakia rikkoneen henkilön (myös hallituksen virkamiehen) oikeuteen ja vaatia tältä vahingonkorvausta sekä tätä koskevaa kielto- tai muuta vastaavaa määräystä lain 1030(g) §:n nojalla riippumatta siitä, onko asiassa nostettu syyte, sillä edellytyksellä, että rikkomukseen liittyy ainakin yksi laissa mainituista monista olosuhteista. Sähköisen viestinnän tietosuojaa koskevassa laissa (Electronic Communications Privacy Act, jäljempänä 'ECPA-laki') säädetään hallituksen pääsystä viestintäpalveluja tarjoavien kolmansien osapuolten hallussa oleviin tallennettuihin sähköisiin viesteihin, liiketapahtumatietoihin ja tilausasiakastietoihin. Ks. 18 U.S.C. §§ 2701–2712. ECPA-laissa annetaan henkilölle, joka katsoo joutuneensa rikkomuksen kohteeksi, mahdollisuus nostaa kanne hallituksen virkamiehiä vastaan sillä perusteella, että nämä ovat tunkeutuneet tallennettuihin tietoihin tahallisesti ja laittomasti. ECPA-lakia sovelletaan kaikkiin henkilöihin kansalaisuudesta riippumatta ja rikkomuksen kohteeksi joutuneet henkilöt voivat saada vahingonkorvausta ja korvauksen asianajajapalkkioistaan. Laki oikeudesta taloudellisen yksityisyyden suojaan (Right to Financial Privacy Act, jäljempänä 'RFPA-laki') rajoittaa Yhdysvaltojen hallituksen pääsyä yksittäisiä asiakkaita koskeviin pankkien ja diilereiden tietoihin. Ks. 12 U.S.C. §§ 3401–3422. RFPA-lain nojalla pankin tai diilerin asiakas voi haastaa Yhdysvaltojen hallituksen oikeuteen ja vaatia tältä vahingonkorvausta sillä perusteella, että asiakkaan tietoja on hankittu laittomasti. Vahingonkorvauksen määrä voi olla laissa määritelty tai perustua toteutuneeseen menetykseen, tai vahingonkorvaus voi olla rankaiseva. Jos laitton tiedonhankinta oli tahallista, kyseisiä hallituksen työntekijöitä koskeva kurinpidollinen tutkinta aloitetaan automaattisesti. Ks. 12 U.S.C. § 3417.

Lopuksi on todettava, että FOIA-lain nojalla kaikilla on pääsy liittovaltion virastojen olemassa oleviin tietoihin. Tiedot voivat koskea mitä tahansa aihetta, tietyin poikkeuksin. Ks. 5 U.S.C. § 552(b). Poikkeuksiin kuuluvat rajoitukset, jotka koskevat pääsyä kansalliseen turvallisuuteen liittyviin turvallisuusluokiteltuihin tietoihin, muiden henkilöiden henkilötietoihin sekä lainvalvonnassa tehtyjen tutkimusten tietoihin. Rajoitukset vastaavat sitä, mitä valtiot ovat säätäneet omissa tiedonsaantia koskevilla laeillaan. Rajoituksia sovelletaan samalla tavalla yhdysvaltalaisiin ja ei-yhdysvaltalaisiin henkilöihin. Jos tietojen luovuttamisesta FOIA-lain nojalla syntyy riitaa, asiassa voidaan tehdä hallinnollinen muutoksenhaku, minkä jälkeen muutosta voidaan hakea liittovaltion tuomioistuimessa. Tuomioistuimen on käsiteltävä asia kokonaan uudestaan päättäessään, oliko tietojen antamatta jättäminen asianmukaista (5 U.S.C. § 552 (a)(4)(B)), ja se voi velvoittaa hallituksen antamaan tiedot. Joissakin tapauksissa tuomioistuin on kumonnut hallituksen väitteet siitä, että tiedot olisi salattava turvallisuusluokituksen vuoksi⁽¹⁾). Vaikka rahamääräisiä vahingonkorvauksia ei voida määrätä, tuomioistuin voi määrätä asianajajan palkkiot korvattavaksi.

VI. PÄÄTELMÄT

Yhdysvaltojen käsityksen mukaan signaalitiedustelussa ja muussa tiedustelussa on otettava huomioon se, että kaikkia yksityishenkilöitä on heidän kansalaisuudestaan tai asuinpaikastaan riippumatta kohdeltava ihmisarvoisesti ja kunnioittavasti ja että kaikilla yksityishenkilöillä on perusteltu tarve yksityisyyden suojaan henkilötietojensa käsittelyssä. Yhdysvallat hyödyntää signaalitiedustelua ainoastaan edistääkseen kansallista turvallisuuttaan ja ulkopoliittisia etujaan sekä suojellakseen omia kansalaisiaan ja liittolaistensa ja kumppaneidensa kansalaisia ongelmilta. Lyhyesti sanottuna tiedusteluyhteisö ei tarkkaile ketään kohdentamattomasti, ei myöskään tavallisia eurooppalaisia ihmisiä. Tietoja kerätään signaalitiedustelun avulla ainoastaan, kun keruuseen on asianmukainen lupa. Lisäksi signaalitiedusteluun ryhdytään vasta sen jälkeen, kun on selvitetty mahdollisuus käyttää vaihtoehtoisia lähteitä, mukaan lukien diplomaattilähteet ja julkiset

⁽¹⁾ Ks. esimerkiksi *New York Times v. oikeusministeriö*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

tiedot. Signaalitiedustelussa annetaan etusija asianmukaisille ja toteuttamiskelpoisille vaihtoehdoille. Signaalitiedustelua toteutetaan aina kun mahdollista siten, että kerätään tietoa ainoastaan erityisestä ulkomaantiedustelun kohteesta tai aiheesta, jonka valinnassa on hyödynnetty erottelukijöitä.

Yhdysvaltojen toimintaperiaatteet signaalitiedustelun suhteen on vahvistettu PPD-28:ssa. Yhdysvaltojen tiedusteluelimillä ei ole näissä oloissa oikeudellista toimivaltaa, resursseja, teknisiä valmiuksia eikä halua salakuunnella maailman kaikkea viestintää. Tiedusteluelimet eivät lue kaikkien yhdysvaltalaisien tai kaikkien maailman ihmisten sähköpostiviestejä. PPD-28:n mukaisesti Yhdysvallat antaa vahvan suojan ei-yhdysvaltalaisien henkilöiden henkilötiedoille, jotka on kerätty signaalitiedustelutoiminnassa. Toimintaperiaatteissa ja menettelytavoissa minimoidaan ei-yhdysvaltalaisien henkilöiden henkilötietojen säilyttäminen ja levittäminen niin suuressa määrin kuin mahdollista kansallinen turvallisuus huomioon ottaen ja sellaisella tavalla että annettu suoja vastaa Yhdysvaltojen kansalaisille annettua suojaa. Lisäksi, kuten edellä on todettu, FISA-lain 702 §:ssä luvalliseksi säädetyn kohdennetun tiedonkeruun valvonta on laajamittaista ja vertaansa vailla. Lopuksi on todettava, että Yhdysvaltojen tiedustelulainsäädännön merkittävät muutokset, jotka ovat tulosta USA FREEDOM Act -laista ja ODNin johdolla toteutetuista, tiedusteluyhteisön läpinäkyvyyden parantamiseen tähtäävistä aloitteista, parantavat merkittävästi kaikkien henkilöiden yksityisyyden suojaa ja kansalaisvapauksia kansalaisuudesta riippumatta.

Kunnioittavasti

Robert S. Litt

21. kesäkuuta 2016

Justin S. Antonipillai
Neuvonantaja
Yhdysvaltojen kauppaministeriö
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ted Dean
Toinen apulaisalivaltiosihteeri
Kauppaministeriön kansainvälisen kaupan osasto
1401 Constitution Avenue, N.W.
Washington, DC 20230

Arvoisa Justin Antonipillai ja arvoisa Ted Dean

Kirjoitan teille antaakseni lisätietoja siitä, millä tavoin Yhdysvallat toteuttaa tietojen valikoimatonta keruuta signaalitiedustelussa. Kuten presidentin määräyksen 28 (PPD-28) alaviitteessä 5 selitetään, "valikoimattomalla" keruulla tarkoitetaan verrattain suuren tietomäärän hankkimista signaalitiedustelun avulla olosuhteissa, joissa tiedusteluyhteisöllä ei ole käytössään tiettyyn kohteeseen liittyvää tunnistetta (kuten kohteen sähköpostiosoitetta tai puhelinnumeroa) eikä keruuta voi tästä syystä kohdentaa tuohon nimenomaiseen kohteeseen. Tämä ei kuitenkaan tarkoita sitä, että tällainen keruu olisi "laajamittaista" tai "kohdentamatonta". PPD-28:ssa tosiaankin edellytetään myös, että signaalitiedustelun on oltava niin räätälöityä kuin mahdollista. Tämän vaatimuksen täyttämiseksi tiedusteluyhteisö pyrkii varmistamaan, että vaikka erityistä tunnistetta ei voidakaan käyttää keruun kohdentamiseen, kerättävä tieto todennäköisesti sisältää ulkomaantiedustelutietoa, joka vastaa Yhdysvaltojen päätöksentekijöiden (aiemmassa kirjeessäni selostettua menetelmää käyttäen) määrittelemää tietotarvetta ja jossa merkityksettömän tiedonkeruun määrä on minimoitu.

Esimerkkinä voidaan mainita, että tiedusteluyhteisöä saatetaan pyytää hankkimaan signaalitiedustelutietoa sellaisen terroristiryhmän toimista, joka operoi jonkin Lähi-idän maan tietyllä alueella ja jonka uskotaan suunnittelevan iskuja Länsi-Euroopan maita vastaan, mutta tiedusteluyhteisö ei välttämättä tiedä tähän terroristiryhmään yhteydessä olevien henkilöiden nimiä, puhelinnumeroja, sähköpostiosoitteita tai muita erityisiä tunnistetta. Voimme päättää kohdentaa tiedustelua tuohon ryhmään siten, että keräämme viestintää, joka suuntautuu tuolle alueelle tai tulee sieltä, ja tarkastamme ja analysoimme näitä viestejä tarkemmin tunnistaksemme ne, jotka liittyvät kyseiseen ryhmään. Tätä tehdessään tiedusteluyhteisö pyrkii rajaamaan keruun niin kapealle alalle kuin mahdollista. Tätä voidaan pitää valikoimattomana keruuna, sillä erottelutekijöitä ei voida käyttää, mutta keruu ei ole laajamittaista eikä kohdentamatonta. Pikemminkin se on niin kohdennettua kuin mahdollista.

Niinpä vaikka keruun kohdentaminen erityisiä valintakriteerejä käyttämällä ei ole mahdollista, Yhdysvallat ei kerää kaikkea viestintää kaikista viestintävälineistä kaikkialta maailmasta vaan käyttää suodattimia ja muita teknisiä välineitä kohdentaakseen keruun viestintävälineisiin, joista todennäköisesti on löydettävissä ulkomaantiedustelun kannalta merkityksellistä viestintää. Näin toimien Yhdysvaltojen signaalitiedustelutoiminta koskee vain murto-osaa internetviestinnästä.

Lisäksi kuten totesin aiemmassa kirjeessäni, koska valikoimattomassa keruussa on suurempi riski siitä, että kerätään merkityksetöntä tietoa, PPD-28:ssa määrätään, että tiedusteluyhteisö voi käyttää valikoimatonta keruuta kuuteen rajattuun käyttötarkoitukseen. PPD-28:ssa ja sen täytäntöönpanemiseksi annetuissa virastojen toimintaperiaatteissa myöskin rajoitetaan signaalitiedustelun avulla hankittujen henkilötietojen säilyttämistä ja levittämistä. Rajoitukset eivät riipu siitä, onko kyse valikoimattomasta vai kohdennetusta keruusta, eivätkä siitä, mikä kohteena olevan henkilön kansallisuus on.

Siten tiedusteluyhteisön valikoimaton keruu ei ole laajamittaista eikä kohdentamatonta, vaan siinä käytetään suodattamismetodeja ja -välineitä, joilla keruu kohdennetaan päätöksentekijöiden esittämiä ulkomaantiedustelun tiedontarpeita vastaavaan aineistoon, samalla kun merkityksettömän tiedon keräämistä minimoidaan ja sen suojelemiseen sovelletaan

tiukkoja sääntöjä. Toimintaperiaatteita ja menettelytapoja, joita tässä kirjeessä kuvataan, sovelletaan kaikkeen valikoimattomaan signaalitiedustelutiedon keruuseen, mukaan lukien valikoimaton keruu, joka koskee Eurooppaan suuntautuvaa ja sieltä lähtevää viestintää. Tällä maininnalla ei vahvisteta eikä kielletä, tapahtuuko tällaista Eurooppaan liittyvää keruuta.

Olette pyytäneet lisätietoja myös yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavasta lautakunnasta (Privacy and Civil Liberties Oversight Board, jäljempänä 'valvontalautakunta') ja virastojen valvontaviranomaisista ja näiden toimivallasta. Valvontalautakunta on toimeenpanohaaraan kuuluva riippumaton virasto. Lautakunnan viisi jäsentä nimittää presidentti, ja nimityksen vahvistaa senaatti ⁽¹⁾. Jäsenet edustavat molempia puolueita. Kunkin lautakunnan jäsenen toimikausi kestää kuusi vuotta. Lautakunnan jäsenille ja henkilöstölle tehdään asianmukaiset turvallisuusselvitykset, jotta he voivat täyttää lakisääteiset tehtävänsä ja velvollisuutensa ⁽²⁾.

Valvontalautakunnan tehtävänä on varmistaa, että liittovaltion hallituksen toimet terrorismin torjumiseksi ovat tasapainossa yksityisyyden ja kansalaisvapauksien suojaamistarpeen kanssa. Lautakunnalla on kaksi perustavanlaatuaista tehtävää – valvonta ja neuvonta. Valvontalautakunta laatii itse oman työohjelmansa ja määrittelee, mitä valvonta- ja neuvontatoimia se haluaa toteuttaa.

Valvontatehtävässään valvontalautakunta tarkastaa ja analysoi toimia, joita toimeenpanohaara toteuttaa suojellakseen kansakuntaa terrorismilta, ja varmistaa, että kyseisten toimien toteuttamistarve on tasapainossa yksityisyyden ja kansalaisvapauksien suojaamistarpeen kanssa ⁽³⁾. Valvontalautakunnan viimeisin päätökseen saatu valvontatehtävä keskittyi FISA-lain 702 §:n nojalla toteutettuihin tarkkailuohjelmiin ⁽⁴⁾. Lautakunta tarkastaa parhaillaan toimeenpanoa- setuksen 12333 nojalla toteutettuja tiedustelutoimia ⁽⁵⁾.

Neuvontatehtävässään valvontalautakunta varmistaa, että kun laaditaan ja pannaan täytäntöön lakeja, asetuksia ja toiminta- periaatteita, jotka liittyvät toimiin kansakunnan suojelemiseksi terrorismilta, kansalaisvapauksiin liittyvät näkökohdat otetaan asianmukaisesti huomioon ⁽⁶⁾.

Tehtävänsä täyttämiseksi lautakunnalla on lakiin perustuva pääsy kaikkiin virastojen merkityksellisiin tietoihin, raportteihin, tarkastuskertomuksiin, arviointeihin, asiakirjoihin, työpapereihin, suosituksiin ja kaikkeen muuhun asiaankuuluvaan aineistoon, kuten turvaluokiteltuihin tietoihin lain määräyksiä noudattaen ⁽⁷⁾. Lisäksi lautakunta voi haastatella ketä tahansa toimeenpanohaaran virkamiestä tai työntekijää ja ottaa tältä lausuntoja tai julkisia todistajan- lausuntoja ⁽⁸⁾. Lisäksi lautakunta voi pyytää kirjallisesti, että oikeusministeri toimittaa lautakunnan puolesta toimeenpa- nohaaran ulkopuoliselle taholle haasteen, jossa tämä veloitetaan antamaan asiaankuuluvaa tietoa ⁽⁹⁾.

Lopuksi on todettava, että valvontalautakunnan on noudatettava läpinäkyvyyttä laissa säädetyllä tavalla. Tähän sisältyy se, että lautakunnan toiminnasta tiedotetaan yleisölle julkisissa kuulemistilaisuuksissa ja että lautakunnan raportit julkistetaan mahdollisimman laajalti noudattaen salaisten tietojen suojaamista koskevia vaatimuksia ⁽¹⁰⁾. Valvontalau- takunnan on lisäksi raportoitava, jos jokin toimeenpanohaaraan kuuluva virasto kieltäytyy noudattamasta sen neuvoja.

Tiedusteluyhteisön valvontaviranomaiset (Inspectors General) tekevät yhteisön ohjelmien ja toimien tarkastuksia ja arviointeja sen selvittämiseksi, onko niissä systemisiä riskejä, heikkouksia ja puutteita. Lisäksi valvontaviranomaiset tutkivat valituksia ja tietoja, jotka sisältävät väitteitä lain, sääntöjen ja asetusten rikkomuksista tai huonosta hallinnosta,

⁽¹⁾ 42 U.S.C. 2000ee(a), (h).

⁽²⁾ 42 U.S.C. 2000ee(k).

⁽³⁾ 42 U.S.C. 2000ee(d)(2).

⁽⁴⁾ Ks. yleisesti <https://www.pclob.gov/library.html#oversightreports>

⁽⁵⁾ Ks. yleisesti <https://www.pclob.gov/events/2015/may13.html>

⁽⁶⁾ 42 U.S.C. 2000ee(d)(1); ks. myös valvontalautakunnan neuvontatoimia koskevasta toimintaperiaatteista ja menettelytavoista annettu asiakirja (PCLOB Advisory Function Policy and Procedure, Policy 2015-004), saatavilla osoitteessa https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf

⁽⁷⁾ 42 U.S.C. 2000ee(g)(1)(A).

⁽⁸⁾ 42 U.S.C. 2000ee(g)(1)(B).

⁽⁹⁾ 42 U.S.C. 2000ee(g)(1)(D).

⁽¹⁰⁾ 42 U.S.C. 2000eee(f).

varojen laajamittaisesta tuhlaamisesta, vallan väärinkäytöstä tai tiedusteluyhteisön ohjelmista ja toimista aiheutuvasta merkittävästä ja erityisestä vaarasta kansanterveydelle ja turvallisuudelle. Valvontaviranomaisen riippumattomuus on keskeistä jokaisen raportin, havainnon ja suosituksen objektiivisuuden ja luotettavuuden kannalta. Riippumattomuuden kannalta seuraavat tekijät ovat kaikkein tärkeimpiä: valvontaviranomaisen nimittämis- ja erottamisprosessi; valvontaviranomaisen toiminnan, talousarvion ja henkilöstöhallinnon eriyttäminen valvottavan viraston toiminnoista; sekä kaksinkertainen raportointi yhtäältä toimeenpanohaaran virastojen päälliköille ja toisaalta kongressille.

Kongressi on perustanut valvontaviranomaisen toimiston jokaiseen toimeenpanohaaran virastoon, myös jokaiseen tiedusteluyhteisön toimijaan⁽¹⁾. Tiedustelutoiminnan talousarviota koskevan vuoden 2015 lain (Intelligence Authorization Act of Fiscal Year 2015) tultua vahvistetuksi lähes kaikkien tiedusteluyhteisön toimijoiden valvontaviranomaiset ovat presidentin nimittämiä ja heidän nimityksensä on senaatin vahvistama. Tämä koskee myös oikeusministeriötä, keskustiedustelupalvelua ja kansallista turvallisuusvirastoa⁽²⁾. Lisäksi valvontaviranomaiset ovat vakinaisia ja puolueisiin kuulumattomia virkamiehiä, jotka ainoastaan presidentti voi erottaa. Vaikka Yhdysvaltojen perustuslaissa säädetään, että presidentti voi erottaa valvontaviranomaisen, erottamisoikeutta on käytetty harvoin, ja sen käyttäminen edellyttää, että presidentti antaa asiasta kongressille kirjallisen perustelun 30 päivää ennen valvontaviranomaisen erottamista⁽³⁾. Näillä menettelytavoilla varmistetaan, että toimeenpanohaaran virkamiehet eivät vaikuta epäasiallisesti valvontaviranomaisen valintaan, nimittämiseen tai erottamiseen.

Valvontaviranomaisella on huomattavat lakiin perustuvat toimivaltuudet toimeenpanohaaran ohjelmien ja operaatioiden tarkastamiseksi, tutkimiseksi ja arvioimiseksi. Niiden tutkimusten ja arviointien lisäksi, jotka tehdään lain määräysten nojalla, valvontaviranomaisella on valvontatyössään laaja harkintavalta ja se voi valita arviointinsa kohteeksi mitkä ohjelmat ja toimet tahansa⁽⁴⁾. Laissa varmistetaan, että valvontaviranomaisella on omat resurssinsa, joiden avulla se voi käyttää toimivaltaansa ja hoitaa tehtävänsä. Valvontaviranomainen voi muun muassa palkata oman henkilökuntansa ja toimittaa kongressille erillisen talousarvioesityksensä⁽⁵⁾. Laissa varmistetaan, että valvontaviranomaisella on pääsy tietoihin, jotka se tarvitsee tehtävänsä hoitamiseksi. Sillä on suora pääsy kaikkiin viraston asiakirjoihin ja tietoihin, joissa on selvityksiä viraston ohjelmista ja operaatioista, eikä tietojen turvaluokituksella ole merkitystä. Sillä on valtuudet hankkia tietoja ja asiakirjoja haasteen avulla, ja se voi vaatia henkilöitä antamaan valahtoisien todistajanlausunnon⁽⁶⁾. Toimeenpanohaaran viraston päällikkö voi rajoitetuissa tapauksissa estää valvontaviranomaisen toiminnan, jos valvontaviranomaisen tarkastus tai tutkimus esimerkiksi heikentäisi merkittävästi Yhdysvaltojen kansallisia turvallisuusintressejä. Tämän toimivaltuuden hyödyntäminen on äärimmäisen epätavallista, ja viraston päällikön on sitä käyttäessään selostettava 30 päivän kuluessa kongressille, miksi hän teki niin⁽⁷⁾. Itse asiassa kansallisen tiedusteluviraston johtaja ei ole koskaan soveltanut tätä rajoittamistoimivaltaa mihinkään valvontaviranomaisen toimeen.

Valvontaviranomaisella on velvollisuus raportoida täysimääräisesti ja ajantasaisesti sekä toimeenpanohaaran virastojen päälliköille että kongressille petoksista ja muista vakavista ongelmista sekä väärinkäytöksistä ja puutteista, jotka se havaitsee toimeenpanohaaran ohjelmissa ja toiminnoissa⁽⁸⁾. Kaksinkertainen raportointi vahvistaa valvontaviranomaisen riippumattomuutta valvontaprosessissa lisäämällä kyseisen prosessin läpinäkyvyyttä ja antaa virastojen päälliköille tilaisuuden panna valvontaviranomaisen suositukset täytäntöön, ennen kuin kongressilla on mahdollisuus ryhtyä lainsäädäntötoimiin. Lain mukaan valvontaviranomaisen on esimerkiksi laadittava puolivuositaisia kertomuksia, joissa kuvaillaan edellä mainittuja ongelmia sekä siihen mennessä toteutettuja korjaustoimia⁽⁹⁾. Toimeenpanohaaran virastot ottavat valvontaviranomaisen havainnot ja suositukset vakavasti, ja valvontaviranomaiset voivat usein sisällyttää näihin ja

⁽¹⁾ Valvontaviranomaisesta vuonna 1978 annetun lain (sellaisena kuin se on muutettuna) 2 ja 4 §; kansallisesta turvallisuudesta vuonna 1947 annetun lain (sellaisena kuin se on muutettuna) 103H §:n b ja e momentti; keskustiedustelupalvelulain 17 §:n a momentti.

⁽²⁾ Ks. julkisoikeudellisia säädöksiä koskeva Pub. L. No. 113-293, 128 Stat. 3990, (19. joulukuuta 2014). Ainoastaan Yhdysvaltojen asevoimien tiedusteluorganisaation ja kansallisen kuvatiedusteluaineistoa käsittelevän viraston valvontaviranomaiset nimittää muu kuin presidentti. Puolustusministeriön ja tiedusteluyhteisön valvontaviranomaisilla on kuitenkin näitä virastoja koskeva rinnakkainen toimivalta.

⁽³⁾ Valvontaviranomaisesta vuonna 1978 annetun lain (sellaisena kuin se on muutettuna) 3 §; kansallisesta turvallisuudesta annetun lain 103H §:n c momentti; keskustiedustelupalvelulain 17 §:n b momentti.

⁽⁴⁾ Ks. valvontaviranomaisesta vuonna 1947 annetun lain 4 §:n a momentti ja 6 §:n a momentin 2 kohta; kansallisesta turvallisuudesta annetun lain 103H §:n e momentti ja g momentin 2 kohdan A alakohta; keskustiedustelupalvelulain 17 §:n a ja c momentti.

⁽⁵⁾ Valvontaviranomaisesta annetun lain 3 §:n d momentti, 6 §:n a momentin 7 kohta ja 6 §:n f momentti; kansallisesta turvallisuudesta annetun lain 103H §:n d, i, j ja m momentti; keskustiedustelupalvelulain 17 §:n e momentin 7 kohta ja f momentti.

⁽⁶⁾ Valvontaviranomaisesta annetun lain 6 §:n a momentin 1, 3, 4, 5 ja 6 kohta; kansallisesta turvallisuudesta annetun lain 103H §:n g momentin 2 kohta; keskustiedustelupalvelulain 17 §:n e momentin 1, 2, 4 ja 5 kohta.

⁽⁷⁾ Ks. esimerkiksi valvontaviranomaisesta annetun lain 8 §:n b momentti ja 8E §:n a momentti; kansallisesta turvallisuudesta annetun lain 103H §:n f momentti; keskustiedustelupalvelulain 17 §:n b momentti.

⁽⁸⁾ Valvontaviranomaisesta annetun lain 4 §:n a momentin 5 kohta; kansallisesta turvallisuudesta annetun lain 103H §:n a momentin b kohdan 3 ja 4 alakohta; keskustiedustelupalvelulain 17 §:n a momentin 2 ja 4 kohta.

⁽⁹⁾ Valvontaviranomaisesta annetun lain 2 §:n 3 momentti ja 4 §:n a momentti ja 5 §; kansallisesta turvallisuudesta annetun lain 103H §:n k momentti; keskustiedustelupalvelulain 17 §:n d momentti. Oikeusministeriön valvontaviranomaisen julkistamat kertomukset ovat saatavilla osoitteessa <http://oig.justice.gov/reports/all.htm>. Vastaavasti tiedusteluyhteisön valvontaviranomainen julkistaa puolivuositaisat kertomuksensa osoitteessa <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>

muihin kertomuksiinsa virastojen ilmoitukset, joiden mukaan virastot hyväksyvät suositukset ja panevat ne täytäntöön, ennen kuin kertomukset toimitetaan kongressille ja toisinaan julkaistaan ⁽¹⁾. Kaksinkertaisen raportoinnin lisäksi valvontaviranomaisilla on velvollisuus ohjata toimeenpanohaarasta tulevia väärinkäytösten paljastajia kuultavaksi asianomaiseen kongressin valvontavaliokuntaan, jossa he voivat selostaa väitteitään toimeenpanohaaran ohjelmissa ja toiminnoissa havaitsemistaan petoksista, varojen tuhlaamisesta tai väärinkäytöksistä. Väärinkäytösten paljastajien henkilöllisyyttä ei kerrota toimeenpanohaaralle, millä suojellaan kyseisiä henkilöitä siltä, että heihin mahdollisesti kohdistettaisiin luvattomia henkilöstötoimia tai turvallisuusselvitystoimia kostoksi raportoisesta valvontaviranomaiselle ⁽²⁾. Kun väärinkäytösten paljastajat ovat usein valvontaviranomaisen tutkimusten tietolähteitä, se, että heitä voidaan kuulla kongressissa ilman että toimeenpanohaara voi vaikuttaa asiaan, lisää valvontaviranomaisen valvonnan vaikuttavuutta. Riippumattomuutensa avulla valvontaviranomainen voi edistää toimeenpanohaaran virastojen taloudellisuutta, tehokkuutta ja vastuuvellisuutta objektiivisesti ja lahjomattomasti.

Lopuksi todetaan, että kongressi on perustanut valvontaviranomaisten neuvoston, joka käsittelee lahjomattomuuteen ja tehokkuuteen liittyviä asioita. Tämä neuvosto muun muassa kehittää valvontaviranomaisille standardeja, jotka koskevat tarkastuksia, tutkimuksia ja arviointeja, sekä edistää koulutusta. Neuvosto, jolla on toimivalta tutkia väitteitä valvontaviranomaisen virkavirheistä, niin ollen valvoo valvontaviranomaisia, jotka valvovat kaikkia muita ⁽³⁾.

Toivon, että näistä tiedoista on Teille hyötyä.

Terveisin
Robert S. Litt
Päälakimies

⁽¹⁾ Valvontaviranomaisesta annetun lain 2 §:n 3 momentti, 4 §:n a momentti ja 5 §; kansallisesta turvallisuudesta annetun lain 103H §:n k momentti; keskustiedustelupalvelulain 17 §:n d momentti. Oikeusministeriön valvontaviranomaisen julkistamat kertomukset ovat saatavilla osoitteessa <http://oig.justice.gov/reports/all.htm>. Vastaavasti tiedusteluyhteisön valvontaviranomainen julkistaa puolivuositaisat kertomuksensa osoitteessa <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>

⁽²⁾ Valvontaviranomaisesta annetun lain 7 §; kansallisesta turvallisuudesta annetun lain 103H §:n g momentin 3 kohta; keskustiedustelupalvelulain 17 §:n e momentin 3 kohta.

⁽³⁾ Valvontaviranomaisesta annetun lain 11 §.

LIITE VII

Yhdysvaltojen oikeusministeriön apulaisoikeusministerin sijaisen ja kansainvälisten asioiden neuvonantajan Bruce Swartzin kirje

19. helmikuuta 2016

Justin S. Antonipillai
Neuvonantaja
Yhdysvaltojen kauppaministeriö
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Toinen apulaisalivaltiosihteeri
Kauppaministeriön kansainvälisen kaupan osasto
1401 Constitution Ave., NW
Washington, DC 20230

Arvoisa Justin Antonipillai ja arvoisa Ted Dean

Tässä kirjeessä esitetään lyhyt yhteenveto tärkeimmistä tutkintavälineistä, joiden avulla yhdysvaltalaisilta yrityksiltä saadaan liiketoimintaan liittyviä ja muita tietoja rikosoikeudellisen lainvalvonnan ja (siviilioikeudellisen ja sääntelyyn liittyvän) yleisen edun nimissä. Kirjeessä kerrotaan myös tietoihin pääsyä koskevista rajoituksista, jotka oikeusperustassa on määrätty⁽¹⁾. Nämä oikeudelliset menettelyt ovat syrjimättömiä siinä mielessä, että niitä käytetään tietojen hankkimiseksi yrityksiltä Yhdysvalloissa, myös sellaisilta yrityksiltä, jotka antavat oman varmennuksensa Privacy Shield-järjestelyssä, eikä rekisteröidyn kansalaisuudella ole merkitystä. Lisäksi yritykset, jotka joutuvat oikeudellisen menettelyn kohteeksi Yhdysvalloissa, voivat nostaa asiaa koskevan kanteen tuomioistuimessa, kuten jäljempänä esitetään⁽²⁾.

Yhdysvaltojen perustuslain neljännellä lisäyksellä on erityistä merkitystä viranomaisten takavarikoidessa tietoja. Lisäyksessä säädetään seuraavaa: "Kansalaisten oikeutta olla turvassa henkilöönsä, taloonsa, asiakirjojihinsa ja muuhun omaisuuteensa kohdistuvilta kohtuuttomilta etsinnöiltä ja takavarikoinneilta älköön loukattako, älköönkään etsintälupaa annettako muutoin kuin todennäköisestä syystä, joka on vahvistettu valalla tai juhlallisella vakuutuksella, ja etsintäluvassa on erityisesti mainittava etsinnän tapahtumapaikka sekä pidettävät henkilöt ja takavarikoitavat esineet." Yhdysvaltojen korkein oikeus totesi asiassa *Berger v. New Yorkin osavaltio* seuraavaa: "kuten tämä tuomioistuin 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). Kun etsintälupavaatimusta ei sovelleta, hallituksen on noudatettava tomissaan neljännen lisäyksen edellyttämää "kohtuutta". Näin ollen perustuslaissa itsessään varmistetaan, että Yhdysvaltojen hallituksen valta takavarikoida kansalaisten tietoja ei ole rajatonta tai mielivaltaista.

Rikoslain valvonnassa hyödynnettävät valtuudet:

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 valamiehaston

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

⁽²⁾ Tässä asiakirjassa käsitellään lainvalvonnan ja sääntelyn oikeusperustaa liittovaltion tasolla. Osavaltiot tutkivat osavaltioiden lakien rikkomukset, ja niitä koskevat asiat käsitellään osavaltioiden tuomioistuimissa. Osavaltioiden lainvalvontaviranomaiset hyödyntävät etsintämääräyksiä ja haasteita, jotka myönnetään 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).

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 kehutus avustaa valamiehistöä tutkimuksessa, joka koskee tiettyä rikoslain rikkomusepäilystä. Haaste annetaan tavallisesti liittovaltion syyttäjän pyynnöstä. Suuret valamiehistöt kuuluvat tuomioistuimen tutkintahaaraan, ja niiden jäsenet valitsee tuomari tai avustava tuomari. Haasteissa 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 valvonnassa. 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 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 meneillään 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 lainvalvojien 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. Rikoslakia valvovien viranomaisten on hankittava haaste, jos he haluavat saada tilausasiakkaiden rekisteröintitietoja, IP-osoitteita ja niihin liittyviä aikaleimoja tai laskutustietoja. Useimpien muiden tallennettujen, ei-sisällöllisten tietojen osalta, kuten sellaisten sähköpostiosoitteiden osalta, joista ei ilmene viestin aihe, lainvalvontaviranomaisten on esitettävä tuomarille erityisiä seikkoja, jotka osoittavat, että pyydytetyt tiedot ovat merkityksellisiä ja olennaisia vireillä olevan rikostutkinnan kannalta. Jotta rikoslain valvonnasta vastaavat viranomaiset voivat saada pääsyn sähköisen viestinnän tallennettuun sisältöön, ne yleensä hankkivat tuomarilta määräyksen, jonka perusteena ovat todennäköiset syyt siitä, että kyseisellä tilillä on todisteita rikoksesta. Tallennettua viestintää koskevassa laissa säädetään myös siviili- ja rikosoikeudellisista seuraamuksista.

Tarkkailua koskevat tuomioistuimen määräykset puhelinkuuntelua koskevan liittovaltion lain nojalla: Lisäksi lainvalvontaviranomaiset voivat rikostutkimustarkoituksissa salakuunnella reaaliaikaisesti langallista, suullista tai sähköistä viestintää puhelinkuuntelua koskevan liittovaltion lain nojalla. Ks. 18 U.S.C. §§ 2510–2522. Tämän välineen käyttäminen edellyttää aina tuomioistuimen määräystä. 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.

Etsintämääräys – sääntö 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 löydetävissä 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. Ks. Yhdysvaltojen perustuslain neljäs lisäys (josta tarkempaa selostusta edellä), liittovaltion rikosprosessisääntöjen kohta 41. Etsintämääräyksen kohde voi pyrkiä kumoamaan määräyksen sillä perusteella, että se on liiallinen, aiheeton tai muuten epäasianmukaisesti hankittu, ja osapuoli, joka katsoo oikeuksiensa tulleen loukatuksi ja jolla on asiavaltuus esillä olevassa asiassa, voi vaatia, että laittomalla etsinnällä saadut todisteet hävitetään. Ks. Mapp v. Ohio, 367 U.S. 643 (1961).

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\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG))). 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 Yhdysvaltojen oikeusministeriön käsikirjassa, joka on saatavilla osoitteessa <http://www.justice.gov/usam/united-states-attorneys-manual>

Siviilihallinto- ja sääntelyviranomaisten (yleisen edun mukaiset) valtuudet:

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 toimivalta 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 heidän hallussaan 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. Ks. 31 U.S.C. § 5318, 31 C.F.R. osa X. Muut yritykset voivat tukeutua luottokelpoisuusraportointia koskevaan Fair Credit Reporting Act -lakiin (ks. 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. §§ 3401–3422. Näin ollen Yhdysvaltojen tuomioistuimet vahtivat, että sääntelyhaastepyyntöt ovat asiallisia, ja valvovat riippumattomasti liittovaltion virastojen toimia.

Lopuksi on todettava, että kaikkien lakisäateisten valtuuksien, jotka hallintoviranomaisilla on tietojen fyysiseen takavarikoimiseen yritykseltä Yhdysvalloissa, on oltava neljännen lisäyksen mukaisia. Ks. See v. Seattlen kaupunki, 387 U.S. 541 (1967).

Päätelmät

Kaikkien lainvalvonta- ja sääntelytoimintojen on noudatettava sovellettavaa lainsäädäntöä Yhdysvalloissa, mukaan lukien perustuslakia, lakeja, sääntöjä ja asetuksia. Toimintojen 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 yhdysvaltalaisia tai ulkomaisia henkilöitä – ja lisäksi annetaan mahdollisuus siihen, että kaikki viranomaisten tietopyynnöt, jotka perustuvat laissa myönnettyihin valtuuksiin, voidaan saattaa oikeudellisen valvonnan kohteeksi tuomioistuimessa.

Kunnioittavasti

Bruce C. Swartz

Apulaisoikeusministerin sijainen ja kansainvälisten
asioiden neuvonantaja
