TIETOSUOJATYÖRYHMÄ

16/FI
WP 238

Lausunto 1/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevasta komission päätösehdotuksesta

Annettu 13. huhtikuuta 2016

TIIVISTELMÄ

Euroopan komissio julkaisi 29. helmikuuta 2016 tietosuojan tason riittävyyttä koskevan tiedonannon, päätösehdotuksen ja sen liitteet, jotka kaikki yhdessä muodostavat uudet puitteet kaupallisessa tarkoituksessa tapahtuvaan henkilötietojen transatlanttiseen vaihtoon: EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn. Sillä on tarkoitus korvata aiemmat safe harbor -periaatteet, jotka Euroopan unionin tuomioistuin (jäljempänä ’unionin tuomioistuin’) mitätöi asiassa Schrems 6. lokakuuta 2015 antamassaan tuomiossa.

Tietosuojatyöryhmä on arvioinut nämä asiakirjat direktiivin 95/46/EY 30 artiklan 1 kohdan c alakohdan mukaisesti antaakseen lausunnon tietosuojan tason riittävyyttä koskevasta päätösehdotuksesta. Tietosuojatyöryhmä on arvioinut sekä Privacy Shield -järjestelyn kaupallisia näkökohtia että mahdollisia poikkeamia järjestelyn periaatteista kansallisen turvallisuuden, lainvalvonnan ja yleisen edun takia.

Tietosuojatyöryhmä on ottanut huomioon direktiivissä 95/46/EY vahvistetun EU:n tietosuojaa koskevan oikeudellisen kehyksen sekä Euroopan ihmisoikeussopimuksen 8 artiklassa ja Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa vahvistetut yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevat perusoikeudet. Lisäksi työryhmä otti huomioon perusoikeuskirjan 47 artiklassa vahvistetun oikeuden tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, samoin kuin eri perusoikeuksiin liittyvän oikeuskäytännön.

Analyysissa on myös otettu huomioon unionin tuomioistuimen Schrems-tuomiossa esittämät perustelut, jotka koskevat komission harkintavaraa tietosuojan tason riittävyyden arvioinnissa. Tietosuojan tason riittävyyttä koskevat vaatimukset on tarkastettava huolellisesti ja niitä on valvottava tarkasti ottaen huomioon yksityisyyttä ja tietosuojaa koskevat perusoikeudet ja niiden henkilöiden lukumäärä, joihin tietojen siirtäminen mahdollisesti vaikuttaa.

Privacy Shield -järjestelyä on tarkasteltava nykyisessä kansainvälisessä kontekstissa, johon liittyvät muun muassa massadatan käsittely ja lisääntyvät turvallisuustarpeet. Henkilötietojen keruun ja käytön ala ja määrä ovat lisääntyneet jyrkästi sen jälkeen, kun alkuperäinen safe harbor -periaatteita koskeva päätös tehtiin vuonna 2000. Euroopan tietosuojaviranomaiset korostavat voimakkaasti, kuinka tärkeitä niiden puolustamat periaatteet ovat.

Aluksi tietosuojatyöryhmä toteaa olevansa tyytyväinen niihin merkittäviin parannuksiin, joita Privacy Shield -järjestelyssä on tehty safe harbor -periaatteisiin verrattuna. Työryhmä panee merkille, että neuvottelijat ovat puuttuneet moniin safe harbor -periaatteiden puutteisiin, joita työryhmä korosti varapuheenjohtaja Redingille 10. huhtikuuta 2014 osoittamassaan kirjeessä.

Privacy Shield -järjestelyn periaatteet ja takeet on esitetty sekä tietosuojan tason riittävyyttä koskevassa päätöksessä että sen liitteissä, mikä hankaloittaa tietojen löytämistä, ja toisinaan tiedot ovat ristiriitaisiakin. Tästäkin syystä uudet puitteet ovat kokonaisuudessaan vaikeaselkoisia, ja tietojen saaminen on vaikeaa niin rekisteröidyille, organisaatioille kuin tietosuojaviranomaisille. Edes käytetty kieli ei ole selkeää. Siitä syystä tietosuojatyöryhmä

kehottaa komissiota selkeyttämään puitteita ja tekemään niistä ymmärrettäviä Atlantin molemmin puolin.

Sovellettavasta laista tietosuojatyöryhmä korostaa, että jos Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskeva päätös tehdään direktiivin 95/46/EY perusteella, päätöksen on oltava EU:n tietosuojaa koskevan oikeudellisen kehyksen mukainen sekä soveltamisalaltaan että termistöltään. Tietosuojatyöryhmä katsoo, että tietosuojan tason riittävyyttä koskevaa päätöstä ja sen liitteitä on tarkasteltava uudelleen pikaisesti sen jälkeen, kun yleistä tietosuoja-asetusta aletaan soveltaa. Siten varmistetaan, että niissä noudatetaan asetuksen mukaista entistä korkeampaa tietosuojan tasoa.

Privacy Shield -järjestelyn kaupallisista näkökohdista

Tietosuojatyöryhmän keskeinen tavoite on varmistaa, että silloin kun henkilötietoja käsitellään Privacy Shield -järjestelyn säännösten mukaisesti, henkilöiden tietosuoja pääosiltaan vastaa tasoa, joka taataan unionissa.. Vaikka tietosuojatyöryhmä ei edellytäkään, että Privacy Shield -järjestely olisi pelkästään perinpohjainen kopio EU:n lainsäädännöstä, se katsoo, että järjestelyyn olisi sisällytettävä olennaiset osat lainsäädännön perusperiaatteista. Sitä kautta järjestelyssä varmistettaisiin, että tietosuoja ”pääosiltaan vastaa tasoa, joka taataan unionissa”.

Privacy Shield -järjestelyyn tehdyistä parannuksista huolimatta tietosuojatyöryhmä katsoo, että joitain eurooppalaisessa oikeudessa esitettyjä keskeisiä tietosuojaperiaatteita joko ei ole otettu huomioon tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa ja sen liitteissä tai niitä on korvattu vaihtoehtoisilla käsitteillä vaillinaisesti.

Esimerkiksi tietojen säilyttämistä koskevaa periaatetta ei erikseen mainita eikä sitä voida selkeästi johtaa tietojen eheyttä ja käyttötarkoituksen rajoittamista koskevan periaatteen nykyisestä sanamuodosta. Lisäksi päätöksessä ei ole mitään säännöstä suojasta, joka olisi annettava yksinomaan automaattiseen tietojenkäsittelyyn perustuvia automatisoituja yksittäispäätöksiä vastaan. Käyttötarkoituksen rajoittamista koskevan periaatteen soveltaminen henkilötietojen käsittelyyn on myös epäselvää. Jotta useita tärkeitä käsitteitä voitaisiin selkeyttää, tietosuojatyöryhmä ehdottaa, että EU:n ja USA:n olisi sovittava käsitteille selkeät määritelmät ja nämä määritelmät olisi sisällytettävä Privacy Shield -järjestelyä koskevaan usein kysyttyjen kysymysten osioon liitettävään sanastoon (*Privacy Shield F.A.Q*).

Koska Privacy Shield -järjestelyä käytetään myös henkilötietojen siirtoon Yhdysvaltojen ulkopuolelle, tietosuojatyöryhmä pitää erityisen tärkeänä, että tietojen siirrossa edelleen Privacy Shield -yksiköltä kolmannen maan vastaanottajalle noudatetaan samaa tietoturvan tasoa kaikkien järjestelyn näkökohtien osalta (myös kansallisen turvallisuuden osalta), eikä siirto saa johtaa EU:n tietosuojaperiaatteiden heikentämiseen tai kiertämiseen. Jos henkilötietojen siirtämistä edelleen suunnitellaan osana Privacy Shield -järjestelyä, jokainen Privacy Shield -järjestelyyn liittynyt organisaatio olisi velvoitettava arvioimaan tietojen tuojaan sovellettavan kolmannen maan kansallisen lainsäädännön mahdolliset pakolliset

vaatimukset ennen tietojen siirtämistä. Tietosuojatyöryhmä toteaa yleisesti, että EU:n henkilötietojen edelleen siirtämistä säännellään riittämättömästi, erityisesti edustajille siirrettävien tietojen alan, käyttötarkoituksen rajoittamisen ja takeiden osalta.

Lopuksi tietosuojatyöryhmä toteaa, että vaikka henkilöille on annettu lisää muutoksenhakukeinoja oikeuksiensa käyttämiseen, uudet oikeussuojakeinot saattavat osoittautua liian monimutkaisiksi ja hankaliksi, jotta EU:n luonnolliset henkilöt voisivat niitä käyttää, ja sen takia tehottomiksi. Sitä varten eri muutoksenhakumenettelyjä on edelleen selkeytettävä. Erityisesti EU:n tietosuojaviranomaiset voisivat niin halutessaan toimia EU:n luonnollisten henkilöiden luontaisina yhteyspisteinä eri menettelyissä. Tietosuojaviranomaiset voisivat myös päättää, että ne toimivat kyseisissä menettelyissä henkilöiden puolesta.

Kansallista turvallisuutta varten tehtävät poikkeukset

Tietosuojatyöryhmä palauttaa mieliin viranomaisten tiedonsaantia EU:ssa ja kolmansissa maissa sekä siihen liittyviä perusoikeuksia koskevan analyysinsa, joka sisältyy valmisteluasiakirjaan WP 237 (*European Essential Guarantees*). Siinä käsitellään oikeutettua puuttumista yksityisyyden ja tietosuojan perusoikeuksiin tarkkailutoimenpitein, kun henkilötietoja siirretään.

Merkittävää edistystä safe harbor -päätökseen verrattuna merkitsee se, että tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa käsitellään nyt laajasti Privacy Shield -järjestelyssä käsiteltyjen tietojen mahdollista käyttöä kansallisen turvallisuuden ja lainvalvonnan tarkoituksiin. Tietosuojatyöryhmä pitää tätä merkittävänä askeleena, samoin kuin Yhdysvaltojen hallinnon entistä suurempaa avoimuutta tiedustelutietojen keruuseen sovellettavan lainsäädännön osalta (liite VI).

Tietosuojatyöryhmä toteaa kuitenkin, että kansallisen tiedusteluviraston johtajan (*Office of the Director of National Intelligence*, ODNI) antamassa vakuutuksessa ei suljeta pois EU:sta peräisin olevien henkilötietojen laajamittaista ja kohdentamatonta keruuta. Tietosuojatyöryhmä muistuttaa kantansa olleen jo pitkään, että henkilöiden laajamittaista ja kohdentamatonta tarkkailua ei koskaan voida pitää oikeasuhteisena tai ehdottoman tarpeellisena demokraattisessa yhteiskunnassa. Perusoikeuksien tarjoama suoja edellyttää tätä. Lisäksi kaikkien tarkkailuohjelmien kattava valvonta on ratkaisevan tärkeää. Tietosuojatyöryhmä toteaa yleisenä suuntauksena olevan, että tietoja kerätään yhä enemmän laajamittaisesti ja kohdentamattomasti terrorismin torjunnan vuoksi. Ottaen huomioon huolet, joita tämä aiheuttaa yksityisyyttä ja tietosuojaa koskevien perusoikeuksien suojelun kannalta, tietosuojatyöryhmä odottaa unionin tuomioistuimen tulevia ratkaisuja laajamittaista ja kohdentamatonta tiedon keruuta koskevissa asioissa.

Tietosuojatyöryhmä on tyytyväinen siihen, että uudeksi oikeussuojakeinoksi on perustettu oikeusasiamiesmekanismi. Se voi merkitä EU:n luonnollisten henkilöiden oikeuksien merkittävää parannusta Yhdysvaltojen tiedustelutoimintaan nähden. Tietosuojatyöryhmä on kuitenkin huolissaan siitä, ettei uusi instituutio ole riittävän riippumaton eikä sillä ole riittäviä

valtuuksia, jotta se voisi hoitaa tehtävänsä tehokkaasti. Se ei myöskään takaa tyydyttävää oikeussuojakeinoa riitatapauksissa.

Yhteinen tarkastelu

Tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa mainittu yhteinen vuotuinen tarkastelumekanismi on keskeinen tekijä Privacy Shield -järjestelyn yleisen uskottavuuden kannalta, ja tietosuojatyöryhmä on erittäin tyytyväinen sen tarjoamasta mahdollisuudesta tietosuojan tason riittävyyttä koskevan päätöksen uudelleentarkasteluun. Tässä suhteessa tietosuojatyöryhmä on ymmärtänyt, että tietosuojatyöryhmän kansalliset edustajat voivat osallistua tarkasteluprosessiin täysimääräisesti, mutta se pyytää selkeyttämään järjestelyjen yksityiskohtia. Menettelytavoista on sovittava hyvissä ajoin ennen ensimmäistä tarkastelua, muun muassa tarkastelun tuloksen raportoinnista, sen julkisuudesta ja mahdollisista seurauksista sekä rahoituksesta.

Päätelmät

Tietosuojatyöryhmä toteaa, että Privacy Shield -järjestely tarjoaa merkittäviä parannuksia safe harbor -periaatteita koskevaan päätökseen verrattuna. Tietosuojatyöryhmä on kuitenkin kartoittanut järjestelyyn liittyviä ongelmakohtia ja pyytänyt selkeyttämään tiettyjä seikkoja. Tämän vuoksi työryhmä kehottaa komissiota ratkaisemaan kyseiset ongelmat, osoittamaan asianmukaiset ratkaisut ja antamaan pyydetyt selvennykset. Näin tietosuojan tason riittävyyttä koskevaa päätösehdotusta voidaan parantaa ja varmistaa, että Privacy Shield –järjestelyn tietosuojan taso todellakin vastaa pääosiltaan EU:ssa tarjottua tasoa.

SISÄLLYSLUETTELO

1. JOHDANTO

Sen jälkeen, kun Euroopan unionin tuomioistuin (jäljempänä ’unionin tuomioistuin’) antoi 6. lokakuuta 2015 tuomionsa asiassa Schrems[1], tietosuojaryhmä kehotti Euroopan unionin (jäljempänä ’EU’) jäsenvaltioita ja muita EU:n toimielimiä aloittamaan Amerikan yhdysvaltojen (jäljempänä ’Yhdysvallat’) viranomaisten kanssa keskustelut, joiden tavoitteena olisi saada aikaan poliittinen, oikeudellinen ja tekninen ratkaisu, jotta tietoja voidaan siirtää Yhdysvaltojen alueelle perusoikeuksia kunnioittaen.

Lähes kahden vuoden neuvottelujen jälkeen Euroopan komissio ja Yhdysvaltojen kauppaministeriö pääsivät 2. helmikuuta 2016 poliittiseen yhteisymmärrykseen uusista puitteista kaupallisessa tarkoituksessa tapahtuvaan henkilötietojen transatlanttiseen vaihtoon eli EU:n ja Yhdysvaltojen välisestä Privacy Shield -järjestelystä (jäljempänä ’Privacy Shield -järjestely’), jolla on tarkoitus korvata Yhdysvaltojen entiset safe harbor -periaatteet.

Komissio julkaisi 29. helmikuuta 2016 tiedonannon[2], ehdotuksen tietosuojan tason riittävyyttä koskevaksi päätökseksi ja sen liitteet, jotka kaikki yhdessä muodostavat Privacy Shield -järjestelyn. Tietosuojatyöryhmä on direktiivin 95/46/EY (jäljempänä ’direktiivi’) 30 artiklan 1 kohdan c alakohdan mukaisesti arvioinut mainittuja asiakirjoja antaakseen ajantasaisen lausunnon komission valmistelemasta tietosuojan tason riittävyyttä koskevasta päätösehdotuksesta, siihen kuuluvat Privacy Shield -asiakirjat mukaan luettuina. Tietosuojatyöryhmä on arvioinnissaan jakanut työn kahteen osaan: Privacy Shield -järjestelyn kaupallisen osan arviointi ja niiden suojatoimien analyysi, jotka koskevat poikkeamia Privacy Shield -periaatteista kansallisen turvallisuuden, lainvalvonnan ja yleisen edun takia.

Schrems-tuomion antamisen jälkeen tietosuojatyöryhmä on järjestänyt useita kokouksia Yhdysvaltojen hallinnon valtuuskuntien sekä EU:n että Yhdysvaltojen kansalaisjärjestöjen edustajien ja tieteellisten asiantuntijoiden kanssa. Tavoitteena on ollut arvioida Schrems-tuomion seurauksia. Uusia kokouksia Euroopan komission ja Yhdysvaltojen hallinnon edustajien välillä on järjestetty Privacy Shield -järjestelyn arvioinnin aikana. Joitakin selvennyksiä on näiden kokousten aikana saatu, ja ne on otettu tässä lausunnossa huomioon. Tietosuojatyöryhmä korostaa, että tässä vaiheessa annetut selvennykset ovat vasta epävirallisia eikä niiden voida katsoa olevan tietosuojan tason riittävyyttä koskevan päätösehdotuksen olennainen osa, koska niitä ei ole esitetty kirjallisesti.

Tietosuojatyöryhmä on kuitenkin erityisen tyytyväinen Yhdysvaltojen kauppaministeriön näissä kokouksissa antamaan sitoumukseen tehdä yhteistyötä EU:n jäsenvaltioiden tietosuojaviranomaisten kanssa Privacy Shield -järjestelyn soveltamisessa ja antaa ohjeita ja oikeudellisia tulkintoja Privacy Shield -järjestelyn soveltamisesta julkaistavaksi niiden verkkosivustoissa.

1 Unionin tuomioistuimen tuomio 6.10.2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (jäljempänä ’Schrems-tuomio’).
2 COM(2016) 117 final, 29.2.2016.

1.1 Yleiset huomautukset

1.1.1 Tietosuojatyöryhmän arvioinnin ulottuvuus

Ensinnäkin tietosuojatyöryhmä on ottanut huomioon EU:n jäsenvaltioissa sovellettavan tietosuojasäännöstön, myös Euroopan ihmisoikeussopimuksen 8 artiklan, jossa annetun suojan piiriin kuuluu oikeus nauttia yksityis- ja perhe-elämän kunnioitusta, ja Euroopan unionin perusoikeuskirjan (jäljempänä 'perusoikeuskirja') 7, 8 ja 47 artiklan, joissa suojataan vastaavasti yksityis- ja perhe-elämän kunnioittamista, henkilötietojen suojaa sekä oikeutta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen. Lisäksi on otettu huomioon asiaankuuluva oikeuskäytäntö ja direktiivin vaatimukset.

Unionin tuomioistuin on Schrems-tuomiossa aiempaa tarkemmin määritellyt vaatimusta, jonka mukaan kolmannen maan on varmistettava riittävä tietosuojan taso. Tuomioistuin selitti ensinnäkin, että direktiivin säännöksiä on tulkittava ”perusoikeuskirjassa taattujen perusoikeuksien valossa”[3] – erityisesti sen 7 ja 8 artiklassa mainittujen oikeuksien valossa. Lisäksi tuomioistuin totesi, että ilmaus ”tietosuojan riittävä taso” on ”ymmärrettävä siten, että sillä tarkoitetaan vaatimusta, että kolmas maa tosiasiallisesti takaa maan sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta perusvapauksien ja -oikeuksien suojan sellaisen tason, joka pääosiltaan vastaa tasoa, joka taataan unionissa direktiivin 95/46, luettuna perusoikeuskirjan valossa, nojalla”[4]. Edellisestä safe harbor -periaatteita koskevasta päätöksestä sellaista arviointia ei koskaan tehty riittävän yksityiskohtaisesti. Siitä syystä tietosuojatyöryhmä on arvioinut tietosuojan tason riittävyyttä koskevaa päätösehdotusta mainitun vaatimuksen pohjalta: analysoidaan, *vastaako* perusoikeuksien ja vapauksien suojan taso *pääosiltaan* tasoa, joka taataan unionissa. Tietosuojatyöryhmä korostaa, että tässä lausunnossa on esitetty sen tärkeimmät huolenaiheet, mutta muitakin ongelmakohtia saattaa myöhemmin tulla esiin, koska tietosuojan tason riittävyyttä koskevan päätösehdotuksen julkaisemisesta on kulunut niin vähän aikaa.

Tietosuojatyöryhmä toteaa, että unionin tuomioistuin on määritellyt Schrems-tuomiossa aiempaa tarkemmin direktiivin 25 artiklan 6 kohdassa käytettyä ilmausta ”riittävä” siten, että sen katsotaan tarkoittavan ”pääosiltaan vastaavaa tietosuojan tasoa”. Lisäksi tuomioistuin korosti, että vaikka ilmauksella ”tietosuojan riittävä taso” ei vaadita kolmatta maata takaamaan tietosuojan tasoa, joka olisi täysin sama kuin unionin oikeusjärjestyksessä taattu taso, ilmaus on kuitenkin ymmärrettävä siten, että sillä tarkoitetaan vaatimusta, että kolmas maa tosiasiallisesti takaa sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta perusvapauksien ja -oikeuksien suojan sellaisen tason, joka *pääosiltaan vastaa* tasoa, joka taataan unionissa direktiivin nojalla perusoikeuskirjan valossa.

3 Schrems-tuomion 38 kohta.
4 Schrems-tuomion 73 kohta.

1.1.2 Tietosuojan tason riittävyyttä koskevan päätösehdotuksen kaupallisen osan arviointi

Tietosuojatyöryhmä on jo valmisteluasiakirjassaan nro 12[5] selittänyt tavan, jolla se soveltaa EU:n keskeisiä tietosuojaperiaatteita henkilötietojen siirtoon kolmansiin maihin (*Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive)*. Tietosuojatyöryhmä yritti kartoittaa sellaisia vastaavia suojatoimia, joilla voitaisiin varmistaa direktiivissä taattuja periaatteita vastaava suojan taso, erityisesti seuraavien seikkojen osalta: käyttötarkoituksen rajoitus, tiedon laatu ja suhteellisuusperiaate, avoimuus, turvallisuus, oikeus saada tietoja, saada ne oikaistuksi ja vastustaa niiden käsittelyä, tietojen säilyttäminen ja tietojen edelleen siirtämistä koskevat rajoitukset. Vastaavaa menetelmää on käytetty tietosuojatyöryhmän lausunnoissa[6], jotka koskevat alkuperäisen safe harbor -periaatteita koskevan päätöksen arviointia, samoin suosituksissa, jotka työryhmä antoi 10. huhtikuuta 2014 julkaistussa kirjeessään komission entiselle varapuheenjohtajalle ja oikeusasioista vastaavalle komission jäsenelle Viviane Redingille[7].

1.1.3 Viranomaisten tiedonsaantioikeutta koskevien poikkeusten ja niitä koskevien suojatoimien arviointi

On monimutkaista arvioida poikkeuksia, jotka koskevat viranomaisten oikeutta saada Privacy Shield -järjestelyyn kuuluvia henkilötietoja, erityisesti kun otetaan huomioon tietosuojaviranomaisten ja suuren yleisön lisääntynyt tietoisuus Yhdysvaltojen tarkkailuohjelmista Snowden-paljastusten jälkeen. Tietosuojatyöryhmä arvostaa Yhdysvaltojen hallinnon pyrkimystä lisätä tarkkailuohjelmien avoimuutta ja sen halukkuutta lisätä Privacy Shield -järjestelyyn uusia suojatoimia ja suhtautuu näihin seikkoihin myönteisesti. Samalla työryhmä korostaa, että kaikenlaisen puuttumisen yksityiselämän ja tietosuojan perusoikeuksiin on demokraattisessa yhteiskunnassa perustuttava oikeutettuihin perusteisiin. Unionin tuomioistuin on arvostellut sitä seikkaa, ettei safe harbor -periaatteita koskeva päätös sisällä mitään toteamusta siitä, onko Yhdysvalloissa valtiollisia sääntöjä, joilla on tarkoitus rajoittaa mahdollista puuttumista perusoikeuksiin. Päätöksessä ei myöskään mainita, että tällaista puuttumista vastaan olisi olemassa tehokasta oikeussuojaa.[8]

Siitä syystä tietosuojatyöryhmä on analysoinut Yhdysvaltojen voimassa olevaa säädöskehystä ja Yhdysvaltojen tiedusteluvirastojen käytäntöjä sellaisina kuin ne on kuvattu päätösehdotuksen liitteissä, samoin kuin edellytyksiä, joissa sallitaan puuttuminen yksityiselämää ja tietosuojaa koskeviin perusoikeuksiin sellaisina kuin niitä suojellaan EU:n lainsäädännössä.

5 Hyväksytty tietosuojatyöryhmässä 24.7.1998. Ks. erityisesti s. 6.
6 Ks. tietosuojatyöryhmän asiakirjat WP 62, WP 32, WP 27, WP 23, WP 21, WP 19, WP 15 ja WP 7.
7 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
8 Schrems-tuomion 87 ja 88 kohta.

Perusoikeuksia koskevan eurooppalaisen oikeuskäytännön valossa on arvioitu, onko puuttuminen perusoikeuksiin oikeutettua demokraattisessa yhteiskunnassa. Oikeuskäytännössä on vahvistettu tiedustelutoimintaa varten neljä olennaista taetta[9]:

A. Tietojenkäsittelyn on oltava lainmukaista, ja sen on perustuttava selkeisiin, täsmällisiin ja helppotajuisiin sääntöihin: tällä tarkoitetaan, että jokaisen suhteellisen hyvin asioista perillä olevan henkilön on voitava ennakoida, mitä hänen tiedoilleen saattaa tapahtua, jos ne siirretään edelleen.
B. Henkilötietojen käsittelyn tarpeellisuus ja oikeasuhteisuus oikeutettujen tavoitteiden näkökulmasta on osoitettava: yksilön oikeudet ja tavoite, jota varten tietoja kerätään ja käytetään, on asetettava tasapainoon.
C. Tarvitaan riippumaton valvontamekanismi, joka on sekä tehokas että puolueeton: se voi olla joko tuomioistuin tai muu riippumaton elin sikäli kuin sillä on riittävät valmiudet tehdä tarvittavat tarkastukset.
D. Henkilön käytettävissä on oltava tehokkaat oikeussuojakeinot: jokaisella on oltava oikeus puolustaa oikeuksiaan riippumattomassa elimessä.

1.2 Tietosuojan tason riittävyyttä koskeva päätösehdotus

Ensinnäkin tietosuojatyöryhmä on tyytyväinen siitä tosiseikasta, että uusi tietosuojan tason riittävyyttä koskeva menettely voidaan aloittaa alle kuuden kuukauden kuluttua siitä, kun unionin tuomioistuin julisti safe harbor -päätöksen pätemättömäksi. Oikeustilanne on syytä selkeyttää nopeasti, kun otetaan huomioon päivittäin EU:n ja Yhdysvaltojen välillä siirrettävien tietojen määrä, jonka tietosuojatyöryhmä tunnustaa olevan talouden elintärkeä osa molemmin puolin Atlanttia.

Tietosuojatyöryhmä pahoittelee kuitenkin sitä, ettei komission julkaisemaan tietosuojan tason riittävyyttä koskevaan päätösehdotukseen sisälly direktiivin 25 artiklan mukaisesti Yhdysvaltojen sisäistä lainsäädäntöä ja kansainvälisiä sitoumuksia koskevaa kattavaa arviointia tietosuojan tason riittävyyttä koskevan selvityksen muodossa, kuten vastaavissa menettelyissä on aiemmin ollut säännönmukaisesti tapana. Tästä syystä tietosuojatyöryhmä ei ole voinut analysoida täydellisesti Privacy Shield -järjestelyn oikeudellista toimintaympäristöä. Työryhmä toteaa esimerkiksi, että nykyisessä tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa ei ole selvitetty Yhdysvalloissa sekä liittovaltion että osavaltion tasolla tai alakohtaisesti voimassa olevaa yksityisyys- ja tietosuojalainsäädäntöä tai lainsäädäntöä, jossa sallitaan muuhun kuin tarkkailuun liittyvä julkinen tiedonsaantioikeus. Siinä ei ole myöskään määritelty Privacy Shield -järjestelyn mukaisten tiedon siirtojen suhdetta muihin voimassa oleviin tietosuojan tason riittävyyttä koskeviin järjestelyihin, kuten matkustajarekisteriä (PNR) ja terrorismin rahoituksen jäljittämisohjelma (TFTP) koskeviin sopimuksiin.

9 Olennaiset eurooppalaiset takeet perustuvat unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. Ne on esitetty yksityiskohtaisesti tietosuojatyöryhmän valmisteluasiakirjassa WP 237, joka julkaistiin 13.4.2016.

1.2.1 EU:n tietosuojalainsäädännön ja erityisesti direktiivin 95/46/EY periaatteiden soveltamisala

Tietosuojatyöryhmä palauttaa mieliin, että EU:n tietosuojalainsäädännön ja erityisesti direktiivin (4 artiklan 1 kohdan) mukaisesti jäsenvaltioiden lakeja on sovellettava henkilötietojen käsittelyyn paitsi silloin, kun käsittely suoritetaan jäsenvaltion alueella sijaitsevassa rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä, myös silloin kun rekisterinpitäjä käyttää varsinkin henkilötietojen keräämiseen välineitä, jotka sijaitsevat EU:n alueella (vaikka ei ole sijoittautunut EU:n alueelle). Tämän takia EU:n jäsenvaltion lakeja sovelletaan kaikkeen käsittelyyn, joka tapahtuu ennen tietojen siirtoa Yhdysvaltoihin, joko EU:hun sijoittautuneen organisaation toiminnan yhteydessä tai EU:ssa sijaitsevan välineistön käytön yhteydessä, vaikka välineitä käyttävä organisaatio ei sijaitse EU:ssa. Tietosuojatyöryhmä pyytää, että tämä tehdään erikseen selväksi tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa.

Olisi oltava selvää, että Privacy Shield -periaatteita sovelletaan siitä ajankohdasta alkaen, jona tiedot siirretään. Lisäksi tietosuojatyöryhmä palauttaa mieliin, että EU:hun sijoittautunut rekisterinpitäjä, joka siirtää tietoja Yhdysvalloissa sijaitsevalle tietojenkäsittelijälle, pysyy EU:n tietosuojalainsäädännön alaisena.

1.2.2 Privacy Shield -asiakirjojen vaikeaselkoisuus

Privacy Shield -järjestelyn periaatteet ja takeet on esitetty sekä tietosuojan tason riittävyyttä koskevassa päätöksessä että sen liitteissä, mikä hankaloittaa tietojen löytämistä, ja toisinaan tiedot ovat ristiriitaisiakin. Tästäkin syystä uudet puitteet ovat kokonaisuudessaan vaikeaselkoisia, ja tietojen saaminen on vaikeaa niin rekisteröidyille, organisaatioille kuin tietosuojaviranomaisille. Edes käytetty kieli ei ole selkeää. Siitä syystä tietosuojatyöryhmä kehottaa komissiota selkeyttämään puitteita ja tekemään niistä ymmärrettäviä Atlantin molemmin puolin.

Tietosuojatyöryhmä ehdottaa, että Privacy Shield -asiakirjoissa käytettävien keskeisten termien määritelmät sisällytetään erilliseen liitteeseen. Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevassa päätöksessä asetettavien velvoitteiden yhteinen ja yksiselitteinen ymmärtäminen on ratkaisevan tärkeää, jotta järjestely toimisi tehokkaasti Atlantin molemmin puolin. Siitä syystä tietosuojatyöryhmä on huolissaan siitä, että lukuisten ristiviittausten ja yhtenäistämättömien muotoilujen sekä puiteasiakirjojen monimutkaisuuden takia Privacy Shield -järjestelyn täytäntöönpanon johdonmukaisuus, ymmärrettävyys ja selkeys kärsivät.

Vielä merkittävämpää on, että Privacy Shield -asiakirjoissa käytettävä termistö ei ole johdonmukaista tietosuojasta EU:ssa yleisesti käytettävän sanaston kanssa. Se ei ole välttämättä ongelma, kunhan on selvää, mitkä termit vastaavat toisiaan EU:n ja Yhdysvaltojen lainsäädännössä. Tietosuojatyöryhmä toteaa kuitenkin harmikseen, ettei näin ole asian laita, ei edes tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa. Esimerkiksi tietosuojan tason riittävyyttä koskevan päätösehdotuksen 3 luvussa sanaa ”access” (suomeksi ”pääsy

tietoihin”) on käytetty merkityksessä, joka viittaa henkilötietojen keräämiseen, sen sijaan, että viitattaisiin siihen, että joku saa nähdä jo kerätyt tiedot. Yritysten pääsy tietoihin ja henkilöiden oikeus saada tietoja ovat kaksi erillistä käsitettä, joita ei pitäisi sekoittaa.

Tietosuojatyöryhmä korostaa, että termistöä olisi käytettävä johdonmukaisesti kaikissa asiakirjoissa, myös tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa. Tällä hetkellä näin ei ole esimerkiksi käsitteiden ’tietojenkäsittely’ ja ’henkilötiedot’ osalta. Molemmat käsitteet on periaatteessa määritelty hyvin liitteessä II, mutta niitä ei ole käytetty johdonmukaisesti kaikissa asiakirjoissa, minkä takia tietosuojaan jää aukkoja.[10, 11]

Tietosuojatyöryhmä on tyytyväinen siitä, että jotkin käytetyistä termeistä on määritelty Privacy Shield -järjestelyn muodostavissa asiakirjoissa. On kuitenkin lukuisia muita keskeisiä termejä, joita ei ole määritelty, kuten *Agent* (’edustaja’), *processor* (’tietojen käsittelijä’), *key-coded data* (’avainkoodatut tiedot’), *anonymized data* (’tiedot, joista nimet on poistettu’) ja *EU individual* (’EU:n kansalainen’). Tietosuojatyöryhmän mielestä EU:n ja Yhdysvaltojen olisi sovittava näille termeille selkeät määritelmät, jotta Privacy Shield -järjestelyä käyttävät rekisterinpitäjät ja tietojen käsittelijät, valvontaviranomaiset ja suuri yleisö välttyisivät myöhemmässä vaiheessa sekaannuksilta. Helppo ratkaisu olisi lisätä termisanasto Privacy Shield -järjestelyä koskevaan usein kysyttyjen kysymysten osioon (*Privacy Shield F.A.Q.*).

Tietosuojatyöryhmä viittaa myös arkaluonteisten tietojen käsittelyn oikeuttaviin perusteisiin, jotka on lueteltu täydentävässä periaatteessa 1 (liite II, III.1), tapauksissa, joissa organisaation ei tarvitse saada nimenomaista suostumusta. Tämän täydentävän periaatteen 1 voidaan ymmärtää luettelevan tietojen keruun oikeutetut perusteet EU:ssa, koska luettelo vastaa direktiivin 8 artiklaa. Tietosuojatyöryhmä haluaa muistuttaa, että kaikenlainen EU:n lainsäädännön alainen arkaluonteisten tietojen käsittely (myös keruu ja siirtäminen) on tehtävä direktiivin 8 artiklan mukaisin oikeutetuin perustein. Privacy Shield -järjestelyn ei voida tulkita tarjoavan vaihtoehtoista perustetta tällaiseen tietojenkäsittelyyn. Tietosuojatyöryhmän mielestä ei esimerkiksi ole mahdollista, että yhdysvaltalainen

10 Joissakin lausekkeissa pelkästään luetellaan erilaisia tietojenkäsittelytoimia sen sijaan, että käytettäisiin termiä ’henkilötietojen käsittely’. Tämän takia tietosuojaan jää aukkoja. Esimerkiksi liitteessä II olevan III.6.f alakohdan mukaisesti Privacy Shield -periaatteita olisi sovellettava vain, jos organisaatio tallentaa, käyttää tai luovuttaa tietoja saatuja tietoja (ts. ei muissa ’henkilötietojen käsittely’ -termin alaan kuuluvissa toimissa, kuten tietojen keruussa, tallentamisessa, muuttamisessa, hakemisessa, tutustumisessa ja poistamisessa). Turvallisuusperiaatetta olisi noudatettava vain organisaatioiden, jotka ”keräävät, säilyttävät, käyttävät tai levittävät henkilötietoja” (liite II, II.4). Lisäksi ’henkilötietojen’ määritelmä on rajoitettu koskemaan ’vastaanotettuja’ tietoja (englanniksi ‘received’ and ‘recorded’). Lisäesimerkkinä voidaan mainita ilmoitusperiaate (liite II, II.1.a.iv), jossa todetaan, että varmennuksen antaneen organisaation on ilmoitettava henkilöille tarkoituksista, joihin se ”kerää ja käyttää” heitä koskevia tietoja. Liitteessä II olevassa III.9.a.11 alakohdassa mainitaan vain tiedot, joita ”siirretään tai annetaan käyttöön”. Vaikka vaikuttaakin siltä, että useimmissa tapauksissa ei ole tarkoitus rajoittaa periaatteiden soveltamisalaa eikä luoda suojaan aukkoja, epäjohdonmukainen termistö tuo mukanaan riskin tällaisten aukkojen syntymisestä. Koska termi ’henkilötietojen käsittely’ on määritelty periaatteissa, on ratkaisevan tärkeää käyttää sitä johdonmukaisesti tekstissä nyt olevien porsaanreikien välttämiseksi. Muutoin jäisi liiaksi oletettavasti tahatonta tulkinnanvaraa, mikä voisi taas johtaa päätöksen sanamuodon väärään tulkintaan.

11 Liitteessä II olevassa I.8.a alakohdassa on määritelty personal data (’henkilötiedot’) seuraavasti: ”*data about an identified or identifiable individual*” (suomeksi ”tunnistetun tai tunnistettavan henkilön tietoja”). Täydentävässä periaatteessa kuitenkin todetaan, että periaatteita sovelletaan henkilöstötietoihin ainoastaan, jos ”*identified records are transferred or accessed*” (suomeksi jos ”siirretään tai annetaan käyttöön yksittäinen henkilötieto, jonka perusteella henkilö tunnistetaan”). Tietosuojatyöryhmä katsoo, että tämä antaa mahdollisuuden käsitellä henkilötietoja tavalla, joka ei ole EU:n tietosuojalainsäädännön periaatteiden eikä Privacy Shield -järjestelyssä annetun henkilötietojen yleisen määritelmän mukaista.

organisaatio keräisi EU:n lainsäädännön alaista tietoa Yhdysvaltojen työoikeuden perusteella (ks. liite II, III.1.a.v). Siitä syystä tietosuojatyöryhmä korostaa, että mahdollinen täydentävän periaatteen 1 tulkinta voi johtaa ainoastaan sen soveltamiseen sellaisiin arkaluonteisiin tietoihin, jotka on jo siirretty sen jälkeen, kun ne on kerätty EU:ssa direktiivin 8 artiklassa luetelluin oikeutetuin perustein.

Lopuksi tietosuojatyöryhmä toteaa olevan epäselvää, kenen voidaan katsoa olevan ”*EU individual” (suomennettu EU:n kansalainen)* ja siten nauttivan Privacy Shield -järjestelyn tarjoamaa suojaa: kaikkien EU:n kansalaisten vai kaikkien EU:ssa oleskelevien henkilöiden. Tämä on erityisen tärkeää oikeussuojan kannalta, oikeus kääntyä oikeusasiamiehen puoleen mukaan luettuna. Lisäksi tietosuojan tason riittävyyttä koskevassa päätöksessä olisi käsiteltävä sitä kysymystä, missä määrin Privacy Shield -järjestelyä sovelletaan myös ETA-alueen ja Sveitsin kansalaisiin/asukkaisiin, jotka aiemmin kuuluivat safe harbor -järjestelmän piiriin.

1.2.3 Yhteinen tarkastelu ja päätöksen soveltamisen keskeyttäminen

Tietosuojatyöryhmä on tyytyväinen siitä, että Euroopan komissio ja Yhdysvaltojen hallinto ovat sopineet Privacy Shield -järjestelyn käytännön soveltamisen säännöllisestä tarkastelusta. Yhteinen tarkastelu on EU:n tietosuojayhteisössä tunnettu käytäntö jo useiden vuosien ajan, erityisesti suhteessa TFTP-sopimukseen ja kolmansien maiden kanssa tehtyihin sopimuksiin, jotka koskevat matkustajarekisteritietojen vaihtoa. Tietosuojatyöryhmä on tyytyväinen myös siitä, että ennalta määrittämätön määrä tietosuojaviranomaisten edustajia voi osallistua yhteiseen tarkasteluun.

Yhteisistä tarkasteluista viime vuosina saadun kokemuksen perusteella tietosuojatyöryhmä haluaa selventää odottavansa, että Privacy Shield -järjestelyä koskeva yhteinen tarkastelu on laajempi kuin PNR- ja TFTP-sopimuksia koskevat yhteiset tarkastelut. On erityisesti toivottavaa, että yhteiseen tarkasteluun kuuluu Yhdysvaltojen virastojen, organisaatioiden ja liikeyritysten edustajien kanssa järjestettävien kokousten lisäksi myös tiettyjä Privacy Shield -järjestelyn osatekijöitä koskevia tarkastuksia paikalla. Yhteiseen tarkasteluun osallistuvien tietosuojaviranomaisten edustajien olisi voitava ehdottaa tällaisia paikan päällä tehtäviä tarkastuksia.

Tietosuojatyöryhmä katsoo, että yhteisen tarkastelun tuloksia olisi arvioitava yhteisesti. Toistaiseksi yhteisten tarkastelujen tulokset on esitetty komission valmisteluasiakirjassa, eikä yhteiseen tarkastelutiimiin kuuluvien komission ulkopuolisten jäsenten ole edellytetty hyväksyvän niitä. Tietosuojatyöryhmä pitäisi arvossa sitä, että Privacy Shield -järjestelyn yhteisen tarkastelun tuloksista laadittaisiin yhteinen selvitys. Vaihtoehtoisesti voitaisiin harkita tietosuojaviranomaisten erillistä yhteisen tarkastelun selvitystä.

Lopuksi tietosuojatyöryhmä muistuttaa, että komissio on luvannut korvata tietosuojatyöryhmän edustajille yhteisten tarkastelujen aikana koituvat kustannukset. Työryhmä olettaa tämän koskevan Privacy Shield -järjestelyn yhteistä tarkastelua ainakin kohtuulliseen tietosuojaviranomaisten edustajien määrään asti.

Tietosuojatyöryhmä suosittaa, että yhteisen tarkastelun menettelytavoista sovitaan komission, Yhdysvaltojen hallinnon ja tietosuojatyöryhmän välillä kirjallisesti vähintään kolme kuukautta ennen ensimmäistä Privacy Shield -järjestelyn yhteistä tarkastelua.

1.2.4 Uudelleentarkasteltava EU:n lainsäädäntö

Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskeva päätös on ensimmäinen tietosuojan tason riittävyyttä koskeva päätös, joka on laadittu sen jälkeen, kun yleisen tietosuoja-asetuksen tekstistä on päästy periaatteelliseen yhteisymmärrykseen. Tietosuojatyöryhmä on kuitenkin varma siitä, että Privacy Shield -järjestely ei vielä vastaa tulevaa tilannetta. Privacy Shield -järjestelyyn ei esimerkiksi ole sisällytetty sellaista uutta käsitettä kuin oikeus siirtää tiedot järjestelmästä toiseen eikä rekisterinpitäjien lisävelvoitteita, joita ovat tietosuojaa koskevan vaikutustenarvioinnin toteuttaminen sekä sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden noudattaminen. Siitä syystä tietosuojatyöryhmä ehdottaa, että samoin kun muita voimassa olevia tietosuojan tason riittävyyttä koskevia päätöksiä, Privacy Shield -järjestelyä tarkastellaan uudelleen pian sen jälkeen, kun yleistä tietosuoja-asetusta on alettu soveltaa. Lopulliseen tietosuojan tason riittävyyttä koskevaan päätökseen olisi hyvä lisätä täsmällinen viittaus tähän tarkasteluprosessiin.

2. TIETOSUOJAN TASON RIITTÄVYYTTÄ KOSKEVAN PÄÄTÖSEHDOTUKSEN KAUPALLISEN OSAN ARVIOINTI

2.1 Yleiset huomautukset

2.1.1 Parannukset

Tietosuojatyöryhmä on tyytyväinen Privacy Shield -järjestelyn tuomiin parannuksiin ja siihen, että neuvottelijat ovat halunneet puuttua safe harbor -periaatteiden puutteisiin, joita tietosuojatyöryhmä oli korostanut, ja ratkaista ongelmat. Safe harbor -periaatteisiin verrattuna voidaan todeta erityisesti seuraavia osatekijöitä koskevat parannukset: Joitakin keskeisiä määritelmiä on lisätty, kuten ’henkilötiedot’, ’henkilötietojen käsittely’ ja ’rekisterinpitäjä’. Privacy Shield -luettelon valvonnan varmistamiseksi on perustettu mekanismi, ja päätöksen noudattamisen ulkoinen tai sisäinen valvonta on nyt pakollista. Myös tiedonsaantiperiaatetta on parannettu, ja tietosuojatyöryhmä toteaa, että oikeus tietojen korjaamiseen ja hävittämiseen taataan, jos tietoja käytetään Privacy Shield -periaatteiden vastaisesti. Lisäksi selvennetään, että henkilön on saatava sekä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään, että kyseiset tiedot nähtäväkseen.

Tietosuojatyöryhmä suhtautuu myönteisesti myös oikeudellisten takeiden vahvistamiseen tapauksissa, joissa tietoja siirretään edelleen, sekä Yhdysvaltojen kauppaministeriön ja liittovaltion kauppakomission (*Federal Trade Commission*, FTC) antamiin sitoumuksiin valvoa Privacy Shield -järjestelyn velvoitteiden noudattamista.

2.1.2 Privacy Shield -järjestelyn soveltaminen henkilötietojen käsittelijöinä (edustajina) toimiviin organisaatioihin

On valitettavasti edelleen epäselvää, missä määrin Privacy Shield -periaatteita sovelletaan varmennuksen antaneihin organisaatioihin, jotka ottavat EU:sta vastaan henkilötietoja pelkästään niiden käsittelyä varten (eli ’edustajiin’ tai ’henkilötietojen käsittelijöihin’). Vaikka liitteessä II olevan III.10.a alakohdan säännöksissä mainitaan tietojen siirrot varmennuksen antaneille organisaatioille tällaisiin tarkoituksiin – eli mainitaan velvoite tehdä sopimus – niissä ei sanota mitään siitä, kuinka Privacy Shield -periaatteita sovelletaan henkilötietojen käsittelijöihin (edustajiin). Tämä aiheuttaa epävarmuutta sekä tietoja niiden käsittelyä varten vastaan ottavissa varmennuksen antaneissa Yhdysvaltojen organisaatioissa että EU:n yrityksissä, jotka siirtävät tietoja henkilötietojen käsittelijöinä toimiville varmennuksen antaneille organisaatioille, samoin kuin henkilöille, joiden tietoja käsitellään. Näin ollen on vaikeaa määrittää, mitä velvoitteita tosiasiassa sovelletaan niihin Privacy Shield -organisaatioihin, jotka käsittelevät EU:sta saatuja tietoja henkilötietojen käsittelijän ominaisuudessa. Sen takia asiaa on varmasti selkeytettävä.

On otettava huomioon, että monet periaatteisiin sisältyvistä velvoitteista eivät sovellu henkilötietojen käsittelijöille, koska rekisterinpitäjä määrittää aina henkilötietojen käyttötarkoituksen ja käsittelytavan (ks. ’rekisterinpitäjän’ määritelmä liitteessä II olevassa I.8.c alakohdassa). Tästä syystä, jos joitakin periaatteisiin sisältyviä velvoitteita sovelletaan edustajana toimivaan organisaatioon, ne saattavat olla ristiriidassa EU:n lainsäädännön mukaisesti edellytetyn henkilötietojen käsittelysopimuksen kanssa (liitteessä II olevassa III.10.a alakohdassa mainittu sopimus). Henkilötietojen käsittelysopimuksessa ei esimerkiksi yleensä anneta tietojenkäsittelijälle (edustajalle) lupaa siirtää tietoja edelleen ulkopuoliselle rekisterinpitäjälle edes liitteessä II olevassa II.3.a alakohdassa mainituissa olosuhteissa. Henkilötietojen siirtämisen edelleen ulkopuoliselle edustajalle pitäisi olla sallittua vain rekisterinpitäjän annettua sille etukäteen hyväksyntänsä. Lisäksi unionin lainsäädännön mukaisesti henkilötietojen käsittelijä (edustaja) ei voi antaa luonnollisille henkilöille ilmoitusperiaatteessa tarkoitettua täyttä ilmoitusta (liite II, II.1) muun muassa sen takia, että organisaatio ei määritä tietojen käsittelyn tarkoitusta.

Siitä syystä periaatteissa on ratkaisevan tärkeää täsmentää, että ristiriitatapauksessa tietojenkäsittelysopimuksen määräykset ja erityisesti henkilötiedot EU:n ulkopuolelle siirtävän organisaation antamat ohjeet ovat etusijalla. Ilman tällaista selvennystä periaatteita voitaisiin tulkita ja soveltaa tavalla, jossa Privacy Shield -edustaja saa liikaa hallintamahdollisuuksia tietoihin, jolloin henkilötietojen EU-viejää uhkaa vaara, että se loukkaa niitä EU:n tietosuojalainsäädännön velvoitteita, joita siihen kohdistuu, kun se siirtää tietoja edustajana toimivalle Privacy Shield -organisaatiolle. Lisäksi vaikeaselkoisesta tekstistä saa sen vaikutelman, että henkilötietojen käsittelijä voisi käyttää tietoja uudelleen haluamallaan tavalla.

Sitä paitsi olisi säädettävä erityissäännöt sellaista tilannetta varten, jossa organisaatio toimii henkilötietojen käsittelijänä (edustajana), jotta varmistetaan, että kyseinen organisaatio noudattaa rekisterinpitäjän ohjeita. Olisi selvästi säädettävä, että yhdysvaltalaiset

organisaatiot, jotka ottavat tietoja vastaan ainoastaan tietojen käsittelyä varten, eivät voi päättää käsitellä tietoja omasta puolestaan. Ellei henkilötietojen käsittelijänä toimivaan organisaatioon sovellettavia erityissääntöjä ole, on vaikea määrittää, mitä sääntöjä koskevan varmennuksen tietojenkäsittelijä (edustaja) voi antaa.

2.1.3 Periaatteiden noudattamisen rajoitukset

Liitteessä II olevassa I.5 kohdassa säädetään poikkeuksia periaatteista muun muassa silloin, kun Privacy Shield -järjestelyn alaan kuuluvia tietoja käytetään kansallisen turvallisuuden[12], julkisen edun tai lainvalvonnan vaatimusten vuoksi taikka sillä perusteella, että lain, hallituksen antaman asetuksen tai tuomioistuimen päätöksen seurauksena syntyy ristiriitaisia velvoitteita tai annetaan nimenomainen lupa tiettyyn toimintaan. Tietosuojatyöryhmän on vaikea arvioida tämän poikkeuksen soveltamisalaa ja harkita rajoituksen oikeutusta demokraattisessa yhteiskunnassa, koska työryhmä ei täysin tunne Yhdysvaltojen lakia sekä liittovaltion että osavaltion tasolla. On olennaisen tärkeää, että Euroopan komissio sisällyttää tietosuojan tason riittävyyttä koskevaan päätösehdotukseen myös analyysin tietosuojan tasosta tapauksissa, joissa edellä mainittuja poikkeuksia sovelletaan. Tietosuojatyöryhmä kehottaa komissiota varmistamaan, että EU saa tiedon kaikista laeista tai hallituksen antamista asetuksista, jotka vaikuttaisivat periaatteiden noudattamiseen, sekä niistä säädöksistä, jotka ovat nykyisin voimassa, että uusista laeista ja asetuksista sitten, kun ne tulevat voimaan Yhdysvalloissa.

2.1.4 Henkilötietojen säilyttämisen rajoittamista koskevan periaatteen puuttuminen

Henkilötietojen säilyttämisen rajoittamista koskeva periaate (direktiivin 6 artiklan 1 kohdan e alakohta) on EU:n tietosuojalainsäädännön perusperiaate. Sen mukaisesti henkilötietoja saa säilyttää ainoastaan sen ajan kuin on tarpeen niiden tarkoitusten toteuttamiseksi, joita varten tiedot kerättiin tai joita varten niitä myöhemmin käsitellään.

Tietosuojatyöryhmä ei ole kuitenkaan löytänyt Privacy Shield -järjestelyn muodostavista asiakirjoista ainuttakaan viittausta siihen, että rekisterinpitäjien olisi varmistettava tietojen hävittäminen sen jälkeen, kun tarkoitus, jota varten ne on kerätty tai jota varten niitä käsitellään, on menettänyt merkityksensä. Vaikuttaa siis siltä, että periaatteissa ei edellytetä varmennuksen antaneelta organisaatiolta tietojen säilyttämisajan rajoittamista samaan tapaan kuin EU:n lainsäädännössä edellytetään.

Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatetta (liite II, II.5) ei mitenkään voida lukea siten, että sen voitaisiin katsoa muodostavan rekisterinpitäjänä toimivalle organisaatiolle velvoitteen hävittää tiedot sen jälkeen, kun niitä ei enää tarvita niiden tarkoitusten toteuttamiseksi, joita varten tiedot kerättiin tai joita varten niitä myöhemmin käsitellään, taikka henkilötietojen käsittelijänä toimivalle organisaatiolle velvoitteen hävittää tiedot palvelusopimuksen päättymisen jälkeen.

12 Lisähuomautuksia Privacy Shield -järjestelyn alaan kuuluvien henkilötietojen käytöstä kansallisen turvallisuuden vuoksi on 3 luvussa ja lainvalvonnan vuoksi 4 luvussa.

Työryhmä korostaa, että Privacy Shield -järjestelyn alaisuuteen kuuluvien henkilötietojen säilyttämisen rajoittamista koskevan säännöksen puuttuminen antaa organisaatioille mahdollisuuden säilyttää tietoja niin pitkään kuin ne haluavat, jopa sen jälkeen, kun ne ovat vetäytyneet Privacy Shield -järjestelystä, mikä ei ole tietojen säilyttämisen rajoittamista koskevan olennaisen periaatteen mukaista.

2.1.5 Luonnollisille henkilöille oikeudellisia vaikutuksia aiheuttavia tai heihin merkittävällä tavalla vaikuttavia, automaattisen käsittelyn perusteella annettavia päätöksiä koskevien takeiden puuttuminen

Privacy Shield -järjestelyssä ei anneta minkäänlaisia oikeudellisia takeita sellaisen tilanteen varalta, että henkilöön kohdistetaan päätös, josta aiheutuu hänelle oikeudellisia vaikutuksia tai joka vaikuttaa häneen merkittävällä tavalla ja joka on tehty ainoastaan automaattisen tietojenkäsittelyn perusteella ja on tarkoitettu hänen tiettyjen henkilökohtaisten ominaisuuksiensa, kuten muun muassa hänen ammatillisen suorituskykynsä, luottokelpoisuutensa, luotettavuutensa ja käyttäytymisensä arviointiin.

Tietosuojatyöryhmä on jo valmisteluasiakirjassa 12 korostanut tarvetta antaa oikeudelliset takeet, jotka koskevat automatisoituja päätöksiä (kun päätöksistä aiheutuu oikeudellisia vaikutuksia tai ne vaikuttavat henkilöön merkittävällä tavalla), jotta tietosuojan tasoa voitaisiin pitää riittävänä.

Tämä tarve on sitäkin keskeisempi, kun yhä uusien tekniikoiden kehittämisen ansiosta yhä useammat yritykset voivat harkita automaattisten päätöksentekojärjestelmien käyttöönottoa. Se voi johtaa luonnollisten henkilöiden aseman heikkenemiseen ilman, että heillä on käytettävissään mitään oikeussuojakeinoja tietokoneiden tekemiä päätöksiä vastaan. Jos tällaiset yksinomaan automaattisten järjestelmien tekemät päätökset aiheuttavat oikeudellisia vaikutuksia tai vaikuttavat henkilöön merkittävällä tavalla (esimerkiksi asettamalla hänet mustalle listalle ja siten riistämällä henkilöltä tämän oikeuksia), on ratkaisevan tärkeää tarjota riittävät suojatoimet, kuten oikeus saada tietoonsa käytetty logiikka ja oikeus pyytää uudelleenharkintaa muulla kuin automaattisen käsittelyn perusteella.

2.1.6 Nykyisiä kauppasuhteita koskeva siirtymäaika

Privacy Shield -järjestelyssä ennakoidaan, että periaatteita sovelletaan heti varmennuksesta alkaen. Kuitenkin organisaatioiden, jotka antavat oman varmennuksensa Privacy Shield -järjestelyssä kahden ensimmäisen kuukauden kuluessa järjestelyn voimaantulopäivästä, on saatettava olemassa olevat liikesuhteensa kolmansien osapuolten kanssa tietojen edelleen siirtämiseen liittyvää vastuuvelvollisuutta koskevan periaatteen mukaisiksi niin pian kuin mahdollista. Niiden olisi joka tapauksessa tehtävä niin yhdeksän kuukauden kuluessa päivästä, jona organisaatio antoi varmennuksensa Privacy Shield -järjestelyssä.

Tämä merkitsee, että nykyiset sopimukset on tarvittavassa määrin saatettava periaatteiden mukaisiksi kahdesta yhdeksään kuukautta varmennuksen antamisen jälkeen. Tänä siirtymäkautena riittää, kun ilmoitus- ja valintaperiaatteita noudatetaan. Tietosuojatyöryhmä

pitää edelleen kiinni siitä, että tietoja pitäisi voida siirtää Privacy Shield -järjestelyn mukaisesti vasta sen jälkeen, kun organisaatio voi täysimääräisesti noudattaa kaikkia Privacy Shield -vaatimuksia. Jos henkilötietoja on mahdollista lähettää siirtymäkauden aikana siten, että niiden vastaanottaja ei pysty täysimääräisesti noudattamaan Privacy Shield -periaatteita, tämän tilanteen ei voida katsoa täyttävän laillisen tietojensiirron edellytyksiä, eikä sitä siten voida hyväksyä.

2.2 Yksittäisiä säännöksiä koskevat huomautukset

2.2.1 Avoimuus

a) Ilmoitusperiaatetta koskevia yleisiä huomautuksia

Tietosuojatyöryhmä on tyytyväinen siitä, että ilmoitusperiaatteeseen on sisällytetty entistä kattavammat ja yksityiskohtaisemmat vaatimukset, erityisesti siitä, että ilmoitukseen on sisällytettävä linkki Privacy Shield -luetteloon tai kyseisen luettelon verkko-osoite ja että siinä on viitattava oikeuteen tutustua itseään koskeviin tietoihin ja sekä vaihtoehtoisiin riidanratkaisumekanismeihin.[13] Tietosuojatyöryhmä ehdottaa kuitenkin, että mainitaan täsmällisesti myös muut järjestelyn alaan kuuluvat oikeudet (oikeus saada tiedot korjatuiksi tai hävitetyiksi, jos ne ovat virheellisiä tai niitä on käsitelty järjestelyn periaatteiden vastaisesti).

Privacy Shield -järjestelyn asiakirjoissa todellinen huolenaihe on ajankohta, jona Privacy Shield -organisaatioiden on annettava ilmoitus henkilölle. Liitteessä II olevan II.1.b alakohdan mukaan ”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.” Tietosuojatyöryhmä katsoo, että yhdysvaltalainen Privacy Shield -organisaatio ei monessa tilanteessa suoraan kerää tietoja rekisteröidyltä, joten ilmoituksen ajankohdaksi olisi määritettävä hetki, jona Privacy Shield -organisaatio tallentaa tiedot.

Tietosuojatyöryhmä toteaa, että ilmoitusperiaatetta ja tietosuojaperiaatteita koskevien vaatimusten todellista soveltamista olisi arvioitava Privacy Shield -järjestelyn ensimmäisen vuotuisen tarkastelun yhteydessä.

b) Tietosuojaperiaatteiden julkinen saatavuus

Tietosuojatyöryhmä suhtautuu myönteisesti siihen, että on täsmällisesti mainittu Yhdysvaltojen kauppaministeriön tarkastavan, ovatko yritykset, joilla on julkinen

13 Liite II, II.1. Lisäksi tietosuojatyöryhmä viittaa tiedonannossa COM(2013) 847 annettuun komission suositukseen nro 2 sekä tietosuojatyöryhmän kirjeeseen varapuheenjohtaja Redingille 10.4.2014 ja erityisesti sen avoimuutta käsittelevän kappaleen neljänteen luetelmakohtaan.

verkkosivusto, julkaisseet tietosuojaperiaatteensa tässä sivustossa, tai ellei verkkosivustoa ole, missä yleisö voi tutustua kyseisiin periaatteisiin.[14]

c) Henkilötietojen käsittelijöiden kanssa tehtävien sopimusten yksityisyyden suojaa koskevien ehtojen julkaiseminen

Privacy Shield -järjestelyn ehdoissa, joiden mukaisesti Privacy Shield -organisaatiot voivat siirtää henkilötietoja tietojenkäsittelijälle (edustajalle), asetetaan oman varmennuksen antaneille organisaatiolle velvoite, jonka mukaan ”sen on pyynnöstä annettava Yhdysvaltojen kauppaministeriölle yhteenveto tai olennaiset osat sisältävä jäljennös yksityisyyden suojaa koskevista määräyksistä, jotka sisältyvät edustajan kanssa tehtyyn sopimukseen” (ks. liite II, II.3.b.v). Työryhmä suhtautuu myönteisesti tähän vaatimukseen tiedottaa avoimesti kauppaministeriölle.

2.2.2 Valintaperiaate

Privacy Shield -järjestelyssä säädetään henkilöiden oikeudesta valita, voiko heidän henkilötietojaan luovuttaa kolmannelle osapuolelle tai käyttää olennaisesti erilaiseen tarkoitukseen kuin mihin ne on alun perin kerätty (liite II, III.2).[15] Lisäksi luonnollisilla henkilöillä on oikeus milloin tahansa kieltää itseään koskevien tietojen käyttäminen suoramarkkinointiin (liite II, III.12.a).[16]

Suoramarkkinointia lukuun ottamatta mitään yksityiskohtaisia säännöksiä kieltäytymistavasta tai -ajankohdasta ei ole annettu. Tietosuojatyöryhmä katsoo, että pelkkä viittaus tämän oikeuden olemassaoloon tietosuojaperiaatteissa ei riitä, vaan olisi tarjottava *henkilökohtainen* mahdollisuus käyttää tätä oikeutta *ennen* henkilötietojen luovuttamista tai uudelleenkäyttöä.

Lisäksi tietosuojatyöryhmä korostaa, että Privacy Shield -järjestelyssä rekisteröidylle olisi tarjottava yleinen oikeus vastustaa itseään koskevien tietojen käsittelyä (hänen tilanteeseensa liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi), mikä ymmärretään oikeutena pyytää lopettamaan henkilötietojen käsittely aina, kun henkilöllä on hänen henkilökohtaiseen tilanteeseensa liittyvät huomattavan tärkeät ja perustellut syyt.[17] Tietosuojatyöryhmä suosittaa voimakkaasti, että tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa selkeytetään, että oikeus vastustaa pätee milloin tahansa eikä vastustamista ole rajoitettu käyttöön suoramarkkinoinnissa.[18]

Tietosuojatyöryhmä pelkää, että teksti johtaa sekavuuteen ja oikeudellisen epävarmuuteen, koska siinä ei ole määritelty, mitä tarkoitetaan käytöllä ”olennaisesti erilaiseen tarkoitukseen”. Olisi selvennettävä, että valintaperiaatetta ei missään tapauksessa voi käyttää

14 Ks. tiedonannossa COM(2013) 847 annettu komission suositus nro 1 sekä tietosuojatyöryhmän kirje varapuheenjohtaja Redingille 10.4.2014 ja erityisesti sen avoimuutta käsittelevän kappaleen kolmas luetelmakohta.

15 Täydentävässä periaatteessa 14.c.1 säädetään oikeudesta vetäytyä kliinisestä kokeesta, mikä saatetaan nähdä oikeutena vastustaa tai peruuttaa suostumus.

16 Safe harbor -järjestelmässä oli samoin (F.A.Q. 12), eikä mikään ole muuttunut tässä suhteessa.

18 Ks. tietosuojatyöryhmän kirje varapuheenjohtaja Redingille, valintaperiaatetta käsittelevä kappale.

käyttötarkoituksen rajoittamisen periaatteen kiertämiseen.[19] Valintaperiaatetta olisi sovellettava ainoastaan, jos käyttötarkoitus on olennaisesti erilainen mutta kuitenkin yhteensopiva alkuperäisen käyttötarkoituksen kanssa, koska henkilötietojen käsittely yhteensopimattomaan tarkoitukseen on kiellettyä (liite II, II.5.a). On selvennettävä, että valintaperiaatteen soveltaminen ei voi antaa organisaatiolle mahdollisuutta käyttää henkilötietoja alkuperäisen käyttötarkoituksen kanssa yhteensopimattomaan tarkoitukseen. Siitä syystä tietosuojatyöryhmä suosittaa, että asiaan liittyvä muotoilu yhtenäistetään käyttämällä yhtä ainoaa määriteltyä muotoilua (esim. ”olennaisesti erilaiseen mutta kuitenkin yhteensopivaan tarkoitukseen”).

Olisi hyvä selventää, milloin päätös, jonka mukaisesti henkilötietoja käytetään muuhun käyttötarkoitukseen kuin mihin ne on alun perin kerätty tai jonka mukaisesti tietoja luovutetaan, kuuluu EU:n lainsäädännön alaisuuteen. Tällaisessa tilanteessa henkilötietojen käsittelyä koskevia tavanomaisia oikeudellisia EU:n edellytyksiä sovelletaan suoraan myös yhdysvaltalaiseen organisaatioon, joka kuuluu unionin lainsäädännön alaisuuteen. Sovellettavia edellytyksiä ovat muun muassa kielto käsitellä henkilötietoja alkuperäisen käyttötarkoituksen kanssa yhteensopimattomaan tarkoitukseen, velvoite esittää henkilötietojen käsittelylle oikeutettu peruste ja tarve ilmoittaa henkilölle tietojenkäsittelystä. Käytännössä tämä merkitsee, että tällöin päätöksen tehneen EU:n viejän on varmistettava henkilötietojen käsittelyn avoimuus ja lainmukaisuus EU:n lainsäädännön mukaisesti. Siitä syystä valintaperiaatetta sovelletaan ainoastaan silloin, kun päätöksen tekee yksin yhdysvaltainen Privacy Shield -organisaatio, joka ei kuulu EU:n lainsäädännön alaisuuteen.

2.2.3 Henkilötietojen siirtäminen edelleen

a) Soveltamisala

Tietosuojatyöryhmä on huolissaan tilanteesta, jossa henkilötietoja siirretään edelleen Yhdysvalloissa sijaitsevalta Privacy Shield -varmennuksen antaneelta organisaatiolta vastaanottajalle kolmannessa maassa.

Privacy Shield -järjestelyä ei pidä nähdä ainoastaan välineenä, jolla EU:n tietoja siirretään EU:sta Yhdysvaltoihin, sillä sitä voidaan käyttää myös välineenä, jolla tietoja siirretään Yhdysvalloista kolmansiin maihin. Henkilötietojen siirtämistä edelleen koskevat säännökset ovat siten Privacy Shield -järjestelyn tärkeä osa, jonka avulla olisi annettava riittävät takeet ja riittävä tietosuojan taso, kun tietoja siirretään edelleen Yhdysvaltojen ulkopuolelle. Kansalliseen turvallisuuteen ja lainvalvontaan liittyy erityinen ongelmakohta.

Tietojen edelleen siirtämiseen liittyvää vastuuvelvollisuutta koskevaa Privacy Shield -järjestelyn periaatetta ei ole rajoitettu koskemaan Yhdysvaltoihin sijoittautuneita tietoja vastaanottavia rekisterinpitäjiä, tietojenkäsittelijöitä tai edustajia. Siitä syystä tietojen siirtäminen edelleen kolmanteen maahan voidaan tehdä Privacy Shield -järjestelyn

19 Käytännön esimerkki valintaperiaatteen mahdollistamasta henkilötietojen jatkokäsittelystä yhteensopimattomaan käyttötarkoitukseen annetaan täydentävässä periaatteessa 9.b.i (ks. tietosuojatyöryhmän sitä koskeva huomautus henkilöstötietoja käsittelevässä kohdassa).

perusteella, vaikka kolmannella maalla olisi lakeja, joissa sallitaan julkinen pääsy henkilötietoihin esimerkiksi tarkkailua varten. Tällöin on uhkana, että EU:sta peräisin olevia henkilötietoja suojeleviin perusoikeuksiin puututaan perusteettomasti.

Kaikissa tapauksissa, joissa tietoja siirretään edelleen kolmanteen maahan, jokainen Privacy Shield -järjestelyyn liittynyt organisaatio olisi velvoitettava arvioimaan tietojen tuojaan sovellettavan kolmannen maan kansallisen lainsäädännön mahdolliset pakolliset vaatimukset ennen tietojen siirtämistä. Jos havaitaan riski siitä, että Privacy Shield -järjestelyn tarjoaman tietosuojan tasoon ja järjestelyn velvoitteisiin ja takeisiin kohdistuu merkittävää haittaa, tietojenkäsittelijänä (edustajana) toimivan yhdysvaltalaisen Privacy Shield -organisaation olisi viipymättä ilmoitettava asiasta EU:n rekisterinpitäjälle, ennen kuin se siirtää tietoja edelleen. Näissä tapauksissa henkilötietojen viejällä on oikeus keskeyttää henkilötietojen siirto ja/tai lopettaa sopimus. Rekisterinpitäjänä toimivalla Privacy Shield -organisaatiolla ei pitäisi olla oikeutta siirtää tietoja edelleen, jos tällainen merkittävien haittavaikutusten riski on olemassa, koska tällöin organisaatio jättäisi täyttämättä velvollisuutensa tarjota sama tietosuojan taso kuin mitä periaatteissa edellytetään henkilötietojen edelleen siirtämisen osalta (k. liite II, II.3.a).

Vastaavasti kun kolmannen maan lainsäädäntöä muutetaan tavalla, joka todennäköisesti vaikuttaisi merkittävällä tavalla haitallisesti Privacy Shield -järjestelyn tarjoaman tietosuojan tasoon ja järjestelyn velvoitteisiin ja takeisiin, henkilötietojen käsittelijänä (edustajana) toimivalla yhdysvaltalaisella Privacy Shield -organisaatiolla olisi oltava Privacy Shield -järjestelyssä edellytetty velvollisuus ilmoittaa tästä muutoksesta henkilötietojen viejälle heti, kun organisaatio saa muutoksesta tiedon. Henkilötietojen viejällä olisi tällöin oikeus keskeyttää henkilötietojen siirto ja/tai lopettaa sopimus. Rekisterinpitäjänä toimivalla Privacy Shield -organisaatiolla ei vastaavasti pitäisi tällaisessa tilanteessa olla oikeutta siirtää tietoja edelleen, koska sillä on velvollisuus tarjota sama tietosuojantaso kuin mitä periaatteissa edellytetään (k. liite II, II.3.a).

Tietosuojatyöryhmä muistuttaa kannastaan, jonka mukaisesti henkilötietojen siirtämistä olisi pidettävä suorana siirtona EU:sta kolmanteen maahan Yhdysvaltojen ulkopuolella, jos EU:n rekisterinpitäjä on tietoinen henkilötietojen siirtämisestä edelleen kolmannelle osapuolelle Yhdysvaltojen ulkopuolella jo ennen, kuin tiedot siirretään Yhdysvaltoihin, tai jos EU:n rekisterinpitäjä on yhteisvastuussa päätöksestä sallia henkilötietojen siirtäminen edelleen. Tämä merkitsee, että henkilötietojen siirtämiseen on sovellettava direktiivin 25 ja 26 artiklaa Privacy Shield -järjestelyn henkilötietojen edelleen siirtämistä koskevan periaatteen sijasta.

b) Henkilötietojen siirtäminen Privacy Shield -organisaatiolta rekisterinpitäjänä toimivalle kolmannelle osapuolelle

Tietosuojatyöryhmä on tyytyväinen velvoitteeseen laatia sopimukset sen varmistamiseksi, että rekisterinpitäjänä toimiva kolmas osapuoli tarjoaa vähintään saman tietosuojan tason kuin Privacy Shield -periaatteissa edellytetään (liite II, II.3.a). Tarkoituksena on varmistaa, että henkilötiedot saavat riittävää suojaa vielä senkin jälkeen, kun ne on siirretty edelleen. Tietosuojatyöryhmällä on kuitenkin joitakin huomautuksia ehdotettuihin edellytyksiin.

Käyttötarkoituksen rajoituksen periaatetta koskevan viittauksen puuttuminen

Tietosuojatyöryhmä suosittaa, että henkilötietojen siirtämistä edelleen rekisterinpitäjänä toimivalle kolmannelle osapuolelle koskeviin ehtoihin (liite II, II.3.a) lisätään myös selkeä viittaus käyttötarkoituksen rajoituksen periaatteeseen (liite II, II.5). Tällöin olisi selvää, että henkilötietoja ei saa siirtää edelleen, jos rekisterinpitäjänä toimiva kolmas osapuoli aikoo käsitellä tietoja alkuperäisen käyttötarkoituksen kanssa yhteensopimattomassa tarkoituksessa.

Rekisterinpitäjien välistä henkilötietojen siirtoa yritysryhmän sisällä koskeva vapautus sopimuksentekovelvoitteesta

Rekisterinpitäjien välinen henkilötietojen siirto yritysryhmän sisällä on vapautettu sopimuksentekovelvoitteesta. Tällaisessa tilanteessa tietosuojan jatkuvuus voidaan periaatteiden mukaan taata yrityksiä koskevilla sitovilla säännöillä tai muilla ryhmän sisäisillä instrumenteilla, kuten vaatimustenmukaisuus- ja valvontaohjelmilla (liite II; III.10.b). Tietosuojatyöryhmä katsoo, ettei yritysryhmän muiden jäsenten oikeudellisesti sitovia sitoumuksia voida taata viittaamalla ”muihin ryhmän sisäisiin instrumentteihin”. Koska tietosuojatyöryhmä yleisesti suosittaa, että yritysryhmän sisäisiin henkilötietojen siirtoihin sovelletaan sitovia sitoumuksia, kuten EU:n lainsäädännössäkin[20] edellytetään, on tärkeää välttää sitä, että Privacy Shield -järjestelyä käytettäisiin tämän vaatimuksen kiertämiseen. Tietosuojatyöryhmä muistuttaa, että joka tapauksessa sellaista henkilötietojen siirtämistä Yhdysvalloista kolmansiin maihin, jota on suunniteltu jo ennen kuin tiedot siirretään Yhdysvaltoihin tai joka tehdään yhdessä EU:n rekisterinpitäjän kanssa,[21] on pidettävä suorana siirtona kolmanteen maahan Yhdysvaltojen ulkopuolella. Siirtoon on siten sovellettava direktiivin 25 ja 26 artiklaa.

c) Henkilötietojen siirtäminen Privacy Shield -organisaatiolta henkilötietojen käsittelijänä (edustajana) toimivalle kolmannelle osapuolelle

Tietosuojatyöryhmä on tyytyväinen siihen, että henkilötietojen siirtäminen edelleen käsittelijänä (edustajana) toimiville yksiköille edellyttää nyt pakollista sopimusta riippumatta siitä, osallistuvatko ne Privacy Shield -järjestelyyn vai kuuluvatko ne jonkin muun tietosuojan tason riittävyyttä koskevan menettelyn piiriin. Myös henkilötietojen siirtämistä edelleen koskevat lisäsuojatoimet tyydyttävät tietosuojatyöryhmää (liite II, II.3.a.i, II.3.a.iii, II.3.a.iv, II.3.a.v ja II.7.d). Viimeksi mainittu alakohta (liite II, II.7.d) koskee vastuun säilyttämisvelvoitetta, jos henkilötiedot luovutetaan edustajalle. Vaikuttaa kuitenkin siltä, ettei tätä taetta sovelleta, jos organisaatio on päättänyt tehdä yhteistyötä tietosuojaviranomaisen kanssa (ks. liitteessä II olevan III.5a alakohdan loppuosa). Tietosuojatyöryhmä ei ymmärrä tällaisen vapautuksen perusteita vaan katsoo, että vastuuta olisi sovellettava tässäkin tapauksessa.

Käyttötarkoituksen rajoituksen periaatetta koskevan viittauksen puuttuminen

20 Sitovien ja täytäntöönpanokelpoisten sitoumusten tarvetta korostetaan myös yleisessä tietosuoja-asetuksessa käytettävästä välineestä riippumatta (yritystä koskevat sitovat säännöt, sopimuslausekkeet, käytännesäännöt tai sertifiointi).
21 Esim. henkilöstötiedot.

Tietosuojatyöryhmä toteaa, että henkilötietojen edelleen siirtämistä koskevan vastuuvelvollisuusperiaatteen mukaisesti henkilötietoja saa siirtää edustajana toimivalle kolmannelle osapuolelle ainoastaan tiettyä rajoitettua tarkoitusta varten (liite II, II.3). Siinä ei kuitenkaan nimenomaan mainita, että tällaisen tietyn rajoitetun tarkoituksen on oltava yhteensopiva sen tarkoituksen kanssa, johon tiedot on alun perin kerätty, ja että rekisterinpitäjän ohjeita on noudatettava. Tätä kohtaa on selkeytettävä. Siitä syystä tietosuojatyöryhmä ehdottaa, että tietosuojan tason riittävyyttä koskevassa päätöksessä annetaan yksityiskohtaisemmat säännökset esimerkiksi viittaamalla selkeästi käyttötarkoituksen rajoittamista koskevaan periaatteeseen (liite II, II.5). Kyseisen periaatteen mukaisesti – kun henkilötietojen edelleen siirtämiseen liittyvää vastuuvelvollisuusperiaatetta sovelletaan – henkilöillä olisi käyttökieltomahdollisuus, minkä lisäksi henkilötietoja ei saisi käsitellä sellaisessa tarkoituksessa (eikä luovuttaa sellaiseen tarkoitukseen), joka on yhteensopimaton alkuperäisen käyttötarkoituksen kanssa.

Henkilötietojen käsittelijänä (edustajana) toimivalle Privacy Shield -organisaatiolle asetettava tietojen siirtämistä edelleen toiselle tietojenkäsittelijälle (edustajalle) koskevia lisävelvoitteita

Järjestelyssä ei ole selkeitä sääntöjä siitä tilanteesta, että Privacy Shield -organisaatio toimii edustajana (ts. EU:n rekisterinpitäjän puolesta). Kyseessä on porsaanreikä, jonka takia EU:n rekisterinpitäjä ei ehkä säilytä henkilötietojen hallintaa. Privay Shield -organisaation, joka ottaa henkilötietoja vastaan EU:n rekisterinpitäjän edustajana, on noudatettava EU:n rekisterinpitäjän ohjeita. Tämä olisi erikseen todettava periaatteissa sen varmistamiseksi, että ohjeiden noudattamatta jättäminen johtaa paitsi sopimusrikkomukseen (liite II, III.10.a.ii) myös Privacy Shield -periaatteiden rikkomiseen.

Privacy Shield -organisaation mahdollisuus toimia edustajana, joka myöhemmin siirtää henkilötiedot edelleen edustajana toimivalle kolmannelle osapuolelle, on tehtävä selväksi rekisterinpitäjälle, jonka on voitava ennakkoon hyväksyä siirto. Siitä syystä olisi selkeästi todettava, että edustajan ja EU:n rekisterinpitäjän allekirjoittamassa sopimuksessa (johon viitataan ”17 artiklan sopimuksena” usein kysyttyjen kysymysten kysymyksessä nro 10) määritetään, onko henkilötietojen siirtäminen edelleen sallittua.[22]

Nykyiset tietojen edelleen siirtämistä edustajalle koskevat edellytykset perustuvat siihen olettamukseen, että Privacy Shield -organisaatio toimii rekisterinpitäjänä ja voi siitä syystä itse päättää mahdollisesta edustajana toimivan kolmannen osapuolen osallistumisesta. Sen ei kuitenkaan pitäisi olla mahdollista, jos Privacy Shield -organisaatio toimii edustajana. Muutoin EU:n rekisterinpitäjä menettää henkilötietojen hallinnan.

Edustajana toimivan kolmannen osapuolen kanssa tehdyn sopimuksen tietosuojaa koskevat määräykset on annettava tiedoksi rekisterinpitäjälle, ja lisäksi niissä on määrättävä vähintään saman tasoisesta suojasta kuin rekisterinpitäjän kanssa allekirjoitetussa sopimuksessa.

22 Ks. tietosuojatyöryhmän kirje varapuheenjohtaja Redingille 10.4.2014, henkilötietojen edelleen siirtämistä käsittelevän kappaleen neljäs luetelmakohta.

2.2.4 Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaate

a) Oikeasuhteisuus

Tietosuojatyöryhmä viittaa sivumennen kirjeeseensä varapuheenjohtaja Redingille. Siinä työryhmä totesi, että henkilötietojen käsittely ei välttämättä ole oikeasuhteista rekisteröidyn tai yhteiskunnan etujen, oikeuksien ja vapauksien kannalta, vaikka siinä noudatettaisiin tiukasti ilmoitus- ja valintaperiaatteita. Työryhmän mukaan oikeasuhteisuusperiaatetta tai kohtuullisuutta on noudatettava kaikissa henkilötietojen käsittelyn vaiheissa, ja sitä olisi sovellettava ilmoitus- ja valintaperiaatteiden ohella.[23]

Privacy Shield -järjestelyssä henkilötietojen laajuus on rajoitettava tietoihin, jotka ovat merkityksellisiä tietojenkäsittelyn tarkoituksen kannalta (liite II, II.5.a). Tietosuojatyöryhmän mielestä olisi parempi, jos tätä muotoilua muutettaisiin lopullisessa tietosuojan tason riittävyyttä koskevassa päätöksessä, koska pelkästään se, että henkilötietojen on oltava tietojenkäsittelyn kannalta merkittäviä, ei riitä tekemään niiden käsittelystä oikeasuhteista. Suhteellisuusperiaatteen noudattamiseksi henkilötietojen käsittely olisi rajoitettava kyseessä olevan käsittelyn kannalta tarpeellisiin tietoihin.

b) Tarkkuus

Lisäksi tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteessa (liite II, II.5) todetaan myös seuraava: ”Organisaation on toteutettava tarvittavat kohtuulliset toimet sen varmistamiseksi, että henkilötiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia.” Tietosuojatyöryhmä toteaa, että safe harbor -järjestelyssä käytettiin täsmälleen samaa muotoilua. Tietosuojatyöryhmän mielestä lisäys ”*to the extent necessary to these purposes*” (siltä osin kuin on käyttötarkoituksen kannalta tarpeen) pitäisi ehkä jättää pois, koska työryhmän mielestä tietojen tarkkuuden ei pitäisi riippua henkilötietojen käsittelyn tarkoituksesta. Tietosuojatyöryhmän mielestä olisi parempi, jos tällaista yhteyttä ei tehtäisi lopullisessa tietosuojan tason riittävyyttä koskevassa päätöksessä.

c) Käyttötarkoituksen rajoittaminen

Jos unioniin sijoittautunut rekisterinpitäjä siirtää henkilötietoja yhdysvaltalaiselle organisaatiolle, tietojen viejän olisi ilmoitettava yhdysvaltalaiselle organisaatiolle täsmällisesti, mihin käyttötarkoitukseen tiedot on alun perin kerätty. Tämä on olennaisen tärkeää, jotta voidaan määrittää, muuttuuko käyttötarkoitus henkilötietojen siirtämisen jälkeen, jolloin on sovellettava ilmoitus- ja valintaperiaatteita, ja samalla se edistäisi riskin ja vastuun jakautumista.

Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteen (liite II, II.5) mukaisesti organisaatio ei saa käsitellä henkilötietoja siten, että niiden käsittelytapa on yhteensopimaton sen käyttötarkoituksen kanssa, johon tiedot on kerätty tai johon henkilö on sittemmin antanut

23 Ks. tietosuojatyöryhmän kirje varapuheenjohtaja Redingille 10.4.2014, s. 8.

suostumuksensa. Valintaperiaatteessa (liite II, II.2) annetaan kuitenkin mahdollisuus erityisellä suostumuksella antaa lupa arkaluonteisten tietojen käyttöön olennaisesti erilaiseen tarkoitukseen kuin siihen, johon ne oli alun perin kerätty tai johon henkilöt ovat sittemmin antaneet suostumuksensa. Arkaluontoisia tietoja ovat muun muassa henkilötiedot, jotka koskevat henkilön terveydentilaa, rotua tai etnistä alkuperää, poliittista kantaa, uskonnollista tai eettistä vakaumusta, kuulumista ammattiliittoon tai sukupuolielämää, samoin kuin rikosrekisteritiedot. Erityistä suostumusta ei edellytetä täydentävässä periaatteessa 1.a mainituissa tilanteissa (liite II, III.1.a). Muiden kuin arkaluonteisten henkilötietojen osalta on säädetty käyttökieltojärjestelmästä.

Tietosuojatyöryhmä toteaa, että käyttötarkoituksen rajoittamista koskevan periaatteen soveltamisala on erilainen ilmoitus-, valinta- ja tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteiden mukaisesti. Samassa tekstissä käytetään sekä ilmauksia ’yhteensopimaton käyttötarkoitus’ että ’olennaisesti erilainen käyttötarkoitus’ niitä tarkemmin määrittelemättä.[24]

Tietosuojatyöryhmä on vakavasti huolissaan siitä, että tällainen epäjohdonmukaisuus saattaa suuresti vaikeuttaa tietojen eheyden ja käyttötarkoituksen rajoittamisen periaatteen (liite II, II.5) sovittamista yhteen valintaperiaatteen (liite II, II.2) kanssa, koska toisessa sanotaan, ettei tietoja saa käyttää tavalla, joka on yhteensopimaton niiden alkuperäisen käyttötarkoituksen kanssa, kun taas toisessa säädetään käyttökieltomenettelystä tapauksissa, joissa käyttötarkoitus on olennaisesti erilainen kuin alkuperäinen käyttötarkoitus.

Valintaperiaatetta voidaan siis tulkita siten, että siinä sallitaan henkilötietojen jatkokäsittely yhteensopimattomaan tarkoitukseen.[25] Tietosuojatyöryhmän mielestä on täsmällisesti ilmaistava, että organisaatio ei saa käsitellä henkilötietoja olennaisesti erilaiseen tarkoitukseen, jos kyseinen käyttötarkoitus on käyttötarkoituksen rajoittamista koskevan periaatteen mukaisesti yhteensopimaton. Toisin sanoen olisi oltava selvää, että valintaperiaate ei ole poikkeus käyttötarkoituksen rajoittamista koskevasta periaatteesta.

Joka tapauksessa silloinkin, kun jatkokäsittelyn voidaan katsoa olevan yhteensopivaa, olisi myös sovellettava ilmoitus- ja valintaperiaatteita.

2.2.5 Journalistiset poikkeukset

Henkilötietojen käsittelyn journalistisia poikkeuksia käsitellään täydentävässä periaatteessa 2 (liite II, III.2). Käsityksemme mukaan nämä säännökset vastaavat Yhdysvaltojen perustuslain sananvapauden suojaa. Siitä syystä Privacy Shield -asiakirjoissa todetaan, että ”Privacy Shield -järjestelyn periaatteiden vaatimukset eivät koske henkilötietoja, – – jotka löytyvät aikaisemmin julkaistusta tiedotusvälineiden arkistoista levitetystä aineistosta” (liite II, III.2.b).

24 Tietosuojatyöryhmä toteaa, että joitain muitakin ilmauksia käytetään: ”käyttötarkoitus ei ole yhteensopiva” (liite II, III.14.b.ii), ”muuhun kuin alkuperäiseen käyttötarkoitukseen” (liite II, III.9.b.i), ”käyttää henkilötietoja muuhun tarkoitukseen kuin siihen, jota varten henkilötiedot siirtävä organisaatio on henkilötiedot alun perin kerännyt” (liite II, II.1.b). Vaikeaselkoisuus saattaa johtaa siihen, että käyttötarkoituksen rajoittamisen periaatetta koskevat takeet ovat riittämättömät.

25 Ks. myös valintaperiaatetta koskeva huomautus. Tietosuojatyöryhmä katsoo tällaisen tulkinnan vaaraa lisäävän se, että henkilötietojen edelleen siirtämistä koskevissa säännöissä (liite II, II.3) mainitaan ainoastaan valintaperiaate eikä käyttötarkoituksen rajoittamista koskevaa periaatetta.

Tämä poikkeus tuntuu sulkevan sisäänsä kaikenlaisen myöhemmän käsittelyn minkä tahansa rekisterinpitäjän tai tietojenkäsittelijän toimesta. Sitä ei toisin sanoen ole rajoitettu myöhempään käsittelyyn journalistisia tarkoituksia varten. Kuten tietosuojatyöryhmä on jo todennut kirjeessään varapuheenjohtaja Redingille 10. huhtikuuta 2014, työryhmä olisi pitänyt parempana rajatumpaa lähestymistapaa journalistisiin poikkeuksiin, mikä olisi enemmän EU:ssa sovellettavan periaatteen mukaista. Työryhmä olisi myös toivonut Google Spain -ratkaisun[26] mukaista oikeutta saada tietonsa poistetuksi luettelosta.

2.2.5 Rekisteröityjen tiedonsaantioikeus sekä oikeus korjata ja poistaa tiedot

Privacy Shield -järjestelyn mukaisesti henkilöillä on oikeus saada organisaatiolta *vahvistus* siitä, käsitteleekö se heitä koskevia henkilötietoja, ja oikeus saada *kyseiset tiedot nähtäväkseen* (liite II, III.8.a.i). Organisaatioille asetettu velvoite vastata henkilöiden kyselyihin, jotka koskevat henkilötietojen käsittelyn tarkoitusta, kyseessä olevia henkilötietojen ryhmiä ja henkilötietojen vastaanottajia tai vastaanottajaryhmiä, on kuitenkin varsin heikko. Tietosuojatyöryhmä katsoo, että rekisteröitäville annettavat yksityiskohtaiset tiedot olisi mainittava itse tekstissä eikä pelkästään alaviitteessä ja ne olisi laadittava selkeän velvoitteen muotoon (joka on yhteydessä liitteessä II olevaan III.8.a.i.1 alakohtaan).

Täydentävän periaatteen 8 mukaan ”Pääsy koskee vain organisaation säilyttämiä henkilötietoja.” (liite II, III.8.d.ii). Tätä sääntöä ei pitäisi tulkita suppeasti sikäli, että periaatteessa on turvattava tiedonsaantioikeus kaikista organisaation jollain lailla käsittelemistä henkilötiedoista, ei pelkästään niistä, joita organisaatio säilyttää. Tehokkaan tiedonsaantioikeuden kannalta onkin tärkeää tehdä selväksi, että ’säilyttäminen’ tarkoittaa ’käsittelemistä’ liitteessä II olevan 1.8.b alakohdan määritelmän mukaisessa merkityksessä. Säännön soveltamiseen olisi kiinnitettävä erityistä huomiota Privacy Shield -järjestelyn yhteisessä tarkastelussa.

Liitteessä II olevassa II.8.e.i alakohdassa annettu poikkeusluettelo, joka muistuttaa safe harbor -periaatteita koskevien usein kysyttyjen kysymysten (*F.A.Q.*) kysymyksen nro 8 yhteydessä annettua luetteloa, herättää edelleen epäilyksiä, koska sillä tuntuu olevan taipumusta painottaa organisaatioiden etuja. Niinpä henkilöille ei anneta tietoja omista henkilötiedoistaan seuraavista syistä: ”tietojen luovuttaminen rikkoo – – ammatillista etuoikeutta tai velvoitetta” (liite II, III.8.e.3); ”tietojen luovuttaminen vaikeuttaa työntekijää koskevan turvallisuusselvityksen tekemistä tai työntekijän tekemän valituksen käsittelyä tai työntekijän seuraajan valintaa koskevaa suunnittelua ja yritysten uudelleenorganisointia” (liite II, III.8.e.4); ja ”tietojen luovuttaminen haittaa luottamuksellisuutta, joka on tarpeen hoidettaessa moitteettomaan hallintoon liittyviä valvonta-, tarkastus- ja sääntelytehtäviä tai käytäessä nyt tai tulevaisuudessa organisaatiota koskevia neuvotteluja” (liite II, III.8.e.5). Näiden syiden lisäksi on otettava huomioon liitteessä II olevaan III.8.c alakohtaan sisällytetty yleinen luottamuksellisia kaupallisia tietoja koskeva vapautus. Siitä syystä henkilöllä ei koskaan ole oikeutta saada itseään koskevia tietoja edellä luetelluissa tilanteissa, eikä yhtäältä

26 Unionin tuomioistuimen tuomio 13.5.2014, Google Spain SL ja Google Inc. v. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, asia C-131/12, ECLI:EU:C:2014:317.

henkilön oikeuksia ja etuja ja toisaalta organisaation oikeuksia ja etuja millään lailla punnita, jotta tiedonsaantipyyntöön voitaisiin saada tasapainoinen ratkaisu.

Tietosuojatyöryhmä muistuttaa, että perusoikeuskirjan 8 artiklan 2 kohdassa annetaan jokaiselle oikeus tutustua itseään koskeviin tietoihin. Vaikkakaan kyseessä ei ole ehdoton oikeus, se on henkilötietojen suojan kannalta perustava, koska se helpottaa rekisteröidyn muiden oikeuksien, kuten tietojen korjaamista ja poistamista koskevien oikeuksien käyttöä.

Tietosuojatyöryhmä on tyytyväinen niihin merkittäviin parannuksiin, joita henkilötietojen korjaamista ja poistamista koskeviin oikeuksiin on Privacy Shield -periaatteissa tehty safe harbor -periaatteisiin verrattuna, sillä kyseiset oikeudet pätevät paitsi tilanteissa, joissa tiedot eivät ole paikkansapitäviä, myös silloin, kun henkilötietoja on käsitelty järjestelyn periaatteiden vastaisesti (liite II, II.6).

2.2.6 Muutoksenhaku-, täytäntöönpano- ja vastuuperiaate (oikeussuojakeinot)

a) EU:n kansalaisten (*EU individuals*) oikeussuojakeinojen tehokas käyttäminen

Tietosuojatyöryhmä antaa tunnustusta Yhdysvaltojen viranomaisten sitoumuksille, jotka koskevat oikeussuojakeinojen eri kerroksia. Tietosuojatyöryhmä pelkää kuitenkin, että oikeussuojakeinojen kokonaisrakenteen vaikeaselkoisuus ja monimutkaisuus saattavat käytännössä rajoittaa rekisteröidyn oikeuksien tehokasta käyttöä. Tietosuojatyöryhmä huomauttaa, että EU:n luonnollisten henkilöiden käytettävissä olevien oikeussuojakeinojen laatu on tärkeämpi kuin niiden määrä. Lisäksi epäillään, että useimmissa muutoksenhakukeinoissa (ellei kaikissa) edellytetään menettelyä Yhdysvalloissa, mikä hankaloittaa EU:n tietosuojaviranomaisten mahdollisuuksia seurata menettelyjä.

Itse asiassa Privacy Shield -järjestelyn muutoksenhakukeinoissa painotetaan ensisijaisesti rekisteröidyn mahdollisuutta puolustaa oikeuksiaan ja puuttua Privacy Shield -periaatteiden loukkaamiseen ottamalla suoraan yhteyttä oman varmennuksen antaneeseen yhdysvaltalaiseen yritykseen.[27] Lisäksi organisaatioiden on nimettävä riippumaton riidanratkaisuelin yksittäisten valitusten käsittelyä ja ratkaisua varten. Tietosuojatyöryhmä on tyytyväinen siitä, että menettely on luonnollisille henkilöille maksuton.

Vaihtoehtoisesti valitukset voidaan tehdä suoraan liittovaltion kauppakomissiolle, vaikkakaan tällä ei ole mitään velvollisuutta käsitellä niitä. Myös tietosuojaviranomainen voi toimittaa valituksen käsiteltäväksi ja Yhdysvaltojen kauppaministeriö on sitoutunut tarkastelemaan valituksia ja pyrkii parhaansa mukaan edistämään sitä, että valitukseen saadaan ratkaisu (liite I), ja liittovaltion kauppakomissio asettaa etusijalle järjestelyn periaatteiden noudattamatta jättämistä koskevat asiat (liite II, III.7.e). Liittovaltion kauppakomission valituksille antama etusija ei kuitenkaan anna rekisteröidylle mitään varmuutta siitä, että hänen valituksensa käsitellään.

27 Euroopan komissio, ehdotus komission täytäntöönpanopäätökseksi Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä, johdanto-osan 30 kappale.

Viimeisenä keinona luonnolliset henkilöt voivat käyttää mahdollisuutta saada asia sitovan välimiesmenettelyn käsiteltäväksi. Välimiespaneeli sijaitsee Yhdysvalloissa, ja sen päätöksiin voidaan hakea muutosta Yhdysvaltojen tuomioistuimilta.

Lisäksi Privacy Shield -järjestelyssä organisaatiolle tarjotaan mahdollisuus valita yhteistyö EU:n tietosuojaviranomaisten kanssa (liite II, III.5.a). Se on jopa pakollista työsuhteen yhteydessä kerättyjen henkilöstötietojen osalta (liite II, III.9.d.ii). Tällaisessa tilanteessa vaihtoehtoista riidanratkaisua ei voida käyttää (liite II, III.5.a). Privacy Shield -järjestelyssä ei suoraan todeta, kuinka yhteistyö EU:n tietosuojaviranomaisten kanssa käytännössä järjestetään. Erityisesti on epäselvää, käsitteleekö yksi paneeli kaikki tapaukset vai käsitelläänkö jokainen erilainen asia eri paneelissa.

Tietosuojatyöryhmä katsoo, että tietosuojan tason riittävyyttä koskevassa päätöksessä on määritettävä yksityiskohtaisemmin tietosuojaviranomaisten toimivalta käsitellä valituksia. Se riippuu ilmeisesti organisaation luokittelusta, mutta on epäselvää, millä tavoin.

Jos organisaatio toimii edustajana EU:n rekisterinpitäjän puolesta, luonnollisilla henkilöillä on joka tapauksessa mahdollisuus valittaa toimivaltaiselle EU:n tietosuojaviranomaiselle. Tilanne on sama sekä henkilöstötietojen että muiden kaupallisten tietojen käsittelyssä.

Jos Privacy Shield -organisaatio toimii rekisterinpitäjänä, tietosuojaviranomaisen toimivalta käsitellä valitusta rajoittuu mahdolliseen EU:n lainsäädännön alaiseen henkilötietojen käsittelyyn. Henkilötietojen käsittely on EU:n lainsäädännön alaista, jos käsittely tapahtuu EU:n rekisterinpitäjän vastuulla – myös jos tietoja hallitaan yhdessä yhdysvaltalaisen organisaation kanssa – tai jos Privacy Shield -organisaatio on suoraan EU:n lainsäädännön alainen esimerkiksi, koska se käyttää EU:ssa sijaitsevia välineitä. Jos henkilötietojen käsittely tapahtuu yksinomaan Yhdysvaltojen lainsäädännön alaisuudessa, sovelletaan yksinomaan Privacy Shield -menettelyjä. Kielimuurin voittamiseksi ja Yhdysvaltojen oikeusjärjestelmän puutteellisen tuntemisen korvaamiseksi voisi olla hyödyksi, jos EU:n tietosuojaviranomaiset saisivat oikeuden toimia luonnollisten henkilöiden valitusten välittäjinä tai auttaa heitä riidanratkaisumenettelyssä yhdysvaltalaisen organisaation kanssa tai yhteyksissä Yhdysvaltojen viranomaisiin, sikäli kuin tietosuojaviranomaiset pitävät sitä asianmukaisena.

Tietosuojatyöryhmä korostaa, että Privacy Shield -järjestelyn mukainen menettely ei vastaa aiempia suosituksia, joiden mukaisesti EU:n kansalaisten (*EU individuals*) olisi voitava nostaa vahingonkorvauskanne Euroopan unionissa sekä saatava oikeus nostaa kanne EU:n jäsenvaltion toimivaltaisessa tuomioistuimessa.[28] Olisi myönteistä, jos Privacy Shield -organisaatiot sisällyttäisivät tällaisen mahdollisuuden tietosuojaperiaatteisiinsa.

Tehokkuuden varmistamiseksi tietosuojatyöryhmä suosittaa, että järjestelmän olisi suotavaa sallia EU:n tietosuojaviranomaisten edustavan rekisteröityä ja toimia tämän puolesta välittäjänä. Vaihtoehtoisesti siihen olisi sisällytettävä erityiset toimivaltalausekkeet, joissa annettaisiin rekisteröidyille oikeus käyttää oikeuksiaan Euroopassa.

28 Ks. tietosuojatyöryhmän kirje varapuheenjohtaja Redingille 10.4.2014.

b) Välimiesmenettely

Lopullisia välimiesmenettelyjä ei ole vielä viimeistelty, mikä vaikeuttaa niiden arviointia tietosuojatyöryhmässä. Koska vaikuttaa siltä, että välimiesjärjestelmä toteutetaan Yhdysvaltojen lainsäädännön alaisuudessa ja ainoa menettelykieli on englanti, EU:n tietosuojaviranomaiset haluavat ehkä toimia luonnollisten henkilöiden apuna prosessissa.

Lisäksi välimiesmenettely on perustettu sen takia, että valituksen käsittelystä liittovaltion kauppakomissiossa ei ole mitään takeita, koska sillä ei ole velvollisuutta käsitellä jokaista valitusta. Jos EU:n luonnollinen henkilö tuntee tarvitsevansa asianajajan apua, tietosuojatyöryhmä toteaa, että hänen olisi huolehdittava asianajopalkkioista itse, mikä voi estää henkilöitä toimittamasta valitustaan välimiesmenettelyyn.

c) Oikeussuojakeinojen valvonta, täytäntöönpano ja tehokkuus

Privacy Shield -järjestelyyn pääsyn ehdot

Unionin tuomioistuimen mukaan ”tällaisen järjestelmän luotettavuus – – perustuu pääasiallisesti sellaisten tehokkaiden havaitsemis- ja valvontamekanismien käyttöönottoon, joiden avulla voidaan käytännössä yksilöidä ja sanktioida mahdollisia perusoikeuksien – – suojan takaamiseksi annettujen sääntöjen rikkomisia”.[29]

Tietosuojatyöryhmä toteaa, että Yhdysvaltojen kauppaministeriön tehtävä Privacy Shield -järjestelyn varmennusprosessissa näyttää supistuneen pelkästään asiakirjojen täydellisyyden tarkistamiseen. Vaikka tietosuojatyöryhmä myöntää, että oma varmennus ei edellytä tietosuojaperiaatteiden järjestelmällistä ennakkotarkastusta, Yhdysvaltojen kauppaministeriön olisi vähintäänkin sitouduttava tarkastamaan järjestelmällisesti, että tietosuojaperiaatteet sisältävät kaikki Privacy Shield -periaatteet. Tällainen sitoumus mainitaan tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa[30], mutta sitä ei voida selvästi todeta Yhdysvaltojen kauppaministeriön vakuutuskirjeestä.

Privacy Shield -periaatteiden noudattamatta jättäminen saattaa jäädä huomaamatta pitkiksi ajoiksi. Se huomataan mahdollisesti vasta sitten, kun rekisteröidyn perusoikeuksia on loukattu siten, että on aiheutettu vakavaa ja mahdollisesti korvaamatonta haittaa. Tällainen lähestymistapa saattaa siten olla ristiriidassa eurooppalaisen varovaisuusperiaatteen kanssa.

Avoimuus Privacy Shield -luettelon ja siitä poistetuista organisaatioista laaditun luettelon avulla

Avoimuutta rekisteröityä kohtaan on parannettu merkittävällä tavalla. Uuteen Privacy Shield -luetteloon sisältyvät kaikki yhdysvaltalaiset organisaatiot, jotka ovat antaneet oman varmennuksen Yhdysvaltojen kauppaministeriölle, ja sen lisäksi myös kaikki organisaatiot,

29 Schrems-tuomion 81 kohta.
30 Euroopan komissio, tietosuojan tason riittävyyttä koskeva päätösehdotus, johdanto-osan 34 kappale.

jotka on poistettu Privacy Shield -luettelosta, samoin kuin syy organisaation poistamiseen.[31] Kauppaministeriön Privacy Shield -verkkosivustossa keskitytään lisäksi aiempaa enemmän kohdeyleisöihin, jotta sivuston avulla on helpompi tarkastaa, minkä tyyppisiä tietoja organisaation oma Privacy Shield -varmennus kattaa, millaisia tietosuojaperiaatteita varmennuksen kattamiin tietoihin sovelletaan ja millä menetelmällä organisaatio varmistaa, että se noudattaa järjestelyn periaatteita.[32] Tietosuojatyöryhmä suhtautuu myönteisesti siihen, että on täsmällisesti mainittu Yhdysvaltojen kauppaministeriön tarkastavan, että yritykset, joilla on julkinen verkkosivusto, julkaisevat tietosuojaperiaatteensa tässä sivustossa, tai ellei verkkosivustoa ole, missä yleisö voi tutustua kyseisiin periaatteisiin.[33] Lisäksi asiakirjoissa annetaan enemmän tietoa tietosuojaperiaatteiden sisällöstä.[34]

Tietosuojatyöryhmän mielestä ongelmia voi syntyä, jos organisaatio, joka on jo Privacy Shield -luettelossa, myöhemmin laajentaa varmennuksensa koskemaan muita henkilötietojen ryhmiä. Tällaisessa tapauksessa luettelosta ei käy ilmi eri ajanjaksot, joina periaatteita sovelletaan eri henkilötietojen ryhmiin. Tällöin on riskinä, että EU:n luonnolliset henkilöt ja yritykset eivät pysty täysin arvioimaan, onko tietty tietokokonaisuus todella Privacy Shield -periaatteiden alainen, jo jos on, mistä lähtien. Tämän puutteen välttämiseksi tietosuojatyöryhmä suosittaa, että Privacy Shield -luettelon organisaatiota koskevissa tiedoissa täsmennetään erikseen jokaisen henkilötietojen ryhmän osalta oman varmennuksen soveltamisen voimaantulopäivä.

Tietosuojatyöryhmä suhtautuu myönteisesti siihen, että Yhdysvaltojen kauppaministeriö pitää yllä luetteloa organisaatioista, jotka on poistettu Privacy Shield -luettelosta, ja että näihin tietoihin liitetään selitys siitä, miksi kyseiset organisaatiot eivät enää ole oikeutettuja Privacy Shield -järjestelyn etuihin. Niiden on kuitenkin edelleen sovellettava järjestelyn periaatteita niihin henkilötietoihin, jotka ne ovat vastaanottaneet ollessaan Privacy Shield -organisaatio, niin kauan kuin niillä on hallussaan tällaisia tietoja (liite I, s. 3). Osa Privacy Shield -luettelosta poistetuista organisaatioista saattaa päättää palauttaa tai poistaa Privacy Shield -järjestelyssä vastaanotetut tiedot, kun taas toiset organisaatiot päättävät säilyttää järjestelyssä vastaanotetut tiedot, minkä takia asiasta on tärkeää antaa henkilöille entistä avoimemmin tietoja. Siitä syystä Yhdysvaltojen kauppaministeriön ylläpitämässä yritysluettelossa olisi ilmoitettava, onko organisaatiolla edelleen Privacy Shield -järjestelyssä vastaanotettuja tietoja vai onko se palauttanut tai poistanut sellaiset tiedot. Jos organisaatiolla on edelleen tällaisia tietoja, luettelossa olisi erikseen todettava, että organisaation on edelleen sovellettava järjestelyn periaatteita tällaisiin tietoihin.

Lisäksi kauppaministeriön ylläpitämässä luettelossa olisi mainittava, että kyseiset organisaatiot eivät enää ole oikeutettuja Privacy Shield -järjestelyn etuihin uusien

31 Liite I, s. 5 ja liite II, II.1. Lisäksi tietosuojatyöryhmä viittaa tiedonannossa COM(2013) 847 tehtyyn komission suositukseen nro 4 sekä tietosuojatyöryhmän kirjeeseen varapuheenjohtaja Viviane Redingille 10.4.2014 ja erityisesti sen avoimuutta käsittelevän kappaleen viidenteen luetelmakohtaan.
32 Liite I, s. 8. Lisäksi tietosuojatyöryhmä viittaa varapuheenjohtaja Viviane Redingille 10.4.2014 osoittamaansa kirjeeseen ja erityisesti sen avoimuutta käsittelevän kappaleen toiseen kohtaan.
33 Liite I, s. 3 ja 4. Lisäksi tietosuojatyöryhmä viittaa tiedonannossa COM(2013) 847 annettuun komission suositukseen nro 1 sekä tietosuojatyöryhmän kirjeeseen varapuheenjohtaja Viviane Redingille 10.4.2014 ja erityisesti sen avoimuutta käsittelevän kappaleen kolmanteen luetelmakohtaan.
34 Liite I, s. 5 ja 6 sekä liite II, III.6.

henkilötietojen siirtojen osalta, mikä merkitsee, ettei organisaatio saa enää ottaa vastaan henkilötietoja EU:sta periaatteiden mukaisesti.

Tarkastusmenettelyt

Organisaatiot voivat tarkastaa, että oma varmennus on todella tehokas käytännössä, tekemällä itsearviointeja tai käyttämällä ulkopuolista vaatimustenmukaisuuden tarkastelua. Tietosuojatyöryhmä pahoittelee sitä, että työntekijöiden kouluttamista edellytetään ainoastaan, jos organisaatio päättää suorittaa tarkastukset itsearviointijärjestelmän avulla (liite II, III.7.c). Vaikuttaa myös siltä kuin tarve todeta, että organisaation tietosuojaperiaatteet ovat täsmällisiä, kattavia, näkyvällä paikalla olevia, täysimääräisesti täytäntöön pantuja ja helposti tutustuttavissa olevia, koskee vain organisaatioita, jotka ovat valinneet sisäisen tarkastelun (itsearvioinnin), ja että ulkoinen tarkastusmenettely rajoittuu koskemaan vain organisaation tietosuojaperiaatteiden noudattamista.

Jälkivalvonta

Tietosuojatyöryhmä on tyytyväinen siihen, että liittovaltion kauppakomissiolle ja kauppaministeriölle on annettu tutkintavaltuudet valitusasioissa. Lisäksi tietosuojatyöryhmä toteaa, että kauppaministeriöllä on mahdollisuus tehdä tarkastuksia omasta aloitteestaan erityisesti lähettämällä kyselylomakkeita. Tietosuojatyöryhmä haluaisi kuitenkin varmistua siitä, että tällainen lähestymistapa riittää täyttämään tehokkaita havaitsemis- ja valvontamekanismeja koskevan unionin tuomioistuimen vaatimuksen. Tietosuojatyöryhmällä onkin edelleen avoimia kysymyksiä: mitkä ovat Yhdysvaltojen valvontaviranomaisten täsmälliset valtuudet tehdä tarkastuksia paikalla oman varmennuksen antaneiden organisaatioiden tiloissa tutkiakseen Privacy Shield -loukkauksia, miten EU:n viranomaisen päätös voidaan saattaa täytäntöönpanokelpoiseksi Yhdysvaltojen alueella ja ovatko Privacy Shield -järjestelyssä määrättävät seuraamukset käytännössä vaikuttavia?

2.2.7 Henkilöstötietojen käsitteleminen

Soveltamisala

Täydentävää periaatetta 9 (liite II, III.9) sovelletaan työsuhteen yhteydessä kerättyihin (nykyisen tai entisen) työntekijän henkilötietoihin. Täydentävän periaatteen 9.a.ii muotoilun mukaisesti Privacy Shield -periaatteita sovelletaan ainoastaan, kun ”identified records are transferred or accessed” (suomeksi ”kun siirretään tai annetaan käyttöön yksittäinen henkilötieto, jonka perusteella henkilö tunnistetaan”). Ilmaisu *identified records* ei ole johdonmukainen liitteessä II olevan I.8.a alakohdan ’henkilötietoja’ koskevan määritelmän kanssa, joka koskee ”tunnistetun tai tunnistettavan henkilön tietoja”, eikä se siten ole direktiivissä käytetyn määritelmän mukainen.[35]

35 Kuten edellä on korostettu, myöskään tietojen siirtämistä tai käyttöön antamista koskeva rajoitus ei vastaa termiä ’henkilötietojen käsittely’ (liite II, I.8.b).

Täydentävässä periaatteessa 9.a.ii todetaan seuraavasti: ”Yhteenlaskettuihin työtekijätietoihin perustuvat tilastot, joissa ei ole henkilötietoja, tai tiedot, joista nimet on poistettu, eivät ole ongelmallisia yksityisyyden suojan kannalta.” Tämä lausuma on ristiriidassa useiden tietosuojatyöryhmän antamien lausuntojen kanssa. Tietosuojatyöryhmä korostaa, että aggregoidut tiedot voidaan silti uudelleentunnistaa ja että niitä olisi siitä syystä pidettävä henkilötietoina.[36]

Ilmoitus-, valinta- ja käyttötarkoituksen rajoittamisen periaatteet

Täydentävässä periaatteessa 9.b.i annetaan esimerkki ilmoitus- ja valintaperiaatteiden soveltamisesta, jos henkilöstötietoja käytetään muuhun kuin alkuperäiseen käyttötarkoitukseen. Esimerkki koskee yhdysvaltalaista organisaatiota, joka aikoo ”käyttää työsuhteessa kerättyjä henkilötietoja muuhun kuin työsuhteeseen liittyvään tarkoitukseen, kuten markkinointiin”. Tässä skenaariossa käyttötarkoituksen muutos sallitaan sillä edellytyksellä, että noudatetaan ilmoitus- ja valintaperiaatteita. Tietosuojatyöryhmän mukaan henkilöstötietojen myöhempi käsittely suoramarkkinointiin on useimmissa tapauksissa katsottava yhteensopimattomaksi tarkoitukseksi, jolloin se on käyttötarkoituksen rajoittamisen periaatteen vastainen (liite II, II.5.a). Lisäksi tietosuojatyöryhmä katsoo, ettei valinta voi olla asianmukainen perusta käyttötarkoituksen muuttumista koskevalle työntekijän ”suostumukselle” (*opt-out*) työsuhteessa, jossa tällainen suostumus ei kenties ole täysin vapaa.

Tietosuojatyöryhmä epäilee vahvasti, ettei valintaperiaatteen painottaminen Privacy Shield -järjestelyssä edellytyksenä henkilötietojen käytölle muuhun kuin alkuperäiseen käyttötarkoitukseen vastaa OECD:n tietosuojaohjeita, koska ei ole riittäviä takeita siitä, ettei tätä *opt-out*-mekanismia käytetä myös henkilötietojen myöhempään, tarkoitukseltaan yhteensopimattomaan käsittelyyn. Täydentävässä periaatteessa 9.b.iv säädetään laaja ja täsmällinen poikkeus ilmoitus- ja valintaperiaatteista ”siinä määrin ja sellaisena ajanjaksona kuin on tarpeellista, jotta organisaation mahdollisuudet nimittää tai ylentää työntekijöitä tai tehdä muita henkilöstöön liittyviä päätöksiä eivät vaarantuisi”. Ensinnäkin henkilöstötietojen käyttö tällaisiin tarkoituksiin olisi nimenomaisesti mainittava jo tietojen keräämisen yhteydessä. Sitä paitsi ilmaus ”muita henkilöstöön liittyviä päätöksiä” on liian epämääräinen ja liian laaja. Sen seurauksena henkilötiedot vapautetaan kokonaan ilmoitus- ja valintaperiaatteiden noudattamisesta silloin, kun niitä käsitellään työsuhteen yhteydessä. Ilmaus on niin laaja, ettei ole mahdollista arvioida, onko myöhempi käyttö yhteensopivaa alkuperäisen käyttötarkoituksen kanssa. Tietosuojatyöryhmä suosittaa, että tämä poikkeus poistetaan.

Tiedonsaantioikeus

Lisäksi täydentävässä periaatteessa 9.e.i säädetään poikkeuksesta, joka koskee tiedonsaantiperiaatteen soveltamista tai velvoitetta tehdä sopimus henkilöstötietojen rekisterinpitäjänä toimivan kolmannen osapuolen kanssa, jos kyse on satunnaisesta

36 Ks. Lausunto 4/2007 henkilötietojen käsitteestä ja Lausunto 5/2014 anonymisointitekniikoista.

henkilöstöön liittyvästä operatiivisesta toimesta, jossa tietoja käytetään esimerkiksi lentolipun tai hotellihuoneen varaamiseen tai vakuutussuojan järjestämiseen ja jos ilmoitus- ja valintaperiaatetta noudatetaan. Tietosuojatyöryhmä ei näe tällaiselle poikkeukselle mitään kohtuullista perustetta ja suosittaa, että tämä kohta poistetaan.

2.2.8 Farmaseuttiset tuotteet ja lääkevalmisteet

Soveltamisala

Privacy Shield -järjestelyssä katsotaan, että avainkoodatun tiedon siirto EU:sta Yhdysvaltoihin ei ole farmaseuttisten tuotteiden ja lääkevalmisteiden yhteydessä sellainen henkilötietojen siirto, johon sovelletaan Privacy Shield -järjestelyn periaatteita (liite II, III.14.g.i). Avainkoodattujen tietojen siirtäminen on kuitenkin suojattu EU:n tietosuojalainsäädännössä. Tämä merkitsee, ettei Privacy Shield -järjestely käytännössä voi koskea tällaista tiedonsiirtoa. Tietosuojatyöryhmä kehottaa EU:n komissiota toteamaan nimenomaisesti, että tietosuojan tason riittävyyttä koskevaa päätösehdotusta ei sovelleta avainkoodattujen tietojen siirtämiseen farmaseuttisista tai lääkinnällisistä syistä ja että sen seurauksena tällaisiin siirtoihin on sovellettava muita suojatoimia, kuten vakiosopimuslausekkeita tai yritystä koskevia sitovia sääntöjä. Tietosuojatyöryhmä ehdottaa, että tämä selkeytetään tietosuojan tason riittävyyttä koskevassa lopullisessa päätöksessä.

Tietojen siirtäminen sääntelyä ja valvontaa varten (liite II, III.14.d)

Tietosuojatyöryhmä on huolissaan siitä, että näiden säännösten mukaisesti henkilötietoja, jotka lääkinnällisen yhteyden vuoksi ovat enimmäkseen luonteeltaan arkaluonteisia, saa siirtää Yhdysvaltojen sääntelyviranomaisille. Privacy Shield -järjestely on suunniteltu henkilötietojen siirtämiseen yksityisten elinten välillä, joten vaikuttaa siltä, että julkinen elin, kuten Yhdysvaltojen sääntelyviranomainen, ei ole kelpoinen antamaan järjestelyssä omaa varmennusta, mikä herättää kysymyksen tällaisen tiedonsiirron riittävästä tietosuojasta. Jos tällainen tietojen siirtäminen on tarpeen sääntelytarkoituksiin, on toteutettava asianmukaiset toimenpiteet, joilla varmistetaan EU:n rekisteröityjen perusoikeuksien jatkuva suojelu. Tietosuojatyöryhmä korostaa, että tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa ei ole lainkaan tätä kohtaa koskevia toteamuksia. Tietosuojatyöryhmällä ei siten ole mitään takeita siitä, että EU:n rekisteröityjen arkaluonteisiin tietoihin sovellettava suoja on tässä yhteydessä riittävä.

Kun on kyse tietojen käsittelystä tulevaisuudessa tehtävää tieteellistä tutkimusta varten, tietosuojatyöryhmä ei myöskään ymmärrä, miksi markkinointi mainitaan esimerkkinä mahdollisesta käyttötarkoituksesta. On myös epäselvää, miksi henkilötietojen siirtäminen edelleen yrityksen muille toimipaikoille ja muille tutkijoille on mainittu otsikon ”Tietojen siirtäminen sääntelyä ja valvontaa varten” alla (liite II, III.14.d). Nämä kysymykset on selkeytettävä tietosuojan tason riittävyyttä koskevassa lopullisessa päätöksessä.

Tuotteen turvallisuuden ja tehon seuranta (myös raportit viranomaisille) ja tiettyjä lääkkeitä tai lääkinnällisiä laitteita käyttävien potilaiden/henkilöiden jäljittäminen

Privacy Shield -järjestelyssä säädetään poikkeus ilmoitus-, valinta-, henkilötietojen edelleen siirtämiseen liittyvästä vastuuvelvollisuus- ja tiedonsaantiperiaatteista, jos periaatteiden noudattaminen estää noudattamasta viranomaisvaatimuksia. Tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa ei ole toteamuksia tilanteista, joissa Privacy Shield -periaatteet estäisivät noudattamasta viranomaisvaatimuksia. Tietosuojatyöryhmä saattaisi ymmärtää sen, että viranomaisten tutkimukset voivat perustellusti edellyttää, että ilmoitus- ja tiedonsaantiperiaatteita rajoitetaan tutkimusten suojaamiseksi, mutta sen sijaan tietosuojatyöryhmä ei näe mitään syitä, joilla voitaisiin oikeuttaa näin laajat poikkeukset, jos henkilötietoja käsittelee yksityisen sektorin organisaatio tai kolmas osapuoli. Potilaiden hoito on esimerkiksi yhä yksilöllisempää, eikä näin laajaa poikkeusta Privacy Shield -periaatteissa tiettyjä lääkkeitä tai lääkinnällisiä laitteita käyttävien potilaiden/henkilöiden jäljittämisessä voida hyväksyä, kun tämän tyyppiset hoitomuodot yleistyvät. Sama pätee myös tilanteisiin, joissa farmaseuttiset yritykset käyttävät henkilötietoja tuotteiden turvallisuuden ja tehon seurantaan (uusien lääkkeiden testaamiseen tai myyntiin).

2.2.9 Julkisesti saatavilla olevat tiedot

Julkisesti saatavilla oleviin tietoihin ja julkisiin rekisteritietoihin sovellettava tiedonsaantioikeutta koskeva poikkeus (liite II, III.15.d) on huolestuttava, sillä on mahdollista, että valvoakseen omien henkilötietojensa käsittelyä henkilö, joka käyttää tiedonsaantioikeuttaan, haluaa tietää, käsitteleekö tietty henkilötietojen käsittelijä häntä koskevia tietoja ja mitä tietoja käsitellään. Tietosuojatyöryhmä on toistuvasti todennut, että EU:n lainsäädännön mukaisesti rekisteröidyillä on aina oikeus saada itseään koskevat tiedot ja vaatia tarvittaessa niiden korjaamista tai poistamista, jos tietoja ei ole käsitelty lainmukaisesti tai jos ne ovat epätäydellisiä tai virheellisiä, siitä riippumatta, onko tiedot julkaistu.[37] Jos henkilön tiedonsaantipyyntö hylätään sillä perusteella, että tiedot on saatu julkisesti saatavilla olevista lähteistä tai julkisista rekistereistä, henkilö menettää mahdollisuuden valvoa tietojen oikeellisuutta ja sekä sitä, onko tiedot alun alkaen saatettu julkisiksi lainmukaisesti.

Privacy Shield -järjestelyssä julkiset rekisterit ja julkisesti saatavilla olevat tiedot vapautetaan kuitenkin ilmoitus-, valinta- ja tiedonsaantiperiaatteiden sekä henkilötietojen edelleen siirtämiseen liittyvän vastuuvelvollisuusperiaatteen noudattamisesta. Poikkeukset vaikuttavat direktiiviin verrattuna liian laajoilta, mikä huolestuttaa, sillä ne heikentävät muun muassa henkilön mahdollisuutta valvoa itseään koskevien tietojen oikeellisuutta ja rajoittaa omien tietojensa levittämistä.

2.3 Päätelmät

Tietosuojatyöryhmä antaa Yhdysvaltojen viranomaisille ja Euroopan komissiolle tunnustusta siitä, että mantereiden välisen henkilötietojen siirron kaupallisia näkökohtia on merkittävästi parannettu. Edellä esitetyn analyysin perusteella tietosuojatyöryhmä kuitenkin toteaa, että

37 Ks. WP 20, s. 4.

Privacy Shield -järjestelyn kaupallista osaa on monessa kohdin edelleen selkeytettävä. Muun muassa henkilötietojen säilyttämistä koskevan nimenomaisen periaatteen puuttuminen huolettaa. Siitä syystä tietosuojatyöryhmällä on vakavia epäilyksiä sen suhteen, voidaanko Privacy Shield -järjestelyllä varmistaa tietosuojan taso, joka pääosin vastaa unionin tasoa.

Tietosuojan tason riittävyyttä koskevassa päätöksessä on tarkemmin selkeytettävä käyttötarkoituksen rajoittamisen periaatetta ja valintaperiaatetta. Useissa periaatteissa on edelleen porsaanreikien riski, erityisesti henkilötietojen edelleen siirtämistä, valitusten käsittelymekanismia ja henkilöstötietojen tai farmaseuttisten tietojen käsittelyä koskevissa periaatteissa. Lisäksi on tarkemmin säädettävä, miten Privacy Shield -periaatteita sovelletaan henkilötietojen käsittelijöihin (edustajiin). Myös termistön yksiselitteiseen ja selkeään käyttöön on kiinnitettävä erityistä huomiota.

3. TIETOSUOJAN TASON RIITTÄVYYTTÄ KOSKEVAN PÄÄTÖSEHDOTUKSEN KANSALLISTA TURVALLISUUTTA KOSKEVIEN TAKEIDEN ARVIOINTI

3.1 Yhdysvaltojen kansallisiin turvallisuusviranomaisiin sovellettavat suojatoimet ja rajoitukset

Puuttuminen yksityisyyden ja henkilötietojen suojan perusoikeuksiin voidaan sallia edellyttäen, että puuttuminen on demokraattisessa yhteiskunnassa oikeutettua. Se tarkoittaa, että yksityisyyden suojaa koskevat periaatteet eivät ole ehdottomia ja että poikkeukset ovat mahdollisia, mutta ainoastaan jos sovellettavat olennaiset takeet täyttyvät. Yksityisyyden suojan tehostamisen tavoitteen mukaisesti organisaatioiden olisi lisäksi pyrittävä panemaan periaatteet täytäntöön kokonaan ja avoimesti sekä ilmoitettava tietosuojaperiaatteissaan, mitä Yhdysvaltojen lainsäädännössä sallittuja poikkeuksia sovelletaan säännöllisesti. Samasta syystä, jos periaatteissa ja/tai Yhdysvaltojen lainsäädännössä sallitaan vaihtoehtoja, organisaatioiden odotetaan valitsevan – milloin mahdollista – korkeimman mahdollisen suojan tason.

Liitteessä II olevassa I.5 kohdassa todetaan seuraavasti: ”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.”

Kysymys kuuluu, ovatko liitteessä II mainitut poikkeukset oikeutettuja demokraattisessa yhteiskunnassa. Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa komissio toteaa, 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"[38].

Tietosuojatyöryhmä on arvioinut Yhdysvaltojen lainsäädäntöä ja Yhdysvaltojen tiedusteluviranomaisten käytäntöjä sekä edellytyksiä, joiden mukaisesti sallitaan puuttuminen EU:n lainsäädännön mukaisiin yksityisyyden ja henkilötietojen suojan perusoikeuksiin. Arvio on tehty tämän lausunnon osiossa 1.2 esitettyjen seikkojen pohjalta ja ottamalla huomioon Yhdysvaltojen viranomaisten vakuutukset ja komission toteamukset. Arvio perustuu seuraavien säädösten analyysiin: presidentin määräys 28 (*Presidential Policy Directive*, jäljempänä 'PPD-28'), toimeenpanoasetus 12333 (*Executive Order*) ja ulkomaantiedustelun valvontaa koskevassa laissa annetut eri oikeusperustat (*Foreign Intelligence Surveillance Act*, jäljempänä 'FISA-laki', 104, 402, 215, 501 ja 702 §). Tietosuojatyöryhmä on hyödyntänyt Privacy Shield -järjestelyn liitettä VI. Liite sisältää Yhdysvaltojen kansallisen tiedusteluviraston johtajan (*Office of the Director of National Intelligence*, jäljempänä 'ODNI') kirjeen, joka koskee Yhdysvaltojen kansallisiin turvallisuusviranomaisiin sovellettavia suojatoimia ja rajoituksia. Kirjeessä esitetään myös tiivistelmä Euroopan komissiolle annetuista tiedoista, jotka koskevat Yhdysvaltojen signaalitiedustelutoimintaa.

3.2 Tae A – Henkilötietojen käsittelyn oltava lainmukaista ja perustuttava selkeisiin, täsmällisiin ja helppotajuisiin sääntöihin

Eurooppalaisen oikeuden mukaisesti puuttumisen perusoikeuksiin olisi perustuttava lakeihin ja vakiintuneisiin toimintalinjoihin ja menettelyihin ja sitä koskevien sääntöjen olisi oltava riittävän selkeitä ja saatavilla (yksittäisten maiden harkintamarginaalin sisällä), jotta kansalaiset saavat riittävän selvän tiedon siitä, missä olosuhteissa ja millä edellytyksillä viranomaisilla on valtuudet käyttää tarkkailutoimenpiteitä.[39]

Tietosuojatyöryhmä toteaa, että signaalitiedustelutoimintaa harjoitetaan ymmärrettävän ja saatavilla olevan lainsäädännön perusteella. Kaikki liitteessä VI mainitut lait (PPD-28, FISA, USA FREEDOM ACT, FOIA) ovat verkossa suuren yleisön saatavilla sekä Yhdysvalloissa että Yhdysvaltojen ulkopuolella. Liitteessä VI esitetään tiivistelmä voimassa olevasta oikeudellisesta sääntelykehyksestä, henkilötietojen keräämisen rajoituksista, niiden säilyttämis- ja levittämisrajoituksista, lakien noudattamisesta ja valvonnasta, avoimuudesta ja oikeussuojakeinoista. Tiedustelutoimintaa koskeva Yhdysvaltojen oikeusjärjestys koostuu useista eri asiakirjoista. Niiden joukkoon kuuluu yksittäisten virastojen raportteja, toimintalinjoja ja menettelyjä, jotka on analysoitava, jotta toimintaa voidaan paremmin

38 Tietosuojan tason riittävyyttä koskeva päätösehdotus, johdanto-osan 75 kappale.

39 Euroopan ihmisoikeustuomioistuimen tuomio 4.12.2015, Roman Zakharov v. Venäjä, 247 kohta: Ihmisoikeustuomioistuin on aiemmin todennut, että oikeuden ennakoitavuuden vaatimus ei mene niin pitkälle, että valtioiden olisi säädettävä säännöksiä, joissa eritellään yksityiskohtaisesti kaikki sellainen käytös, joka saattaisi johtaa päätökseen kohdistaa henkilöön salaista tarkkailua kansallisten turvallisuuden perusteella. Kansalliseen turvallisuuteen kohdistuvat uhat ovat luonteeltaan vaihtelevia, eikä niitä aina voi ennakoida taikka niitä on vaikea määritellä etukäteen (ks. em. tuomio, Kennedy, 159 kohta). Samalla ihmisoikeustuomioistuin on korostanut myös sitä, että oikeusvaltioperiaate on eräs Euroopan ihmisoikeussopimuksessa vahvistetuista demokraattisen yhteiskunnan perusperiaatteista, ja perusoikeuksiin liittyvissä asioissa olisi oikeusvaltioperiaatteen vastaista, jos toimeenpanovallalla olisi kansalliseen turvallisuuteen liittyvissä asioissa rajattomiin valtuuksiin perustuva harkintavalta. Näin ollen laissa on ilmoitettava riittävän selkeästi toimivaltaisille viranomaisille mahdollisesti annettu harkintavalta ja tapa, jolla sitä voidaan käyttää, ottamalla huomioon kyseessä oleva oikeutettu tavoite, jotta henkilö saisi riittävän suojan mielivaltaista puuttumista vastaan.

ymmärtää sekä teoriassa että käytännössä. Tietosuojatyöryhmä on tältä osin keskittynyt rajoitettuun määrään ratkaisevan tärkeinä pitämiään kohtia.

3.2.1 Toimeenpanoasetus 12333 ja presidentin määräys 28

Toimeenpanoasetuksen 12333 (*Executive Order*) soveltamisala on laaja; periaatteessa Yhdysvaltojen presidentillä on asetuksen perusteella harkintavalta määrätä mitä tahansa ulkomaantiedustelutietoa kerättäväksi. On kuitenkin väitetty, että FISA-lain voimaantulon jälkeen toimeenpanoasetusta 12333 voidaan käyttää vain tietojen keräämiseen Yhdysvaltojen alueen ulkopuolella. Tietosuojatyöryhmä toteaa, ettei toimeenpanoasetuksessa 12333 ole juurikaan selvitystä sen maantieteellisestä soveltamisalasta, siitä, missä määrin tietoja voidaan kerätä, säilyttää tai levittää edelleen, eikä siitä, millaiset rikkomukset mahdollisesti antavat aiheen tarkkailuun tai millaisia tietoja voidaan kerätä tai käyttää.

Tietosuojatyöryhmän käsityksen mukaan presidentin määräyksen 28 (*Presidential Policy Directive*, jäljempänä ’PPD-28’) tarkoituksena on määrittää henkilötietojen keräämisen ja käsittelyn rajat, riippumatta siitä, mitä tarkkailuohjelmaa käytetään ja mistä tiedot saadaan.

PPD-28 on Yhdysvaltojen presidentin antama määräys. Siinä esitetään yhdenmukaisuusperiaatteet, joiden mukaisesti signaalitiedustelutietojen keräämiseen annetaan lupa ja joiden mukaisesti sitä toteutetaan, mutta PPD-28 ei ole tietojen keräämisen oikeusperusta. PPD-28 toimii tehokkaasti velvoittamalla tiedusteluyhteisön elimet toteuttamaan kyseisiä periaatteita toimintalinjoissaan ja menettelyissään. Määräystä sovelletaan signaalitiedustelutoimintaan riippumatta tietojen sijainnista niiden keruuajankohtana, olipa sijaintipaikka Yhdysvalloissa ja tai Yhdysvaltojen ulkopuolella. Siitä syystä sitä sovelletaan myös EU:sta Yhdysvaltoihin siirrettäviin henkilötietoihin, kun niitä kerätään signaalitiedustelutarkoituksiin.

PPD-28:n mukaan signaalitiedustelutoiminnan suunnittelussa korostetaan sitä, että toiminnan on oltava mahdollisimman räätälöityä.[40] Tietojen käytön osalta määräyksessä vahvistetaan menettelyt, jotka koskevat tietojen minimointia (myös tietojen säilyttämistä ja levittämistä koskevat ehdot), tietoturvaa, asiaankuuluvan henkilöstön käyttöoikeuksia (eli säännöt sisältävät väärinkäytön riskien ja epäasiallisen käytön rajoittamista koskevat suojatoimet), tietojen laatua ja valvontaa. Takeita sovelletaan rekisteröidyn kansallisuudesta riippumatta, siis sekä yhdysvaltalaisiin että muihin henkilöihin.

PPD-28:ssa vahvistettuja suojatoimia sovelletaan myös silloin, kun tietoja siirretään Yhdysvaltoihin. Liitteessä VI annetussa ODNIn sitoumuksessa todetaan, että jos Yhdysvaltojen tiedusteluyhteisö keräisi transatlanttisista kaapeleista Yhdysvaltoihin lähetettävää tietoa, ”se tehtäisiin noudattaen tässä selostettuja rajoituksia ja suojatoimia, mukaan lukien PPD-28:n vaatimuksia”[41]. Tietosuojatyöryhmä toteaa, ettei edelleenkään ole

40 PPD-28, 1.d §: Signaalitiedustelun on oltava niin räätälöityä kuin mahdollista. Kun tiedusteluyhteisö päättää, kerätäänkö signaalitiedustelutietoa, sen on otettava huomioon, onko muuta tietoa saatavilla, mukaan lukien diplomaattitieto ja julkinen tieto, ja sen on annettava etusija näille muille tiedonhankintatavoille..

41 Privacy Shield -järjestelyn liite VI, Yhdysvaltojen kansallisten turvallisuusviranomaisiin sovellettavia suojatoimia ja rajoituksia koskeva ODNIn kirje, s. 2.

olemassa oikeuskäytäntöä, jossa ratkaistaisiin jonkin maan toteuttaman kaapelisignaalitiedustelun laillisuus. Yhdysvallat ei kuitenkaan sen enempää myönnä kuin kiellä harjoittavansa kaapelisignaalitiedustelua tiedustelutietojen keruumenetelmänä.

'Signaalitiedustelun' käsitettä ei määritellä PPD-28:ssa eikä missään muussakaan sovellettavassa tekstissä.

3.2.2 Ulkomaantiedustelun valvontaa koskeva laki (FISA)

Ulkomaantiedustelun valvontaa koskevan FISA-lain teksti vaikuttaa kokonaisuudessaan edellä käsiteltyjä säädöksiä selkeämmältä ja täsmällisemmältä. Monia sen säännöksiä tulkitaan kuitenkin PPD-28:n pohjalta, ja siten niiden käytännön soveltaminenkin riippuu suuresti eri virastojen toteutustavoista. Vaikka uusien suojatoimien täytäntöönpanoa koskeva täydellinen raportti ei ole vielä saatavilla, Yhdysvaltojen valtuuskunnan jäsenet ovat ilmoittaneet tietosuojatyöryhmän edustajille, että PPD-28:n sisältämät suojatoimet on pantu kokonaisuudessaan täytäntöön ja niitä toteutetaan samalla lailla koko Yhdysvaltojen tiedusteluyhteisössä.

Tarkemmin sanoen FISA-lain 501 § on suhteellisen selkeä sen suhteen, millaisiin tiedusteluoperaatioihin voidaan antaa valtuutus: jonkin konkreettisen esineen hankkiminen (myös kirjan, tallenteen, asiakirjan ja muun tavaralajin). On kuitenkin huomattava, että valtuutuksen soveltamisala on varsin laaja, koska 'konkreettisen esineen' määritelmä sisältää myös "muut tavaralajit".

FISA-lain 702 §:ssä sallitaan tietojen kerääminen ulkomaan tiedustelutiedon saamiseksi ei-yhdysvaltalaisilta henkilöiltä, joiden voidaan kohtuudella olettaa oleskelevan Yhdysvaltojen ulkopuolella.[42] Pykälä ei kuitenkaan ole yhtä yksityiskohtainen kuin 501 §. Soveltamisalaltaan 702 § on kohdennettu Yhdysvaltoihin sijoittautuneisiin sähköisten viestintäpalvelujen tarjoajiin, ja sen tavoitteena on ulkomaan tiedustelutietojen kerääminen Yhdysvaltojen ulkopuolella oleskelevista henkilöistä. 'Ulkomaan tiedustelutiedon' määritelmä on laaja. Siihen kuuluvat muun muassa vierasta valtaa tai ulkomaista aluetta koskevat tiedot, jotka liittyvät Yhdysvaltojen ulkoasioiden hoitoon.[43] Se herättää jonkin verran epävarmuutta siitä, minkä tyyppisiä tietoja käytännössä voidaan kerätä.

FISA-lain soveltaminen, myös sen soveltamisala ja erityisten valintaehtojen käyttö, on edelleen epäselvää ja hämmentävää, vaikka tiettyjä asiakirjoja ei enää luokitella salaisiksi (raportit kongressille ja yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan (PCLOB) valvontaraportit). Erityisten valintaehtojen käyttöön viitataan PCLOB:n raportissa[44], mutta tietosuojatyöryhmän käsityksen mukaan ne eivät vastaa 702 §:n[45] mukaisia kohdentamissääntöjä. Tietosuojatyöryhmän saamien tietojen mukaan niihin ei viitata yleisesti saatavilla olevissa säännöissä.

42 50 U.S. Code §1881a (D)(1).
43 50 U.S. Code § 1801 (e) (2).
44 PCLOB, *Report on the Surveillance program operated pursuant of Section 702 FISA*, s. 32.
45 50 U.S. Code § 1881a(D).

3.2.3 Päätelmät

Tietosuojatyöryhmä toteaa yleisesti, että tiedustelutoimintaan sovellettavat tekstit ovat saatavilla verkossa ja että Yhdysvaltojen viranomaiset ovat toteuttaneet useita tärkeitä toimia avoimuuden lisäämiseksi.

Tietosuojatyöryhmä antaa arvoa sille, että vuoden 2013 jälkeen suuri määrä asiakirjoja on julkaistu, kuten toimintalinjoja, menettelyjä, FISC-tuomioistuimen ratkaisuja ja muita asiakirjoja, joiden luokitusta on muutettu. Lisäksi PCLOB on julkaissut tärkeitä raportteja 702 §:n ja USA FREEDOM -lain perusteella toteutetusta toiminnasta. Vastaavaa raporttia odotetaan toimeenpanoasetuksen 12333 perusteella toteutetusta toiminnasta.

Useat säädösliitteet, joista voisi saada tietoa toimeenpanoasetuksen vaikutuksista henkilöihin Yhdysvaltojen ulkopuolella ja mahdollisesti sovellettavista suojatoimista, on luokiteltu salaisiksi, joten yleisöllä tai liitteiden vaikutuspiiriin mahdollisesti joutuvilla henkilöillä ei ole mahdollisuutta tutustua niihin. Tekstit, joiden luokitus on muutettu julkiseksi, antavat vain vähän lisäarvoa, eikä niiden avulla juuri saa tarkempaa kuvaa tiedustelutoiminnasta.

Toimeenpanoasetuksen 12333 nykyinen käytännön soveltaminen on edelleen hämärän peitossa, vaikka toimeenpanoasetuksen 12333 toimintaa on Snowden-paljastusten jälkeen pyritty selkeyttämään varsinkin antamalla PPD-28. Tietosuojatyöryhmä toteaa, että Privacy Shield -järjestelyn liitteessä IV ei kuvata yksityiskohtaisesti toimeenpanoasetuksen 12333 toimintaa.

Tietosuojatyöryhmä suhtautuu myönteisesti PPD-28:n mukanaan tuomiin rajoituksiin. On kuitenkin vaikea sanoa, onko tarkkailua koskeva Yhdysvaltojen säädöskehys riittävän ennakoitava, toisin sanoen, sisältääkö se Euroopan ihmisoikeustuomioistuimen edellyttämällä tavalla riittävät tiedot siitä, missä olosuhteissa viranomaisilla on valtuudet käyttää tällaisia toimenpiteitä. Lisäselvitystä siis odotetaan, myös toimeenpanoasetusta 12333 koskevaa PCLOB:n raporttia.

3.3 Tae B – Osoitettava henkilötietojen käsittelyn tarpeellisuus ja oikeasuhteisuus oikeutettujen tavoitteiden kannalta

3.3.1 Presidentin määräys 28

Presidentin määräyksellä PPD-28 rajoitetaan tarkoituksia, joihin henkilötietoja voidaan käyttää, ja edellytyksiä, joiden mukaisesti niitä voidaan levittää. PPD-28 vaikuttaa signaalitiedustelutietojen keräämiseen käytettävästä oikeusperustasta riippumatta.

PPD-28:n 1 §:n mukaan signaalitiedustelutoiminnan suunnittelussa korostetaan varsinkin sitä, että tiedustelun on oltava mahdollisimman räätälöityä. Vaikka on totta, että tämä rajoitus on olemassa, on vaikea määrittää, tarkoittaako ”mahdollisimman räätälöity” sitä, että kaikki tiedonkeruu on tarpeellista ja oikeasuhteista.

PPD-28:ssa todetaan, että valikoimaton tiedonkeruu on edelleen sallittua, jotta voidaan ”tunnistaa uusia tai syntymässä olevia uhkia” ja hankkia ”muuta elintärkeää kansalliseen turvallisuuteen liittyvää tietoa, joka on usein kätkettynä modernien maailmanlaajuisten yhteyksien suureen ja monimutkaiseen järjestelmään”.[46] Tietosuojatyöryhmä toteaa, että PPD-28:n mukaan ’valikoimattoman signaalitiedustelutiedon keräämisellä’ tarkoitetaan luvallista laajamittaista signaalitiedustelutiedon keräämistä, jossa ei teknisistä tai operatiivisista syistä käytetä erottelutekijöitä (esimerkiksi tunnisteet, valintakriteerit jne.).

PPD-28:ssa rajoitetaan valikoimatonta signaalitiedustelutiedon keruuta käyttötarkoituksen osalta. Tietoa voidaan kerätä valikoimattomasti kuuteen tarkoitukseen, ja niihin sisältyvät muun muassa terrorismin torjunta ja muut vakavat (ylikansalliset) rikosmuodot. Tietosuojatyöryhmän analyysista voidaan päätellä, että käyttötarkoituksen rajoitus on melko (mahdollisesti liian) laaja, jotta sitä voitaisiin pitää kohdennettuna.

PPD-28 ei ole poistanut mahdollisuutta kerätä henkilötietoja kohdentamattomasti eikä valikoimatta eikä sitä, että tällaisen tiedonkeruun mahdollisuudet ovat edelleen epäselviä ja mahdollisesti laajoja. Tietosuojatyöryhmä toteaa tältä osin ODNIn vahvistavan liitteessä VI, että ”Yhdysvaltojen tiedusteluyhteisön signaalitiedustelulla suorittama mahdollinen valikoimaton internet-viestinnän tiedonkeruu kohdistuu vain pieneen osaan internetiä”[47], ja siksi työryhmä pitäisi arvossa, jos avoimuustoimenpiteiden avulla asiasta toimitettaisiin lisänäyttöä.

3.3.2 Ulkomaantiedustelun valvontaa koskeva laki (FISA)

FISA-lain 215 ja 702 §:ään on lisätty minimointimenettelyt, jotta yhdysvaltalaisten henkilöiden henkilötietoja voidaan suojella julkishallinnon pitkälle menevältä käytöltä. Näitä rajoituksia ei virallisesti sovelleta ulkomaalaisiin, vaikka Yhdysvaltojen hallituksen virkamiehet ovat toistuvasti todenneet sekä julkisissa että yksityisissä tapaamisissa tietosuojatyöryhmän edustajien kanssa, että minimointimenettelyjen soveltaminen on sen jälkeen käytännössä ulotettu koskemaan kaikkia henkilöitä heidän kansallisuudestaan tai asuinpaikastaan riippumatta.

Lain 702 §:ssä täsmennetään, että tietojenhankinta, jolle on annettu lupa, on tehtävä Yhdysvaltojen perustuslain neljännen lisäyksen mukaisesti rajoittamalla tietojenkeruu siihen, minkä katsotaan olevan kohtuullisen etsinnän periaatteen mukaista. Pykälän mukaan tältä osin ei tehdä eroa yhdysvaltalaisten ja muiden yritysten välillä. Toisin sanoen, edellyttäen, että neljättä lisäystä sovelletaan kaikkeen Yhdysvalloissa kerättyyn tietoon, valikoimaton tiedonkeruu Yhdysvalloissa olisi ”kohtuutonta” ja siten perustuslain vastaista.

46 PPD-28:n 2 § ja Privacy Shield -järjestelyn liite VI, Yhdysvaltojen kansallisten turvallisuusviranomaisiin sovellettavia suojatoimia ja rajoituksia koskeva ODNIn kirje, s. 3.

47 Privacy Shield -järjestelyn liite VI, Yhdysvaltojen kansallisiin turvallisuusviranomaisiin sovellettavia suojatoimia ja rajoituksia koskeva ODNIn kirje, s. 4. Tietosuojatyöryhmä palauttaa tässä yhteydessä mieleen EU:n ja Yhdysvaltojen ad hoc -tietosuojatyöryhmän EU:n yhteispuheenjohtajien havainnoista laaditun kertomuksen, jossa todetaan, että viestintädata muodostaa hyvin pienen osan maailmanlaajuisesta internet-liikenteestä, kun otetaan huomioon, että selvästi suurin osa maailmanlaajuisesta internet-liikenteestä on suurivolyymisia suoratoistoja ja latauksia, kuten televisiosarjoja, elokuvia ja urheilulähetyksiä (kertomuksen 3.1.2 kohta).

Tietosuojatyöryhmä on tyytyväinen PCLOB:n raportissa esitettyyn toteamukseen, jonka mukaan myös ei-yhdysvaltalaiset henkilöt hyötyvät henkilötietojen saantia ja säilyttämistä koskevista rajoituksista, joita eri virastojen minimointi- ja/tai kohdennusmenettelyissä edellytetään. Se johtuu raportin mukaan siitä, että yhdysvaltalaisten henkilöiden tietojen tunnistaminen ja poistaminen suuresta tietomassasta olisi niin kallista ja hankalaa, että tavallisesti koko tietojoukkoa käsitellään yhdysvaltalaisia tietoja koskevien tiukempien vaatimusten mukaisesti.

Lisäksi tietosuojatyöryhmä toteaa, että PCLOB:n mukaan ”ohjelmassa ei toimita keräämällä viestintää valikoimattomasti”. Tämä toteamus vahvistetaan ODNIn raportissa 2014 *Statistical Transparency Report*. Lisäksi PCLOB:n raportin[48] mukaan tarkkailun kohdentamiseen käytetään valintakriteerejä, kuten sähköpostiosoitetta tai puhelinnumeroa.

Kohdentamista koskevissa julkisesti saatavilla olevissa säännöissä ei kuitenkaan määrätä tällaista kohdentamista, vaan niiden ainoa tavoite on välttää kohdentaminen yhdysvaltalaisiin henkilöihin tai Yhdysvalloissa asuviin henkilöihin. Sitä paitsi edut, joita PCLOB:n mukaan sovelletaan käytännössä myös ei-yhdysvaltalaisiin, eivät ole oikeudellisesti sitovia eivätkä lakisääteisiä, koska kohdentamista koskevassa saatavilla olevassa lainsäädännössä ei ole säädetty tällaisista kohdentamissäännöistä, vaan ainoa tavoite on välttää kohdentaminen yhdysvaltalaisiin henkilöihin tai Yhdysvalloissa asuviin henkilöihin.

Tietosuojatyöryhmä palauttaa myös mieliin, että 702 §:n soveltamiseksi ’henkilöitä’ eivät ole ainoastaan luonnolliset henkilöt, vaan myös ryhmät, yhteisöt, yhdistykset, yritykset tai vieraat vallat. Sitä paitsi pykälässä edellytetään, että tietojen keräämisen merkittävä tarkoitus on ulkomaan tiedustelutietojen hankkiminen, mikä jättää hieman epävarmaksi sen tarkoituksen ja tarpeellisuuden. Tietosuojatyöryhmä on kuitenkin tyytyväinen siihen liitteessä VI annettuun tietoon, että 702 §:n mukaisesti kohteena olleiden luonnollisten henkilöiden kokonaismäärä oli vuonna 2014 noin 90 000 henkilöä.[49] Privacy Shield -järjestelyn ensimmäinen tarkastelu tarjoaa tilaisuuden saada lisää näyttöä kohdennussäännöistä.

Toistaiseksi siitä, milloin laajamittainen ja kohdentamaton tietojenkeruu ja sen jälkeen henkilötietojen käyttö rikoksen torjuntatarkoituksiin on laillista, ei ole mitään lopullista oikeuskäytäntöä, ei myöskään siitä, missä olosuhteissa tällaista henkilötietojen keräämistä ja käyttöä voitaisiin harjoittaa. Unionin tuomioistuimen odotetaan käsittelevän tätä kysymystä ainakin joltain osin vuoden 2016 aikana yhdistetyissä asioissa Tele2 Sverige AB v. Post- och telestyrelsen ja Secretary of State for the Home Department v. Davis ym.[50] Lisäksi odotetaan unionin tuomioistuimen kannanottoa Kanadan kanssa tehdystä PNR-sopimuksesta.[51] Niitä odotellessa tietosuojatyöryhmä muistuttaa johdonmukaisesti katsoneensa, että laajamittaista ja kohdentamatonta tietojenkeruuta ei voida missään tapauksessa pitää oikeasuhteisena.[52]

48 PCLOB, *Report on the Surveillance program operated pursuant of Section 702 FISA*, s. 32.
49 Liite VI, s. 11.
50 Unionin tuomioistuin, yhdistetyt asiat C-203/15 ja C-698/15.
51 Unionin tuomioistuin, asia A-1/15.
52 WP 215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fi.pdf

3.3.3 Päätelmät

Tietosuojatyöryhmällä on edelleen epäilyksiä varsinkin tietojenkeruun oikeasuhteisuudesta huolimatta rajoituksista, joita PPD-28:ssa on asetettu. Ensinnäkin on merkkejä siitä, että Yhdysvallat kerää jatkossakin tietoja laajamittaisesti ja kohdentamattomasti tai ainakaan ei sulje tätä mahdollisuutta pois tulevaisuudessa. Tietosuojatyöryhmä on johdonmukaisesti katsonut, ettei tällainen tietojenkeruu ole unionin lainsäädännön mukaista eikä sitä siten voida hyväksyä.

Toiseksi tietosuojatyöryhmä toteaa, että myös kohdennetun tietojenkäsittelyn – tai ns. mahdollisimman räätälöidyn tietojenkäsittelyn – voidaan katsoa olevan laajamittaista. Tällaisen laajamittaisen tiedonkeruun sallittavuutta käsitellään parhaillaan unionin tuomioistuimessa vireillä olevassa asiassa. Tästä syystä tietosuojatyöryhmä ei anna lopullista arviotaan kohdennetun laajamittaisen henkilötietojen käsittelyn laillisuudesta. Työryhmä korostaa kuitenkin, että jos kohdennettu laajamittainen henkilötietojen käsittely sallitaan, kohdennusperiaatteita olisi sovellettava sekä henkilötietojen keräämiseen että niiden myöhempään käyttöön, ei pelkästään käyttöön. Joka tapauksessa tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa on selkeytettävä niitä kuutta PPD-28:ssa mainittua tarkoitusta, joihin tietoa voidaan kerätä ”valikoimattomasti”. Tässä vaiheessa tietosuojatyöryhmä ei ole vakuuttunut siitä, että nämä tarkoitukset ovat riittävän rajoitettuja, jotta henkilötietojen kerääminen olisi todella rajoitettu siihen, mikä on tarpeellista ja oikeasuhteista.

3.4 Tae C – Riippumaton valvontamekanismi

Yhdysvalloissa ei ole liittovaltion tasolla yhtä ainoaa valvontaelintä, jonka tehtävänä olisi valvoa tiedustelu- ja tarkkailuohjelmien vaikutuksia yksityisyyden ja henkilötietojen suojaan. Sen sijaan Yhdysvaltojen tiedustelutoimintaan sovelletaan monikerroksista valvontaprosessia, jossa voidaan tehdä ero sisäisen ja ulkoisen valvonnan välille. Tietosuojatyöryhmä myöntää, että Yhdysvaltojen valvontaelinten raportointikäytäntö on hyvin yksityiskohtainen ja suurelta osin julkinen.

3.4.1 Sisäinen valvonta

Kaikissa tiedustelu- ja turvallisuusvirastoissa jotkut henkilöstön jäsenet ovat vastuussa lainsäädäntökehyksen noudattamisesta. Niissä on myös valvontaviranomaisia (*Inspectors-General*), joiden tärkein tehtävä on arvioida virastojen työtä kokonaisuudessaan lainsäädännön noudattamisen kannalta, myös muttei yksinomaan yksityisyyden ja henkilötietojen suojaa koskevan lainsäädännön kannalta. Valvontaviranomaisista säädetään laissa, ja presidentti on nimittänyt (tai nimittää) heidät kaikki, minkä jälkeen senaatti vahvistaa nimitykset. Tällä tavoin pyritään varmistamaan, että he ovat organisatorisesti riippumattomia ja raportoivat kongressille. Tietosuojatyöryhmä katsoo, että tällä perusteella valvontaviranomaisten voidaan todennäköisesti katsoa täyttävän organisatorisen riippumattomuuden vaatimuksen siten kuin unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin sen ovat määritelleet, ainakin sen jälkeen, kun uutta nimitysprosessia

aletaan soveltaa kaikkiin valvontaviranomaisiin. Toistaiseksi epäilyksiä liittyy vielä niihin valvontaviranomaisiin, jotka nimittää edelleen heidän valvomansa viraston johtaja.

Valvontaviranomaiset voivat antaa suosituksia, jotka voidaan sitten siirtää oikeusministeriölle ja PCLOB:lle tai jopa kongressin komitealle täytäntöönpanoa varten. Jos valvontaviranomainen toteaa rikkomuksen, sitä voidaan käsitellä sisäisin ja toimintapoliittisin keinoin ja siitä voidaan raportoida kongressille. Valvontaviranomaisella on valtuudet tehdä sekä yleisiä että tapauskohtaisia tarkastuksia.

Tietosuojatyöryhmä panee merkille, että valvontaviranomaisen raportit voidaan pitää salassa julkisuudelta ja että valvontaviranomaista voidaan myös estää raportoimasta, jos tarkastettava tieto on luokiteltu salaiseksi. Kongressi kuitenkin joka tapauksessa seuraa raportteja, mikä on olennainen suojatoimi, vaikkakaan se ei ole yksilöllisen muutoksenhaun peruste.

Jokaisella virastolla on yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaava virkamies, joka toimii kongressin valvonnassa ja avustaa pakollisessa itseraportointijärjestelmässä.

Kaiken kaikkiaan käytössä olevia sisäisiä valvontajärjestelmiä voidaan pitää melko vahvoina, mutta valvonnan pitäisi olla täysin riippumatonta, jotta yksityisyyden ja henkilötietojen suojan perusoikeuksiin puuttuminen olisi oikeutettua. Ja vaikka tietosuojaryhmä kunnioittaa ja arvostaa yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavien eri virkamiesten työtä, heidän ei kuitenkaan voida todeta täyttävän riippumattomalta valvojalta edellytettävää riippumattomuuden tasoa.

3.4.2 Ulkoinen valvonta

Ulkoinen valvonta muodostuu useista eri mekanismeista: FISA-lain mukaisen tuomioistuimen (jäljempänä ’FISC-tuomioistuin’) toteuttama 501 ja 702 §:n mukainen tuomioistuinvalvonta, tiedustelua käsittelevän kongressin erityiskomitean valvonta ja PCLOB:n tehtävät.

Tietosuojatyöryhmä palauttaa mieliin, että valvonnan pitäisi ihannetapauksessa olla tuomarin käsissä, jotta menettelyn riippumattomuus ja puolueettomuus voidaan varmistaa, kuten unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin ovat myös todenneet. Vielä viime aikoihin saakka FISC-menettely oli ex parte -menettely, eikä asianomaisella henkilöllä ollut mahdollisuutta tulla kuulluksi tai hänelle ei edes ilmoitettu asian käsittelystä. Nykyäänkin FISC-menettely on edelleen ex parte -menettely, mutta USA FREEDOM -lain säätämisen jälkeen FISC-menettelyyn lisättiin *amici curiae* -toiminto. *Amici curiae* -asianajajat toimivat riippumattomasti, mutta heidän tehtävänään ei ole hoitaa asiaan mahdollisesti liittyvien henkilöiden puolustusta.

USA Freedom -lailla perustettiin *amici curiae* -ryhmä, jonka tehtävänä on taustoittaa tärkeitä asioita FISC-tuomioistuimelle. Tuomioistuin on valinnut viisi asianajajaa, joista on tehty tarvittavat turvallisuusselvitykset ja jotka antavat teknisiä neuvoja, osallistuvat FISC-tuomioistuimen istuntoihin, toimittavat katsauksia ja ottavat kantaa asian perusteisiin

yksityisyyden suojan ja kansalaisoikeuksien näkökulmasta. He osallistuvat kuitenkin vain merkittävien asioiden käsittelyyn tai kun esiin tulee uusia oikeudellisia kysymyksiä.[53]

FISA-lain 215 § on lähes täysin tuomioistuimen ennakkovalvonnassa (muttei jälkivalvonnassa), koska FISC-tuomioistuin hyväksyy kaikki ohjelmat, joiden oikeusperusta on 215 §. PCLOB:n raportissa esitetyn täsmennyksen mukaan 702 § eroaa FISA-lain mukaisesta perinteisestä sähköisen tarkkailun sääntelykehyksestä paitsi sovellettavien normien puolesta myös siten, että FISC-tuomioistuin ei tee yksittäistapauksia koskevia päätöksiä. Lain mukaisesti oikeusministeri ja kansallisen tiedusteluviraston johtaja toimittavat FISC-tuomioistuimelle vuotuisen sertifioinnin, jossa valtuutetaan ulkomaan tiedustelutiedon hankkiminen kohdistamalla tiedustelu Yhdysvaltojen ulkopuolella olevaan ei-yhdysvaltalaiseen henkilöön täsmentämättä tuomioistuimelle, keistä ei-yhdysvaltalaisista henkilöistä tarkalleen on kyse. Toisin kuin perinteisessä FISA-laissa, 702 §:ssä ei raportin mukaan myöskään edellytetä, että hallitus osoittaisi todennäköisen syyn, jonka perusteella voitaisiin olettaa, että 702 §:n kohde olisi vieras valta tai vieraan vallan agentti.[54]

Kongressin erityiskomiteoilla on tehtävänään valvoa myös tiedustelutoimintaa hyväksymällä toiminta erityisesti budjettiäänestysten yhteydessä. Tiedustelua käsittelevät senaatin ja edustajainhuoneen erityiskomiteat saavat tiedustelutoiminnasta salaisiksi luokiteltuja tietoja. Oikeusministerin on raportoitava näille komiteoille FISA-lain mukaisesta sähköisestä tarkkailusta joka kuudes kuukausi. Tietosuojatyöryhmä ei edelleenkään ole selvillä siitä, missä määrin komiteoissa on mahdollista keskustella yksittäisten henkilöiden, varsinkin muiden kuin yhdysvaltalaisten henkilöiden, henkilötietojen käsittelystä.

PCLOB on Yhdysvaltojen hallinnon toimeenpanevan haaran itsenäinen osa, jolla on kaksi perustoimivaltuutta: 1) tarkastella ja analysoida toimia, joita toimeenpanovalta toteuttaa suojellakseen Yhdysvaltojen kansakuntaa terrorismilta, ja varmistaa, että tällaisten toimien tarve on tasapainossa yksityisyyden ja kansalaisvapauksien suojelun tarpeen kanssa, ja 2) varmistaa, että vapausnäkökohdat otetaan asianmukaisesti huomioon niiden lakien, asetusten ja toimintalinjojen suunnittelussa ja toteutuksessa, jotka liittyvät pyrkimyksiin suojella kansakuntaa terrorismilta. Tietosuojatyöryhmä panee merkille, että PCLOB:llä on haasteoikeus ja pääsy salaisiksi luokiteltuihin tietoihin. Tehtäviään suorittaessaan se tarkastaa myös seurantaohjelmien tehokkuuden. Sen valvonta ei ole ennakko- vaan jälkivalvontaa. PCLOB on osoittanut riippumattomat valtuutensa olemalla oikeudellisista kysymyksistä eri mieltä Yhdysvaltojen presidentin kanssa. Se on erityisesti todennut, että 215 §:n mukainen puhelinmetadataa koskeva ohjelma ei ollut lainmukainen ja ettei se ollut tehokas, koska häiritsevistä hyökkäyksistä ei ollut näyttöä. PCLOB on tehnyt myös vuoden pituisen tutkimuksen 702 §:n mukaisesta ohjelmasta ja todennut, että se on selvästi lainmukainen. Lisäksi se totesi, että 702 § on osoittautunut erittäin tehokkaaksi myös terrorismin torjunnassa. Lisäksi PCLOB on käsitellyt avoimuusvaatimusta ja todennut, että useat salaisiksi luokitellut tosiseikat eivät edellyttäneet salassapitoa. Ilmeisesti PCLOB antaa lähitulevaisuudessa raportin PPD-28:n täytäntöönpanosta. PCLOB katsoo siihen liittyen, että

53 Freedom Act, IV osasto, Foreign Intelligence Surveillance Court Reforms, 401 §, *amici curiae* -asianajajien nimittäminen.
54 PCLOB, *Report on the Surveillance program operated pursuant of Section 702 FISA*, s. 24 ja 25.

tietojen säilyttämiseen ulkomaalaisesta ei riitä se pelkästään se seikka, että henkilö on ulkomaalainen.

Lopuksi tietosuojatyöryhmä toteaa, ettei toimeenpanoasetuksessa 12333 säädetä minkäänlaisesta tuomioistuin- tai muusta valvonnasta, eikä oikeussuojakeinoista, jotka koskisivat sen perusteella toteuttavia tarkkailuohjelmia.

3.4.3 Päätelmät

Tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa osoitetaan, että Yhdysvalloissa on käytössä monikerroksinen sekä sisäisiin että ulkoisiin valvontamekanismeihin perustuva lähestymistapa. Tietosuojatyöryhmä on tyytyväinen siihen, että käytössä on yleisesti riittävät sisäiset valvontamekanismit, vaikka niiden toiminta on toisinaan vaikeaselkoista. Tietosuojatyöryhmä on kuitenkin huolissaan siitä, että toimeenpanoasetuksen 12333 perusteella toteuttavien tarkkailuohjelmien valvonta on riittämätöntä.

Tietosuojatyöryhmä toteaa, että sen aiempaa kritiikin aihetta eli kontradiktorisen menettelyn puuttumista FISC-tuomioistuimessa on lievennetty vain jossain määrin ottamalla käyttöön *amici curiae*, joiden tehtävänä on edistää henkilöiden yksityisyyden ja kansalaisvapauksien suojelua. FISC-tuomioistuimen valvonta ei kuitenkaan ole tehokasta ei-yhdysvaltalaisiin henkilöihin kohdentuvan seurannan osalta. Lisäksi on edelleen epävarmaa, pystyykö FISC-tuomioistuin tehokkaasti arvioimaan kohdentamis- ja minimointimenettelyjä, minkä myös PCLOB on todennut.[55]

3.5 Tae D – Tehokkaat oikeussuojakeinot luonnollisten henkilöiden käyttöön

3.5.1 Oikeussuojakeinot tuomioistuimessa

3.5.1.1 Asiavaltuusvaatimus

Yhdysvaltojen oikeussuojakeinojärjestelmässä on merkittävä rajoitus: Yhdysvaltojen perustuslain mukaan henkilön on osoitettava asiavaltuutensa eli näytettävä, että kantaja on kärsinyt tai kärsii välitöntä vahinkoa tai haittaa ja että kyseiseen haittaan on mahdollista hakea hyvitystä. Perustuslain mukaan henkilö tai ryhmä ei voi nostaa kannetta liittovaltion tasolla pelkästään sillä perusteella, että on tyytymätön hallituksen toimintaan tai hallituksen antamaan lakiin.[56] Asiavaltuusvaatimus vaikuttaa merkityksettömältä, koska henkilöille ei ilmoiteta tarkkailusta edes sen jälkeen, kun toimenpiteet ovat päättyneet. Unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin ovat toistuvasti todenneet, että henkilön on voitava käyttää hallinnollisia tai oikeudellisia oikeussuojakeinoja. Euroopan ihmisoikeustuomioistuin on Zakharov-ratkaisussa vahvistanut, että oikeuskäytäntöön

55 PCLOB, *Report on the Surveillance program operated pursuant of Section 702 FISA*, s. 11.
56 https://www.law.cornell.edu/wex/standing;
https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper v. Amnesty International USA.

perustuen kuka tahansa voi saattaa asian tuomioistuimen käsiteltäväksi, jos hänellä on perusteltu syy epäillä perusoikeuksien loukkausta.[57]

Sitä paitsi Yhdysvaltojen ulkopuolella oleskelevat henkilöt eivät saa Yhdysvalloissa täyttä perustuslaillista suojelua Yhdysvaltojen korkeimman oikeuden oikeuskäytännön[58] perusteella. Tämä koskee erityisesti neljättä lisäystä, joka suojaa Yhdysvaltojen kansalaisia – mutta ei muita – kohtuuttomilta etsinnöiltä ja takavarikoilta ja josta suuri osa Yhdysvaltojen yksityisyydensuojaa koskevasta oikeudesta juonnetaan. EU:n kansalaiset ja muut eurooppalaiset, jotka asuvat Yhdysvaltojen ulkopuolella, on yksinkertaisesti suljettu neljännen lisäyksen antaman suojan ulkopuolelle.[59]

Oikeussuojakeinoja koskeva Yhdysvaltojen laki (*Judicial Redress Act*) ei käy tehokkaasta oikeussuojakeinosta kaikille luonnollisille henkilöille, joihin kansallisen turvallisuuden takia toteutettava tiedustelu ja tarkkailu kohdistuu. Tämä johtuu seuraavista syistä: laissa on monia poikkeuksia; on oikeudellisesti epävarmaa, mihin virastoihin lakia sovelletaan: lakia sovelletaan rajoitetusti sekä aineellisesti, koska kansallinen turvallisuus on suljettu sen soveltamisalan ulkopuolelle, että suhteessa henkilöihin, jotka voivat vedota lakiin.

3.5.1.2 Presidentin määräys 28

Tietosuojatyöryhmä toteaa, että PPD-28 on vain määräys, eikä sillä siten voida luoda oikeuksia henkilöille, sillä oikeuksien luomiseen vaaditaan lainsäädäntötoimi. Siitä syystä henkilöt eivät voi saattaa asiaa tuomioistuimen käsiteltäväksi PPD-28:n mukaisten suojatoimien väitetyn loukkaamisen perusteella.

3.5.1.3 Ulkomaantiedustelun valvontaa koskeva laki (FISA)

FISA-laissa säädetään joistakin henkilöiden oikeussuojakeinoista lainvastaisen tarkkailun varalta. FISA-lain mukaan muu loukattu henkilö kuin vieras valta tai vieraan vallan agentti, johon on kohdistettu sähköistä tarkkailua tai josta sähköisen tarkkailun avulla hankittuja tietoja on luovutettu tai käytetty lain kyseisen osaston 1809 §:n vastaisesti, saa nostaa kanteen sitä henkilöä vastaan, joka rikkomukseen on syyllistynyt. Vieras valta tai vieraan vallan agentti suljetaan kuitenkin nimenomaisesti edellä mainitun säännöksen soveltamisalan ulkopuolelle. Kuten jo edellä todettiin, kantajan on kuitenkin pystyttävä osoittamaan asiavaltuus, mikä ei ole käytännössä mahdollista.

FISC-tuomioistuimeen luotiin USA Freedom -lailla *amicus curiae* -neuvonantajapaneeli, joka voi (valinnaisesti) antaa neuvoja merkittävissä uutta oikeudellista tulkintaa edellyttävissä asioissa. Neuvonantajien tehtävänä on kuitenkin antaa puolueetonta neuvontaa, ei puolustaa tietyn henkilön etuja tämän pyynnöstä.

57 Euroopan ihmisoikeustuomioistuimen tuomio 4.12.2015, Roman Zakharov v. Venäjä, 171 kohta.
[58] Yhdysvallat v Verdugo-Urquidez, s. 264–266.
[59] EU:n yhteispuheenjohtajien kertomus, 2 jakso.

3.5.2 Hallinnolliset oikeussuojakeinot

3.5.2.1 Valvontaviranomaiset

Toinen mahdollisuus saada oikeussuojaa on tehdä valitus valvontaviranomaiselle. Valvontaviranomaisilla ei kuitenkaan ole velvollisuutta tutkia jokaista yksittäistä valitusta; oikeutta tulla kuulluksi ei ole, vaan asia on lähinnä valvontaviranomaisen harkintavallassa. Valvontaviranomainen voi myös antaa raportteja todetuista rikkomuksista, joita koskevien tietojen salassapitoluokitus on poistettu. Jos henkilö voisi olettaa, että raportti vaikuttaa häneen, hän voisi sen perusteella saattaa lainvastaisuuden tuomioistuimen käsiteltäväksi.

3.5.2.2 Tiedonvapauslaki

Kaikkien käytettävissä oleva oikeussuojakeino on tiedonvapauslakiin (*Freedom of Information Act*, FOIA) perustuva tiedonsaantipyyntö. Yhdysvaltojen hallinnon mukaan yleensä kuka tahansa henkilö, olipa tämä Yhdysvaltojen kansalainen tai ei, voi tehdä FOIA-pyynnön yksinkertaisesti pyytämällä minkä tahansa viraston asiakirjaa. Tähän kuuluvat myös henkilöä koskevat tallenteet, vaikkakin sellaisessa tapauksessa on esitettävä henkilötodistus. Jos tiedot on kuitenkin luokiteltu salaisiksi kansallisen turvallisuuden suojelemiseksi, FOIA-pyyntö ei todennäköisesti menesty, koska poikkeusta sovelletaan: virastoilla ei ole velvoitetta antaa tutustua salaisiksi luokiteltuihin tietoihin silloinkaan, kun kyseiset tiedot koskevat pyynnön tehnyttä henkilöä. Käynnissä olevia poliisitutkintoja koskevat tiedot on kokonaan suljettu FOIA-menettelyn ulkopuolelle. Lisäksi tietosuojatyöryhmän käsityksen mukaan FOIA-pyyntö ei anna oikeutta siihen, että riippumaton viranomainen tutkisi henkilötietojen käsittelyn lainmukaisuuden.

3.5.3 Privacy Shield -järjestelyn oikeusasiamies

3.5.3.1 Oikeusasiamiesmekanismin perustaminen

Privacy Shield -järjestelyyn kuuluu uusi mekanismi, jonka avulla EU:n luonnolliset henkilöt voivat esittää Yhdysvaltojen signaalitiedustelua koskevia pyyntöjä vasta perustetulle Privacy Shield -järjestelyn oikeusasiamiehelle. Yhdysvaltojen ulkoministerin John Kerryn 22. helmikuuta 2016 päivättyyn kirjeeseen liitetyn muistion mukaan oikeusasiamiehen virkaan nimitetään alivaltiosihteeri Catherine Novelli. Hän hoitaa virkaa toisen toimensa ohella, sillä hän toimii myös tietotekniikkaan liittyvän kansainvälisen diplomatian johtavana koordinaattorina (*Senior Coordinator for International Information Technology Diplomacy*), tehtävässä, joka on perustettu PPD-28:n 4.d §:ssä. Kirjeessä ja muistiossa korostetaan, että alivaltiosihteeri ”raportoi suoraan ulkoministerille” ja ”on riippumaton tiedusteluyhteisöstä”.

Huolimatta nimestä ”Privacy Shield -järjestelyn oikeusasiamies” muistiosta käy ilmi, että oikeusasiamiehen käsiteltäväksi tulevat pyynnöt liittyvät paitsi kansallisen turvallisuuden vuoksi EU:sta Yhdysvaltoihin siirrettyihin tietoihin myös tietoihin, jotka on siirretty vakiosopimuslausekkeiden, yrityksiä koskevien sitovien sääntöjen, (direktiivin 95/46/EY 26 artiklan mukaisten) poikkeusten nojalla taikka muistion alaviitteessä 2 määriteltyjen mahdollisten tulevien poikkeusten nojalla.

Mekanismin on määrä tiivistetysti toimia seuraavalla tavalla: EU:n luonnollinen henkilö tekee pyynnön kansallisten turvallisuuspalvelujen valvonnasta vastaavalle jäsenvaltion elimelle tai keskitetylle ”kansalaisten valituksia käsittelevälle EU:n elimelle”, sikäli kuin viimeksi mainittu perustetaan tai nimitetään. Pyynnön oikeusasiamiehelle edelleen lähettävän viranomaisen on ensin tarkastettava, että pyyntö on kirjeen 3.b alakohdassa määritellyllä tavalla täydellinen.[60] Sen jälkeen, kun pyyntö on toimitettu Privacy Shield -järjestelyn oikeusasiamiehelle ja todettu 3.b alakohdan mukaiseksi, oikeusasiamies antaa siihen vastauksen, millä tarkoitetaan, että hän vahvistaa seuraavat seikat: ”i) valitus on tutkittu asianmukaisesti, ja ii) tietojenkäsittelyssä on noudatettu Yhdysvaltojen lainsäädäntöä, toimeenpanoasetuksia, presidentin määräyksiä ja virastojen toimintaperiaatteita, joissa on säädetty ODNIn kirjeessä kuvatuista rajoituksista ja suojatoimista; siinä tapauksessa, että mainittuja säännöksiä ei ole noudatettu, vahvistetaan, että sääntöjenvastaisuudet on korjattu”.[61] Oikeusasiamies ei vastauksessa ”vahvista eikä kiistä, onko henkilö ollut tarkkailun kohteena, eikä ilmoita, mitä nimenomaista korjaavaa toimenpidettä asiassa on sovellettu”.[62] Oikeusasiamiehen tutkintamenetelmistä muistiossa kerrotaan, että Privacy Shield -järjestelyn oikeusasiamies ”tekee tiivistä yhteistyötä muiden Yhdysvaltojen hallituksen virkamiesten, mukaan lukien riippumattomien valvontaelinten kanssa”,[63] ja selitetään tarkemmin, että ”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”.[64] Koordinoinnilla varmistetaan, että Privacy Shield -järjestelyn oikeusasiamies voi lähettää edellä kuvatut vahvistukset sisältävän vastauksen.

3.5.3.2 Uutta oikeusasiamiesmekanismia koskeva arviointi

Työryhmä antaa arvoa Euroopan komission ja Yhdysvaltojen hallinnon työlle, jonka ansiosta otetaan käyttöön uusi mekanismi Yhdysvaltojen tarkkailutoimintaa koskevien oikeussuojakeinojen parantamiseksi. Työryhmä ymmärtää, että kun kyseessä on täysin uusi

60 ”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.”
61 Privacy Shield -järjestelyn liite III, 4.e alakohta.
62 Privacy Shield -järjestelyn liite III, 4.e alakohta.
63 Privacy Shield -järjestelyn liite III, 2.a alakohta.
64 Privacy Shield -järjestelyn liite III, 2.a alakohta.

signaalitiedustelua tai kansallista turvallisuutta kansainvälisissä suhteissa koskeva väline, sen arviointi on erityisen tärkeää.

Tietosuojatyöryhmä arvioi tässä osiossa, missä suhteessa Privacy Shield -järjestelyn oikeusasiamiehen perustaminen on perusoikeuskirjassa, Euroopan ihmisoikeussopimuksessa ja Euroopan tuomioistuinten oikeuskäytännössä edellytettyyn vaatimukseen luonnollisten henkilöiden käytettävissä olevista oikeussuojakeinoista.

3.5.3.3 Onko oikeusasiamiehen perustaminen sinällään riittävä toimenpide?

Perusoikeuskirjan 47 artiklassa edellytetään tehokasta oikeussuojakeinoa puolueettomassa tuomioistuimessa[65], joten ensimmäiseksi on kysyttävä, voidaanko ”oikeusasiamiehen” perustamista ylipäätään pitää perusoikeuskirjan 47 artiklan mukaisena ainakaan, ellei mitään muuta tehokasta oikeussuojakeinoa ole käytettävissä. Tämä on tärkeää, koska unionin tuomioistuin viittaa Schrems-tuomion perustelujen tärkeässä 95 kohdassa perusoikeuskirjan 47 artiklaan ilman mitään viittausta siihen, että 47 artiklan tulkinta muuttuisi tarkkailutoimenpiteiden yhteydessä. Päinvastoin unionin tuomioistuin on jo Kadi II -asiassa[66] soveltanut perusoikeuskirjan 47 artiklaa kansallista ja kansainvälistä turvallisuutta koskeviin tarkkailutoimenpiteisiin[67].

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä on kuitenkin tehty erittäin selväksi, että tarkkailujärjestelmä voidaan todeta Euroopan ihmisoikeussopimuksen 8 (ja 13) artiklan mukaiseksi edellyttämättä oikeussuojakeinoa yleisessä tuomioistuimessa.[68] Ihmisoikeustuomioistuin on pikemminkin katsonut 8 artiklan osalta, että tarkkailutoimintaa koskevana tarpeellisena suojatoimena oikeussuojakeino muun viranomaisen edessä voi olla paikallaan. Euroopan ihmisoikeustuomio asettaa kuitenkin muulle kuin lainkäyttöviranomaiselle kovat vaatimukset, jotta niiden voidaan katsoa tarjoavan tehokkaan oikeussuojakeinon. Ihmisoikeustuomioistuimen mukaan tällaisen viranomaisen on oltava riippumaton tarkkailua suorittavasta viranomaisesta ja omattava riittävät valtuudet ja toimivalta harjoittaa tehokasta ja jatkuvaa valvontaa.[69]

Euroopan ihmisoikeustuomioistuin on Kennedy- ja Klass-asioissa täsmentänyt, mitä näillä vaatimuksilla voidaan salaisen tarkkailun yhteydessä tarkoittaa, jos rekisteröidylle ei ilmoiteta häntä koskevien tietojen käsittelystä. Ihmisoikeustuomioistuin katsoi kummassakin tuomiossa

65 Perusoikeuskirjan selityksissä todetaan lisäksi, että 47 artiklaa on tulkittava siten, että siinä turvataan oikeus tehokkaisiin oikeussuojakeinoihin tuomarin edessä (Euroopan unionin perusoikeuskirjan selitykset, Selitys 47 artiklaan (EUVL C 303, 14.12.2007, s. 17).

66 Unionin tuomioistuimen tuomio 18.7.2013, Euroopan komissio ja Yhdistynyt kuningaskunta v. Yassin Abdullah Kadi, yhdistetyt asiat C-584/10 P, C-593/10 P ja C-595/10 P, ECLI:EU:C:2013:518, jäljempänä ’Kadi II -tuomio’.

67 Kadi II -tuomion 97 ja 100 kohta: ”unionin tuomioistuinten on niille perussopimuksessa myönnetyn toimivallan mukaisesti valvottava, pääsääntöisesti täysimääräisesti, kaikkien unionin toimien laillisuutta perusoikeuksien kannalta, jotka ovat erottamaton osa unionin oikeusjärjestystä, myös silloin, kun tällaisilla toimilla on tarkoitus panna täytäntöön päätöslauselmia, jotka turvallisuusneuvosto on antanut Yhdistyneiden Kansakuntien peruskirjan VII luvun nojalla” (VII luku koskee toimenpiteitä ”rauhaa uhattaessa tai rikottaessa taikka hyökkäystekojen sattuessa”.)

68 Euroopan ihmisoikeussopimuksen 13 artiklassa velvoitetaan jäsenvaltiot varmistamaan, että ”Jokaisella, jonka – – oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä”. Sen ei välttämättä tarvitse olla lainkäyttöviranomainen, kuten Euroopan ihmisoikeustuomioistuin on selventänyt 6.9.1978 antamansa tuomion Klass ja muut v. Saksa (jäljempänä ’Klass-tuomio’) 56 ja 67 kohdassa.

69 Klass-tuomion 56 ja 67 kohta.

asianomaisten viranomaisten olevan riippumattomia, erityisesti riippumattomia tarkkailua suorittavista elimistä mutta myös riippumattomia minkään muun viranomaisen ohjeista.[70] Kennedy-asiassa ihmisoikeustuomioistuin hyväksyi riippumattoman ja puolueettoman viranomaisen, joka oli vahvistanut oman työjärjestyksensä ja jonka jäsenillä oli runsaasti kokemusta tuomarin työstä tai asianajoammatista.[71]

Molemmissa tuomioissa asianomaisilla viranomaisilla oli lisäksi oikeus tutustua kaikkiin merkityksellisiin tietoihin, myös niihin, jotka olivat salaisia. Kummallakin oli myös valtuudet korjata sääntöjenvastaisuudet.[72]

Sen lisäksi, että tutkitaan, voidaanko oikeusasiamiehen katsoa olevan 'tuomioistuin', perusoikeuskirjan 47 artiklan 2 kohdan soveltaminen sisältää lisähaasteen, koska sen mukaan tuomioistuimen on oltava "lailla perustettu". On epävarmaa, voidaanko muistiota, jossa selostetaan uuden mekanismin toimintaa, pitää 'lakina'.

Sen takia työryhmä päätti kehitellä perusoikeuskirjan 7, 8 ja 47 artiklan perusoikeuksia sekä Euroopan ihmisoikeussopimuksen 8 (ja 13) artiklan ihmisoikeuksia vastaavia oikeussuojakeinoja ja oikeussuojan saatavuutta koskevia erityisvaatimuksia oikeuskäytännön pohjalta ja pitämällä mielessään periaatteen, jonka mukaisesti tietoturvan tason on pääosiltaan vastattava unionissa taattua tasoa, sen sijaan, että arvioitaisiin, voidaanko oikeusasiamiestä muodollisesti pitää laissa perustettuna tuomioistuimena. Tietosuojatyöryhmä keskittyy siten uuden mekanismin soveltamisalaan liittyvässä jatkoanalyysissaan seuraaviin kriteereihin: vaatimus toimittaa pyyntö oikeusasiamiehelle ja saada vastaus ('asiavaltuus'), oikeusasiamiehen riippumattomuus, sen tutkintavaltuudet tutustua tarvittaviin aineistoihin, myös salassa pidettäviin asiakirjoihin, ja pyytää apua muilta virastoilta ja viimeiseksi sen valtuudet korjata sääntöjenvastaisuudet.

3.5.3.4 Oikeusasiamiesmekanismin soveltamisala

Tietosuojatyöryhmä katsoo, että Privacy Shield -järjestelyn mukaisten suojatoimien, kuten oikeuden saattaa asia oikeusasiamiehen käsiteltäväksi, olisi koskettava kaikkia unionin lainsäädännön alaisuuteen kuuluvia henkilöitä. Kansallisuuteen perustuvan eron tekemistä ei voitaisi hyväksyä, etenkään kun otetaan huomioon, että unionin perusoikeudet koskevat jokaista, eivät ainoastaan unionin passin haltijoita. Liitteessä III viitataan EU:n luonnollisiin henkilöihin (*EU individuals*) määrittelemättä sen tarkemmin, keitä sillä tarkoitetaan. Työryhmä pahoittelee tätä epävarmuutta ja ehdottaa tekstin selkeyttämistä siten, että kaikilla unionin lainsäädännön alaisuuteen kuuluvilla henkilöillä on oikeus saattaa pyyntönsä oikeusasiamiehen käsiteltäväksi muistion mukaisin edellytyksin. Lisäksi komission ja Yhdysvaltojen olisi käsiteltävä sitä, missä määrin Privacy Shield -järjestelyä sovelletaan myös ETA-alueen ja Sveitsin kansalaisiin/asukkaisiin, jotka aiemmin kuuluivat safe harbor -järjestelmän piiriin.

70 Klass-tuomio, 21 ja 53 kohta.
71 Saksan G 10 -komissioon kuului (tuomion antamisajankohtana) kolme jäsentä, joista puheenjohtajalla oli oltava tuomarin pätevyys (Klass-tuomion 21 ja 53 kohta).
72 Euroopan ihmisoikeustuomioistuimen tuomio 18.5.2010, Kennedy v. Yhdistynyt kuningaskunta, 167 kohta (jäljempänä 'Kennedy-tuomio'), ja Klass-tuomion 21 ja 53 kohta.

Tietosuojatyöryhmä toteaa myös oikeusasiamiesmekanismin soveltamisalan olevan jossain määrin epävarma. Muistiossa säädetään toisaalta, että oikeusasiamiehen tehtävänä on käsitellä pyyntöjä, jotka liittyvät kansallisen turvallisuuden vuoksi EU:sta Yhdysvaltoihin kaikkien unionin lainsäädännössä sallittujen siirtovälineiden avulla siirrettyjä tietoja, mutta toisaalta muistiossa tehdään selväksi, että siinä vahvistetaan ”signaalitiedustelua koskeva” mekanismi. Viimeksi mainitusta ilmauksesta voitaisiin päätellä, että mekanismi koskee vain signaalitiedustelun avulla kerättyjä tietoja, ja siitä taas herää kysymys, pidetäänkö esimerkiksi FISA-lain mukaisesti kerättyjä tietoja signaalitiedusteluna. Niin näyttää olevan 702 §:n osalta, kuten ODNIn vakuutuksessa selitetään sivulla 10.[73] Tietosuojatyöryhmä pahoittelee kuitenkin sitä, että signaalitiedustelu-termin käyttö luo tässä yhteydessä tarpeetonta epävarmuutta.

Toisena seurauksena tietosuojatyöryhmän käsityksen mukaan on, että oikeusasiamiesmekanismi ei koske lainvalvontaviranomaisten tietojen saantia koskevia pyyntöjä.[74] Näin ollen olisi edelleen epäselvää, kuuluisivatko joidenkin virastojen, erityisesti CIA:n, pyynnöt mekanismin alaisuuteen.

3.5.3.5 Asiavaltuus ja pyyntömenettely

On hyvin vaikea nostaa Yhdysvaltojen hallinnon tarkkailutoimenpiteitä vastaan kanne Yhdysvaltojen yleisissä tuomioistuimissa. Tietosuojatyöryhmä on tietoinen Yhdysvaltojen korkeimman oikeuden ratkaisusta, jonka mukaan tiedustelua koskevissa asioissa ei ole asiavaltuutta, kun kantaja ei ole pystynyt osoittamaan henkilökohtaista, konkreettista, yksilöityä ja todellista tai välittömästi uhkaavaa haittaa tai vahinkoa.[75] Tässä suhteessa oikeusasiamiehen perustaminen on tärkeä askel, koska se on uusi väline saada jonkinlaista oikeussuojaa, jota muutoin ei olisi olemassa. Siitä syystä työryhmä on tyytyväinen 3.c alakohdassa esitettyyn selvennykseen. Tämän kohdan mukaan uuden mekanismin mukaisen pyynnön esittämiseksi ei ole tarpeen osoittaa, että pyytäjän tietoja on tosiasiassa käytetty signaalitiedustelutoiminnassa.

Työryhmä hyväksyy suurelta osin oikeusasiamiesmekanismissa käytettävän valittajan tunnistamismenettelyn. On täysin järkevää, että tunnistaminen tapahtuu EU:n alueella. Samoin menetellään EU:n ja Yhdysvaltojen TFTP2-sopimuksen mukaisessa tiedonsaantimekanismissa. Tietosuojatyöryhmä ei kuitenkaan ymmärrä, miksi EU:ssa tehtävä tarkastus olisi annettava ”jäsenvaltioiden valvontaviranomaisille, joilla on toimivalta valvoa kansallisia turvallisuuspalveluja”. Kun otetaan huomioon Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohta, vaikuttaa ensinnäkin epätodennäköiseltä, että Euroopan komissio voisi osoittaa tehtäviä näille viranomaisille, jotka selvästi kuuluvat jäsenvaltioiden toimivallan piiriin.

Kun lisäksi otetaan huomioon, että kansallisten turvallisuuspalvelujen valvontamekanismit ovat eri jäsenvaltioissa hyvin erilaisia, vastaavien viranomaisten osallistuminen saattaisi vakavasti haitata järjestelmän tehokkuutta jäsenvaltioiden kansalaisten kannalta. Näin on

73 Privacy Shield -järjestelyn liite VI, s. 10.
74 Muistio oikeusasiamiehen perustamisesta, s. 1.
75 Clapper v. Amnesty International USA, 568 U.S. ___ (2013) II. s. 10.

esimerkiksi tapauksissa, joissa kansallisten turvallisuuspalvelujen valvonnasta vastaavia viranomaisia on useita, jolloin henkilön voi olla vaikea tietää, minkä viranomaisen puoleen olisi käännyttävä, tai jos sovellettavissa kansallisissa oikeussäännöissä ei säädetä henkilön mahdollisuudesta ottaa yhteyttä asiaankuuluvaan valvontaviranomaiseen taikka jos kyseisiä viranomaisia ei ole perustettu siten, että niiden olisi mahdollista suorittaa tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa heille osoitettuja tehtäviä.[76] Kun otetaan huomioon tietosuojaviranomaisten osallistuminen Privacy Shield -järjestelyn soveltamiseen ja valvontaan, olisi paljon järkevämpää osoittaa tämä tehtävä jäsenvaltioiden tietosuojaviranomaisille. Työryhmä tähdentää olevan sen mielestä epätodennäköistä, että Privacy Shield -järjestelyn oikeusasiamiehen menettelyn osana käsiteltäisiin salaisiksi luokiteltuja tietoja, koska mahdollinen vastaus kuuluu pelkästään joko, että säännöksiä on noudatettu tai että niitä ei ole noudatettu mutta ne on korjattu.

3.5.3.6 Riippumattomuus

Ulkoasiainministerin antamassa vakuutuksessa tehdään selväksi, että oikeusaseman tehtävää hoitaa ulkoasiainministeriön alivaltiosihteeri. Hänet nimittää presidentti, ja nimitys edellyttää senaatin hyväksyntää. Oikeusasiamiehen asema ei edellytä lisähyväksyntää, vaan oikeusasiamiehen asemaan osoittaminen riittää. Alivaltiosihteerin nimittää Yhdysvaltojen presidentti, ulkoasiainministeri ohjeistaa hänet oikeusasiamiehen tehtävään, ja senaatti vahvistaa hänen asemansa alivaltiosihteerinä. Oikeusasiamies ”on riippumaton tiedusteluyhteisöstä”, kuten kirjeessä ja muistiossa painotetaan. Tietosuojatyöryhmällä on kuitenkin epäilyksiä sen suhteen, onko ulkoasiainministeriö paras mahdollinen valinta oikeusasiamiehen perustamiseen. Tiedusteluyhteisön toiminnasta tarvitaan nähtävästi jonkin verran tietoa ja ymmärrystä, jotta oikeusasiamiehen tehtävät voidaan hoitaa tehokkaasti, kun samalla tosiaan edellytetään riittävää etäisyyttä tiedusteluyhteisöstä, jotta oikeusasiamies voi toimia riippumattomasti.

Privacy Shield -järjestelyssä ei aseteta mitään oikeusasiamiehen erottamista koskevia kriteerejä. Näin ollen oikeusasiamies voidaan tietosuojatyöryhmän käsityksen mukaan erottaa tehtävästään oikeusasiamiehenä samalla tavoin kuin hänet voidaan erottaa tehtävästään ulkoasiainministeriön alivaltiosihteerinä, mikä saattaa mahdollisesti heikentää oikeusasiamiehen riippumatonta asemaa.

Päällisin puolin katsottuna ulkoasiainministeriön alivaltiosihteerin nimittäminen oikeusasiamieheksi poikkeaa riippumattomuuden kannalta selvästi siitä, että yleiselle tuomioistuimelle annetaan toimivalta käsitellä henkilön sen käsiteltäväksi saattamaa asiaa. Onkin ratkaistava, voidaanko oikeusasiamiestä pitää riippumattomuuden kannalta vastaavana kuin muita riippumattomia valvontaelimiä, joiden on todettu täyttävän vaatimukset. Tarkkailutoiminnan yhteydessä sopivia vertailukohteita ovat varsinkin *Investigatory Powers Tribunal* (IPT) Yhdistyneessä kuningaskunnassa ja *G10-Kommission* Saksassa.

Asian ratkaisemiseksi on arvioitava lisäksi ”riippumattomalle” elimelle annettuja valtuuksia.

76 Esimerkiksi joissakin EU:n jäsenvaltioissa luonnolliset henkilöt voivat saada kansallisten turvallisuuspalvelujen hallussa olevia tietoja ainoastaan esittämällä pyynnön korkeimman oikeuden tuomarille.

3.5.3.7 Tutkintavaltuudet

Kadi II -asiaa koskevassa unionin tuomioistuimen ratkaisussa todetaan perusoikeuskirjan 47 artiklasta seuraavasti: ”asianomaisen on voitava saada tieto häntä koskevan päätöksen perusteluista joko suoraan päätöksestä itsestään tai ilmoituksella asianomaisen pyynnöstä, millä ei puututa toimivaltaisen tuomioistuimen oikeuteen vaatia kyseessä olevaa viranomaista ilmoittamaan ne, jotta hän voi puolustaa oikeuksiaan parhain mahdollisin edellytyksin”.[77] Euroopan unionin tuomioistuinten on varmistettava, että päätös perustuu riittävän vankkaan tosiseikastoon.[78] Unionin tuomioistuin toteaa selkeästi, että ainakaan Euroopan unionin tuomioistuinten edessä ”ei voida vedota tietojen tai todisteiden salaisuuteen tai luottamuksellisuuteen”.[79] Edellä sanotun perusteella tietosuojatyöryhmä toteaa, että oikeusasiamiehelle on annettava toimenpiteen toteutuksen taustalla olevia syitä tukevat tiedot ja todisteet, jotta se täyttäisi unionin tuomioistuimen asettamat vaatimukset.[80]

On kuitenkin vielä epäselvää, kuinka laajat tutkintavaltuudet oikeusasiamies saa. Sen enempää komission päätösehdotuksessa kuin ulkoasiainministeriön toimittamassa liitteessä III ei kovin laajasti selvitetä tätä kysymystä. Tietosuojatyöryhmän ymmärryksen mukaan oikeusasiamiehen olisi saatava riittävästi tietoja, jotta hän pystyy toteamaan, onko henkilötietojen käsittely turvallisuuspalvelussa ollut lainmukaista, ja jos näin ei ole, hänen olisi voitava varmistaa, että sääntöjenvastaisuudet korjataan. Sen enempää ulkoasiainministeriön kirjeessä kuin komission päätösehdotuksessa ei kuitenkaan täsmennetä, saako oikeusasiamies kyseistä henkilöä koskevat tiedot suoraan käyttöönsä ja voiko hän siten suorittaa oman tutkintansa vai onko hänen vain luotettava Yhdysvaltojen virkamiesten antamiin selvityksiin.

3.5.3.8 Korjaavat toimivaltuudet

Muistiosta ei käy edelleenkään selväksi, millä tavoin oikeusasiamies voi määrätä sääntöjenvastaisuudet korjattaviksi. Sen lisäksi, että tutkintavaltuudet ovat epäselviä, on lisäksi edelleen epäselvää, missä määrin oikeusasiamies voi sinänsä tehokkaasti määrätä sääntöjenvastaisuudet korjattaviksi ja millainen tämän toimenpiteen lopputulos olisi. Voiko tämä tarkoittaa, että sääntöjenvastaisesti (eli laittomasti) saatuja henkilötietoja ei enää voisi käyttää missään menettelyssä vaan ne olisi hävitettävä?

Lisäksi Privacy Shield -järjestelyssä ei tietosuojatyöryhmän käsityksen mukaan säädetä oikeusasiamiehen päätöstä koskevasta muutoksenhaku- tai uudelleentarkastelumahdollisuudesta.

Kaiken päätteeksi oikeusasiamiehen valittajalle hänen valituksensa käsittelyn jälkeen antamassa vastauksessa ei saa paljastaa, onko tiedusteluyhteisö menetellyt jotenkin laittomasti. Vastaus on aina sama ja luonteeltaan yleinen. Unionin tuomioistuimen Kadi

77 Kadi II -tuomion 100 kohta.
78 Kadi II -tuomion 119 kohta.
79 Kadi II -tuomion 125 kohta.
80 Kadi II -tuomion 122 kohta. Viranomaisen ei kuitenkaan tarvitse esittää kaikkia tietoja ja todisteita, joilla toimenpidettä perustellaan.

II -tuomion mukaan Euroopan unionin toiminnasta tehdyn sopimuksen 296 artiklassa määrätty perusteluvelvollisuus ei ulotu niin pitkälle, että siinä velvoitettaisiin vastaamaan yksityiskohtaisesti henkilön esittämiin huomautuksiin, mutta toimivaltaisella viranomaisella on (valvontaelimenä) velvollisuus kaikissa olosuhteissa eritellä yksilökohtaiset, erityiset ja konkreettiset syyt.[81]

3.5.4 Päätelmät

Tietosuojatyöryhmällä on edelleen epäilyksiä sen suhteen, onko luonnollisten henkilöiden käytettävissä tehokkaat oikeussuojakeinot. Tietosuojan tason riittävyyttä koskevassa päätösehdotuksessa ei ennen kaikkea selkeästi vastata siihen kysymykseen, missä tilanteessa ja millaisin ennakkoedellytyksin henkilöt voivat nostaa kanteen oikeuksiensa määrittämiseksi.

Tietosuojatyöryhmä antaa kuitenkin arvoa sille, että on perustettu vaihtoehtoinen oikeussuojakeino, oikeusasiamiesmekanismi, mikä merkitsee ainutlaatuista kehitystä EU:n ja kolmannen maan välisissä suhteissa. Huomioon ottamatta sitä, että käsite *EU individuals* (EU:n luonnollinen henkilö / EU:n kansalainen) olisi selkeytettävä, kuten edellä on todettu, mekanismilla luodaan uusi mahdollisuus saada oikeussuojaa Yhdysvaltojen hallinnossa sen varmistamiseksi, että valittajan henkilötietoja käsitellään Yhdysvaltojen lainsäädännön mukaisesti.

Samalla tietosuojatyöryhmä on kuitenkin todennut merkittäviä puutteita arvioidessaan oikeusasiamiesmekanismia suhteessa vaatimuksiin, joita perusoikeuskirjan 47 artiklassa riippumattomalle tuomioistuimelle asetetaan, ja vaatimuksiin, jotka unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin ovat tarkkailutapauksia koskevassa oikeuskäytännössään vahvistaneet. Ensinnäkin on epävarmaa, voidaanko oikeusasiamiestä pitää (muodollisesti ja täysin) riippumattomana, varsinkin kun ottaa huomioon, että poliittiseen virkanimitykseen perustuvasta virasta on suhteellisen helppoa erottaa. Toiseksi on edelleen epäselvää, riittävätkö oikeusasiamiehen valtuudet tehokkaan ja jatkuvan valvonnan harjoittamiseen. Tietosuojatyöryhmä ei voi liitteestä III saatavien tietojen perusteella päätellä, onko oikeusasiamiehellä aina mahdollisuus päästä suoraan tutustumaan kaikkiin tarvitsemiinsa tietoihin, tiedostoihin ja tietojärjestelmiin, jotta hän voisi tehdä oman arvionsa, eikä liioin sitä, voiko hän todella pakottaa vastuulliset tiedusteluvirastot lopettamaan sääntöjenvastaisen henkilötietojen käsittelyn, varsinkaan, jos vallitsee erimielisyys siitä, onko tietojen käsittely lainmukaista vai ei. Mahdollisesti tietosuojatyöryhmän epäilykset voidaan poistaa antamalla lisäselvityksiä oikeusasiamiehen asemasta ja valtuuksista.

3.6 Yhdysvaltojen kansallisiin turvallisuusviranomaisiin sovellettavia suojatoimia ja rajoituksia koskevat loppuhuomautukset

Ensinnäkin tietosuojatyöryhmä haluaa kiittää komissiota ja Yhdysvaltojen viranomaisia pyrkimyksistä kertoa aiempaa avoimemmin niistä vaikutuksista, joita Yhdysvaltojen tarkkailuohjelmilla saattaa olla Privacy Shield -järjestelyn – tai yleensä minkä tahansa välineen – mukaisesti siirrettyihin henkilötietoihin. Kesäkuussa 2013 tehtyjen ensimmäisten

81 Kadi II -tuomion 116 kohta.

Snowden-paljastusten jälkeen on edistytty merkittävästi. Tietosuojatyöryhmä toteaa kuitenkin, että huolenaiheita on edelleen. Privacy Shield -järjestelyn mukaisista oikeuksista ja velvollisuuksista tarvitaan vähintäänkin lisäselityksiä ja -tarkennuksia.

Tietosuojatyöryhmän kaksi tärkeintä huolenaihetta ovat se seikka, etteivät Yhdysvaltojen viranomaiset sulje pois laajamittaista ja kohdentamatonta tietojenkeruuta, ja se, ettei oikeusasiamiehen valtuuksia ja asemaa ole määritetty riittävän yksityiskohtaisesti. Lisäksi kansallisilla tietosuojaviranomaisilla olisi oltava toimivalta panna vireille menettely oikeusasiamiehen edessä luonnollisen henkilön puolesta tiedusteluviranomaisten valvontaelinten sijaan. Vaikka tietosuojatyöryhmä antaa tietenkin arvoa ponnisteluille vastata tietosuojaviranomaisten esiin ottamiin huolenaiheisiin, lisäsuojatoimet olisivat tervetulleita sen varmistamiseksi, että Yhdysvaltojen tarkkailuohjelmien mahdollinen puuttuminen perusoikeuksiin on tarpeen demokraattisessa yhteiskunnassa.

4. PRIVACY SHIELD -JÄRJESTELYN LAINVALVONTAA KOSKEVIEN TAKEIDEN ARVIOINTI

4.1 Johdanto

Tietosuojatyöryhmä huomauttaa oikeudesta päästä tarkastelemaan henkilötietoja lainvalvonnan nimissä, että Privacy Shield -järjestelyn liitteessä II esitettyihin yksityisyyden suojaa koskeviin periaatteisiin sisältyy poikkeus, joka on täysin samanlainen kuin yksityisyyden suojaa koskevissa safe harbor -periaatteissa. Poikkeuksen yleinen luonne on siten säilytetty, mikä tarkoittaa, että uudet Privacy Shield -periaatteet mahdollistavat ”Yhdysvaltojen kansallisen turvallisuuden ja yleisen edun tai sisäisen lainsäädännön vaatimuksiin perustuvan puuttumisen niiden henkilöiden perusoikeuksiin, joiden henkilötiedot siirretään – – unionista Yhdysvaltoihin”[82].

Unionin tuomioistuimen Schrems-tuomiossa safe harbor -päätöksestä esittämä pääasiallinen kritiikki koski kuitenkin sitä, ettei se ”sisällä mitään toteamusta siitä, että Yhdysvalloissa olisi valtiollisia sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista puuttumista henkilöiden, joiden tietoja siirretään unionista Yhdysvaltoihin, perusoikeuksiin”.

Tietosuojatyöryhmä suhtautuu siten myönteisesti Yhdysvaltojen hallinnon pyrkimyksiin tarjota enemmän tietoa oikeudellisesta kehyksestä, joka koskee lainvalvonnan nimissä tapahtuvaa puuttumista Privacy Shield -järjestelyn puitteissa siirrettyjen henkilötietojen suojaan, sovellettavat rajoitukset ja suojatoimet mukaan luettuina. Samalla työryhmä korostaa, että kaikenlaisen puuttumisen yksityiselämän ja tietosuojan perusoikeuksiin on demokraattisessa yhteiskunnassa perustuttava oikeutettuihin perusteihin. Työryhmä on siitä syystä analysoinut Privacy Shield -järjestelyn lainvalvontaa koskevia takeita tämän lausunnon osiossa 1.2 esitettyjen seikkojen pohjalta.

82 Schrems-tuomion 87 kohta.

4.2 Olennaisten eurooppalaisten takeiden soveltaminen tapauksissa, joissa lainvalvontaviranomaiset saavat henkilötietoja yrityksiltä

4.2.1 Lainvalvontaviranomaisten oikeutta saada henkilötietoja käytettävä lainmukaisesti ja tiedonsaannin perustuttava selkeisiin, täsmällisiin ja helppotajuisiin sääntöihin

Privacy Shield -järjestelyn liitteessä VII on Yhdysvaltain oikeusministeriön kirje, jossa ”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.”

Kaikki liitteessä VII mainitut menettelyt juontavat juurensa joko suoraan Yhdysvaltojen perustuslaista (neljäs lisäys), lainsäädännöstä ja prosessioikeudellisista säännöksistä tai oikeusministeriön suuntaviivoista ja toimintaperiaatteista. Liitteessä VII ei kuitenkaan viitata nimenomaisesti kaikkiin niihin säädöksiin, joissa säädetään näistä menettelyistä, vaan keskitytään sen sijaan kuvailemaan lyhyesti itse menettelyjä. Lisäksi liitteessä VII mainitaan, että ”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 tietyntyyppistä”, ja mainitaan useita esimerkkitapauksia, kuten pankkisalaisuudesta annettu *Bank Secrecy Act* -laki, luottokelpoisuusraportointia koskeva *Fair Credit Reporting Act* -laki sekä kansalaisten pankkitietoja koskeva *Right to Financial Privacy Act* -laki.

Tietosuojatyöryhmä huomauttaa, että säädöksiä, menettelyjä ja politiikkoja koskeva kehys on sirpaloitunut ja että tiettyyn tiedonsaantipyyntöön sovellettava oikeusperusta riippuu pyydettyjen tietojen luonteesta, yrityksen luonteesta, oikeudellisten menettelyjen (rikosoikeudellinen, hallinnollinen tai muu yleiseen etuun liittyvä) luonteesta ja tietoja pyytävän yhteisön luonteesta.

Koska kaikki sovellettavat säännöt, joilla rajoitetaan lainvalvontaviranomaisten oikeutta tutustua Privacy Shield -järjestelyn puitteissa siirrettäviin tietoihin, perustuvat perustuslakiin, lainsäädäntöön ja oikeusministeriön läpinäkyviin politiikkoihin, tietosuojatyöryhmä on ottanut huomioon olettaman näiden sääntöjen saatavuudesta. Sääntöjen selkeyttä ja täsmällisyyttä voidaan kuitenkin arvioida ainoastaan kunkin menettelytyypin ja tiedonsaantipyynnön kannalta. Tietosuojatyöryhmä pahoittelee siitä syystä, ettei sellaista arviointia voida tehdä tällä hetkellä saatavilla olevien Privacy Shield -järjestelyn liitteessä VII kuvattujen detaljien ja päätösehdotuksessa esitettyjen toteamusten perusteella.

4.2.2 Osoitettava henkilötietojen käsittelyn tarpeellisuus ja oikeasuhteisuus oikeutettujen tavoitteiden kannalta

Tietosuojatyöryhmä toteaa asianmukaisesti, että lainvalvontatarkoituksiin tehtävillä tiedonsaantipyynnöillä voidaan katsoa olevan oikeutettu tavoite. Esimerkiksi Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdan mukaan viranomaiset saavat puuttua

yksityiselämän suojaa koskevan oikeuden käyttämiseen ”yleisen turvallisuuden – – vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi”. Sellainen puuttuminen voidaan kuitenkin hyväksyä vain, jos se on tarpeen ja oikeasuhteista[83].

Suhteellisuusperiaate edellyttää Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan, että ”*kyseessä olevan säännöstön* legitiimit tavoitteet ovat toteutettavissa” yksityisyyttä ja henkilötietojen suojaa koskevien oikeuksien käyttöön puuttumista koskevilla lainsäädäntötoimilla ”ja että niillä ei ylitetä niitä rajoja, jotka johtuvat siitä, mikä on tarpeellista näiden tavoitteiden toteuttamiseksi ja tähän soveltuvaa”[84] (kursivointi työryhmän). Tarpeellisuuden ja oikeasuhteisuuden arviointi tehdään siten aina suhteessa johonkin tiettyyn lainsäädännössä tarkoitettuun toimenpiteeseen.

Yhdysvaltojen viranomaiset täsmentävät liitteessä VII, että liittovaltion syyttäjät ja liittovaltion tutkijat voivat saada organisaatiot luovuttamaan asiakirjoja ja muita tietoja ”hyödyntämällä useita pakollisia oikeudellisia menettelyjä. Näitä ovat suuren valamiehistön haasteet, hallinnolliset haasteet ja etsintäluvat.” Muita viestintätietoja voidaan hankkia ”sellaisten rikostutkimuksia koskevien liittovaltion oikeudellisten välineiden nojalla, jotka liittyvät lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmiin”[85]. Lisäksi virastot, joilla on siviilihallinto- ja sääntelytehtäviä, voivat toimittaa organisaatioille haasteita, ”joissa ne vaativat luovuttamaan liiketoimintatietoja, sähköisesti tallennettua tietoa tai muita aineellisia esineitä”[86]. Lisäksi liitteessä VII täsmennetään, että näitä oikeudellisia menettelyjä käytetään yleensä tietojen hankkimiseksi yrityksiltä Yhdysvalloissa, riippumatta siitä, onko ne sertifioitu Privacy Shield -järjestelyssä, ”eikä rekisteröidyn kansalaisuudella ole merkitystä”. Toisin sanoen vaikuttaa siltä, että näiden suojatoimien kohteena ovat organisaatiot, eivätkä henkilöt itse.

Liitteen VII lisäksi myös Privacy Shield -periaatteisiin perustuvassa päätösehdotuksessa esitetään komission toteamuksia Yhdysvalloissa käytössä olevista säännöistä, joilla rajoitetaan puuttumista henkilöiden perusoikeuksiin silloin kun heidän henkilötietojaan siirretään unionista Yhdysvaltoihin Privacy Shield -järjestelyn nojalla.

Päätösehdotuksessa esitetyt toteamukset koskevat erityisesti Yhdysvaltojen perustuslain neljännen lisäyksen mukaisesti sovellettavia rajoituksia ja suojatoimia, joissa edellytetään, että lainvalvontaviranomaisten etsintöihin ja takavarikoihin on pääasiallisesti saatava todennäköisiin syihin perustuva tuomioistuimen määräys.[87] Toteamuksissa viitataan myös siihen, että niissä poikkeuksellisissa tapauksissa, joissa tuomioistuimen lupaa ei edellytetä, lainvalvontaan sovelletaan ”kohtuustestiä”[88].

---

83 Ks. olennaisia eurooppalaisia takeita koskeva valmisteluasiakirja (European Essential Guarantees), s. 7–9. Tarpeellisuus- ja oikeasuhteisuuskäsitteiden yleisen arvioinnin osalta ks. 27.2.2014 annettu tietosuojatyöryhmän Lausunto 01/2014 välttämättömyyden ja oikeasuhteisuuden käsitteiden soveltamisesta ja tietosuojasta lainvalvonnan alalla.

84 Unionin tuomioistuimen tuomio 8.4.2014, Digital Rights Ireland, C-293/12 ja C-594/12, ECLI:EU:C:2014:238, 46 kohta oikeuskäytäntöviittauksineen.

85 Liite VII, s. 2.

86 Liite VII, s. 4.

87 Tietosuojan tason riittävyyttä koskeva päätösehdotus, johdanto-osan 107 kappale.

88 Privacy Shield -järjestely, johdanto-osan 107 kappale.

Toteamuksissa ei kuitenkaan täsmennetä, kuinka kyseisiä suojatoimia sovelletaan ei-yhdysvaltalaisiin henkilöihin. Itse asiassa päätösehdotuksen johdanto-osan eräässä kappaleessa todetaan, että neljännen lisäyksen mukainen suoja ei ulotu sellaisiin ei-yhdysvaltalaisiin henkilöihin, jotka eivät asu Yhdysvalloissa.[89] Lisäksi päätösehdotuksen samassa kohdassa todetaan, että ei-yhdysvaltalaiset henkilöt hyötyvät välillisesti henkilötietoja hallussaan pitäville lainvalvontaviranomaisten tietojensaantipyyntöjä saaville yhdysvaltalaisille yrityksille annetusta suojasta. Tietosuojaryhmä kuitenkin pahoittelee, ettei kyseisessä toteamuksessa viitata mihinkään oikeudelliseen lähteeseen – ei lainsäädäntöön eikä oikeuskäytäntöön.

Tietosuojatyöryhmä huomauttaa, että järjestelmä on toimenpideympäristönä kaiken kaikkiaan monimutkainen, kun otetaan huomioon tutkintavälineet, joiden avulla yhdysvaltalaisilta yrityksiltä saadaan liiketoimintaan liittyviä ja muita tietoja rikosvalvonnan tai yleisen edun nimissä – tietoihin pääsyä koskevat rajoitukset ja suojatoimet mukaan luettuina. Käytettävissä olevien tietojen perusteella järjestelmää ei voida tällä hetkellä arvioida yleisesti. Yksittäistapauksia on arvioitava erikseen, jotta voidaan todella arvioida lainvalvontaan liittyvien tutkintatoimien tarpeellisuutta ja oikeasuhteisuutta suhteessa yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin.

4.2.3 Riippumaton valvontamekanismi

Tietosuojatyöryhmä on ottanut asianmukaisesti huomioon sen, että useimpiin liitteessä VII kuvattuihin menettelyihin liittyy edellytys, jonka mukaan tietoja voidaan luovuttaa viranomaisille vasta, kun on olemassa tuomioistuimen määräys (esim. lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien käyttölupaa koskevat tuomioistuimen määräykset, puhelinkuuntelua koskevan liittovaltion lain nojalla suoritettavaa tarkkailua koskevat tuomioistuimen määräykset ja etsintämääräykset – sääntö 41). Vaikuttaa kuitenkin siltä, ettei kaikkiin menettelyihin tarvita tuomioistuimen lupaa. Esimerkiksi siviili- ja sääntelyviranomaiset ”voivat toimittaa – – haasteita”[90]. Näissä tapauksissa haasteen kohtuullisuutta voidaan valvoa jälkikäteen tuomioistuimessa, sillä ”hallinnollisen haasteen vastaanottaja voi nostaa kanteen tuomioistuimessa ja vastustaa haasteen täytäntöönpanoa”[91].

Tietosuojatyöryhmä toteaa käytettävissä olevien tietojen perusteella, että lainvalvontaviranomaisten oikeutta tutustua yhdysvaltalaisten yritysten hallussaan pitämiin tietoihin koskee ilmeisesti melko vahva riippumaton valvontamekanismi.

4.2.4 Tehokkaat oikeussuojakeinot luonnollisten henkilöiden käyttöön

Kuten edellä on todettu, ”neljännen lisäyksen mukainen suoja ei ulotu sellaisiin ei-yhdysvaltalaisiin henkilöihin, jotka eivät asu Yhdysvalloissa”[92]. Se tarkoittaa, että ei-yhdysvaltalainen henkilö ei voi vastustaa määräysten tai haasteiden täytäntöönpanoa tuomioistuimessa vetoamalla neljänteen lisäykseen. Tietosuojan tason riittävyyttä koskevassa

89 Tietosuojan tason riittävyyttä koskeva päätösehdotus, johdanto-osan 108 kappale.
90 Liite VII, s. 4.
91 Liite VII, s. 4.
92 Tietosuojan tason riittävyyttä koskeva päätösehdotus, johdanto-osan 108 kappale.

päätösehdotuksessa täsmennetään, että ei-yhdysvaltalaiset henkilöt hyötyvät välillisesti henkilötietoja hallussaan pitäville lainvalvontaviranomaisten tietojensaantipyyntöjä saaville yhdysvaltalaisille yrityksille annetusta suojasta. Tietosuojatyöryhmä huomauttaa kuitenkin, että vaikka kyseinen oikeussuojakeino olisi tehokas, tämä ei tarkoita, että tehokkaat oikeussuojakeinot ovat henkilöiden käytettävissä, koska vaikuttaa siltä, että tässä skenaariossa oikeus tehokkaisiin oikeussuojakeinoihin on tiedonsaantipyynnön vastaanottavalla yrityksellä, eikä sillä henkilöllä, jonka tiedoista on kyse.

Liitteeseen VII ei sisälly muita tietoja ei-yhdysvaltalaisten henkilöiden mahdollisesti käytettävissä olevista lakisääteisistä oikeussuojakeinoista tilanteessa, jossa viranomaiset tai yritykset lainvastaisesti tarjoavat tai saavat pääsyn heitä koskevien tietojen sisältöön.

Tietosuojatyöryhmä on tyytyväinen siihen, että äskettäin annetussa oikeussuojakeinoja koskevassa Yhdysvaltojen laissa (*Judicial Redress Act*)[93] säädetään ei-yhdysvaltalaisten henkilöiden oikeudesta oikeudelliseen muutoksenhakuun. Nämä oikeudet koskevat kuitenkin ainoastaan selkeästi määriteltyjä kanneperusteita: oikeutta saada tiedot korjattua, oikeutta saada tietoja ja asianajopalkkioita, jos nimetty liittovaltion virasto tai sen yksikkö kieltää tietojen muuttamisen tai tiedonsaannin; sekä oikeutta yksityisoikeudellisiin oikeussuojakeinoihin tapauksissa, joissa on kyseessä tarkoituksellinen tai tahallinen tietojen julkistaminen.

Lisäksi on todettava, ettei päätösehdotuksen asiaa koskevien johdanto-osan kappaleiden alaviitteissä mainitulla Yhdysvaltojen oikeuskäytännöllä ole merkitystä arvioitaessa, voivatko ei-yhdysvaltalaiset henkilöt nostaa kanteen tuomioistuimessa riitauttaakseen yksityisyyden suojaansa puuttumisen laillisuuden[94] (erityisesti asiat Ontario, CA v. Quon[95], Maryland v. King[96] ja Samson v. Kalifornia[97]). Kaikissa näissä tapauksissa viitataan yhdysvaltalaisten henkilöiden yksityisyyttä koskevaan oikeuteen, ja niihin kaikkiin sisältyy Yhdysvaltojen korkeimman oikeuden päätöksiä, joilla itse asiassa rajoitetaan neljännen lisäyksen soveltamista.

Kaiken kaikkiaan tietosuojatyöryhmä panee tyytyväisenä merkille oikeussuojakeinoista annetun Yhdysvaltojen lain, mutta pitää kyseenalaisena, ovatko tehokkaat oikeussuojakeinot tosiasiallisesti rekisteröityjen käytettävissä.

93 *Judicial Redress Act of 2015*, H.R. 1428.

94 Tuomioistuin katsoi asiassa Ontario v. Quon, ettei Ontarion kaupunki loukannut työntekijöidensä neljännen lisäyksen mukaisia oikeuksia. Ontarion kaupungin pääsy kyseisen työntekijän yksityisten viestien sisältöön oli kohtuullista, koska se perustui työhön liittyvään legitiimiin tarkoitukseen, eikä sen soveltamisala ollut liian laaja. Asiassa Samson v. Kalifornia tuomioistuin katsoi, ettei neljännessä lisäyksessä estetä poliisia suorittamasta ehdonalaisvankiin kohdistuvaa henkilöntarkastusta jopa tapauksissa, joissa epäilyksiä ei ole. Tuomioistuin katsoi asiassa Maryland v. King, että kun poliisit pidättävät todennäköisin syin epäillyn henkilön vakavan rikoksen vuoksi ja tuovat hänet poliisiasemalle tutkintavankeuteen ottamista varten, pidätetyn henkilön sylkinäytteen ottaminen ja analysoiminen DNA:n tutkimiseksi on sormenjälkien ottamisen ja valokuvauksen tavoin poliisin laillinen kirjaamismenettely, joka on neljännessä lisäyksessä tarkoitetulla tavalla kohtuullinen.

95 Ontario, CA v. Quon, 130 S. Ct. 2619, 2630 (2010).

96 Maryland v. King, 133 S. Ct. 1958, 1970 (2013).

97 Samson v. Kalifornia, 547 U.S. 843, 848 (2006).

4.3 Loppuhuomautukset

Tietosuojatyöryhmä panee tyytyväisenä merkille Yhdysvaltojen hallinnon pyrkimykset tarjota aiempaa enemmän tietoa oikeudellisesta kehyksestä, joka koskee lainvalvontatarkoituksiin tapahtuvaa puuttumista EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa siirrettyjen henkilötietojen suojaan, sovellettavat rajoitukset ja suojatoimet mukaan luettuina.

Tietosuojatyöryhmä huomauttaa, että lainvalvontaviranomaisten tutkintavälineiden järjestelmä, sovellettavat rajoitukset ja suojatoimet mukaan luettuina, on luonteeltaan erittäin laaja ja monimutkainen ja että Privacy Shield -järjestelyyn sisältyvät tiedot ovat suppeat. Tietosuojatyöryhmä pahoittelee näin ollen sitä, ettei se tällä hetkellä pysty esittämään laajaa arviointia sovellettavien sääntöjen saatavuudesta, ennakoitavuudesta, tarpeellisuudesta ja oikeasuhteisuudesta (Privacy Shield -järjestelyn liitteessä VII olevien ja päätösehdotuksen toteamuksiin perustuvien) suppeiden tietojen perusteella. Sellainen arviointi voisi olla osa Privacy Shield -järjestelyn vuotuista tarkastelua riippumatta järjestelyä koskevista muista toteamuksista, joita tietosuojatyöryhmä on tässä lausunnossa esittänyt.

Tietosuojatyöryhmä toteaa, että lainvalvontaviranomaisten tiedonsaantioikeutta koskee ilmeisesti melko vahva riippumaton valvontamekanismi. Lisäksi tietosuojatyöryhmä pitää myönteisenä oikeussuojakeinoista annettua Yhdysvaltojen lakia, jossa annetaan ei-yhdysvaltalaisille henkilöille oikeus muutoksenhakuun tuomioistuimessa. Tietosuojatyöryhmä huomauttaa kuitenkin, että oikeus on luonteeltaan rajattu. Ei-yhdysvaltalainen henkilö ei voi vastustaa etsintämääräysten tai haasteiden täytäntöönpanoa tuomioistuimessa vetoamalla neljänteen lisäykseen, minkä lisäksi tietosuojatyöryhmä epäilee edelleen, onko lainvalvonnan alalla tosiasiallisesti tehokkaita oikeussuojakeinoja rekisteröityjen käytettävissä.

5. PÄÄTELMÄT JA SUOSITUKSET

Tietosuojatyöryhmä on ensinnäkin tyytyväinen siitä, että viiden kuukauden kuluessa safe harbor -periaatteiden mitätöinnistä on esitetty uusi tietosuojan tason riittävyyttä koskeva päätösehdotus, joka sisältää monia parannuksia edelliseen mekanismiin verrattuna. Työryhmä on erityisen tyytyväinen lisääntyneeseen avoimuuteen, joka johtuu siitä, että Yhdysvaltojen kauppaministeriön verkkosivustoon lisätään kaksi Privacy Shield -luetteloa: toisessa luettelossa annetaan niiden organisaatioiden tiedot, jotka ovat sitoutuneet noudattamaan Privacy Shield -järjestelyä, ja toisessa niiden organisaatioiden tiedot, jotka ovat aiemmin kuuluneet Privacy Shield -järjestelyyn mutta eivät enää kuulu siihen. On samaten hyvä asia, että Privacy Shield -järjestelyn kautta siirrettyjen henkilötietojen julkisesta käytöstä kansallisuuden turvallisuuden tai lainvalvonnan tarkoituksiin on nyt saatavilla aiempaa enemmän tietoa. Lopuksi tietosuojatyöryhmä on erityisen iloinen saatuaan tietää, että kaikkiin Yhdysvaltoihin siirrettäviin henkilötietoihin sovelletaan vastedes saman tasoista suojaa, sillä mitään erityissäännöksiä tiettyjen välineiden suosimiseksi ei ole.

5.1 Kolme huolenaihetta

Edelleen on kuitenkin kolme tärkeää huolenaihetta, joita on tietosuojatyöryhmän mielestä käsiteltävä.

Ensimmäinen huolenaihe on se, ettei tietosuojan tason riittävyyttä koskevan päätösehdotuksen sanallinen muotoilu velvoita organisaatioita hävittämään tietoja sen jälkeen, kun niitä ei enää tarvita. EU:n tietosuojalainsäädännön olennainen tekijä on varmistaa, että henkilötietoja säilytetään vain niin kauan kuin niitä tarvitaan siihen tarkoitukseen, johon ne on kerätty. Toiseksi tietosuojatyöryhmä ymmärtää liitteen VI siten, että Yhdysvaltojen hallinto ei täysin sulje pois mahdollisuutta jatkaa laajamittaista ja kohdentamatonta tietojenkeruuta. Tietosuojatyöryhmä on johdonmukaisesti katsonut, että tällainen henkilötietojen kerääminen on henkilöiden perusoikeuksien perusteeton loukkaus. Kolmas huolenaihe koskee oikeusasiamiesmekanismin käyttöönottoa. Tietosuojatyöryhmä on tietenkin tyytyväinen tällaisesta ennennäkemättömästä askeleesta, jonka avulla luonnolliset henkilöt saavat lisää oikeussuojaa ja uuden valvontamekanismin, mutta samalla se on huolissaan siitä, onko oikeusasiamiehellä riittävät valtuudet tehokkaaseen toimintaan. Sekä oikeusasiamiehen valtuuksia että hänen asemaansa on vähintään selkeytettävä, jotta voidaan osoittaa, että hänen asemansa on todella riippumaton ja että hän voi tarjota tehokkaan oikeussuojakeinon sääntöjenvastaista henkilötietojen käsittelyä vastaan.

5.2. Suositeltavat selvennykset

Edellä mainittujen seikkojen lisäksi tietosuojatyöryhmä on lausunnossaan esittänyt useita kohtia, joissa tietosuojan tason riittävyyttä koskevaa päätöstä on paikallaan selkeyttää. Tärkeintä on varmistaa, että Privacy Shield -järjestelyssä käytettävät keskeiset henkilötietojen suojaa koskevat käsitteet määritellään ja niitä sovelletaan johdonmukaisesti. Näin ei tällä hetkellä ole. Privacy Shield -järjestelyä koskevaan usein kysyttyjen kysymysten osioon (*Privacy Shield F.A.Q.*) olisi hyvä lisätä sanasto, jonka termimääritelmät olisi ihannetapauksessa sovittu yhteisesti EU:n ja Yhdysvaltojen välillä. Tietosuojatyöryhmä toteaa myös, että EU:n henkilötietojen edelleen siirtämistä säännellään riittämättömästi, erityisesti edustajille siirrettävien tietojen alan, käyttötarkoituksen rajoittamisen ja takeiden osalta. Lainvalvontaviranomaisten oikeus käyttää Privacy Shield -järjestelyn tietoja ja erityisesti sitä koskevan lainsäädännön ennakoitavuus on toinen huolenaihe sen takia, että Yhdysvaltojen lainvalvontajärjestelmä on luonteeltaan erittäin laaja ja monimutkainen sekä liittovaltion että osavaltioiden tasolla, ja sitä koskevia tietoja on tietosuojan riittävyyttä koskevassa päätöksessä rajoitetusti.

Privacy Shield -järjestely on ensimmäinen tietosuojan tason riittävyyttä koskeva päätös, joka on laadittu sen jälkeen, kun yleisen tietosuoja-asetuksen tekstistä oli periaatteessa sovittu. Siitä huolimatta monia asetuksessa säädettyjä henkilöiden tietosuojan tason parannuksia ei ole otettu huomioon Privacy Shield -järjestelyssä. Siitä syystä tietosuojatyöryhmä suosittelee, että tätä tietosuojan tason riittävyyttä koskevaa päätöstä, samoin kuin muita kolmansia maita koskevia tietosuojan tason riittävyyttä koskevia päätöksiä, tarkastellaan uudelleen pian sen jälkeen, kun yleistä tietosuoja-asetusta aletaan soveltaa.

Viimeinen tietosuojatyöryhmän esittämä suositus koskee yhteistä tarkastelua. Tietosuojatyöryhmä on tyytyväinen siihen, että Privacy Shield -järjestelyn tietosuojan tason riittävyyttä koskevaa päätöstä tarkastellaan uudelleen vuosittain, siten että tietosuojaviranomaiset ja muut merkittävät osapuolet osallistuvat tarkasteluun laajasti. Tietosuojatyöryhmän mielestä kaikkien osapuolten olisi hyvissä ajoin ennen ensimmäistä tarkastelua sovittava yhteisten tarkastelujen osatekijät, kuten tarkasteluraportin laatiminen ja esittely.