EUROOPAN
KOMISSIO

Bryssel 27.11.2013
COM(2013) 847 final

# KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

## safe harbor -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta

**KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE**

**safe harbor -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta**

## 1 JOHDANTO

Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24. lokakuuta 1995 annetussa direktiivissä (jäljempänä 'tietosuojadirektiivi') säädetään henkilötietojen siirroista EU:n jäsenvaltioista unionin ulkopuolisiin maihin[1] siltä osin kuin siirrot kuuluvat kyseisen säädöksen soveltamisalaan[2].

Tietosuojadirektiivin nojalla komissio voi todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, mikä johtuu kyseisen maan sisäisestä lainsäädännöstä tai kansainvälisistä sitoumuksista, jotka on tehty yksilöiden oikeuksien suojaamiseksi. Tällaiseen maahan tapahtuviin tiedonsiirtoihin ei sovelleta erityisrajoituksia. Näitä komission päätöksiä kutsutaan yleisesti '**tietosuojatason riittävyyttä koskeviksi päätöksiksi**'.

Komissio teki 26. heinäkuuta 2000 päätöksen 520/2000/EY[3] (jäljempänä '**safe harbor -päätös**'), jossa todetaan, että safe harbor -periaatteet ja Yhdysvaltojen kauppaministeriön julkaisemat tavallisimmat kysymykset (jäljempänä 'FAQ'), tarjoavat riittävän suojan EU:sta käsin tehtäville henkilötietojen siirroille. Safe harbor -päätös tehtiin 29 artiklan mukaisen tietosuojatyöryhmän annettua lausuntonsa ja 31 artiklalla perustetun komitean annettua jäsenvaltioiden määräenemmistöllä hyväksytyn lausuntonsa. Neuvoston päätöksen 1999/468/EY mukaisesti safe harbor -päätös oli ennen sen tekemistä Euroopan parlamentin tarkasteltavana.

Nykyisellä safe harbor -päätöksellä sallitaankin henkilötietojen siirtäminen vapaasti[4] EU:n jäsenvaltioista[5] sellaisille Yhdysvalloissa sijaitseville yrityksille, jotka ovat sitoutuneet noudattamaan safe harbor -periaatteita tilanteissa, joissa tiedonsiirto ei muutoin vastaisi EU:n vaatimuksia tietosuojatason riittävyydestä EU:n ja Yhdysvaltojen tietosuojamenettelyjen merkittävien erojen vuoksi.

Nykyisen safe harbor -järjestelmän toiminta perustuu siihen osallistuvien yritysten sitoumuksiin ja omiin varmennuksiin. Järjestelmään liittyminen on vapaaehtoista, mutta säännöt sitovat yrityksiä, jotka ovat ilmoittaneet noudattavansa niitä. Safe harbor -järjestelmän keskeiset periaatteet ovat

a) järjestelmään osallistuvien yritysten tietosuojakäytäntöjen avoimuus,

b) safe harbor -periaatteiden sisällyttäminen yritysten tietosuojakäytäntöihin ja

---

1 Tietosuojadirektiivin 25 ja 26 artikla muodostavat säädöskehyksen henkilötietojen siirrolle EU:sta ETA-alueen ulkopuolisiin kolmansiin maihin.

2 Rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta 27. marraskuuta 2008 tehdyn puitepäätöksen 2008/977/YOS 13 artikla sisältää lisäsäännöksiä, joita sovelletaan silloin, kun jäsenvaltio siirtää henkilötietoja toiseen jäsenvaltioon tai asettaa ne sen saataville ja kun jälkimmäisen aikomuksena on myöhemmin siirtää kyseiset tiedot edelleen kolmannelle valtiolle tai kansainväliselle elimelle rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöön panemiseksi.

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

4 Edellä todettu ei estä soveltamasta tietojenkäsittelyyn muita mahdollisia vaatimuksia, jotka johtuvat EU:n tietosuojadirektiivin täytäntöönpanoa varten annetusta kansallisesta lainsäädännöstä.

5 Tämä on koskenut myös ETA-sopimuksen kolmesta valtio-osapuolesta tehtäviä tiedonsiirtoja siitä lähtien, kun direktiivi 95/46/EY ulotettiin koskemaan ETA-sopimusta. ETA:n sekakomitean päätös 38/1999, tehty 25 päivänä kesäkuuta 1999, EYVL L 296, 23.11.2000, s. 41.

c) täytäntöönpano, jota toteuttavat myös viranomaiset.

Safe harbor -järjestelmän keskeistä perustaa on nyt arvioitava **uudenlaisessa tilanteessa**, jota leimaavat

a) räjähdysmäinen kasvu tietovirroissa, jotka aiemmin olivat vain apukeino mutta nykyään keskeinen tekijä digitaalitalouden nopeassa kasvussa sekä tietojen keruun, käsittelyn ja käytön erittäin merkittävässä kehityksessä,

b) tietovirtojen ratkaiseva merkitys erityisesti transatlanttisen talouden kannalta,[6]

c) nopea kasvu safe harbor -järjestelmään kuuluvien yhdysvaltalaisyritysten määrässä, joka on kahdeksankertaistunut vuodesta 2004 (400 vuonna 2004, mutta 3 246 vuonna 2013),

d) Yhdysvaltojen vakoiluohjelmista hiljattain julkisuuteen tulleet tiedot, jotka herättävät uusia kysymyksiä safe harbor -järjestelmän takaamasta suojatasosta.

Tässä tiedonannossa tarkastellaan safe harbor -järjestelmän toimintaa näistä lähtökohdista käsin. Tiedonanto **perustuu** komission kokoamiin **tietoihin**, tietosuojaa käsitelleen EU:n ja Yhdysvaltojen kontaktiryhmän toimintaan vuonna 2009, riippumattoman alihankkijan vuonna 2008 laatimaan selvitykseen[7] sekä Yhdysvaltojen vakoiluohjelmien julkitulon jälkeen perustetussa EU:n ja Yhdysvaltojen ad hoc -tietosuojatyöryhmässä saatuihin tietoihin (*ks. rinnakkaisasiakirja*). Tämä tiedonanto on jatkoa safe harbor -järjestelmän käynnistysvaiheessa laadituille **komission kahdelle arviointikertomukselle**, joista ensimmäinen ilmestyi vuonna 2002[8] ja toinen vuonna 2004[9].

## 2 SAFE HARBOR -JÄRJESTELMÄN RAKENNE JA TOIMINTA

### 2.1 Safe harbor -järjestelmän rakenne

Yhdysvaltalaisen yrityksen, joka haluaa liittyä safe harbor -järjestelmään, on a) mainittava yleisesti saatavilla olevassa tietosuojaselosteessaan, että se on sitoutunut safe harbor -periaatteisiin ja todella noudattaa niitä, ja lisäksi b) annettava Yhdysvaltojen kauppaministeriölle oma varmennus, toisin sanoen ilmoitettava sille toimivansa kyseisten periaatteiden mukaisesti. Oma varmennus on annettava uudestaan joka vuosi. Safe harbor -päätöksen liitteessä I esitettyihin safe harbor -periaatteisiin kuuluu vaatimuksia, jotka koskevat sekä henkilötietojen aineellisoikeudellista suojaa (tietojen koskemattomuutta, sekä turvallisuutta, valintaa ja tiedon edelleen siirtämistä koskevat periaatteet) että rekisteröityjen menettelyllisiä oikeuksia (ilmoitus-, tiedonsaanti- ja täytäntöönpanoperiaatteet).

Safe harbor -järjestelmän täytäntöönpanossa on keskeisessä asemassa kaksi yhdysvaltalaista viranomaistahoa: Yhdysvaltojen kauppaministeriö ja Federal Trade Commission eli FTC (liittovaltion kilpailuviranomainen).

---

6 Eräissä selvityksissä on todettu, että jos palveluille ja rajat ylittäville tietovirroille aiheutuisi häiriötä yrityksiä sitovien sääntöjen, mallisopimuslausekkeiden ja safe harbor -periaatteiden noudattamisen keskeytymisen seurauksena, EU:n BKT:hen kohdistuva negatiivinen vaikutus saattaisi olla 0,8–1,3 prosentin luokkaa ja EU:n palveluvienti Yhdysvaltoihin saattaisi pienentyä 6,7 prosenttia kilpailukyvyn heikkenemisen vuoksi. Ks. ECIPEn (European Centre for International Political Economy) Yhdysvaltain keskuskauppakamarille laatima selvitys maaliskuulta 2013, ”The Economic Importance of Getting Data Protection Right”.

7 Vaikutustenarviointiselvitys, jonka Namurin yliopiston CRID-keskus (Centre de Recherche Informatique et Droit) laati Euroopan komissiota varten vuonna 2008.

8 Komission yksiköiden valmisteluasiakirja ”The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbor Privacy Principles and related FAQs issued by the US Department of Commerce”, SEC (2002) 196, 13.12.2002.

9 Komission yksiköiden valmisteluasiakirja ”The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbor Privacy Principles and related FAQs issued by the US Department of Commerce”, SEC (2004) 1323, 20.10.2004.

**Yhdysvaltojen kauppaministeriö** arvioi kaikki yrityksiltä saamansa safe harbor -järjestelmää koskevat omat varmennukset ja niiden vuosittaista uudelleenvarmennusta varten toimittamat kirjeet varmistaakseen, että ne täyttävät kaikilta osin järjestelmään kuulumisen vaatimukset.[10] Se pitää ajan tasalla luetteloa yrityksistä, jotka ovat toimittaneet omaa varmennusta koskevat kirjeet, ja julkaisee luettelon ja kirjeet verkkosivuillaan. Se myös valvoo safe harbor -järjestelmän toimintaa ja poistaa luettelosta yritykset, jotka eivät noudata kyseisiä periaatteita.

**FTC** puuttuu Free Trade Commission Act -lain 5 §:ssä tarkoitettuihin sopimattomiin tai harhaanjohtaviin käytäntöihin kuluttajansuojelun alaa koskevien toimintavaltuuksiensa mukaisesti. FTC:n täytäntöönpanotoimia ovat muun muassa tutkimukset, jotka koskevat safe harbor -järjestelmään kuulumista koskevia perusteettomia väitteitä tai järjestelmään kuuluvia yrityksiä, jotka eivät noudata safe harbor -periaatteita. Silloin kun kyse on lentoyhtiöistä, safe harbor -periaatteiden toimivaltainen täytäntöönpanoviranomainen on Yhdysvaltojen liikenneministeriö.[11]

Voimassa oleva safe harbor -päätös on osa unionin lainsäädäntöä, jota jäsenvaltioiden viranomaisten on noudatettava. EU-maiden **tietosuojaviranomaisilla** on päätöksen nojalla oikeus tietyissä tapauksissa keskeyttää safe harbor -periaatteita noudattaviin yrityksiin suunnatut tiedonsiirrot.[12] Päätöksen tultua voimaan vuonna 2000 Euroopan komission tietoon ei ole tullut tapauksia, joissa kansallinen tietosuojaviranomainen olisi keskeyttänyt tiedonsiirtoja. Päätöksen mukaisesta toimivallastaan riippumatta EU-maiden tietosuojaviranomaisilla on oikeus toteuttaa toimia, joilla varmistetaan vuoden 1995 tietosuojadirektiivissä säädettyjen yleisten tietosuojaperiaatteiden noudattaminen myös silloin, kun on kyse kansainvälisistä tiedonsiirroista.

Kuten safe harbor -päätöksessä muistutetaan, **komissiolla** – joka toimii asetuksessa (EU) N:o 182/2011 säädetyn tarkastelumenettelyn mukaisesti – **on toimivalta** milloin tahansa muuttaa päätöstä, keskeyttää sen soveltaminen tai rajoittaa sen soveltamisalaa päätöksen täytäntöönpanosta saatujen kokemusten perusteella. Tähän turvaudutaan erityisesti siinä tapauksessa, että Yhdysvaltojen järjestelmä toimii puutteellisesti, esimerkiksi jos safe harbor -periaatteiden noudattamisen valvonnasta Yhdysvalloissa vastaava elin ei tosiasiallisesti täytä tehtäväänsä tai jos Yhdysvaltojen lainsäädäntö antaa safe harbor -periaatteiden takaamaa suojatasoa paremman suojan. Muiden komission päätösten tavoin myös tätä päätöstä voidaan muuttaa muistakin syistä tai se voidaan jopa kumota.

## 2.2 Safe harbor -järjestelmän toiminta

**Oman varmennuksensa antaneiden 3 246**[13] **yrityksen** joukossa on sekä pieniä että suuria yrityksiä[14]. Rahoituspalvelut ja televiestintäteollisuus eivät kuulu FTC:n

---

10 Jos yrityksen antama oma varmennus tai uudelleenvarmennus ei täytä safe harbor -vaatimuksia, kauppaministeriö huomauttaa tästä yritykselle ja pyytää sitä ryhtymään toimiin (esim. tekemään tietosuojaselosteeseensa selvennyksiä ja muutoksia) ennen kuin yrityksen varmennus voidaan hyväksyä lopullisesti.

11 United States Coden 49 osaston 41712 §:n nojalla.

12 Tiedonsiirron keskeytystä voidaan vaatia erityisesti seuraavissa kahdessa tilanteessa:
a) kyseinen Yhdysvaltojen valtiollinen elin on todennut, että organisaatio loukkaa yksityisyyden suojaa koskevia safe harbor -periaatteita, tai
b) on huomattavan todennäköistä, että safe harbor -periaatteita loukataan; on kohtuullinen syy uskoa, että asianomainen täytäntöönpano-organisaatio ei ole ryhtynyt tai ryhdy riittäviin ja ajankohtaisiin toimenpiteisiin kyseessä olevan tapauksen ratkaisemiseksi; tietojen siirron jatkaminen aiheuttaisi välittömän vakavan haitan vaaran rekisteröidyille; ja jäsenvaltion toimivaltaiset viranomaiset ovat olosuhteisiin nähden kohtuullisessa määrin pyrkineet antamaan organisaatiolle ilmoituksen ja tilaisuuden vastata siihen.

13 Safe harbor -luetteloon 26. syyskuuta 2013 kirjatuista organisaatioista **3 246**:n kohdalle oli merkitty ***current*** (voimassa) ja **935**:n kohdalle ***not current*** (ei voimassa).

14 Enintään 250 työntekijän safe harbor -organisaatioita oli **60 prosenttia** (1 925 kaikkiaan 3 246:sta). Vähintään 251 työntekijän safe harbor -organisaatioita oli **40 prosenttia** (1 295 kaikkiaan 3 246:sta).

täytäntöönpanovaltuuksien piiriin, joten ne jäävät safe harbor -järjestelmän ulkopuolelle, mutta muutoin järjestelmään kuuluvat yritykset edustavat monia teollisuuden ja palvelujen aloja. Niiden joukossa on tunnettuja internetpalvelujen tarjoajia, ja teollisuudenalojen kirjo ulottuu tietotekniikka- ja tietokonepalveluista lääketeollisuuteen ja edelleen matkailuun ja matkailupalveluihin sekä terveydenhuolto- ja luottokorttipalveluihin[15]. Kyse on lähinnä EU:n sisämarkkinoilla palveluja tarjoavista yhdysvaltalaisyrityksistä, mutta mukana on myös muutamien EU:n yritysten, esimerkiksi Nokian ja Bayerin, tytäryhtiöitä. Näistä yrityksistä 51 prosenttia käsittelee Euroopassa asuvien työntekijöiden henkilötietoja, joita siirretään Yhdysvaltoihin henkilöstöhallintosyistä.[16]

Jotkin EU-maiden tietosuojaviranomaisista ovat **yhä huolestuneempia** nykyisen safe harbor -järjestelmän puitteissa tehtävistä tiedonsiirroista. Joidenkin jäsenvaltioiden tietosuojaviranomaiset ovat kritisoineet safe harbor -periaatteiden varsin yleisluonteista sanamuotoa ja sitä, että järjestelmä perustuu paljolti yritysten antamaan omaan varmennukseen ja itsesääntelyyn. Myös elinkeinoelämän taholta on tuotu esiin samanlaisia huolenaiheita ja huomautettu, että puutteellinen täytäntöönpano aiheuttaa kilpailun vääristymistä.

Voimassa oleva safe harbor -järjestelmä perustuu yritysten vapaaehtoiseen sitoutumiseen, tällaisten yritysten antamaan omaan varmennukseen sekä viranomaisvalvontaan, joka koskee varmennukseen liittyvien sitoumusten noudattamista. Siksi riittämätön avoimuus ja puutteellinen täytäntöönpano heikentävät safe harbor -järjestelmän perusrakenteita.

Jos avoimuudessa tai täytäntöönpanossa ilmenee puutteita Yhdysvalloissa, vastuu siirtyy Euroopan tietosuojaviranomaisille ja safe harbor -järjestelmää hyödyntäville yrityksille. Saksan tietosuojaviranomaiset tekivät 29. huhtikuuta 2010 päätöksen, jonka mukaan Euroopasta Yhdysvaltoihin tietoja siirtävien yritysten olisi aktiivisesti varmistettava, että tietoja tuovat yhdysvaltalaisyritykset todellakin noudattavat safe harbor -periaatteita, ja jossa suositellaan, että ”tietoja vievä yritys ainakin selvittää, onko tietoja tuovan yrityksen antama safe harbor -periaatteita koskeva oma varmennus yhä voimassa”.[17]

Sen jälkeen kun tiedot Yhdysvaltojen vakoiluohjelmista olivat tulleet julki, Saksan tietosuojaviranomaiset menivät 24. heinäkuuta 2013 vielä pidemmälle ja toivat esiin huolensa näin: ”On huomattavan todennäköistä, että komission päätöksissä esitettyjä periaatteita loukataan.”[18] Joissain tapauksissa (esimerkiksi Bremenissä) tietosuojaviranomaiset ovat pyytäneet yritystä, joka siirtää henkilötietoja yhdysvaltalaisille palveluntarjoajille, kertomaan tietosuojaviranomaisille, huolehtivatko asianomaiset palveluntarjoajat ja miten ne huolehtivat siitä, ettei Yhdysvaltojen kansallinen turvallisuusvirasto NSA (National Security Agency) pääse käsiksi kyseisiin tietoihin. Irlannin tietosuojaviranomainen on kertonut saaneensa hiljattain kaksi valitusta, joissa vedotaan safe harbor -ohjelmaan, sen jälkeen kun

---

15 Esimerkiksi MasterCard, joka toimii yhteistyössä tuhansien pankkien kanssa, on selvä esimerkki tapauksesta, jossa safe harbor -periaatteita ei voida korvata muilla henkilötietojen siirtoja käsittelevillä oikeusvälineillä, kuten yrityksiä sitovilla säännöillä tai sopimusjärjestelyillä.

16 Sellaisia safe harbor -organisaatioita, joiden varmennus kattaa henkilöstöä koskevat tiedot (ja jotka ovat näin ollen sitoutuneet tekemään yhteistyötä EU:n tietosuojaviranomaisten kanssa ja noudattamaan niiden ohjeita), oli **51 prosenttia** (1 671 kpl kaikkiaan 3 246:sta).

17 Ks. Saksan tietosuojaviranomaisten yhteistyöelimen (Düsseldorfer Kreis) päätös, tehty 28. ja 29. huhtikuuta 2010, ”Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover”: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile. Euroopan tietosuojavaltuutettu Peter Hustinx toi kuitenkin Euroopan parlamentin LIBE-valiokunnan 7. lokakuuta 2013 järjestämässä julkisessa kuulemistilaisuudessa esiin sen käsityksen, että safe harbor -järjestelmään on tehty merkittäviä parannuksia ja että useimmat kiistakysymykset on ratkaistu: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Ks. Saksan tietosuojavaltuutettujen konferenssin päätöslauselma, jossa korostetaan sitä, että tiedustelupalvelut merkitsevät massiivista uhkaa Saksan ja Euroopan ulkopuolisten maiden väliselle tietoliikenteelle: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

Yhdysvaltojen tiedustelupalveluiden vakoiluohjelmista oli kerrottu tiedotusvälineissä. Se jätti kuitenkin valitukset tutkimatta sillä perusteella, että kyseiset henkilötiedot siirrettiin kolmanteen maahan Irlannin tietosuojalainsäädännön vaatimusten mukaisesti. Vastaavanlaisen valituksen saanut Luxemburgin tietosuojaviranomainen totesi, että Microsoft ja Skype ovat noudattaneet Luxemburgin tietosuojalainsäädäntöä siirtäessään henkilötietoja Yhdysvaltoihin.[19] Irlannin High Court on sittemmin ottanut tutkittavakseen laillisuusvalvontakanteen, joka koskee sitä, ettei Irlannin tietosuojavaltuutettu tutkinut Yhdysvaltojen vakoiluohjelmiin liittyvää valitusta. Irlannin tietosuojaviranomaisen vastaanottamista kahdesta valituksesta toisen oli tehnyt opiskelijaryhmä nimeltä Europe versus Facebook (EvF), joka teki myös Saksassa Yahoota vastaan samankaltaisen valituksen, jota toimivaltaiset tietosuojaviranomaiset parhaillaan käsittelevät.

Tietosuojaviranomaisten erilaiset suhtautumistavat vakoilupaljastuksiin osoittavat, että safe harbor -järjestelmän pirstoutumisen vaara on todellinen, ja herättävät kysymyksiä siitä, missä määrin täytäntöönpanoa valvotaan.

## 3 JÄRJESTELMÄÄN OSALLISTUVIEN YRITYSTEN TIETOSUOJAKÄYTÄNTÖJEN AVOIMUUS

Safe harbor -päätöksen liitteessä II esitetyssä FAQ 6:ssa edellytetään, että safe harbor -järjestelmän mukaisen oman varmennuksen antamisesta kiinnostuneet yritykset toimittavat kauppaministeriöön tietosuojaselosteensa ja julkistavat sen. Selosteen on sisällettävä sitoutuminen safe harbor -periaatteiden noudattamiseen. Vaatimus siitä, että oman varmennuksensa antaneiden yritysten on **asetettava yleisesti saataville tietosuojaselosteensa** ja sitoutumisensa kyseisten periaatteiden noudattamiseen, on ratkaisevan tärkeä koko järjestelmän toiminnan kannalta.

Jos tällaisten yritysten tietosuojaselosteita ei julkaista, yksityishenkilöille, joiden henkilötietoja kerätään ja käsitellään, koituu vahinkoa, ja kyseessä voi olla **ilmoitusperiaatteen loukkaus**. Ne, joiden henkilötietoja siirretään EU:n ulkopuolelle, voivat tällöin olla tietämättömiä oikeuksistaan ja oman varmennuksensa antaneiden yritysten velvollisuuksista.

Lisäksi yritysten sitoutuminen safe harbor -periaatteiden noudattamiseen **antaa FTC:lle valtuudet toteuttaa täytäntöönpanotoimia** silloin, kun yritykset eivät noudata näitä periaatteita vaan syyllistyvät sopimattomiin tai harhaanjohtaviin käytäntöihin. Avoimuuden puute yhdysvaltalaisyritysten toiminnassa hankaloittaa FTC:n valvontatyötä ja vie tehoa täytäntöönpanolta.

Merkittävä osa oman varmennuksensa antaneista yrityksistä ei vuosien mittaan ollut julkistanut tietosuojaselostettaan eikä sitoutumistaan safe harbor -periaatteiden noudattamiseen. Safe harbor -järjestelmää käsittelevässä komission kertomuksessa vuodelta 2004 huomautettiin, että kauppaministeriön olisi syytä **omaksua aktiivisempi ote tämän vaatimuksen noudattamisen valvontaan**.

Kauppaministeriö on vuoden 2004 jälkeen kehitellyt **uusia viestintävälineitä** tarkoituksenaan auttaa yrityksiä noudattamaan avoimuusvelvoitteita. Hankkeesta on saatavilla tietoa safe harbor -järjestelmää käsittelevillä kauppaministeriön verkkosivuilla[20], joille yritysten on myös mahdollista siirtää tietosuojaselosteensa. Kauppaministeriön mukaan yritykset ovat tarttuneet tähän tilaisuuteen ja lähettäneet tietosuojaselosteitaan kauppaministeriön verkkosivuille

[19] Ks. 18. marraskuuta 2013 päivätty Luxemburgin tietosuojaviranomaisen lausunto.

[20] http://www.export.gov/SafeHarbor/

hakiessaan jäsenyyttä safe harbor -järjestelmässä.[21] Lisäksi kauppaministeriö julkaisi vuosina 2009–2013 useita jäsenyydestä kiinnostuneille yrityksille tarkoitettuja oppaita, joissa muun muassa selostetaan omaa varmennusta (*Guide to Self-Certification*) ja periaatteiden noudattamista koskevan ilmoituksen antamista (*Helpful Hints on Self-Certifying Compliance*).[22]

Yritykset noudattavat avoimuusvelvoitteita vaihtelevasti. Osa niistä vain toimittaa omaan varmennukseen liittyvän menettelyn yhteydessä kauppaministeriöön kuvauksen tietosuojakäytännöstään, mutta valtaosa julkistaa tietosuojaselosteensa verkkosivuillaan ja siirtää sen myös kauppaministeriön verkkosivuille. **Tietosuojaselosteet eivät silti aina ole kuluttajaystävällisiä ja helppolukuisia**. Tietosuojaselosteisiin johtavat hyperlinkit eivät aina toimi kunnolla eivätkä aina ohjaa asiaankuuluville verkkosivuille.

Safe harbor -päätöksestä ja sen liitteistä seuraa, että tietosuojaselosteen julkistamisvaatimuksen täyttämiseksi **ei riitä, että yritys ilmoittaa** omasta varmennuksestaan kauppaministeriölle. FAQ:ssa esitettyihin, varmennusta koskeviin vaatimuksiin kuuluu kuvaus yrityksen tietosuojakäytännöstä ja selkeä mainінta siitä, missä yleisö voi tutustua siihen.[23] Tietosuojaselosteiden täytyy olla selkeitä ja vaivattomasti kaikkien saatavilla. Niissä on oltava hyperlinkki kauppaministeriön safe harbor -verkkosivuille, joilta löytyy luettelo kaikista järjestelmässä kulloinkin mukana olevista jäsenistä (*current*-merkintä), ja vaihtoehtoisen riitojenratkaisuelimen verkkosivuille ohjaava linkki. Monet järjestelmään kuuluvista yrityksistä eivät vuosina 2000–2013 kuitenkaan noudattaneet kyseisiä vaatimuksia. Yhteydenpidossaan komission kanssa helmikuussa 2013 Yhdysvaltojen kauppaministeriö toi julki sen, että mahdollisesti jopa 10 prosenttia oman varmennuksensa antaneista yrityksistä ei ole asettanut julkisille verkkosivuilleen tietosuojaselostetta, joka sisältäisi ilmoituksen niiden sitoutumisesta safe harbor -periaatteiden noudattamiseen.

Tuoreiden tilastotietojen mukaan alituisena ongelmana ovat myös **safe harbor -järjestelmään kuulumista koskevat perusteettomat väitteet**. Niistä yrityksistä, jotka väittävät kuuluvansa järjestelmään, noin 10:tä prosenttia ei ole kirjattu kauppaministeriön ylläpitämään luetteloon järjestelmässä parhaillaan mukana olevina jäseninä.[24] Perusteettomia väitteitä ovat esittäneet sekä yritykset, jotka eivät ole koskaan osallistuneet järjestelmään, että yritykset, jotka ovat liittyneet siihen mutta eivät sittemmin ole uusineet omaa varmennustaan kauppaministeriölle vuoden välein. Tällöin yritykset pidetään edelleen ministeriön safe harbor -luettelossa, mutta oman varmennuksen osalta merkintänä on *not current* (ei voimassa), mikä tarkoittaa, että kyseinen yritys on kuulunut järjestelmään, joten sillä on velvollisuus edelleenkin taata suoja jo käsitellyille henkilötiedoille. FTC:llä on valtuudet toimia silloin, kun kyse on harhaanjohtavista käytännöistä tai safe harbor -periaatteiden noudattamatta jättämisestä (ks. jäljempänä 5.1 luku). Perusteettomiin väitteisiin liittyvät epäselvyydet heikentävät järjestelmän uskottavuutta.

Euroopan komissio huomautti Yhdysvaltojen kauppaministeriölle niiden säännöllisessä yhteydenpidossa vuosina 2012 ja 2013, ettei avoimuusvelvoitteiden noudattamiseksi riitä vain se, että yritykset toimittavat kauppaministeriöön kuvauksen tietosuojakäytännöstään, vaan ne

---

21 https://SafeHarbor.export.gov/list.aspx

22 Oppaat löytyvät ohjelman verkkosivuilta osoitteista http://export.gov/SafeHarbor/ ja http://export.gov/SafeHarbor/eu/eg_main_018495.asp

23 Yhdysvaltojen kauppaministeriö vahvisti 12. marraskuuta 2013 seuraavaa: ”Nykyään yritysten, joilla on julkiset verkkosivut ja jotka käsittelevät kuluttaja-, asiakas- tai kävijätietoja, on julkaistava verkkosivuillaan safe harbor -periaatteiden mukainen tietosuojaseloste” (asiakirja ”U.S.-EU Cooperation to Implement the Safe Harbor Framework”, 12. marraskuuta 2013).

24 Galexia-niminen australialainen konsulttiyritys vertaili syyskuussa 2013 safe harbor -jäsenyyttä koskevia perusteettomia väitteitä vuosilta 2008 ja 2013. Sen keskeisenä havaintona oli, että safe harbor -jäsenten määrässä vuosina 2008–2013 tapahtuneen kasvun ohella (1 109:stä 3 246:een) myös perusteettomien väitteiden määrä oli lisääntynyt 206:sta 427:een. http://www.galexia.com/public/about/news/about_news-id225.html

täytyy asettaa yleisesti saataville. Kauppaministeriötä pyydettiin myös **tehostamaan valvontatoimia, joita se kohdistaa ajoittain yritysten verkkosivuihin** ensimmäisen oman varmennuksen antamisen tai sen vuotuisen uudistamisen yhteydessä toimitettavan todentamismenettelyn jälkeen, ja ryhtymään toimiin niiden yritysten suhteen, jotka eivät noudata avoimuusvaatimuksia.

EU:n tuotua esiin nämä tärkeinä pitämänsä asiat **Yhdysvaltojen kauppaministeriö määräsi** ensimmäisenä toimenaan **maaliskuusta 2013 lähtien pakolliseksi** sen, että safe harbor -järjestelmään kuuluva yritys, jolla on julkiset verkkosivut, asettaa asiakas- ja käyttäjätietoja koskevan tietosuojaselosteensa helposti saataville näille verkkosivuille. Samalla kauppaministeriö otti tavakseen kehottaa yrityksiä, joiden tietosuojaselosteita ei vielä ollut linkitetty kauppaministeriön safe harbor -sivuille, luomaan tällaisen linkin, jotta yrityksen sivuilla käyvien kuluttajien olisi helppoa päästä suoraan tutustumaan viralliseen safe harbor -luetteloon ja -sivuihin. Tällä tavoin eurooppalaiset rekisteröidyt voivat välittömästi varmistaa yritysten kauppaministeriöön toimittamat sitoumukset tekemättä lisähakuja internetissä. Kauppaministeriö ryhtyi myös huomauttamaan yrityksille, että niiden on mainittava riippumattoman riitojenratkaisuelimensä yhteystiedot julkaisemissaan tietosuojaselosteissa.[25]

**Tätä prosessia on vauhditettava** sen varmistamiseksi, että kaikki oman varmennuksensa antaneet yritykset noudattavat safe harbor -vaatimuksia kaikilta osin viimeistään maaliskuussa 2014 (joka on yritysten oman varmennuksen uusimisen vuotuinen määräaika laskettuna maaliskuussa 2013 käyttöön otetuista uusista vaatimuksista).

Tästä huolimatta on yhä epävarmaa, noudattavatko kaikki oman varmennuksensa antaneet yritykset avoimuusvaatimuksia kokonaisuudessaan. Kauppaministeriön täytyykin aiempaa tiukemmin seurata ja tutkia niiden velvoitteiden noudattamista, joihin yritykset sitoutuvat antaessaan ensi kerran oman varmennuksensa ja uusiessaan sen vuosittain.

## 4 SAFE HARBOR -PERIAATTEIDEN SISÄLLYTTÄMINEN YRITYSTEN TIETOSUOJAKÄYTÄNTÖIHIN

Oman varmennuksensa antaneiden yritysten on noudatettava safe harbor -päätöksen liitteessä I esitettyjä periaatteita voidakseen saada ja säilyttää safe harbor -etuudet.

Kertomuksessaan vuodelta 2004 komissio totesi, että huomattavan monet **yritykset eivät olleet sisällyttäneet safe harbor -periaatteita asianmukaisesti** tietojenkäsittelykäytäntöihinsä. Asianomaisille ei esimerkiksi aina kerrottu selkeästi ja avoimesti, missä tarkoituksissa heidän henkilötietojaan käsitellään, tai heille ei annettu mahdollisuutta kieltää tietojensa luovuttamista kolmansille osapuolille tai niiden käyttöä tarkoitukseen, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta. Kertomuksessa katsottiin, että kauppaministeriön olisi tiedotettava aloitteellisemmin safe harbor -järjestelmän jäsenyyden edellytyksistä ja safe harbor -periaatteista.[26]

Tässä on tapahtunut vain vähäistä edistystä. Kauppaministeriö on 1. tammikuuta 2009 lähtien ennen varmennuksen uusimista arvioinut kaikkien yritysten tietosuojakäytännöt niiden toimittaessa sille vuosittain uusittavan oman varmennuksensa. Arvio on kuitenkin suppeahko. Se **ei käsitä** oman varmennuksensa antaneiden yritysten **todellisten käytäntöjen**

---

25 Maalis–syyskuussa 2013 kauppaministeriö
• huomautti niille 101 yritykselle, *jotka olivat jo siirtäneet safe harbor -periaatteiden mukaisen tietosuojaselosteensa ministeriön safe harbor -verkkosivuille*, että niiden täytyy julkaista se myös omilla verkkosivuillaan.
• huomautti niille 154 yritykselle, jotka eivät olleet sitä vielä tehneet, että niiden täytyy linkittää tietosuojaselosteensa ministeriön safe harbor -sivuille.
• huomautti yli 600 yritykselle, että niiden täytyy mainita riippumattoman riitojenratkaisuelimen yhteystiedot tietosuojaselosteessaan.

26 Ks. komission kertomus SEC (2004) 1323, s. 8.

**perusteellista arviointia**, vaikka sellainen lisäisi huomattavasti kyseisen menettelyn uskottavuutta.

Komission esitettyä vaatimuksia siitä, että kauppaministeriön olisi valvottava oman varmennuksensa antaneita yrityksiä tiukemmin ja järjestelmällisemmin, **omaa varmennusta koskeviin uusiin ilmoituksiin kiinnitetään nykyään enemmän huomiota**. Niiden uusien ilmoitusten määrä, joita ei ole hyväksytty vaan jotka on lähetetty takaisin yrityksille kehottaen niitä tekemään parannuksia tietosuojakäytäntöönsä, kasvoi merkittävästi vuosina 2010–2013: se kaksinkertaistui oman varmennuksensa uusineiden yritysten osalta ja kolminkertaistui järjestelmään vasta liittyvien osalta.[27] Kauppaministeriö on vakuuttanut komissiolle, että omat varmennukset tai niiden uusinnat voidaan hyväksyä lopullisesti vasta, kun yrityksen tietosuojakäytäntö täyttää kaikki vaatimukset. Niiden on varsinkin käsitettävä nimenomainen sitoumus noudattaa asiaankuuluvia safe harbor -periaatteita, ja tietosuojaselosteen on oltava yleisesti saatavilla. Yrityksen on mainittava safe harbor -luettelossa esitetyissä tiedoissaan, missä sen tietosuojaseloste on saatavilla. Sen on myös nimettävä verkkosivuillaan vaihtoehtoinen riitojenratkaisuelin ja luotava linkki safe harbor -järjestelmään liittyvää omaa varmennusta käsitteleville kauppaministeriön verkkosivuille Arviolta yli 30 prosenttia järjestelmään kuuluvista yrityksistä ei tästä huolimatta esitä verkkosivuillaan julkaisemassaan tietosuojaselosteessa lainkaan tietoja riitojenratkaisusta.[28]

Suurin osa kauppaministeriön safe harbor -luettelostaan poistamista yrityksistä poistettiin niiden omasta pyynnöstä (esimerkiksi siksi, että ne olivat fuusioituneet tai ne oli ostettu, tai koska ne olivat vaihtaneet toimialaa tai lopettaneet toimintansa). Vähäisempi määrä jäsenyydestä luopuneiden yritysten tietoja poistettiin luettelosta siksi, että yritysten ilmoittamat verkkosivut osoittautuivat toimimattomiksi ja niiden omaa varmennusta koskevien tietojen kohdalla oli jo usean vuoden ajan ollut merkintä *not curren*t.[29] On tärkeätä huomata, ettei yksikään näistä poistoista ilmeisesti johtunut siitä, että kauppaministeriön tekemässä todennuksessa olisi ilmennyt safe harbor -periaatteiden noudattamiseen liittyviä ongelmia.

Safe harbor -luettelo on yrityksen tietosuojasitoumuksista kertova julkinen tietolähde. **Sitoutumista safe harbor -periaatteiden noudattamiseen ei ole rajoitettu ajallisesti** niiden tietojen osalta, jotka yritys on saanut ollessaan oikeutettu safe harbor -etuihin, ja sen on edelleen sovellettava periaatteita tällaisiin tietoihin niin pitkään kuin se tallentaa, käyttää tai luovuttaa niitä, vaikka se myöhemmin jostain syystä jättäytyisi safe harbor -järjestelmän ulkopuolelle.

Safe harbor -järjestelmään hakeneita yrityksiä, jotka **eivät läpäisseet kauppaministeriön suorittamaa arviointia** ja joita ei siksi otettu safe harbor -luetteloon, on esiintynyt seuraavasti: Vuonna **2010** ensi kerran oman varmennuksensa antaneista 513 yrityksestä vain **6:ta prosenttia** (33 kpl) ei otettu safe harbor -luetteloon, koska ne eivät täyttäneet oman varmennuksen antamista koskevia kauppaministeriön vaatimuksia. Vuonna **2013** ensi kerran oman varmennuksensa antaneista 605 yrityksestä **12:ta prosenttia** (75 kpl) ei otettu safe

---

27 Komissiolle syyskuussa 2013 toimittamiensa tilastotietojen mukaan Yhdysvaltojen kauppaministeriö oli vuonna 2010 huomauttanut 18 prosentille (93 kpl) kaikista 512:sta ensi kerran oman varmennuksensa antaneista yrityksistä ja 16 prosentille (231 kpl) kaikista 1 417:sta uudelleenvarmennuksen tehneistä yrityksistä, että niiden on tehtävä parannuksia tietosuojakäytäntöönsä ja/tai safe harbor -järjestelmään liittymistä koskeviin hakemuksiinsa. Komission esittämiin vaatimuksiin kaikkien ilmoitusten tiukoista, huolellisista ja järjestelmällisistä tarkastuksista kauppaministeriö reagoi huomauttamalla syyskuun puoliväliin mennessä 56 prosentille (340 kpl) kaikkiaan 602:sta ensi kerran oman varmennuksensa antaneista yrityksistä ja 27 prosentille (493 kpl) 1 809:sta uudelleenvarmennuksen tehneistä yrityksistä, että niiden on tehtävä parannuksia tietosuojakäytäntöönsä.

28 Chris Connollyn (Galexia) puheenvuoro Euroopan parlamentin LIBE-valiokunnan järjestämässä julkisessa kuulemistilaisuudessa 7. lokakuuta 2013.

29 Joulukuusta 2011 lähtien Yhdysvaltojen kauppaministeriö on poistanut safe harbor -luettelosta kaikkiaan 323 yritystä: 94 yritystoiminnan lakkauttamisen vuoksi, 88 yritysoston tai fuusion vuoksi, 95 emoyhtiön pyynnöstä, 41 koska ne olivat toistuvasti jättäneet hakematta uudelleenvarmennusta ja 5 erinäisistä muista syistä.

harbor -luetteloon, koska ne eivät täyttäneet oman varmennuksen antamista koskevia kauppaministeriön vaatimuksia.

Valvonnan avoimuuden lisäämiseksi kauppaministeriön on vähintäänkin nimettävä verkkosivuillaan kaikki safe harbor -luettelosta poistetut yritykset ja kerrottava syyt siihen, miksi niiden omaa varmennusta ei ole uusittu. Ministeriön ylläpitämässä safe harbor -yritysten luettelossa olevan *not current* -merkinnän ei pitäisi olla pelkästään tiedottava, vaan sen yhteydessä pitäisi näkyä sekä sanallinen että graafinen **selkeä varoitus** siitä, ettei kyseinen yritys parhaillaan täytä safe harbor -vaatimuksia.

Kaikki yritykset eivät lisäksi vieläkään ole sisällyttäneet tietosuojakäytäntöihinsä kaikkia safe harbor -periaatteita. Edellä 3 luvussa mainitun avoimuusongelman lisäksi oman varmennuksensa antaneiden yritysten tietosuojaselosteista puuttuu usein selvä maininta tarkoituksista, joihin henkilötietoja kerätään, tai rekisteröidyn oikeudesta päättää itse, saako tietoja luovuttaa kolmansille osapuolille. Tällöin on syytä epäillä, noudattaako yritys ilmoitusta ja valintaa koskevia safe harbor -periaatteita. Ilmoitus ja valinta ovat keskeisen tärkeitä, jotta rekisteröidyt voivat itse valvoa, mitä heidän henkilötiedoillaan tehdään.

Safe harbor -järjestelmään kuulumisen kriittistä ensivaihetta eli safe harbor -periaatteiden sisällyttämistä yritysten tietosuojakäytäntöihin ei ole varmistettu riittävän hyvin. Kauppaministeriön olisi puututtava asiaan mitä kiireellisimmin luomalla menettely kyseisten periaatteiden noudattamiseksi yritysten käytännön toiminnassa ja niiden asiakassuhteissa. **Kauppaministeriön on seurattava aktiivisesti, että yritykset todella sisällyttävät safe harbor -periaatteet tietosuojakäytäntöihinsä**, eikä täytäntöönpanotoimien toteuttaminen saa jäädä vain rekisteröityjen itsensä esittämien valitusten varaan.

## 5 TÄYTÄNTÖÖNPANON VIRANOMAISVALVONTA

On olemassa useita menettelyjä, joilla voidaan valvoa safe harbor -järjestelmän täytäntöönpanoa ja joihin henkilö voi vedota, mikäli häntä koskeviin tietoihin ei ole sovellettu safe harbor -periaatteita.

Täytäntöönpanoperiaate edellyttää, että oman varmennuksensa antaneiden organisaatioiden tietosuojakäytännöt sisältävät tehokkaan menettelyn, jolla varmistetaan safe harbor -periaatteiden noudattaminen. Täytäntöönpanoperiaatetta selostetaan tarkemmin FAQ 11:ssä, FAQ 5:ssä ja FAQ 6:ssa, ja sen mukaisesti tämä vaatimus voidaan täyttää käyttämällä **riippumatonta valitusmenettelyä**, josta vastaava organisaatio on julkisesti ilmoittanut olevansa toimivaltainen käsittelemään safe harbor -periaatteiden noudattamatta jättämistä koskevia yksittäisiä valituksia. Toinen vaihtoehto on se, että organisaatio sitoutuu yhteistyöhön **EU:n tietosuojapaneelin** kanssa.[30] Oman varmennuksensa antaneet yritykset kuuluvat lisäksi FTC:n toimivaltaan Federal Trade Commission -lain 5 §:n nojalla, jossa kielletään kauppaa koskevat tai kauppaan vaikuttavat sopimattomat tai harhaanjohtavat toimet tai käytännöt.[31]

Komissio toi vuoden 2004 kertomuksessaan myös esiin huolensa Safe harbor -järjestelmän täytäntöönpanosta, sillä se katsoi, että FTC:n olisi aktiivisemmin käynnistettävä tutkimuksia

30 EU:n tietosuojapaneeli on toimivaltainen tutkimaan ja ratkaisemaan yksityishenkilöiden tekemät valitukset, joissa väitetään safe harbor -järjestelmään kuuluvan yhdysvaltalaisen yrityksen rikkoneen safe harbor -periaatteita. Yritysten, jotka ilmoittavat noudattavansa safe harbor -periaatteita, on sitouduttava joko käyttämään riippumatonta valitusmenettelyä tai tekemään yhteistyötä EU:n tietosuojapaneelin kanssa sellaisten ongelmien ratkaisemiseksi, jotka johtuvat safe harbor -periaatteiden noudattamatta jättämisestä. Yhteistyö EU:n tietosuojapaneelin kanssa on kuitenkin pakollista, jos kyseinen yhdysvaltalainen yritys käsittelee henkilöstöä koskevia henkilötietoja työsuhteen yhteydessä. Jos yritys sitoutuu yhteistyöhön EU:n tietosuojapaneelin kanssa, sen on myös sitouduttava noudattamaan paneelin antamia ohjeita, joiden mukaan sen on safe harbor -periaatteiden noudattamiseksi toteutettava erityistoimia, joihin kuuluvat myös oikeuskeinot ja korvaukset.

31 Yhdysvaltojen liikenneministeriöllä on samankaltainen toimivalta lentoyhtiöihin nähden United States Coden 49 osaston 41712 §:n perusteella.

ja tiedotettava kansalaisille näiden oikeuksista. Se piti huolestuttavana myös sitä, että on epäselvää, ulottuuko periaatteita koskeva FTC:n täytäntöönpanotoimivalta henkilöstötietoihin.

EU:n tietosuojapaneeli, joka on henkilöstöä koskevista tiedoista vastaava valituselin, on vastaanottanut yhden valituksen, jonka aiheena ovat henkilöstöä koskevat tiedot.[32] Sen perusteella, että valituksia ei ole tehty, ei kuitenkaan voida päätellä järjestelmän toimivan täysin moitteettomasti. Olisi otettava käyttöön viran puolesta tehtäviä tarkastuksia sen varmistamiseksi, että tietosuojasitoumuksia todella noudatetaan. Lisäksi EU:n tietosuojaviranomaisten olisi ryhdyttävä toimiin paneelin olemassaolosta tiedottamiseksi.

Ongelmia on aiheuttanut myös tapa, jolla vaihtoehtoiset riitojenratkaisuelimet toimivat täytäntöönpanoeliminä. Monilla niistä ei ole asianmukaisia keinoja päättää seuraamuksista tapauksissa, joissa safe harbor -periaatteita ei ole noudatettu. Tämä puute on korjattava.

### 5.1 Federal Trade Commission

Federal Trade Commission (FTC, liittovaltion kilpailuviranomainen) voi toteuttaa täytäntöönpanotoimenpiteitä silloin, kun yritykset ovat toimineet safe harbor -sitoumustensa vastaisesti. Kun safe harbor -järjestelmä perustettiin, FTC sitoutui asettamaan tarkastelussaan etusijalle kaikki EU:n jäsenvaltioiden viranomaisten sille toimittamat tapaukset.[33] Koska FTC ei järjestelmän ensimmäisinä kymmenenä toimintavuotena saanut yhtään valitusta, se päätti pyrkiä kaikkien yksityisyyden suojaa ja tietosuojaa koskevien tutkimustensa yhteydessä selvittämään, oliko safe harbor -periaatteita loukattu. FTC on vuodesta 2009 lähtien toteuttanut 10 täytäntöönpanotoimea safe harbor -periaatteita loukanneita yrityksiä vastaan. Täytäntöönpanotoimet ovat muun muassa johtaneet huomattavia sakkoja käsittäviin FTC:n määräyksiin, joissa kielletään harhaanjohtavien tietojen antaminen yksityisyydensuojasta, myös safe harbor -periaatteiden noudattamisesta, ja joissa yritykset velvoitetaan ottamaan käyttöön kattavat tietosuojakäytännöt ja yksityisyyden suojaa koskevat tarkastukset 20 vuoden ajaksi. Yritysten on suostuttava siihen, että niiden tietosuojakäytännöistä suoritetaan riippumattomia arviointeja FTC:n pyynnöstä. Näistä arvioinneista raportoidaan säännöllisesti FTC:lle. FTC:n määräyksissä kielletään kyseisiä yrityksiä myös antamasta harhaanjohtavia tietoja tietosuojakäytännöistään ja osallistumisestaan safe harbor -järjestelmään tai muihin vastaaviin tietosuojajärjestelyihin. Tästä oli kyse muun muassa Googlea, Facebookia ja Myspacea koskevissa FTC:n tutkimuksissa.[34] Google suostui vuonna 2012 maksamaan 22,5 miljoonan Yhdysvaltain dollarin sakot, koska sen väitettiin rikkoneen sovintomääräystä (*consent order*). FTC selvittää kaikkien yksityisyydensuojatutkimustensa yhteydessä viran puolesta, onko safe harbor -periaatteita loukattu.

FTC on hiljattain toistanut aiemmat lausumansa sekä sitoumuksensa asettaa tarkastelussaan etusijalle tapaukset, joita sille toimittavat yksityisyydensuojan itsesääntelystä vastaavat yritykset ja EU:n jäsenvaltiot, jotka katsovat, ettei safe harbor -periaatteita ole noudatettu.[35]

---

32 Koska valituksen oli tehnyt Sveitsin kansalainen, EU:n tietosuojapaneeli siirsi sen Sveitsin tietosuojaviranomaisten käsiteltäväksi (Yhdysvalloilla on erillinen safe harbor -järjestelmä Sveitsin kanssa).

33 Katso 26. heinäkuuta 2000 tehdyn komission päätöksen 2000/520/EY liite V.

34 FTC on vuosina 2009–2012 saattanut päätökseen 10 safe harbor -sitoumuksiin liittyvää täytäntöönpanotoimea: FTC v. Javian Karnani ja Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011) ja Myspace LLC (2012). Ks. ”Federal Trade Commission of Safe Harbour Commitments”: http: //export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Ks. myös ”Case Highlights”: http: //business.ftc.gov/us-eu-Safe-Harbour-framework. Useimmissa ongelmatapauksissa oli kyse sellaisista harbor -järjestelmään liittyneistä yrityksistä, jotka myöhemmin väittivät kuuluvansa järjestelmään, vaikka olivat jättäneet uusimatta vuosittaisen varmennuksensa.

35 Tämän sitoumuksen toisti FTC:n jäsen Julie Brill kokouksessa, joka pidettiin EU:n tietosuojaviranomaisten (29 artiklan mukaisen tietosuojatyöryhmän) kanssa Brysselissä 17. huhtikuuta 2013.

Eurooppalaiset tietosuojaviranomaiset ovat kolmen viime vuoden aikana toimittaneet FTC:n käsiteltäväksi vain muutamia tapauksia.

Tietosuojaviranomaisten välinen transatlanttinen yhteistyö on alkanut kehittyä viime kuukausina. FTC esimerkiksi allekirjoitti 26. kesäkuuta 2013 Irlannin tietosuojavaltuutetun kanssa yhteistyömuistion keskinäisestä avunannosta sellaisten lakien täytäntöönpanossa, joilla suojellaan henkilötietoja yksityisellä sektorilla. Muistiossa luodaan puitteet tietosuojalainsäädännön täytäntöönpanoyhteistyön lisäämiselle, yksinkertaistamiselle ja tehostamiselle.[36]

FTC ilmoitti elokuussa 2013 tehostavansa entisestään sellaisten yritysten tarkastuksia, joilla on hallussaan henkilötietoja sisältäviä suuria tietokantoja. Se on myös perustanut verkkosivuston, jolla kuluttajat voivat tehdä yksityisyyden suojaa koskevan valituksen yhdysvaltalaisista yrityksistä.[37]

FTC:n olisi myös tutkittava tehokkaammin safe harbor -periaatteiden noudattamista koskevat perusteettomat väitteet. Yritys, joka verkkosivuillaan väittää noudattavansa safe harbor -periaatteita mutta jota ei ole kirjattu Yhdysvaltojen kauppaministeriön ylläpitämään järjestelmässä mukana olevien luetteloon, johtaa kuluttajia harhaan ja käyttää väärin heidän luottamustaan. Perusteettomat väitteet heikentävät koko järjestelmän uskottavuutta, joten ne olisi välittömästi poistettava kyseisten yritysten verkkosivuilta. Nämä yritykset olisi velvoitettava täytäntöönpanokelpoisella vaatimuksella olemaan johtamatta kuluttajia harhaan. FTC:n olisi jatkossakin pyrittävä tunnistamaan safe harbor -järjestelmään kuulumista koskevia perusteettomia väitteitä, jollaisesta oli kyse esimerkiksi Javian Karnania vastaan nostetussa oikeusjutussa. Kyseisessä tapauksessa FTC sulki kalifornialaisen verkkosivuston, koska se sisälsi perusteettoman väitteen safe harbor -rekisteröinnistä ja sen kautta harjoitettiin vilpillistä sähköistä kaupankäyntiä, joka kohdistui eurooppalaisiin kuluttajiin.[38]

FTC ilmoitti 29. lokakuuta 2013 ”käynnistäneensä viime kuukausina useita safe harbor -periaatteiden noudattamista koskevia tutkimuksia” ja että ”lähikuukausina” oli odotettavissa asiaa koskevia uusia täytäntöönpanotoimia. Se myös vahvisti olevansa ”sitoutunut etsimään keinoja tehokkuutensa parantamiseksi” ja ”ottavansa jatkossakin mielellään vastaan kaikki merkittävät johtolangat, jollainen oli Euroopassa toimivalta kuluttaja-asiamieheltä syyskuussa saatu valitus, jossa mainittiin lukuisia väitettyjä safe harbor -periaatteiden loukkauksia”.[39] FTC sitoutui lisäksi ”seuraamaan järjestelmällisesti safe harbor -määräysten noudattamista, kuten se seuraa kaikkien määräysten noudattamista”.[40]

FTC ilmoitti Euroopan komissiolle 12. marraskuuta 2013, että ”**jos yrityksen tietosuojaselosteessa luvataan safe harbor -suoja, pelkästään se, että kyseinen yritys ei rekisteröidy tai pidä rekisteröitymistään voimassa, ei todennäköisesti estä FTC:tä toteuttamasta kyseisiä safe harbor -sitoumuksia koskevia täytäntöönpanotoimia**”[41].

Yhdysvaltojen kauppaministeriö ilmoitti marraskuussa 2013 Euroopan komissiolle ”ryhtyvänsä ottamaan yhteyttä safe harbor -yrityksiin kuukautta ennen niiden varmennuksen uusimispäivää kertoakseen niille, kuinka niiden on toimittava, jos ne eivät aio uusia varmennustaan. Näin kauppaministeriö pyrkii osaltaan varmistamaan, että yritykset eivät perusteettomasti väitä kuuluvansa safe harbor -järjestelmään”. **Kauppaministeriö** totesi

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Kuluttajat voivat tehdä valituksen seuraavan FTC-sivuston kautta: https://www.ftccomplaintassistant.gov/. Kansainväliset kuluttajat voivat tehdä valituksen seuraavan sivuston kautta: http://www.econsumer.gov.

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf ja http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf.

40 FTC:n puheenjohtajan Edith Ramirezin kirje varapuheenjohtaja Viviane Redingille.

41 FTC:n puheenjohtajan Edith Ramirezin kirje varapuheenjohtaja Viviane Redingille.

”**määräävänsä tällaiset yritykset** poistamaan tietosuojaselosteestaan ja verkkosivuiltaan kaikki viittaukset safe harbor -järjestelmään osallistumiseen sekä kauppaministeriön safe harbor -sertifiointimerkin **ja ilmoittavansa niille selvästi, että määräyksen noudattamatta jättäminen saattaa johtaa FTC:n täytäntöönpanotoimiin**”.[42]

Safe harbor -järjestelmään kuulumista koskevien perusteettomien väitteiden vähentämiseksi olisi oman varmennuksensa antaneiden yritysten verkkosivuilla julkaistujen tietosuojaselosteiden aina sisällettävä linkki Yhdysvaltojen kauppaministeriön safe harbor -verkkosivuille, joilla on luettelo järjestelmässä kulloinkin mukana olevista yrityksistä. Näin eurooppalaiset rekisteröidyt voivat välittömästi ja ilman lisähakuja tarkistaa, onko kyseisen yrityksen safe harbor -jäsenyys voimassa. Yhdysvaltojen kauppaministeriö on maaliskuusta 2013 lähtien pyytänyt yrityksiä toimimaan näin, mutta prosessia olisi tehostettava.

Järjestelmän asianmukaisen ja tehokkaan toiminnan varmistamiseksi on edelleen ensisijaisen tärkeää, että edellä kuvattujen Yhdysvaltojen kauppaministeriön toteuttamien toimenpiteiden lisäksi FTC jatkuvasti valvoo safe harbor -periaatteiden noudattamista ja toteuttaa tarvittaessa täytäntöönpanotoimia. On erityisen tärkeää entistä useammin **tarkastaa ja tutkia omaaloitteisesti, noudattavatko yritykset** safe harbor -periaatteita. Periaatteiden noudattamatta jättämistä koskevien valitusten tekemistä FTC:lle olisi myös edelleen helpotettava.

## 5.2 EU:n tietosuojapaneeli

EU:n tietosuojapaneeli on perustettu safe harbor -päätöksellä. Se on toimivaltainen tutkimaan yksityishenkilöiden tekemiä valituksia, jotka koskevat työsuhteen yhteydessä kerättyjä henkilötietoja, ja tapauksia, jotka koskevat oman varmennuksensa antaneita yrityksiä, jotka ovat valinneet safe harbor -järjestelmässä tämän riitojenratkaisumenettelyn (53 prosenttia kaikista yrityksistä). EU:n tietosuojapaneeli koostuu EU:n eri tietosuojaviranomaisten edustajista.

Tähän mennessä paneeli on saanut neljä valitusta (kaksi vuonna 2010 ja kaksi vuonna 2013). Vuonna 2010 se siirsi kaksi valitusta kansallisten (Yhdistyneen kuningaskunnan ja Sveitsin) tietosuojaviranomaisten käsiteltäväksi. Kolmas ja neljäs valitus ovat parhaillaan käsiteltävinä. Valitusten vähäinen määrä selittyy sillä, että paneelin toimivalta rajoittuu tietynlaisiin tietoihin, kuten edellä on todettu.

Paneelin käsiteltäväksi tulevien tapausten vähäisyys voi johtua myös siitä, että sen olemassaolosta ei tiedetä. Komissio on vuodesta 2004 lisännyt paneelia koskevien tietojen näkyvyyttä verkkosivuillaan.[43]

Jotta paneelia hyödynnettäisiin entistä paremmin, olisi niiden yhdysvaltalaisten yritysten, jotka ovat päättäneet tehdä yhteistyötä paneelin kanssa ja noudattaa sen päätöksiä joidenkin tai kaikkien niiden omassa varmennuksessa mainittujen henkilötietotyyppien osalta, mainittava siitä selvästi ja näkyvästi tietosuojaselosteeseensa sisältyvissä sitoumuksissa, jotta Yhdysvaltojen kauppaministeriö voi tutkia asian. EU:n kaikkien tietosuojaviranomaisten verkkosivuille olisi perustettava erityinen safe harbor -sivu tiedon lisäämiseksi asiasta eurooppalaisten yritysten ja rekisteröityjen keskuudessa.

---

42 ”U.S.-EU Cooperation to Implement the Safe Harbor Framework”, 12. marraskuuta 2013.

43 Vuoden 2004 kertomuksen mukaan komission verkkosivuilla (oikeusasioiden pääosasto) oli julkaistu kysymysten ja vastausten muodossa EU:n tietosuojapaneelin ilmoitus, jonka tarkoituksena oli lisätä yksityishenkilöiden tietoisuutta ja auttaa heitä tekemään valitus, mikäli he katsovat henkilötietojaan käsitellyn safe harbor -periaatteiden vastaisesti: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Valituslomake on saatavissa seuraavassa osoitteessa: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf

### 5.3 Täytäntöönpanon parantaminen

Edellä mainitut puutteet avoimuudessa ja täytäntöönpanossa ovat johtaneet siihen, että eurooppalaiset yritykset epäilevät safe harbor -järjestelmän vaikuttavan haitallisesti kilpailukykyynsä. Kun eurooppalainen yritys kilpailee sellaisen yhdysvaltalaisyrityksen kanssa, joka kuuluu safe harbor -järjestelmään mutta ei käytännössä noudata järjestelmän periaatteita, sen kilpailuasema on huonompi kuin yhdysvaltalaisyrityksen.

Lisäksi FTC:n toimivaltaan kuuluvat ”kauppaa koskevat tai kauppaan vaikuttavat” sopimattomat tai harhaanjohtavat toimet tai käytännöt. Federal Trade Commission -lain 5 §:ssä säädetään poikkeuksista FTC:n sopimattomia tai harhaanjohtavia toimia tai käytäntöjä koskevaan toimivaltaan muun muassa **televiestintäoperaattoreiden** osalta. Koska televiestintäoperaattorit eivät kuulu FTC:n täytäntöönpanotoimivallan piiriin, ne eivät voi liittyä safe harbor -järjestelmään. Teknologioiden ja palvelujen lähentyessä yhä enemmän toisiaan, monet niiden yhdysvaltalaisista tietotekniikka-alan suorista kilpailijoista kuitenkin kuuluvat safe harbor -järjestelmään. Osa eurooppalaisista televiestintäoperaattoreista on huolissaan siitä, että televiestintäoperaattorit eivät voi osallistua safe harbor -järjestelmän mukaiseen tiedonvaihtoon. Alan eurooppalainen kattojärjestö, Euroopan kiinteän verkon operaattoreiden järjestö (European Telecommunications Network Operators’ Association, ETNO) katsoo, että tämä on selkeässä ristiriidassa televiestintäoperaattoreiden tärkeimmän pyynnön kanssa, joka koskee yhtäläisiä toimintamahdollisuuksia.[44]

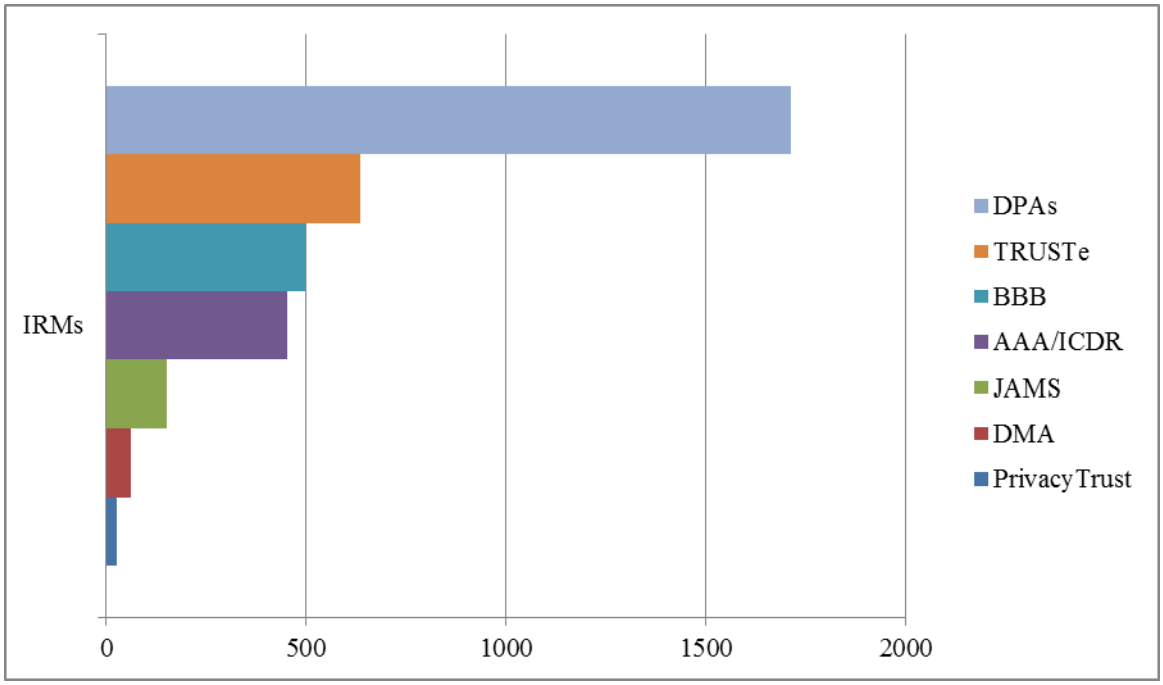
## 6 YKSITYISYYDEN SUOJAA KOSKEVIEN SAFE HARBOR -PERIAATTEIDEN VAHVISTAMINEN

### 6.1 Vaihtoehtoinen riitojenratkaisu

Täytäntöönpanoperiaate edellyttää, että on olemassa **helposti käytettävissä oleva ja kohtuuhintainen riippumaton valitusmenettely**, jolla tutkitaan yksityishenkilöiden valitukset ja ratkaistaan kiistat. Tätä varten safe harbor -järjestelmässä perustetaan vaihtoehtoinen riitojenratkaisujärjestelmä[45], jossa ratkaisijana toimii riippumaton kolmas osapuoli ja jonka avulla yksityishenkilöt voivat saada asiaansa nopean ratkaisun. Kolme tärkeintä valituselintä ovat EU:n tietosuojapaneeli, BBB (Better Business Bureaus) ja TRUSTe.

44 Komission 4. lokakuuta 2013 vastaanottamassa asiakirjassa ”ETNO considerations” käsitellään myös seuraavia aiheita: 1) henkilötietojen määritelmä safe harbor -järjestelmässä, 2) safe harbor -järjestelmän valvonnan puute ja 3) se, että yhdysvaltalaiset yritykset voivat siirtää tietoja huomattavasti vähemmin rajoituksin kuin eurooppalaiset yritykset, mikä merkitsee eurooppalaisten yritysten selkeää syrjintää ja vaikuttaa niiden kilpailukykyyn. Safe harbor -sääntöjen mukaan organisaatio voi antaa tietoja kolmannelle osapuolelle ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Organisaatio voi halutessaan antaa tietoja kolmannelle osapuolelle, joka toimii kyseisen organisaation puolesta, jos se ensin varmistaa, että kolmas osapuoli noudattaa safe harbor -periaatteita tai on direktiivin tai muun tietosuojan riittävyyden takaavan säädöksen alainen, taikka jos organisaatio tekee kolmannen osapuolen kanssa kirjallisen sopimuksen, jossa vaaditaan, että kolmas osapuoli tarjoaa vähintään samantasoisen suojan kuin vastaavilla safe harbor -periaatteilla taataan.

45 Kuluttajariitojen vaihtoehtoisesta riidanratkaisusta annetussa EU:n direktiivissä 2013/11/EU korostetaan riippumattomien, puolueettomien, avointen, tehokkaiden, nopeiden ja oikeudenmukaisten vaihtoehtoisten riidanratkaisumenettelyjen tärkeyttä.




Vaihtoehtoisen riitojenratkaisun käyttö on lisääntynyt vuoden 2004 jälkeen, ja Yhdysvaltojen kauppaministeriö on tehostanut yhdysvaltalaisten vaihtoehtoisten riitojenratkaisuelinten seurantaa sen varmistamiseksi, että niiden valitusmenettelystä antamat tiedot ovat selkeitä, helposti saatavilla ja helposti ymmärrettäviä. Järjestelmän tehokkuus ei kuitenkaan ole vielä joutunut koetukselle, koska käsiteltäviä tapauksia on ollut hyvin vähän.[46]

Vaikka Yhdysvaltojen kauppaministeriö on onnistunut laskemaan vaihtoehtoisten riitojenratkaisuelinten veloittamia maksuja, kaksi seitsemästä tärkeimmästä vaihtoehtoisesta riitojenratkaisuelimestä perii edelleen maksun valituksen tekeviltä yksityishenkilöiltä.[47] Safe harbor -järjestelmään kuuluvista yrityksistä noin 20 prosenttia käyttää tällaisia vaihtoehtoisia riitojenratkaisuelimiä. Ne ovat valinneet vaihtoehtoisen riitojenratkaisuelimen, joka perii kuluttajilta maksun valituksen tekemisestä. Tällainen menettely on vastoin safe harbor -järjestelmän täytäntöönpanoperiaatetta, jonka mukaan yksityishenkilöillä on oikeus ”helposti käytettävissä olevaan ja kohtuuhintaiseen riippumattomaan valitusmenettelyyn”. Euroopan unionissa EU:n tietosuojapaneelin tarjoama riippumaton riitojenratkaisupalvelu on maksuton kaikille rekisteröidyille.

46 Yksi merkittävimmissä palveluntarjoajista (TRUSTe) esimerkiksi kertoi saaneensa vuonna 2010 881 pyyntöä, mutta niistä vain kolmea pidettiin perusteltuina ja voitiin ottaa käsiteltäväksi. Ne johtivat siihen, että kyseisiä yrityksiä vaadittiin tekemään muutoksia tietosuojakäytäntöönsä ja verkkosivuihinsa. Vuonna 2011 valituksia saatiin 879, ja yhdessä tapauksessa yritys joutui muuttamaan tietosuojakäytäntöään. Yhdysvaltojen kauppaministeriön mukaan valtaosa vaihtoehtoisille riitojenratkaisuelimille tehdyistä valituksista tulee kuluttajilta, esimerkiksi käyttäjiltä, jotka ovat unohtaneet salasanansa eivätkä ole saaneet sitä internet-palvelusta. Komission esittämien useiden pyyntöjen jälkeen Yhdysvaltojen kauppaministeriö laati uudet tilastointiperusteet, joita kaikkien vaihtoehtoisten riitojenratkaisuelinten on käytettävä. Uusissa perusteissa erotetaan toisistaan pelkät pyynnöt ja valitukset, ja valitustyyppi on yksilöitävä selvemmin. Uusista perusteista on kuitenkin vielä keskusteltava sen varmistamiseksi, että vuoden 2014 uudet tilastot koskevat kaikkia vaihtoehtoisia riitojenratkaisuelimiä, ovat vertailukelpoisia ja tuottavat olennaisia tietoja, joiden avulla valitusmenettelyn tehokkuutta voidaan arvioida.

47 International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA) veloittaa 200 Yhdysvaltain dollarin ja JAMS 250 Yhdysvaltain dollarin käsittelymaksun. Yhdysvaltojen kauppaministeriö ilmoitti komissiolle tehneensä yhteistyötä AAA:n kanssa – joka oli yksityishenkilöille kallein riitojenratkaisuelin – kehittääkseen safe harbor -järjestelmää koskevan erityisohjelman, jonka avulla saatiin alennettua kuluttajille koituvat kustannukset useista tuhansista dollareista kiinteään 200 dollarin summaan.

Yhdysvaltojen kauppaministeriö vahvisti 12. marraskuuta 2013, että se jatkaa työtä EU:n kansalaisten yksityisyyden hyväksi ja tekee yhteistyötä vaihtoehtoisten riitojenratkaisuelinten kanssa sen selvittämiseksi, voiko näiden perimiä maksuja vielä alentaa.

Kaikilla vaihtoehtoisilla riitojenratkaisuelimillä ei ole mahdollisuutta määrätä seuraamuksia tapauksissa, joissa safe harbor -periaatteita ei ole noudatettu. Kaikkien vaihtoehtoisten riitojenratkaisuelinten määräämiin seuraamuksiin tai toimenpiteisiin ei myöskään näytä kuuluvan rikkomistapausten julkistaminen.

Vaihtoehtoisten riitojenratkaisuelinten on myös saatettava FTC:n käsiteltäväksi tapaukset, joissa yritys ei noudata vaihtoehtoisen riitojenratkaisumenettelyn lopputulosta tai ei hyväksy riitojenratkaisuelimen päätöstä, jotta FTC voi arvioida ja tutkia tapaukset sekä toteuttaa tarvittaessa täytäntöönpanotoimenpiteitä. Vaihtoehtoiset riitojenratkaisuelimet eivät kuitenkaan toistaiseksi ole saattaneet safe harbor -periaatteiden rikkomistapauksia FTC:n käsiteltäväksi.[48]

Vaihtoehtoisten riitojenratkaisuelinten verkkosivuilla luetellaan niiden palveluja käyttävät yritykset (*Dispute Resolution Participants*). Näin kuluttajien on helppo tarkistaa, voiko yksityishenkilö tehdä valituksen kyseiselle riitojenratkaisuelimelle, jos hänelle tulee kiistaa tietyn yrityksen kanssa. Esimerkiksi BBB pitää luetteloa kaikista riitojenratkaisujärjestelmäänsä kuuluvista yrityksistä. Lukuisat yritykset väittävät kuitenkin kuuluvansa johonkin tiettyyn riitojenratkaisujärjestelmään, vaikka niitä ei mainita kyseisen vaihtoehtoisen riitojenratkaisuelimen osallistujaluetteloissa.[49]

Vaihtoehtoisten riitojenratkaisumenettelyjen olisi oltava riippumattomia ja kohtuuhintaisia sekä helposti yksityishenkilöiden käytettävissä. Valituksen tekemisen täytyy olla rekisteröidylle vaivatonta. Kaikkien vaihtoehtoisten riitojenratkaisuelinten olisi julkaistava verkkosivuillaan tilastot käsittelemistään valituksista sekä tarkat tiedot niiden lopputuloksista. Jotta riitojenratkaisusta tulisi tehokas, luotettava ja tuloksekas menettely, olisi myös seurannan avulla varmistettava, että vaihtoehtoisten riitojenratkaisuelinten tarjoamat tiedot menettelystä ja valituksen tekemisestä ovat selkeät ja helposti ymmärrettävät. On myös syytä toistaa, että safe harbor -periaatteiden rikkomistapausten julkistamisen olisi kuuluttava vaihtoehtoisten riitojenratkaisuelinten käytettävissä oleviin seuraamuksiin.

### 6.2 Tiedon siirtäminen edelleen

Tietovirtojen kasvaessa räjähdysmäisesti on tarpeen varmistaa henkilötietojen jatkuva suojelu niiden kaikissa käsittelyvaiheissa ja etenkin silloin, kun safe harbor -järjestelmään kuuluva yritys siirtää tietoja **ulkopuoliselle käsittelijälle**. Tarve parantaa safe harbor -järjestelmän täytäntöönpanoa koskee näin ollen safe harbor -järjestelmään kuuluvien yritysten lisäksi niiden alihankkijoita.

Safe harbor -järjestelmässä organisaatio voi antaa tietoja kolmannelle osapuolelle, joka toimii kyseisen organisaation puolesta, jos se ensin ”varmistaa, että kolmas osapuoli noudattaa safe harbor -periaatteita tai on direktiivin tai muun tietosuojan riittävyyden takaavan säädöksen alainen, taikka jos organisaatio tekee kolmannen osapuolen kanssa kirjallisen sopimuksen, jossa vaaditaan, että kolmas osapuoli tarjoaa vähintään samantasoisen suojan kuin vastaavilla

48 Ks. FAQ 11.

49 Esimerkkejä: Amazon on ilmoittanut Yhdysvaltojen kauppaministeriölle käyttävänsä riitojenratkaisuelimenään BBB:tä. BBB ei kuitenkaan ole maininnut Amazonia riitojenratkaisuja koskevassa osallistujaluettelossaan. Pilvipalvelujen tarjoaja Arsalon Technologies (www.arsalon.net) puolestaan mainitaan kyseisessä BBB:n luettelossa, vaikka se ei ole parhaillaan mukana safe harbor -järjestelmässä (tilanne 1. lokakuuta 2013). BBB:n, TRUSTen ja muiden vaihtoehtoisten riitojenratkaisuelinten olisi poistettava tai oikaistava varmennusväite. Ne olisi velvoitettava täytäntöönpanokelpoisella vaatimuksella varmentamaan vain safe harbor -järjestelmässä mukana olevia yrityksiä.

safe harbor -periaatteilla taataan”[50]. Yhdysvaltojen kauppaministeriö esimerkiksi vaatii, että pilvipalvelujen tarjoaja, joka vastaanottaa henkilötietoja käsiteltäväksi, tekee sopimuksen, vaikka se noudattaisi safe harbor -periaatteita.[51] Tätä koskeva säännös safe harbor -päätöksen liitteessä II ei kuitenkaan ole selvä.

Koska alihankkijoiden käyttö on lisääntynyt viime vuosina huomattavasti etenkin pilvipalvelujen yhteydessä, safe harbor -periaatteita noudattavan yrityksen olisi ennen tällaisen sopimuksen tekemistä ilmoitettava asiasta kauppaministeriölle ja julkaistava tietosuojatoimensa.[52]

Edellä mainitut kolme seikkaa, eli vaihtoehtoinen riitojenratkaisu, valvonnan tehostaminen ja tiedon siirtäminen edelleen, kaipaavat lisäselvennystä.

## 7 PÄÄSY SAFE HARBOR -JÄRJESTELMÄN PUITTEISSA SIIRRETTYIHIN TIETOIHIN

Yhdysvaltojen vakoiluohjelmien laajuudesta ja kattavuudesta vuoden 2013 aikana saadut tiedot ovat herättäneet epäilyjä sellaisten henkilötietojen suojelun jatkuvuudesta, jotka on siirretty laillisesti Yhdysvaltoihin safe harbor -järjestelmän mukaisesti. Esimerkiksi kaikki yritykset, jotka osallistuvat PRISM-ohjelmaan ja jotka sallivat Yhdysvaltojen viranomaisten pääsyn Yhdysvalloissa tallennettuihin ja käsiteltyihin tietoihin, näyttävät kuuluvan safe harbor -järjestelmään. Näin safe harbor -järjestelmästä on tullut yksi väylistä, joiden kautta Yhdysvaltojen tiedusteluviranomaiset pääsevät keräämään alun perin EU:ssa käsiteltyjä henkilötietoja.

Safe harbor -päätöksen liitteessä I säädetään, että safe harbor -periaatteiden noudattamista voidaan rajoittaa, jos se on tarpeen kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi, sekä lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä. Jotta perusoikeuksien rajoittaminen olisi oikeutettua, rajoitusten on oltava suppeita; ne on sisällytettävä yleisesti saatavilla olevaan lainsäädäntöön, ja niiden on oltava välttämättömiä ja kohtuullisia demokraattisessa yhteiskunnassa. Safe harbor -päätöksessä täsmennetään etenkin, että periaatteiden noudattamista voidaan rajoittaa vain ”**siinä määrin, kuin se on tarpeen**” kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi.[53] Safe harbor -järjestelmässä sallitaan poikkeuksellisesti tietojen käsittely kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi, mutta päätöstä hyväksyttäessä ei voitu

---

50 Ks. komission päätös 2000/520/EY, sivu 7 (tiedon siirtäminen edelleen).

51 Ks. ”Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing”: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Nämä huomautukset koskevat pilvipalveluja, jotka eivät kuulu safe harbor -järjestelmään. Konsulttiyritys Galexian (http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf) mukaan varsin suuri osa pilvipalvelujen tarjoajista kuuluu safe harbor -järjestelmään (ja noudattaa safe harbor -periaatteita). Niillä on yleensä monikerroksinen yksityisyyden suoja, jossa yhdistyvät suorat sopimukset asiakkaiden kanssa ja yleinen tietosuojakäytäntö. Muutamaa merkittävää poikkeusta lukuun ottamatta safe harbor -järjestelmään kuuluvat pilvipalvelujen tarjoajat noudattavat riitojenratkaisua ja täytäntöönpanoa koskevia keskeisiä säännöksiä. Järjestelmään kuulumista koskevia perusteettomia väitteitä esittäneiden luettelossa ei tällä hetkellä ole yhtään merkittävää pilvipalvelujen tarjoajaa.(Galexiaa edustava Chris Connolly Euroopan parlamentin LIBE-valiokunnan kuulemistilaisuudessa, jonka aiheena oli EU:n kansalaisten sähköinen joukkotarkkailu.)

53 Ks. safe harbor -päätöksen liite I: ”Näiden periaatteiden noudattamista voidaan rajoittaa a) siinä määrin, kuin se on tarpeen kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi, b) lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, joilla syntyy ristiriitaisia velvoitteita tai joilla selkeästi annetaan lupa tiettyyn toimintaan, sillä edellytyksellä, että aina tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi, c) jos direktiivissä tai jäsenvaltion lainsäädännössä sallitaan poikkeuksia ja jos tällaisia poikkeuksia sovelletaan vastaavissa yhteyksissä. Yksityisyyden suojan kohentamista koskevan tavoitteen mukaisesti organisaatioiden tulisi pyrkiä toteuttamaan nämä periaatteet täysimittaisesti ja avoimesti ja osoittamaan yksityisyyden suojaa koskevassa politiikassaan, missä kohdin edellä b kohdassa sallittuja periaatteiden poikkeuksia sovelletaan säännönmukaisesti. Jos vaihtoehto on sallittu periaatteiden ja/tai Yhdysvaltojen lainsäädännön nojalla, organisaatioiden odotetaan samasta syystä noudattavan tiukempaa suojaa, kun tämä on mahdollista.”

ennakoida, että tiedustelupalvelut pääsisivät käsiksi valtaviin määriin Yhdysvaltoihin kaupallisten liiketoimien yhteydessä siirrettyjä tietoja.

Lisäksi Yhdysvaltojen kauppaministeriön olisi avoimuuden ja oikeusvarmuuden vuoksi ilmoitettava Euroopan komissiolle kaikista laeista tai hallituksen asetuksista, jotka vaikuttavat yksityisyyden suojaa koskevien safe harbor -periaatteiden noudattamiseen.[54] Poikkeusten sallimista olisi seurattava tarkoin, eikä niitä saa käyttää **safe harbor -periaatteiden** mukaisen tietosuojan heikentämiseen.[55] Etenkin se, että Yhdysvaltojen viranomaiset ovat keränneet valtavia määriä safe harbor -järjestelmään kuuluvien yritysten käsittelemiä tietoja, uhkaa heikentää sähköisen viestinnän luottamuksellisuutta.

### 7.1 Kohtuullisuus ja välttämättömyys

EU:n ja Yhdysvaltain ad hoc -tietosuojatyöryhmän havaintojen mukaan Yhdysvaltojen lainsäädäntö sisältää useita oikeusperustoja, jotka sallivat Yhdysvaltoihin sijoittautuneiden yritysten tallentamien tai muulla tavoin käsittelemien henkilötietojen laajamittaisen keräämisen ja käsittelemisen. Tähän voi kuulua tietoja, jotka on aiemmin siirretty EU:sta Yhdysvaltoihin safe harbor -järjestelmän mukaisesti, ja onkin epävarmaa, sovelletaanko näihin tietoihin edelleen safe harbor -periaatteita. Koska ohjelmat ovat niin laajamittaisia, Yhdysvaltojen viranomaiset saattavat kerätä ja käsitellä safe harbor -järjestelmän mukaisesti siirrettyjä tietoja laajemmin kuin on ehdottoman välttämätöntä ja kohtuullista kansallisen turvallisuuden suojelemiseksi, mikä olisi vastoin safe harbor -päätöksessä säädettyä poikkeusta.

### 7.2 Rajoitukset ja valituskeinot

EU:n ja Yhdysvaltain ad hoc -tietosuojatyöryhmä on todennut, että Yhdysvaltojen lainsäädännön mukaiset suojakeinot ovat enimmäkseen vain Yhdysvaltojen kansalaisten ja Yhdysvalloissa laillisesti asuvien käytettävissä. EU:n tai Yhdysvaltojen rekisteröidyillä ei myöskään ole mahdollisuutta saada itseään koskevia tietoja tai saada ne oikaistuksi tai poistetuksi, eivätkä he voi valittaa hallinto- tai oikeusteitse Yhdysvaltojen vakoiluohjelmien puitteissa tapahtuvasta henkilötietojensa edelleenkäsittelystä.

### 7.3 Avoimuus

Yritykset eivät aina mainitse tietosuojaselosteessaan, milloin ne soveltavat poikkeuksia safe harbor -periaatteisiin. Yksityishenkilöt ja yritykset eivät siksi tiedä, mitä heitä ja niitä koskevilla tiedoilla tehdään. Tämä koskee erityisesti edellä tarkoitettuja Yhdysvaltojen vakoiluohjelmia ja niiden toimintaa. Yhdysvaltalaiset yritykset, joille on siirretty eurooppalaisten tietoja safe harbor -järjestelmän mukaisesti, eivät siis aina kerro asianomaisille, että näiden tietoja voidaan käsitellä edelleen.[56] Voidaankin kysyä, noudatetaanko avoimuutta koskevia safe harbor -periaatteita. Avoimuuden olisi oltava niin suurta kuin mahdollista ilman, että kansallinen turvallisuus vaarantuu. Sen lisäksi, että

---

54 ”Safe harbor” -periaatteiden tarjoaman tietosuojan tasosta 16. toukokuuta 2000 annettu 29 artiklan mukaisen tietosuojatyöryhmän lausunto 4/2000.

55 ”Safe harbor” -periaatteiden tarjoaman tietosuojan tasosta 16. toukokuuta 2000 annettu 29 artiklan mukaisen tietosuojatyöryhmän lausunto 4/2000.

56 Jotkin safe harbor -järjestelmään kuuluvat eurooppalaiset yritykset antavat tietoja verrattain avoimesti. Esimerkiksi Nokia, joka toimii myös Yhdysvalloissa ja kuuluu safe harbor -järjestelmään, toteaa tietosuojaselosteessaan seuraavaa:
*"Sitova lainsäädäntö saattaa velvoittaa meidät luovuttamaan henkilötietojasi tietyille viranomaisille tai muille kolmansille osapuolille, esimerkiksi lainvalvontaviranomaisille, maissa, joissa toimimme itse tai joissa kolmannet osapuolet toimivat puolestamme."*

yritysten on nykyisten vaatimusten mukaisesti mainittava tietosuojaselosteessaan, onko safe harbor -periaatteita rajoitettu lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, niitä olisi kannustettava mainitsemaan samassa yhteydessä, soveltavatko ne periaatteisiin poikkeuksia kansallisen turvallisuuden, yleisen edun tai lainsäädännön vaatimusten vuoksi.

## 8 PÄÄTELMÄT JA SUOSITUKSET

Vuonna 2000 perustettu safe harbor -järjestelmä muodostaa nykyään väylän, jonka kautta EU:sta siirtyy henkilötietoja Yhdysvaltoihin. Henkilötietojen tehokas suojelu niitä siirrettäessä on yhä tärkeämpää, koska digitaalisen talouden edellyttämät tietovirrat ovat kasvaneet räjähdysmäisesti ja tietojen kerääminen, käsittely ja käyttö ovat kehittyneet erittäin merkittävästi. Googlen, Facebookin, Microsoftin, Applen ja Yahoon kaltaisilla verkkoyhtiöillä on Euroopassa satoja miljoonia asiakkaita, ja ne siirtävät Yhdysvaltoihin käsiteltäväksi niin valtavia määriä henkilötietoja, ettei sitä voinut kuvitella vuonna 2000, kun safe harbor -järjestelmä luotiin.

Avoimuuden ja täytäntöönpanon puutteiden vuoksi järjestelmässä esiintyy yhä seuraavanlaisia ongelmia, jotka olisi ratkaistava:

a) safe harbor -järjestelmään kuuluvat organisaatiot eivät noudata avoimuusperiaatetta tietosuojakäytännöissään

b) yhdysvaltalaiset yritykset eivät todellisuudessa sovella safe harbor -periaatteita

c) täytäntöönpano on tehotonta.

Koska **tiedustelupalvelut ovat keränneet laajamittaisesti safe harbor -järjestelmään kuuluvien yritysten Yhdysvaltoihin siirtämiä tietoja**, on lisäksi syytä pohtia vakavasti, toteutuvatko eurooppalaisten tietosuojaoikeudet senkin jälkeen, kun heidän tietonsa on siirretty Yhdysvaltoihin.

Komissio on edellä sanotun pohjalta laatinut seuraavat **suositukset**:

**Avoimuus**

1. *Oman varmennuksensa antaneiden yritysten olisi julkaistava tietosuojaseloste.* Ei riitä, että yritykset toimittavat Yhdysvaltojen kauppaministeriöön kuvauksen tietosuojakäytännöstään, vaan niiden olisi asetettava verkkosivuilleen yleisesti saataville selkeä ja helppolukuinen tietosuojaseloste.

2. *Oman varmennuksensa antaneiden yritysten verkkosivuilla olevien tietosuojaselosteiden olisi aina sisällettävä linkki Yhdysvaltojen kauppaministeriön safe harbor -verkkosivuille, joilla luetellaan järjestelmässä kulloinkin mukana olevat yritykset.* Tällöin eurooppalaiset rekisteröidyt voivat välittömästi ja ilman lisähakuja tarkistaa, onko kyseisen yrityksen safe harbor -jäsenyys voimassa. Näin vähennettäisiin mahdollisuuksia esittää perusteettomia väitteitä safe harbor -järjestelmään kuulumisesta ja lisättäisiin siten järjestelmän uskottavuutta. Yhdysvaltojen kauppaministeriö on maaliskuusta 2013 lähtien pyytänyt yrityksiä toimimaan näin, mutta prosessia olisi tehostettava.

3. *Oman varmennuksensa antaneiden yritysten olisi julkaistava kaikkien sellaisten sopimustensa tietosuojaehdot, joita ne tekevät alihankkijoidensa, esimerkiksi pilvipalveluyritysten, kanssa.* Safe harbor -säännöissä sallitaan tietojen siirtäminen edelleen safe harbor -järjestelmään kuuluvilta yrityksiltä

sellaisille kolmansille osapuolille, jotka toimivat kyseisten yritysten puolesta, esimerkiksi pilvipalveluyrityksille. Komission käsityksen mukaan Yhdysvaltojen kauppaministeriö vaatii varmennuksensa antaneita yrityksiä tällöin tekemään sopimuksen. Sopimuksen tehdessään safe harbor -järjestelmään kuuluvan yrityksen olisi kuitenkin myös ilmoitettava asiasta Yhdysvaltojen kauppaministeriölle, ja se olisi velvoitettava julkaisemaan yksityisyyden takaavat suojatoimensa.

4. *Yhdysvaltojen kauppaministeriön verkkosivuilla olisi selvästi merkittävä kaikki yritykset, joiden jäsenyys järjestelmässä ei ole voimassa.* Yhdysvaltojen kauppaministeriön verkkosivuilla olevassa safe harbor -järjestelmään kuuluvien yritysten luettelossa olevaan *not current* (ei voimassa) -merkintään olisi liitettävä selkeä varoitus siitä, että kyseinen yritys ei parhaillaan täytä safe harbor -vaatimuksia. *Not current* -merkittyjen yritysten olisi kuitenkin edelleen sovellettava safe harbor -vaatimuksia kyseisen järjestelmän mukaisesti vastaanottamiinsa tietoihin.

**Valituskeinot**

5. Yritysten verkkosivuilla olevien tietosuojaselosteiden olisi sisällettävä linkki vaihtoehtoisen riitojenratkaisuelimen tai EU:n tietosuojapaneelin tai molempien verkkosivuille. Näin eurooppalaiset rekisteröidyt voivat ongelmatapauksessa ottaa välittömästi yhteyttä vaihtoehtoiseen riitojenratkaisuelimeen tai EU:n tietosuojapaneeliin. Yhdysvaltojen kauppaministeriö on maaliskuusta 2013 lähtien pyytänyt yrityksiä toimimaan näin, mutta prosessia olisi tehostettava.

6. Vaihtoehtoisen riitojenratkaisumenettelyn olisi oltava helposti käytettävissä ja kohtuuhintainen. Jotkin safe harbor -järjestelmään kuuluvista vaihtoehtoisista riitojenratkaisuelimistä perivät yksityishenkilöiltä yhä valituksen käsittelystä maksuja, jotka voivat olla näiden kannalta varsin korkeita (200–250 Yhdysvaltain dollaria). Sen sijaan Euroopassa safe harbor -järjestelmää koskevia valituksia käsittelevän tietosuojapaneelin käyttö on maksutonta.

7. Yhdysvaltojen kauppaministeriön olisi valvottava järjestelmällisemmin, julkaisevatko vaihtoehtoiset riitojenratkaisuelimet tietoja käyttämästään menettelystä ja seuraamuksista, joihin valitus voi johtaa, ja ovatko nämä tiedot helposti saatavilla. Näin riitojenratkaisumenettelystä tulee tehokas, luotettava ja tuloksekas. On myös syytä toistaa, että safe harbor -periaatteiden rikkomistapausten julkistamisen olisi kuuluttava vaihtoehtoisten riitojenratkaisuelinten käytettävissä oleviin seuraamuksiin.

**Täytäntöönpano**

8. *Safe harbor -järjestelmän mukaisesti varmennetuista tai uudelleenvarmennetuista yrityksistä olisi tutkittava viran puolesta tietty prosenttiosuus sen varmistamiseksi, että ne todella noudattavat tietosuojakäytäntöään (tutkimus ei koskisi pelkästään virallisten vaatimusten noudattamista).*

9. *Jos valituksen tai tutkimuksen perusteella havaitaan, että yritys ei noudata tietosuojakäytäntöään, kyseisessä yrityksessä olisi vuoden kuluttua suoritettava erityinen seurantatutkimus.*

10. *Jos epäillään, että jokin yritys ei noudata tietosuojakäytäntöään, tai yrityksestä on vireillä valitus, Yhdysvaltojen kauppaministeriön olisi ilmoitettava asiasta EU:n toimivaltaiselle tietosuojaviranomaiselle.*

11. *Safe harbor -järjestelmään kuulumista koskevat perusteettomat väitteet olisi jatkossakin tutkittava.* Yritys, joka verkkosivuillaan väittää noudattavansa safe harbor -vaatimuksia mutta jota ei ole kirjattu Yhdysvaltojen kauppaministeriön ylläpitämään, järjestelmässä mukana olevien yritysten luetteloon, johtaa kuluttajia harhaan ja käyttää väärin heidän luottamustaan. Perusteettomat väitteet heikentävät koko järjestelmän uskottavuutta, ja ne olisi siksi välittömästi poistettava kyseisten yritysten verkkosivuilta.

**Yhdysvaltojen viranomaisten pääsy tietoihin**

12. *Oman varmennuksensa antaneiden yritysten tietosuojaselosteissa olisi mainittava, missä määrin viranomaiset voivat Yhdysvaltojen lainsäädännön mukaisesti kerätä ja käsitellä safe harbor -järjestelmän puitteissa siirrettyjä tietoja. Yrityksiä olisi etenkin kannustettava mainitsemaan tietosuojaselosteissaan, milloin ne soveltavat safe harbor -periaatteisiin poikkeuksia kansallisen turvallisuuden, yleisen edun tai lainsäädännön vaatimusten vuoksi.*

13. *On tärkeää, että safe harbor -päätöksessä säädettyä kansalliseen turvallisuuteen perustuvaa poikkeusta käytetään vain silloin, kun se on ehdottoman välttämätöntä ja kohtuullista.*