**Oikeusministeriö** E-KIRJE OM2014-00098

LAVO Rantalankila Leena 18.03.2014

*Suuri valiokunta*

Asia
**EU/OSA; Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon**

**U/E/UTP-tunnus**

**EUTORI-tunnus**
EU/2013/1783, EU/2013/1782, EU/2013/1781

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys Euroopan komission 27.11.2013 esittämistä toimista, jotka se katsoo tarpeellisiksi luottamuksen palauttamiseksi EU:n ja Yhdysvaltain väliseen tietojen siirtoon tilanteessa, jossa Yhdysvaltain harjoittamaa laajamittaista tiedustelutietojen keruuta koskevat paljastukset ovat herättäneet syvää huolta ja vaikuttaneet haitallisesti transatlanttisiin suhteisiin.

Asko Välimaa
Ylijohtaja

Leena Rantalankila
Neuvotteleva virkamies

LIITTEET Oikeusministeriön muistio 6.3.2014 ja asiakirjat COM(2013)846 final, COM(2013) 847 final, 16987/13, COM(2013) 844 final ja COM(2013) 843 final

Viite

| | |
|---|---|
| Asiasanat | henkilötiedot, lentoliikenne, terrorismi, tietosuoja, Yhdysvallat, sähköinen viestintä |
| **Hoitaa** | **LVM, OM, SM, UM, VM** |
| Tiedoksi | ALR, EUE, MAVI, MMM, OKM, PE, PLM, STM, TEM, TPK, TRAFI, TULLI, VNK, YM |

LAVO Rantalankila Leena 06.03.2014

Asia
**EU/OSA; Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon**

Kokous

**U/E/UTP-tunnus**

## Käsittelyvaihe ja jatkokäsittelyn aikataulu

E-kirjeen tarkoituksena on informoida eduskuntaa Euroopan komission 27.11.2013 esittämistä toimista, jotka se katsoo tarpeellisiksi luottamuksen palauttamiseksi EU:n ja Yhdysvaltain väliseen tietojen siirtoon tilanteessa, jossa Yhdysvaltain harjoittamaa laajamittaista tiedustelutietojen keruuta koskevat paljastukset ovat herättäneet syvää huolta ja vaikuttaneet haitallisesti transatlanttisiin suhteisiin.

Komission esittämät toimet perustuvat heinäkuussa 2013 perustetun EU:n ja Yhdysvaltain tietosuojatyöryhmän tuloksiin, komission suorittamaan olemassa olevien EU:n ja Yhdysvaltain välisten tietojenvaihtosopimusten uudelleenarviointiin sekä EU:n ja Yhdysvaltain väliseen poliittiseen vuoropuheluun.

Komissio julkaisi 27.11.2013

1) tiedonannon luottamuksen palauttamisesta EU:n ja Yhdysvaltojen väliseen tietojen siirtoon

2) tiedonannon EU:n ja Yhdysvaltain välillä tapahtuvaa kaupallista tiedonsiirtoa sääntelevän safe harbor -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta

3) raportin heinäkuussa 2013 perustetun EU:n ja Yhdysvaltain tietosuojatyöryhmän tuloksista,

4) kertomuksen matkustajarekisteritietoja koskevan sopimuksen (EU-USA PNR-sopimus) yhteisestä tarkastelusta, ja

5) tiedonannon komission ja Yhdysvaltojen valtiovarainministeriön yhteisestä kertomuksesta, jossa tarkastellaan terrorismin rahoituksen jäljittämisohjelmaa koskevan sopimuksen (EU-USA TFTP -sopimus) hyödyllisyyttä

## Suomen kanta

Suomi ei hyväksy kansalaisiin kohdistuvaa oikeudetonta verkkoseurantaa. Suomi pitää ensisijaisen tärkeänä, että EU huolehtii siitä, että unionin kansalaiset ovat tietoisia heihin

kohdistuvasta oikeudettomasta verkkoseurannasta ja että kansalaisia informoidaan keinoista, joiden avulla verkkoseurantaa voidaan välttää.

Yhdysvaltojen NSA:n harjoittamaa laajamittaista urkintaa koskevat paljastukset ovat horjuttaneet vakavasti eurooppalaisten luottamusta verkkoviestintään. Kansalaisilla on perusteltu syy uskoa, että heidän oikeuttaan henkilötietojen suojaan ja yksityisyyteen on vakavasti loukattu. Internet on yhteiskunnallinen katalyytti, jonka onnistunut hyödyntäminen on tulevaisuudessa suomalaisen yhteiskunnan kenties tärkein hyvinvoinnin ja kasvun edellytys. On erittäin tärkeää, että luottamus digitaaliseen maailmaan pystytään säilyttämän, jotta jatkossakin voitaisiin hyödyntää internetin potentiaalia. Luottamus sähköisiin palveluihin on välttämätöntä, jos haluamme saada aikaan taloudellista kasvua ja uusia työpaikkoja niiden avulla. Suomen tulisi pyrkiä vahvistamaan mainettaan korkean tietosuojan ja tietoturvan maana sekä turvallisena ja luotettavana tiedon säilytyspaikkana. Luottamuksen palauttamiseksi sekä EU:n että Yhdysvaltojen tulisi pikaisesti sitoutua toimenpiteisiin, joilla luottamus voitaisiin pyrkiä palauttamaan. EU:n komission 27.11.2013 julkaisema tiedonanto luottamuksen palauttamisesta EU:n ja Yhdysvaltojen väliseen tietojen siirtoon ja presidentti Obaman linjapuhe 17. tammikuuta 2014 ovat hyvä pohja tälle työlle.

Koska komission tammikuussa 2012 ehdottamalla EU:n tietosuojalainsäädännön uudistuksella on merkittäviä ja laaja-alaisia vaikutuksia, on välttämätöntä, että uudistus toteutetaan huolellisesti valmistellulla hyvällä lainsäädännöllä. Uudistamistyön yhteydessä on tärkeää perusteellisesti selvittää, voidaanko ja missä määrin EU:n lainsäädännöllä estää edellä mainitun kaltainen kolmannen maan toimesta tapahtuva EU:n kansalaisten henkilötietojen väärinkäyttö.

Komission tavoin Suomi katsoo, että Yhdysvaltain viranomaisten olisi sitouduttava soveltamaan lainvalvontatarpeisiin perustuvissa tiedonsiirtovaatimuksissa pääsääntöisesti keskinäistä oikeusapua koskevaa sopimusta tai EU:n ja Yhdysvaltain välisiä alakohtaisia sopimuksia.

Yhdysvaltojen kanssa neuvoteltavana olevalla lainvalvonnan alan tietosuojapuitesopimuksella olisi taattava kansalaisille korkeatasoinen tietosuoja ja samat oikeudet Atlantin molemmin puolin. EU:n kansalaisille olisi taattava oikeus käyttää yhdysvaltalaisia oikeussuojakeinoja, vaikka he eivät asuisi Yhdysvalloissa.

Saatujen tietojen valossa Suomi pitää perusteltuna, että safe harbour -järjestelmää kehitetään siten, että rekisteröityjen yksityisyyden suojalle on riittävät takeet siirrettäessä tietoja järjestelmän puitteissa. Safe harbour-järjestelmän uudelleenarviointi olisi tehtävä mahdollisimman pian ja viimeistään syksyllä 2014.

Suomella ei ole toistaiseksi ollut juurikaan tarvetta TFTP-järjestelmän suoraan käyttöön. EU:n ja Yhdysvaltojen välinen TFTP -sopimus on kuitenkin selkeästi hyödyttänyt terrorismin torjuntaa EU:n alueella.

**Pääasiallinen sisältö**

Komissio katsoo, että tietojen siirtoa EU:n ja Yhdysvaltain välillä voidaan jatkaa vain, jos varmistetaan koreatasoinen tietosuoja. Komissio kehottaa 27.11.2013 julkaisemassaan lehdistötiedotteessa ryhtymään toimiin kuudella alalla:

**- EU:n tietosuojauudistuksen nopea vahvistaminen**

Komissio katsoo, että nyt jos koskaan tarvitaan vahvoja tietosuojasääntöjä, jotka ovat selkeät ja täytäntöönpanokelpoiset myös silloin, kun tietoja siirretään ulkomaille ja käsitellään ulkomailla. Sen vuoksi EU:n tietosuojauudistus tulisi saada hyväksyttyä keväällä 2014. Näin varmistetaan, että henkilötiedoilla on tehokas ja kattava suoja.

**- Safe Harbour -järjestelmästä turvallisempi**

Komissio antaa 13 suositusta järjestelmän toimivuuden parantamiseksi, koska järjestelmä toimii monessa suhteessa puutteellisesti. Korjaavia keinoja pitäisi löytää kesään 2014 mennessä, minkä jälkeen komissio arvioi järjestelyn toimivuutta antamiensa suositusten pohjalta.

**- Tietosuojatakeiden lujittaminen lainvalvonnan saralla**

Meneillään olevat neuvottelut tietosuojapuitesopimuksesta, joka koskee tiedonsiirtoa ja tietojen käsittelyä oikeus- ja poliisiyhteistyössä, olisi saatettava viipymättä päätökseen. Sopimuksella on taattava kansalaisille korkeatasoinen tietosuoja ja samat oikeudet Atlantin molemmin puolin. Etenkin olisi taattava EU:n kansalaisille oikeus käyttää yhdysvaltalaisia oikeussuojakeinoja, vaikka he eivät asuisi Yhdysvalloissa.

**- Keskinäistä oikeusapua koskevan sopimuksen ja alakohtaisten sopimusten käyttäminen tietojen saamiseksi**

Yhdysvaltain viranomaisten olisi sitouduttava soveltamaan lainvalvontatarpeisiin perustuvissa tiedonsiirtovaatimuksissa pääsääntöisesti keskinäistä oikeusapua koskevaa sopimusta tai EU:n ja Yhdysvaltain välisiä alakohtaisia sopimuksia (esim. matkustajarekisteritietoja koskevaa sopimusta eli ns. PNR-sopimusta tai terrorismin rahoituksen jäljittämisohjelmaa koskevaa sopimusta eli ns. TFTP-sopimusta) tai muuta vastaavaa oikeusperustaa. Suoraan yrityksille esitettävien tiedonantovaatimusten tulisi olla mahdollisia vain selkeästi määritellyissä poikkeustilanteissa, ja vaatimukset olisi voitava saattaa tuomioistuimen käsiteltäviksi.

**- Eurooppalaisiin huolenaiheisiin puuttuminen Yhdysvaltain uudistusprosessissa**

Yhdysvaltain presidentti Barack Obama on ilmoittanut, että maan kansallisten turvallisuusviranomaisten toimintaa tarkastellaan uudelleen. Prosessin tulisi hyödyttää myös EU:n kansalisia. Tärkeintä olisi ulottaa yhdysvaltalaisille annetut takeet koskemaan myös EU:n kansalaisia, vaikka nämä eivät asuisi Yhdysvalloissa, ja parantaa valvontaa.

**- Yksityisyyden suojaa koskevien sääntöjen edistäminen kansainvälisesti**

Yhdysvaltain olisi liityttävä yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskevaan Euroopan neuvoston yleissopimukseen, kuten se on liittynyt tietoverkkorikollisuutta koskevaan vuoden 2001 yleissopimukseen.

1) Komission tiedonanto luottamuksen palauttamisesta EU:n ja Yhdysvaltojen väliseen tietojen siirtoon (COM(2013) 846 final)

Transatlanttista tiedonsiirtoa koskevassa tiedonannossa määritetään Yhdysvaltain tiedustelutietojen hankintaohjelmia koskevista paljastuksista johtuvat haasteet ja riskit sekä toimet niihin puuttumiseksi.

Tiedonannossa todetaan, että luottamus EU:n ja Yhdysvaltain strategiseen kumppanuuteen on heikentynyt, joten nyt tarvitaan toimia sen palauttamiseksi. Yhdysvaltojen harjoittamaa laajamittaista tiedustelutietojen keruuta koskevat paljastukset ovat herättäneet syvää huolta EU:ssa erityisesti siltä osin kuin on kyse henkilötietojen suojasta. Yksityisen viestinnän joukkoseurantaa ei voida hyväksyä.

Henkilötietojen siirto on tärkeä ja välttämätön osa transatlanttisia suhteita. Se on olennainen osa Atlantin yli käytävää kauppaa. Henkilötietojen siirto on tärkeä osatekijä myös EU:n ja Yhdysvaltojen lainvalvonta-alan yhteistyössä ja jäsenvaltioiden ja Yhdysvaltojen yhteistyössä kansallisen turvallisuuden alalla. Yhdysvallat ja EU ovat useilla sopimuksilla ja järjestelyillä pyrkineet helpottamaan tietojen siirtoa ja samalla varmistamaan, että EU:n lainsäädännön edellyttämä korkeatasoinen tietosuoja säilytetään. Näitä välineitä käytetään toimintaympäristössä, jossa henkilötietojen siirron merkitys kasvaa koko ajan.

Digitalouden kehitys on johtanut siihen, että laadultaan ja luonteeltaan erilaisten tietojenkäsittelytoimien määrä on kasvanut voimakkaasti. Henkilötiedoista on tullut arvokasta omaisuutta. Sähköisen viestinnän ja tietojenkäsittelypalveluiden, muun muassa pilvipalveluiden, käytön lisääntyminen on lisännyt merkittävästi myös Atlantin yli tapahtuvan tiedonsiirron laajuutta ja merkitystä. Kuluttajatietojen laajamittaiseen käsittelyyn kaupallisia tarkoituksia varten on uusia menetelmiä ja tiedustelupalveluilla on aiempaa parempia valmiuksia viestintätietojen laajamittaiseen seurantaan.

Yhdysvaltojen käyttämät ohjelmat laajamittaiseen tiedustelutietojen keruuseen (esimerkiksi Prism-ohjelma) loukkaavat eurooppalaisten perusoikeuksia ja erityisesti heidän oikeuttaan yksityisyyteen ja henkilötietojen suojaan. Tämänkaltaiset ohjelmat viittaavat siihen, että viranomaisten harjoittaman valvonnan ja yksityisten yritysten, erityisesti yhdysvaltalaisten internet-yritysten, suorittaman tietojenkäsittelyn välillä on yhteys. Kasvu saattaa hidastua, jos luottamus digitalouteen heikentyy.

Tämä kehitys tuo uusia haasteita tietojen siirrolle EU:n ja Yhdysvaltojen välillä. Tiedonannossa tarkastellaan tulevia toimia niiden havaintojen pohjalta, jotka sisältyvät EU:n ja Yhdysvaltojen erityistyöryhmän EU:ta edustavien puheenjohtajien raporttiin ja safe harbour -järjestelmää koskevaan tiedonantoon. Tiedonannossa pyritään esittämään tehokas tapa palauttaa luottamus ja vahvistaa sekä EU:n ja Yhdysvaltojen välistä yhteistyötä näillä aloilla että transatlanttisia suhteita laajemminkin.

Tiedonannossa korostetaan, että kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla.

Tiedonannossa käsitellään vaikutuksia tietojen siirrossa käytettäviin safe harbour -järjestelmään ja lainvalvonnan alan PNR- ja TFTP-sopimuksiin sekä tietosuojan tehokkuuden varmistamista. Viimeksi mainittuun liittyen tiedonannossa käsitellään EU:n tietosuojauudistusta, safe harbour -järjestelmän turvallisuuden lisäämistä, tietosuojatakeiden lujittamista lainvalvonta-alan yhteistyössä, eurooppalaisten näkökohtien huomioon ottamista Yhdysvalloissa meneillään olevassa uudistusprosessissa ja yksityisyyden suojaa koskevien sääntöjen edistämistä kansainvälisesti.

*Tiedonannon päätelmät ja suositukset:*

Tiedonannon mukaan luottamuksen palauttaminen edellyttää toimia sekä Yhdysvalloilta että Euroopan unionilta ja sen jäsenvaltiolta.

Tietojenvaihtoon liittyvien ongelmien vuoksi EU:n ja sen jäsenvaltioiden olisi syytä edetä ripeästi ja määrätietoisesti tietosuojalainsäädännön uudistamisessa. Tarvitaan vahvoja tietosuojasääntöjä, jotka ovat selkeät ja täytäntöönpanokelpoiset myös silloin, kun tietoja siirretään ulkomaille. Sen vuoksi tulisi jatkaa työtä, jotta EU:n tietosuojauudistus saadaan hyväksyttyä keväällä 2014. Näin varmistetaan, että henkilötiedoilla on tehokas ja kattava suoja.

On tärkeää, että tiedonsiirron perustana olevissa välineissä otetaan huomioon digitaaliajan haasteet ja mahdollisuudet sekä uusi teknologia, esimerkiksi pilvipalvelut. Nykyisillä ja tulevilla järjestelyillä ja sopimuksilla olisi varmistettava korkeatasoisen tietosuojan jatkuvuus transatlanttisessa tietojenvaihdossa.

Safe harbour -järjestelmää olisi lyhyellä aikavälillä vahvistettava paremman seurannan ja täytäntöönpanon keinoin, ja sen toimintaa olisi tämän pohjalta arvioitava kattavasti. Yhdysvaltojen viranomaisten tulisi seurata ja valvoa tehokkaammin sitä, miten oman varmennuksen antaneet yritykset noudattavat yksityisyyden suojaa koskevia safe harbour -periaatteita. Safe harbour -päätöksessä kansallisen turvallisuuden perusteella sallittua poikkeusta tulisi käyttää ainoastaan silloin kun se on ehdottoman välttämätöntä ja oikeasuhteista.

Neuvoteltavana oleva lainvalvonnan alan tietosuojapuitesopimus vahvistaisi luottamusta ja tarjoaisi perustan EU:n ja Yhdysvaltojen turvallisuusyhteistyön ja -kumppanuuden jatkokehittämiselle. Neuvotteluissa olisi saatava sitoumuksia siitä, että eurooppalaisilla on oikeus menettelytakeisiin, myös oikeussuojakeinoihin, vaikka he eivät asuisi Yhdysvalloissa.

Yhdysvaltojen hallinnolta olisi pyrittävä saamaan sitoumukset siitä, että maan lainvalvontaviranomaiset eivät hanki suoraan käyttöönsä yksityisten yritysten hallussa EU:ssa olevia henkilötietoja muutoin kuin virallisia yhteistyökanavia käyttäen (esim. oikeusapu- ja PNR- ja TFTP-sopimukset). Muussa tapauksessa tietojen suora käyttöön antaminen sallittaisiin vain, jos se tapahtuu selkeästi määritellyissä poikkeustapauksissa ja asia on mahdollista saattaa tuomioistuimen käsiteltäväksi.

Yhdysvaltojen olisi ulotettava Yhdysvaltojen kansalaisille ja muille asukkaille annetut takeet koskemaan myös EU:n kansalaisia, vaikka nämä eivät asuisi Yhdysvalloissa, varmistettava ohjelmien tarpeellisuus ja oikeasuhteisuus ja lisättävä avoimuutta ja valvontaa siltä osin kuin on kyse maan kansallisiin turvallisuusviranomaisiin sovellettavasta lainsäädännöstä.

2) Komission tiedonanto safe harbour -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta (COM(2013) 847 final)

Tiedonanto sisältää analyysin EU:n ja Yhdysvaltain välillä tapahtuvaa kaupallista tiedonsiirtoa sääntelevän safe harbour -järjestelmän toimivuudesta.

EU:n ja kolmansien maiden välisille tietojen siirroille asetetaan säännöt yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetussa direktiivissä 95/46/EY (henkilötietodirektiivi). Direktiivin mukaan komissio

voi tehdä päätöksen tietosuojan riittävästä tasosta kolmannessa maassa. Komissio teki 26.6.2000 päätöksen (520/2000), jolla vahvistettiin että Yhdysvaltojen kauppaministeriön julkaisemat yksityisyyden kansainvälistä suojaa koskevat safe harbor -periaatteet antavat riittävän suojan EU:sta Yhdysvaltoihin siirrettäville henkilötiedoille. (Safe Harbour) EU:sta voidaan siirtää safe harbour -ohjelmaan liittyneille yrityksille henkilötietoja. Safe harbouriin liittyminen on yrityksille vapaaehtoista. Safe harbour -säännöt ovat kuitenkin sitovia yrityksille niiden liityttyä ohjelmaan. Ohjelman keskeiset periaatteet ovat 1) Ohjelmaan liittyvien yritysten yksityisyyden suojaa koskevien linjausten läpinäkyvyys. 2) Safe harbour periaatteiden sisällyttäminen yritysten yksityisyyden suojaa koskeviin linjauksiin. 3) Täytäntöönpano, viranomaistahot mukaan lukien.

*Safe harbour järjestelmän rakenne ja toiminta*
Safe harbor -järjestelmän täytäntöönpanossa on keskeisessä asemassa kaksi yhdysvaltalaista viranomaistahoa. Yhdysvaltojen kauppaministeriö (Department of Commerce**)** käy läpi safe harbour-ohjelmaan liittyvien yritysten itse-sertifioinnit ja uudelleen sertfioinnit. Liittovaltion kilpailuviranomainen (Federal Trade Commission, FTC**)** puolestaan puuttuu tilanteisiin, joissa esimerkiksi epäillään, että yritys ei noudata safe harbour -periaatteita. Nykyisin EU:n kansallisilla tietosuojaviranomaisilla on oikeus keskeyttää henkilötietojen siirrot safe harbour -yritykselle tietyissä tilanteissa. Nykyisen päätöksen puitteissa komissiolla on toimivalta keskeyttää tai rajoittaa safe harbourin soveltamisalaa.

Syyskuussa 1993 safe harbour -ohjelman piiriin kuului 3246 suurta ja pientä yritystä. Mukana on myös joidenkin EU -yritysten tytäryhtiöitä, esimerkiksi Nokian ja Bayerin.

*Tietosuojakäytäntöjen läpinäkyvyys*
Safe harbour -ohjelmaan liittyneiden yritysten tulisi pitää yleisesti saatavilla niiden yksityisyyden suojaa koskevat menettelytavat (käytännöt). Läpinäkyvyyden puute hankaloittaa Federal Trade Commissionin mahdollisuuksia valvoa järjestelmää. Läpinäkyvyydessä on ollut puutteita ja komission ja Department of Commercen välillä käydyissä keskusteluissa on käynyt ilmi, että 10 % ohjelmaan kuuluvista yrityksistä ei pidä www-sivuillaan kuvausta yksityisyyden suojaa koskevista menettelytavoistaan. Lisäksi tuoreet tilastot osoittavat, että noin 10 % yrityksistä, jotka väittävät kuuluvansa safe harbour -ohjelmaan, ei ole Department of Commercen voimassaolevalla safe harbour -listalla. Department of Commerce on vastannut komission ilmaisemiin huoliin siten, että safe harbourin piirissä olevien yritysten on tullut maaliskuusta 2013 lähtien ilmoittaa www-sivuillaan yksityisyyden suojaa koskevat käytäntönsä. Department of Commerce on myös edellyttänyt, että yritysten www-sivuilla on linkki Department of Commercen ylläpitämään safe harbour -listaan.

*Täytäntöönpanon viranomaisvalvonta*
Yhdysvalloissa Federal Trade Commission voi ryhtyä täytäntöönpanotoimiin, jos safe harbour -ohjelmaan kuuluvaa yritys laiminlyö velvoitteitaan. Koska EU:n jäsenvaltioiden viranomaisilta ei tullut ohjelman kymmenen ensimmäisen vuoden aikaan valituksia, on Federal Trade Commission päättänyt tutkia, noudattaako yritys safe harbour -periaatteita joka kerta kun se tutkii, onko yksityisyyden suojaa tai tietoturvaa rikottu. Safe Harbour -päätöksen puitteissa on myös luotu EU:n tietosuojapaneeli (EU Data Protection Panel). Paneeli tutkii kaikki valitukset, jotka koskevat työsuhteen yhteydessä tapahtuvaa henkilötietojen käsittelyä. Lisäksi yritys voi valita tämän menettely riidanratkaisua varten. (53 5 safe harbourin piiriin kuuluvuista yrityksistä on valinnut tämän muodon). Paneelilla on ollut neljä asiaa ratkaistavanaan tähän mennessä.

*Yksityisyyden suojaa koskevien safe harbour -periaatteiden vahvistaminen*

Täytäntöönpano edellyttää, että on olemassa helposti käytettävissä oleva ja kohtuuhintainen riippumaton valitusmenettely, jolla tutkitaan yksityishenkilöiden valitukset ja ratkaistaan kiistat. Tässä tarkoituksessa safe harbour -ohjelman puitteissa on luoto vaihtoehtoinen riidanratkaisumenettely, jossa kolmas itsenäinen osapuoli tarjoaa nopeita ratkaisuja. Kolme suosituinta mekanismia on tällä hetkellä EU:n tietosuojapaneeli, BBB (Better Business Bureau) ja TRUST.

*Pääsy safe harbour -ohjelman puitteissa siirrettyihin tietoihin*
Vuoden 2013 aikana Yhdysvaltojen tiedusteluohjelmien tiedonkeruun laajuus on puhututtanut Euroopassa. Kaikki PRISM -ohjelmaan kuuluneet yritykset kuuluivat myös safe harbour -ohjelmaan. Safe harbourista on tullut reitti Yhdysvaltojen tiedustelupalvelulle saada henkilötietoja, joita on alun perin käsitelty EU:ssa. Safe harbourin puitteissa taatusta yksityisyyden suojasta on mahdollista poiketa muun muassa kansallisen turvallisuuden ja yleisen edun vuoksi. Poikkeusten tulee kuitenkin perustua julkisesti saatavilla olevaan lakiin ja niiden on oltava välttämättömiä ja suhteellisia demokraattisessa yhteiskunnassa.

*Komission johtopäätökset ja suositukset*
Tietojenkäsittelyn läpinäkyvyyttä ja täytäntöönpanoa koskevien puutteiden vuoksi tiettyjä toistuvia ongelmia tulisi käsitellä.

a) Safe harbour -ohjelmaan kuuluvien läpinäkyvyyttä ja yksityisyyden suojaa koskevat käytännöt
b) Yhdysvalloissa olevien yritysten yksityisyyden suojaa koskevien periaatteiden tehokas täytäntöönpano
c) täytäntöönpanon tehokkuus

Lisäksi tiedustelupalvelun laajat oikeudet päästä käsiksi safe harbourin puitteissa siirrettyihin tietoihin herättää huolia siitä, miten tietosuojan tason jatkuvuus voidaan taata siirrettäessä tietoja Euroopasta Yhdysvaltoihin.

*<u>Läpinäkyvyyttä koskevat suositukset</u>*

1) Itse-sertifioitujen yritysten tulisi saattaa yleisön saataville niiden yksityisyyden suojaa koskevat linjaukset.
2) Itse-sertifioitujen yritysten www-sivuilla tulisi yksityisyyden suojaa koskevien linjausten yhteydessä olla aina linkki Yhdysvaltojen Department of Commercen sivuilla, joilla on päivitetty lista safe harbour -ohjelmaan kuuluvista yrityksistä.
3) Itse-sertifioitujen yritysten tulisi julkistaa yksityisyyden suojaa koskevat ehdot niistä sopimuksista, joita ne tekevät alihankkijoiden kanssa, ts. pilvipalveluiden tarjoajien kanssa.
4) Selkeä merkintä Department of Commercen ylläpitämillä www-sivuilla niissä tapaukissa, joissa safe harbour -listalla oleva yritys ei nykyhetkellä täytä ohjelman vaatimuksia.

*<u>Oikaiseminen</u>*

5) Yritysten www-sivuilla olevien yksityisyyden suojaa koskevien linjausten tulisi sisältää linkki vaihtoehtoiseen riidanratkaisumenettelyyn ja/tai Euroopan tietosuojapaneeliin.
6) Vaihtoehtoisen riidanratkaisumenettelyn tulisi olla valmiiksi saatavilla ja kustannuksiltaan kohtuullinen.
7) Department of Commercen tulisi valvoa järjestelmällisemmin vaihtoehtoisen riidanratkaisun tarjoajia.

*<u>Täytäntöönpano</u>*

8) Yritysten itse-sertifioinnin ja uudelleen sertifioinnin seurauksena tietyn prosenttiosuuden ohjelmaan kuuluvista yrityksistä tulisi olla ex officio -tarkastuksen kohteen.
9) Tilanteissa, joissa yrityksen on todettu rikkovan safe harbour -ohjelman periaatteita, tulisi yrityksen käytännöt tarkastaa vuoden kuluttua tästä havainnosta uudemman kerran.
10) Tilanteissa, joissa epäillään, että yritys ei täytä velvoitteitaan, tulisi Department of Commercen informoida toimivaltaista EU:n tietosuojaviranomaista.
11) Perusteettomia ilmoituksia safe harbour -ohjelmaan kuulumisesta tulisi tutkia.

*Yhdysvaltojen viranomaisten oikeus saada tietoja*

12) Itse-sertifioitujen yritysten yksityisyyden suojaa koskevien linjausten tulisi sisältää tieto siitä, missä laajuudessa Yhdysvaltojen viranomaisilla on kansallisen lainsäädännön perusteella oikeus ohjelman puitteissa kerättyihin henkilötietoihin. Yrityksiä tulisi erityisesti kannustaa siihen, että ne ilmoittavat, jos ne soveltavat ohjelman sallimia poikkeuksia kansallisen turvallisuuden, yleisen edun tai täytäntöönpanosyiden vuoksi.
13) On tärkeää, että safe harbourin sallimaa kansallista turvallisuutta koskevaa poikkeusta sovelletaan ainoastaan täysin välttämättömissä tilanteissa suhteellisuusperiaatetta noudattaen.

3) Raportti EU:n ja Yhdysvaltain tietotosuojatyöryhmän tuloksista (16987/13)

Yhdysvaltojen turvallisuuspalvelun NSA:n harjoittamaa verkkotiedustelua koskevaa asiaa on hoidettu EU:ssa kahdella raiteella. 1 raide käsittelee EU kansalaisten henkilötietojen suojaa koskevia asioita ja 2 raide tiedustelutietojen keräämistä. EU:n instituutioihin kohdistunutta vakoilua selvitellään erikseen. Mahdolliset 2 raiteen keskustelut tiedustelutietojen keräämisestä käydään Yhdysvaltojen ja kunkin jäsenvaltion kesken erikseen, koska kansallista turvallisuutta ja tiedustelutoimintaa koskevat asiat kuuluvat jäsenvaltioiden kansalliseen toimivaltaan.

1 raidetta varten perustettiin EU:n ja Yhdysvaltojen välinen tietosuojatyöryhmä, joka keskusteli vakoiluohjelmien vaikutuksista EU-kansalaisten henkilötietojen suojaan. Työryhmän EU:ta edustavat puheenjohtajat antoivat 27.11.2013 raportin työryhmän työn tuloksista.

Raportti perustuu USA:n antamiin tietoihin, julkisesti saatavilla olleisiin asiakirjoihin, mukaan lukien mediassa julkaistut salassa pidettävät asiakirjat, joiden oikeellisuutta Yhdysvallat ei ole vahvistanut. Raportissa käsitellään valvontaohjelmiin liittyvää oikeudellista kehikkoa, valvontaohjelmien puitteissa tapahtuvaa henkilötietojen keräämistä ja käyttöä sekä valvontaa ja oikeussuojakeinoja.

Oikeudellisen kehikon muodostavat mm. presidentin asema ja valtaoikeudet, Section 702 of the Foreign Intelligence Act of 1978 (FISA) ja Section 215 of the USA PATRIOT Act 20001. FISA Court (FISC) voi antaa luvan FISA:n ja Patriot Actin mukaiseen tietojen keruuseen ja se valvoo tietojen keruuta.

Raportin pääasialliset tulokset:

1) USA:n lainsäädännössä on useita oikeudellisia perustoja laaja-alaiselle henkilötietojen keräämiselle ja käsittelylle ulkomaantiedustelua varten (foreign intelligence purposes).

Epäselväksi on jäänyt mm. kuinka moneen EU:n kansalaiseen urkintaohjelmat vaikuttavat.

2) EU:n kansalaisiin ja USA:n kansalaisiin sovellettavat suojatoimet ovat erilaiset.

- USA:n kansalaisia koskevia tietoja voidaan pitää ”ulkomaantiedustelutietona” (foreign intelligence) vain, jos tieto on tarpeen tiettyä tarkoitusta varten. EU:n kansalaisten osalta riittää, että tieto liittyy tavoiteltuun tarkoitukseen. Kynnys kerätä tietoja EU:n kansalaisista on siten matalampi.
- urkintaohjelmien valvonnan pääasiallisena tarkoituksena on suojata USA:n kansalaisia
- perustuslain suoja (First and Fourth Amendments) ei ulotu EU:n kansalaisiin jotka eivät asu USA:ssa

3) Valvontaohjelmissa erityyppisiin tietoihin ja niiden eri käsittelyvaiheisiin sovelletaan eriasteisia tietosuojasääntöjä

4) Kaikista tietojen käsittelyn oikeuttavista oikeusperustoista ja olemassa olevista valvontaohjelmista ei ole selvyyttä

5) FISA-tuomioistuimen (FISA Court) määräykset ovat salaisia ja yritysten on pidettävä salassa, mitä apua ne on velvoitettu antamaan FISA-tuomioistuimelle. Tämän vuoksi EU:n ja USA:n kansalaisilla ei ole reittiä, jota kautta he voisivat saada tietää, onko heidän tietojaan kerätty tai jatkokäsitelty. Henkilöillä ei ole mitään mahdollisuuksia saada tarkastaa tietonsa tai saada ne korjatuiksi tai poistetuiksi eikä hallinnollisia tai oikeudellisia oikeussuojakeinoja.

6) Ei ole olemassa oikeudellista hyväksymismenettelyä, jossa hyväksyttäisiin yksittäiset perusteet (individual selectors) Section 215 nojalla kerättyjen tietojen käyttämiselle tai Section 702 nojalla tapahtuvalle tietojen keruulle. FISC toimii *ex parte* ja *in camera*. Oikeudellinen valvonta ei kata tiedustelutietojen keräämistä USA:n ulkopuolella Executive Orderin 12333 nojalla.

4) Komission kertomus matkustajarekisteritietojen käsittelyä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen täytäntöönpanon yhteisestä tarkastelusta (COM(2013) 844 final)

Komission kertomuksen liitteenä on kertomus EU:n ja USA:n suorittamasta EU-PNR -sopimuksen yhteisestä tarkastelusta SEC(2013) 630 final.

EU:n arviointiryhmä pitää yhteisarviointia hyvänä työkaluna selvitettäessä kuinka Department of Homeland Security (DHS) noudattaa PNR-sopimuksessa asetettuja henkilötietojen käsittelyedellytyksiä. EU:n arviointiryhmä on tarkastelun yhteydessä saanut mahdollisuuden nähdä, kuinka henkilötietoja käsitellään käytännössä. Työryhmällä on ollut mahdollisuus kontakteihin tiedon analysoijien, kohdentajien (targeter) ja muiden PNR-tietoja käsittelevien viranomaisten kanssa.

EU:n arviointityöryhmän käsityksen mukaan DHS on implementoinut sopimuksen siinä asetettujen ehtojen mukaisesti. DHS noudattaa velvoitteita, joiden mukaan matkustajilla tulee olla oikeus tarkastaa itseään koskevat tiedot. Lisäksi DHS on luonut mekanismin sen varmistamiseksi, että tietojen käsittely ei johda laittomaan syrjintään. Arviointiryhmä pitää erityisesti huomionarvoisena, että Yhdysvallat on saattanut kotimaiseen järjestelmään säännöiksi velvoitteensa EU:ta kohtaan.

Joidenkin sitoumusten tekninen toteuttaminen on hyvin haastavaa. Näin on esimerkiksi push-järjestelmän implementoiminen. DHS:n tulisi kuitenkin vahvistaa pyrkimyksiään sen varmistamiseksi, että koko lentoliikenne käyttää push-metodia heinäkuuhun 2014 mennessä. DHS:n tulisi aktiivisesti työskennellä kansainvälisellä forumilla tämän ongelman ratkaisemiseksi, mukaan luettuna yhteisen standardin löytämiseksi ad hoc -push tilanteisiin.

DHS:lle on osoitettu useita suosituksia. Nämä suositukset koskevat mekanismeja, joilla henkilötietoja depersonalisoidaan, ad hoc pull-järjestelmän käyttöä ja korvausmekanismeja. Lisäksi vastaisuudessa tulisi edelleen kehitellä yksittäisten PNR:n tietojen ja analyysien vastavuoroista jakamista jäsenvaltioiden, Europolin ja Eurojustin kanssa.

Seuraava yhteinen arviointi PNR-sopimuksesta on suunniteltu vuoden 2015 ensimmäiselle puolikkaalle.

5) Komission tiedonanto Euroopan komission ja Yhdysvaltojen valtiovarainministeriön yhteisestä kertomuksesta, jossa tarkastellaan toimitettujen TFTP-tietojen hyödyllisyyttä rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä Euroopan unionista Yhdysvaltoihin terrorismin rahoituksen jäljittämisohjelman tarkoituksiin tehdyn Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen 6 artiklan 6 kohdan nojalla (COM(2013) 843 final)

Komissio ja Yhdysvaltojen valtiovarainministeriö ovat laatineet TFTP-sopimuksen 6 artiklan 6 kohdassa tarkoitetun yhteisen kertomuksen TFTP-sopimuksen (aikaisemmin ns. SWIFT-sopimus) nojalla toimitettujen TFTP-tietojen hyödyllisyydestä. Kertomuksessa keskitytään erityisesti useita vuosia säilytettävien tietojen ja 13 artiklan mukaisesti suoritetusta yhteisestä tarkastelusta saatujen asianmukaisten tietojen hyödyllisyyteen.

Kertomuksen laatimisessa käytetyt tiedot ovat peräisin Yhdysvaltojen valtiovarainministeriöltä, Europolilta ja EU:n jäsenvaltioilta.

Yhdysvaltojen tarkasteluvaltuuskunta arvioi TFTP-sopimuksen nojalla toimitettujen tietojen hyödyllisyyttä haastattelemalla eri virastoissa työskenteleviä terrorismintutkijoita, tarkastelemalla terrorismintorjuntatapauksia, joissa oli hyödynnetty TFTP-tietoja, ja analysoimalla yli tuhat TFTP-raporttia.

Kertomuksessa keskitytään siihen, millä tavoin TFTP-tietoja on käytetty ja mitä hyötyä niistä on ollut terrorismintorjuntatutkimuksissa Yhdysvalloissa ja EU:ssa. Kertomuksessa esitetään useita käytännön esimerkkejä siitä, miten kolme vuotta tai kauemmin säilytetyt TFTP-tiedot ovat edistäneet terrorismintorjuntatutkimuksia Yhdysvalloissa ja EU:ssa jo ennen kuin TFTP-sopimus tuli voimaan 1. elokuuta 2010 ja sen jälkeen. Sopimuksen tekemisen jälkeen TFTP-ohjelmaa on käytetty mm. seuraavien tehtyjen tai suunniteltujen merkittävien terrori-iskujen tutkinnassa: pommi-iskut Bostonin maratonilla huhtikuussa 2013, Lontoon kesäolympialaisiin kohdistuneet uhkat vuonna 2012, salahanke Saudi-Arabian Yhdysvaltojen-lähettilään murhaamiseksi vuonna 2001, Anders Breivikin Norjassa toteuttamat iskut heinäkuussa 2011 ja Nigerian itsenäisyyspäivän autopommi-iskut lokakuussa 2010. Kertomukseen sisältyy lisäksi useita esimerkkejä siitä, miten TFTP-tietoja on käytetty EU:n jäsenvaltioissa.

Kertomuksessa tarkastellaan myös sitä, miten Yhdysvaltojen valtiovarainministeriö on tarkastellut tietojen säilyttämisaikoja ja valikoimattomien tietojen poistamista.

Kertomuksen katsotaan osoittavan, että TFTP-sopimuksen nojalla toimitetut tiedot, mm. tiedot, joita on säilytetty usean vuoden ajan, ovat olleet erittäin hyödyllisiä terrorismintorjuntatutkimuksissa sekä Yhdysvalloissa että Euroopassa ja muuallakin. Paikkansapitävien TFTP-tietojen ansiosta on mahdollista tunnistaa ja jäljittää terroristeja ja heidän tukiverkostojaan kaikkialla maailmassa. TFTP-tietojen avulla voidaan parantaa terroristijärjestöjen taloudellisten rakenteiden tuntemusta ja havaita uusia taloudellisen tuen virtoja sekä aiemmin tuntemattomia yhteistyökumppaneita ja uusia terroristiepäiltyjä. TFTP-tietojen avulla voidaan myös arvioida ja vahvistaa aiemmin saatuja tiedustelutietoja ja varmistaa, että henkilö todella on terroristijärjestön jäsen, ja paikata tiedoissa olevia aukkoja.

Terrorismintorjuntaviranomaiset ovat kertomuksen mukaan osoittaneet, että usean vuoden ajan säilytetyistä rahaliikenteen tiedoista, ns. historiatiedoista, on terrorismintorjuntatutkimuksissa erittäin suurta hyötyä. Kertomuksessa päädytään siihen, että TFTP-tietojen säilytysajan lyhentäminen alle viiden vuoden heikentäisi huomattavasti mahdollisuuksia saada tietoja terroristiryhmien rahoituksesta ja toiminnasta.

Kertomuksessa todetaan, että samanaikaisesti kertomuksen laatimisen kanssa on komission pyynnöstä käynnistetty sopimuksen 19 artiklan nojalla neuvottelut, joiden taustalla ovat tiedotusvälineissä esitetyt väitteet, joiden mukaan Yhdysvaltojen viranomaiset olisivat rikkoneet sopimuksen määräyksiä. Yhdysvaltojen valtiovarainministeriön toimittaman lisäselvennyksen perusteella ei ole todettu minkäänlaista sopimusmääräysten rikkomista.

Komissio ja Yhdysvaltojen valtiovarainministeriö ovat sopineet, että seuraava sopimuksen13 artiklan mukainen yhteinen tarkastelu tehdään keväällä 2014.

**EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely**

Komission tiedonanto ei ole SEUT 288 artiklassa tarkoitettu unionin säädös. EU-USA PNR-sopimuksen oikeusperusta on SEUT (sopimus Euroopan unionin toiminnasta) 82 artiklan 1 kohdan d alakohta ja 87 artiklan 2 kohdan a alakohta. EU-USA TFTP-sopimuksen oikeusperusta on SEUT 87 artiklan 2 kohdan a alakohta ja 88 artiklan 2 kohta.

**Käsittely Euroopan parlamentissa**

Euroopan parlamentin LIBE-valiokunta hyväksyi 12.2.2014 Yhdysvaltojen NSA:n urkintaa koskevan mietintönsä NSA:n valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa. Mietinnön hyväksymistä edelsi kuukausia kestänyt tutkimus kuulemistilaisuuksineen. Claude Moraesin (S&D, UK) laatima mietintö hyväksyttiin äänin 33 puolesta, 7 vastaan ja 17 tyhjää. Euroopan parlamentin täysistunto äänestää mietinnöstä 12.3.2014.

Mietinnön keskeisimpiä teesejä on massiivisen ja systemaattisen henkilöitä koskevan tiedonkeruun tuomitseminen (terrorismin vastainen taistelu ei voi sitä oikeuttaa).

Mietintö sisältää seuraavat suositukset:

- EP:n pitäisi pidättyä hyväksymästä neuvoteltavana olevaa EU:n ja Yhdysvaltojen vapaakauppasopimusta (TTIP-sopimus) mikäli sopimus ei noudata EU:n perusoikeuskirjan asettamia perusoikeuksia. Tietosuojakysymys tulisi jättää kauppaneuvottelujen ulkopuolelle.

- Safe harbor -järjestely tulisi keskeyttää välittömästi, koska se ei tarjoa riittävää tietosuojan tasoa EU-kansalaisille. USA:n toivotaan ehdottavan uusia toimivia tietosuojaperiaatteita.

- TFTP-sopimuksen toimeenpano tulisi keskeyttää kunnes saadaan selvitys syytöksiin, jotka koskevat Yhdysvaltojen viranomaisten pääsyä EU kansalaisten pankkitietoihin ohi sopimuksen.

- Neuvoteltavana olevan EU:n ja Yhdysvaltain välisen lainvalvonnan alan tietosuojapuitesopimuksen tulee varmistaa tarvittava oikeussuoja EU-kansalaisille, joita koskevaa tietoa siirretään USA:han.

- EU tarvitsee digitaalisen "new dealin". Lisäksi EU:n uusi tietosuojalainsäädäntö tulisi hyväksyä vuoden 2014 loppuun mennessä ja EU:n tulisi kehittää omia pilvipalveluitaan korkean tietosuojan tason varmistamiseksi.

- Ilmiantajien (whistleblowers) oikeuksia tulee kehittää, mm. David Mirandan tapaus mainitaan erikseen.

- Jäsenmaiden toivotaan tarkastelevan omaa tiedustelutoimintaa valvovaa lainsäädäntöään. Erikseen mainitaan Yhdistyneet kuningaskunnat, Ranska, Saksa, Ruotsi, Alankomaat, Puola, Tanska, Belgia, Italia ja Espanja.

**Kansallinen valmistelu**

E-kirje on käsitelty kirjallisessa menettelyssä oikeus- ja sisäasiat jaostossa (EU 7) 3.-6.3.2014 ja viestintäjaostossa (EU19) 28.2. - 6.3.2014.

**Eduskuntakäsittely**

**Kansallinen lainsäädäntö, ml. Ahvenanmaan asema**

**Taloudelliset vaikutukset**

**Muut asian käsittelyyn vaikuttavat tekijät**

Presidentti Obaman hallinnon viime vuoden elokuussa perustama tiedustelutapojen ja -tekniikoiden arviointiryhmä (*Review group on intelligence and communications*

*technologies*) antoi raporttinsa joulukuun puolivälissä. Raportti sisälsi 46 suositusta harkittavaksi hallinnolle. Obama palasi asiaan 17.1.2014 linjapuheessaan Yhdysvaltain tiedustelutoiminnasta ja sen uudistuksista. Puhe oli puheenvuoro tiedustelutoiminnan puolesta ja yksityisyyden suojan tärkeydestä. Puheen keskeinen tavoite oli luottamuksen palauttaminen kansallisesti ja kansainvälisesti sekä vastuunkannon osoittaminen. Obama ilmoitti useista uudistuksista siinä hengessä, että niiden yksityiskohtia vielä pohditaan. NSA organisoidaan uudelleen, avoimuutta ja valvontaa lisätään ja meta-tietojen kerääminen organisoidaan uudelleen. Kansainvälisten kumppanien tärkeyttä painotettiin ja yksityisyyden suojaa muihin kuin Yhdysvaltain kansalaisiin tullaan laajentamaan, mutta tämä valmistellaan erikseen. Tarkoituksena on tarkastella erityisesti ulkomaalaisista kerätyn tiedon säilyttämisaikoja samoin kuin tiedon käyttämisen perusteita.

Uudistusavauksista moni vaatii jatkotyötä ja on luonteeltaan institutionaalinen. Suurena haasteena Obamalla tuleekin olemaan, että hänen on saatava kongressi työskentelemään kanssaan, mikä ei ole helppoa nykyisessä poliittisessa tilanteessa.

**Asiakirjat**

COM(2013) 846 final (kohta 1)
COM(2013) 847 final (kohta 2)
16987/13 (kohta 3)
COM(2013) 844 final (kohta 4)
COM(2013) 843 final (kohta 5)

**Laatijan ja muiden käsittelijöiden yhteystiedot**

Leena Rantalankila, OM (laatija, kohdat 1, 3 ja 5)
leena.rantalankila@om.fi, GSM: 02951 50152

Anu Talus, OM (laatija, kohdat 2 ja 4)
anu.talus@om.fi, GSM: 02951 50586

Laura Kamras/UM/POL-10, puh: 0295 351192
Hannele Taavila/SM, puh: 0718788568
Tiina Piipponen/SM/Supo, puh: 0295 4484931
Laura Tarhonen/LVM, puh: 0295 342073
Tia-Maaret Möller/VNK, puh: 0295 160325

**EUTORI-tunnus**

EU/2013/1783, EU/2013/1782, EU/2013/1781

**Liitteet**

**Viite**

Asiasanat
**Hoitaa**

Tiedoksi

EUROOPAN
KOMISSIO

Bryssel 27.11.2013
COM(2013) 846 final

# KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

## Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon

## 1. JOHDANTO: EU:N JA YHDYSVALTOJEN VÄLISEN TIEDONSIIRRON MUUTTUVA TOIMINTAYMPÄRISTÖ

Euroopan unioni ja Yhdysvallat ovat strategisia kumppaneita, ja tällä kumppanuudella on ratkaiseva merkitys, kun pyrimme edistämään yhteisiä arvojamme, turvallisuuttamme ja yhteistä johtajuuttamme maailmanlaajuisissa asioissa.

Luottamus tähän kumppanuuteen on kuitenkin heikentynyt, joten nyt tarvitaan toimia sen palauttamiseksi. Yhdysvaltojen harjoittamaa laajamittaista tiedustelutietojen keruuta koskevat paljastukset ovat herättäneet syvää huolta EU:ssa ja sen jäsenvaltioiden ja Euroopan kansalaisten keskuudessa erityisesti siltä osin kuin on kyse henkilötietojen suojasta[1]. Yksityisen viestinnän joukkoseurantaa, kohdistuipa se sitten kansalaisiin, yrityksiin tai poliittisiin johtajiin, ei voida hyväksyä.

Henkilötietojen siirto on tärkeä ja välttämätön osa transatlanttisia suhteita. Se on olennainen osa Atlantin yli käytävää kauppaa, jonka yhteydessä siirretään suuria tietomääriä EU:sta Yhdysvaltoihin. Tämä koskee myös muun muassa sosiaalisen median tai pilvipalvelujen alalla toimivia uusia kasvavia digitaaliyrityksiä. Henkilötietojen siirto on tärkeä osatekijä myös EU:n ja Yhdysvaltojen lainvalvonta-alan yhteistyössä ja jäsenvaltioiden ja Yhdysvaltojen yhteistyössä kansallisen turvallisuuden alalla. Yhdysvallat ja EU ovat useilla sopimuksilla ja järjestelyillä pyrkineet helpottamaan tietojen siirtoa ja samalla varmistamaan, että EU:n lainsäädännön edellyttämä korkeatasoinen tietosuoja säilytetään.

Kauppaan liittyvistä tiedonsiirtokysymyksistä säädetään päätöksessä 2000/520/EY,[2] jäljempänä ’safe harbor -päätös’. Tämä päätös muodostaa oikeusperustan siirrettäessä henkilötietoja EU:sta safe harbor -periaatteita noudattaville yhdysvaltalaisyrityksille.

Lainvalvontatarkoituksessa – kuten terrorismin ja muunlaisen vakavan rikollisuuden ehkäisemiseksi ja torjumiseksi – tehtävästä henkilötietojen vaihdosta EU:n ja Yhdysvaltain välillä on tehty useita EU:n tason sopimuksia: sopimus keskinäisestä oikeusavusta[3], sopimus matkustajarekisteritietojen (PNR) käytöstä ja siirtämisestä[4], sopimus rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä terrorismin rahoituksen jäljittämisohjelman (TFTP) tarkoituksiin[5] ja Europolin ja Yhdysvaltojen välinen sopimus. Näillä sopimuksilla vastataan merkittäviin turvallisuushaasteisiin ja EU:n ja Yhdysvaltojen yhteisiin turvallisuustarpeisiin ja varmistetaan samalla henkilötietojen korkeatasoinen suoja. Lisäksi

---

1 Kun tässä tiedonannossa viitataan EU:n kansalaisiin, tämä käsittää myös muiden kuin EU-maiden kansalaiset, jotka kuuluvat Euroopan unionin tietosuojalainsäädännön soveltamisalaan.

2 Komission päätös 2000/520/EY, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä (EYVL L 215, 25.8.2000, s. 7).

3 Neuvoston päätös 2009/820/YUTP, tehty 23 päivänä lokakuuta 2009, rikoksen johdosta tapahtuvaa luovuttamista koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen ja keskinäistä oikeusapua koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä Euroopan unionin puolesta (EUVL L 291, 7.11.2009, s. 40).

4 Neuvoston päätös 2012/472/EU, annettu 26 päivänä huhtikuuta 2012, matkustajarekisteritietojen käyttöä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen tekemisestä (EUVL L 215, 11.8.2012, s. 4).

5 Neuvoston päätös, annettu 13 päivänä heinäkuuta 2010, terrorismin rahoituksen jäljittämisohjelmaa varten tapahtuvaa rahaliikenteen sanomanvälitystietojen käsittelyä ja siirtämistä Euroopan unionista Yhdysvaltoihin koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä (EUVL L 195, 27.7.2010, s. 3).

EU ja Yhdysvallat neuvottelevat parhaillaan tietosuojaa oikeus- ja poliisiyhteistyössä koskevasta puitesopimuksesta[6]. Tavoitteena on varmistaa korkeatasoinen tietosuoja niiden kansalaisten osalta, joita koskevia tietoja vaihdetaan, ja edistää näin EU:n ja Yhdysvaltojen yhteistyötä rikollisuuden ja terrorismin torjunnassa yhteisten arvojen ja yhdessä sovittujen suojatoimien pohjalta.

Näitä välineitä käytetään toimintaympäristössä, jossa henkilötietojen siirron merkitys kasvaa koko ajan.

Digitaalitalouden kehitys on ensinnäkin johtanut siihen, että laadultaan ja luonteeltaan erilaisten tietojenkäsittelytoimien määrä on kasvanut voimakkaasti. Kansalaiset käyttävät jokapäiväisessä elämässään yhä enemmän sähköisiä viestintäpalveluja. Henkilötiedoista on tullut arvokasta omaisuutta: EU:n kansalaisia koskevien tietojen arvo oli arviolta 315 miljardia euroa vuonna 2011. Vuonna 2020 arvo on vuositasolla mahdollisesti jo biljoona euroa[7]. Suurten tietokokonaisuuksien analysoinnin markkinat kasvavat maailmanlaajuisesti 40 prosentilla vuodessa[8]. Lisäksi esimerkiksi pilvipalveluihin liittyvän tekniikan kehitys tuo uuden ulottuvuuden kansainvälisen tiedonsiirron käsitteeseen, sillä valtioiden rajat ylittävästä tietojen siirrosta on tulossa päivittäistä todellisuutta[9].

Sähköisen viestinnän ja tietojenkäsittelypalveluiden, muun muassa pilvipalveluiden, käytön lisääntyminen on lisännyt merkittävästi myös Atlantin yli tapahtuvan tiedonsiirron laajuutta ja merkitystä. Tämän myötä ovat entistä tärkeämmiksi muodostuneet sellaiset tekijät kuin yhdysvaltalaisten yritysten keskeinen asema digitaalitaloudessa[10], sähköisen viestinnän reititys suurelta osin Atlantin yli ja EU:n ja Yhdysvaltojen välisten sähköisten tietovirtojen volyymi.

Toisaalta nykyaikaiset henkilötietojen käsittelymenetelmät nostavat esiin uusia tärkeitä kysymyksiä. Tämä koskee sekä yksityisten yritysten uusia menetelmiä kuluttajatietojen laajamittaiseen käsittelyyn kaupallisia tarkoituksia varten että tiedustelupalvelujen aiempaa parempia valmiuksia viestintätietojen laajamittaiseen seurantaan.

Yhdysvaltojen käyttämät ohjelmat laajamittaiseen tiedustelutietojen keruuseen (esimerkiksi Prism-ohjelma) loukkaavat eurooppalaisten perusoikeuksia ja erityisesti heidän oikeuttaan yksityisyyteen ja henkilötietojen suojaan. Tämänkaltaiset ohjelmat viittaavat siihen, että viranomaisten harjoittaman valvonnan ja yksityisten yritysten, erityisesti yhdysvaltalaisten internet-yritysten, suorittaman tietojenkäsittelyn välillä on yhteys. Tämän vuoksi niillä saattaa olla myös taloudellisia vaikutuksia. Jos kansalaiset ovat huolissaan yksityisten yritysten suorittamasta henkilötietojensa laajamittaisesta käsittelystä tai siitä, että tiedustelupalvelut tarkkailevat heidän tietojaan internet-palvelujen käytön yhteydessä, tämä saattaa heikentää heidän luottamustaan digitaalitalouteen, mikä puolestaan saattaa hidastaa kasvua.

---

6 Neuvosto hyväksyi 3. joulukuuta 2010 päätöksen, jolla komissio valtuutetaan neuvottelemaan sopimus. Ks. IP/10/1661, 3.12.2010.

7 Ks. Boston Consulting Groupin julkaisu ”The Value of our Digital Identity”, marraskuu 2012.

8 Ks. ”Big data: The next frontier for innovation, competition, and productivity”, McKinsey, 2011.

9 Tiedonanto ”Pilvipalvelujen potentiaali käyttöön Euroopassa”, COM(2012) 529 final.

10 Esimerkiksi Microsoft Hotmail-, Google Gmail- ja Yahoo! Mail -sähköpostipalveluilla oli kesäkuussa 2012 yhteensä yli 227 miljoonaa eri käyttäjää Euroopan maista, mikä on selvästi enemmän kuin kaikilla muilla palveluntarjoajilla. Facebook- ja Facebook Mobile -yhteisöpalveluilla oli maaliskuussa 2012 yhteensä 196,5 miljoonaa yksittäistä eurooppalaista käyttäjää, mikä tekee Facebookista Euroopan suurimman verkkoyhteisön. Googlea käyttää 90,2 prosenttia internetin käyttäjistä kaikkialla maailmassa, joten se on johtava internet-hakukone. Yhdysvaltalaista WhatsApp-pikaviestipalvelua käytti vuoden 2013 kesäkuussa 91 prosenttia saksalaisista iPhone-puhelimen käyttäjistä.

Tämä kehitys tuo uusia haasteita tietojen siirrolle EU:n ja Yhdysvaltojen välillä. Nämä haasteet ovat tämän tiedonannon aiheena. Siinä tarkastellaan tulevia toimia niiden havaintojen pohjalta, jotka sisältyvät EU:n ja Yhdysvaltojen erityistyöryhmän EU:ta edustavien puheenjohtajien raporttiin ja safe harbor -järjestelmää koskevaan tiedonantoon.

Tässä tiedonannossa pyritään esittämään tehokas tapa palauttaa luottamus ja vahvistaa sekä EU:n ja Yhdysvaltojen välistä yhteistyötä näillä aloilla että transatlanttisia suhteita laajemminkin.

Tiedonannon lähtökohtana on se, että henkilötietojen suojan tasoa on käsiteltävä sen oikeassa asiayhteydessä niin, että tämä kysymys ei vaikuta EU:n ja Yhdysvaltojen suhteiden muihin ulottuvuuksiin, kuten käynnissä oleviin neuvotteluihin transatlanttisesta kauppa- ja investointikumppanuudesta. Tästä syystä tietosuojavaatimuksista ei tulla neuvottelemaan osana transatlanttista kauppa- ja investointikumppanuutta, jonka yhteydessä noudatetaan kaikilta osin tietosuojaa koskevia sääntöjä.

On tärkeää huomata, että vaikka EU voi toteuttaa toimia toimivaltaansa kuuluvilla aloilla, erityisesti EU:n lainsäädännön soveltamisen varmistamiseksi[11], kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla[12].

## 2. VAIKUTUKSET TIETOJEN SIIRROSSA KÄYTETTÄVIIN VÄLINEISIIN

Ensinnäkin voidaan todeta, että safe harbor -järjestelmä on osoittautunut merkittäväksi välineeksi, kun tietoja siirretään EU:n ja Yhdysvaltojen välillä kaupallisessa tarkoituksessa. Sen kaupallinen merkitys on kasvanut sitä mukaa, kun henkilötietojen siirtäminen on saanut näkyvämmän aseman transatlanttisissa kauppasuhteissa. Safe harbor -järjestelmä on 13 viime vuoden aikana laajentunut käsittämään yli 3 000 yritystä, joista yli puolet on liittynyt siihen viimeisten viiden vuoden aikana. Samalla ovat kuitenkin lisääntyneet epäilykset siitä, minkä tasoisen suojan EU:n kansalaisten henkilötiedot saavat, kun ne siirretään Yhdysvaltoihin safe harbor -järjestelmän mukaisesti. Järjestelmän vapaaehtoisuus ja ilmoitusluonteisuus on johtanut siihen, että sen avoimuuteen ja noudattamisen valvontaan on alettu kiinnittää yhä enemmän huomiota. Vaikka suurin osa yhdysvaltalaisista yrityksistä noudattaa sen periaatteita, osa oman varmennuksen antaneista yrityksistä ei tee niin. Se, että osa oman varmennuksen antaneista yrityksistä ei noudata yksityisyyden suojaa koskevia safe harbor -periaatteita, antaa niille kilpailuetua suhteessa samoilla markkinoilla toimiviin eurooppalaisiin yrityksiin.

Lisäksi vaikka safe harbor -järjestelmässä sallitaan tietosuojasääntöjen rajoitukset, jos ne ovat tarpeen kansalliseen turvallisuuteen perustuvista syistä[13], keskustelua on herättänyt se, onko Yhdysvaltojen valvontaohjelmiensa puitteissa suorittama henkilötietojen laajamittainen keruu ja käsittely tarpeen ja oikeasuhteista kansallisen turvallisuuden kannalta. EU:n ja Yhdysvaltojen erityistyöryhmän työn tulokset ovat lisäksi osoittaneet selvästi, että nämä ohjelmat eivät takaa EU:n kansalaisille samoja oikeuksia ja menettelytakeita kuin amerikkalaisille.

---

[11] Ks. unionin tuomioistuimen 4.6.2013 antama tuomio asiassa C-300/11, ZZ vastaan Secretary of State for the Home Department.

[12] SEU-sopimuksen 4 artiklan 2 kohta.

[13] Ks. esim. safe harbor -päätöksen liite I.

Näiden ohjelmien laajuus ja EU:n kansalaisten eriarvoinen kohtelu niiden yhteydessä herättää epäilyjä siitä, onko safe harbor -järjestelyn tarjoama suojan taso riittävä. Yhdysvaltojen viranomaiset voivat saada käyttöönsä Yhdysvaltoihin safe harbor -järjestelmän mukaisesti lähetetyt EU:n kansalaisten henkilötiedot ja käsitellä niitä edelleen tavalla, joka on ristiriidassa tietojen keruuseen EU:ssa alun perin johtaneiden perusteiden ja niiden tarkoitusten kanssa, joita varten tiedot siirrettiin Yhdysvaltoihin. Suurin osa niistä yhdysvaltalaisista internet-yrityksistä, joihin nämä ohjelmat näyttäisivät suoremmin liittyvän, ovat mukana safe harbor -järjestelmässä.

Kun on kyse lainvalvontatarkoituksessa tapahtuvasta tietojenvaihdosta, voidaan todeta, että voimassa olevat sopimukset (PNR, TFTP) ovat osoittautuneet erittäin hyödyllisiksi välineiksi käsiteltäessä yhteisiä turvallisuusuhkia, jotka liittyvät vakavaan kansainväliseen rikollisuuteen ja terrorismiin. Samalla niihin sisältyy kuitenkin myös takeita, joilla varmistetaan korkeatasoinen tietosuoja[14]. Nämä takeet koskevat myös EU:n kansalaisia, ja sopimuksissa määrätään mekanismeista, joiden avulla voidaan tarkastella niiden täytäntöönpanoa ja ratkaista tähän liittyviä ongelmia. TFTP-sopimuksella perustetaan lisäksi valvontajärjestelmä, jonka puitteissa EU:n riippumattomat valvojat tarkastavat, millaisia hakuja Yhdysvalloissa tehdään sopimuksen soveltamisalaan kuuluviin tietoihin.

EU:ssa herännyt huoli Yhdysvaltojen valvontaohjelmista on saanut komission käyttämään näitä mekanismeja tarkoituksenaan tarkistaa, miten kyseisiä sopimuksia sovelletaan. PNR-sopimuksen täytäntöönpanosta tehtiin yhteinen arviointi, johon osallistui tietosuoja-asiantuntijoita niin EU:sta kuin Yhdysvalloistakin[15]. Arvioinnissa ei tullut ilmi mitään, mikä viittaisi siihen, että Yhdysvaltojen valvontaohjelmat koskisivat PNR-sopimuksen soveltamisalaan kuuluvia matkustajatietoja tai vaikuttaisivat niihin. TFTP-sopimuksen tapauksessa komissio aloitti viralliset neuvottelut sen jälkeen, kun oli esitetty väitteitä, joiden mukaan Yhdysvaltojen tiedusteluviranomaiset olisivat sopimuksen vastaisesti hankkineet suoraan käyttöönsä henkilötietoja EU:n alueelta. Näissä neuvotteluissa ei saatu näyttöä siitä, että TFTP-sopimusta olisi rikottu. Yhdysvallat antoi neuvottelujen tuloksena kirjallisen vakuutuksen, jonka mukaan tietoja ei ole kerätty suoraan sopimuksen määräysten vastaisella tavalla.

Yhdysvaltojen valvontaohjelmien puitteissa tapahtuva laajamittainen henkilötietojen keruu ja käsittely edellyttää kuitenkin jatkossakin sitä, että PNR- ja TFTP-sopimusten täytäntöönpanoa seurataan erittäin tarkasti. EU ja Yhdysvallat ovat tästä syystä sopineet aikaistavansa TFTP-sopimuksen seuraavaa yhteistä tarkastelua, joka suoritetaan keväällä 2014. Sen ja tulevien yhteisten tarkastelujen yhteydessä on tarkoitus selostaa avoimemmin valvontajärjestelmän toimintatapaa ja sitä, miten järjestelmällä suojataan EU:n kansalaisia koskevia tietoja. Samalla toteutetaan toimia sen varmistamiseksi, että valvontajärjestelmässä seurataan edelleen tarkoin sitä, miten Yhdysvaltoihin sopimuksen mukaisesti siirrettyjä tietoja käsitellään. Huomiota kiinnitetään tässä yhteydessä erityisesti siihen, miten tällaisia tietoja jaetaan yhdysvaltalaisten viranomaisten kesken.

---

[14] Ks. TFTP-ohjelman puitteissa toimitettavien tietojen hyödyllisyyttä koskeva komission ja Yhdysvaltojen valtiovarainministeriön yhteinen kertomus, joka on annettu rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä Euroopan unionista Yhdysvaltoihin terrorismin rahoituksen jäljittämisohjelman tarkoituksiin tehdyn Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen 6 artiklan 6 kohdan mukaisesti.

[15] Ks. komission kertomus matkustajarekisteritietojen käsittelemistä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen täytäntöönpanon yhteisestä arvioinnista.

Erilaisten oikeudellisten ja hallinnollisten takeiden merkitys on korostunut käsiteltävien henkilötietojen määrän kasvaessa. EU:n ja Yhdysvaltojen erityistyöryhmän yhtenä tavoitteena oli määrittää ne suojatoimet, joita soveltamalla voidaan minimoida tietojen käsittelyn vaikutukset EU:n kansalaisten perusoikeuksiin. Suojatoimia tarvitaan myös yritysten suojelemiseksi. Tietyt Yhdysvaltojen lait (esimerkiksi Patriot Act -säädös) antavat Yhdysvaltojen viranomaisille mahdollisuuden pyytää yrityksiltä suoraan käyttöönsä EU:ssa tallennettuja tietoja. Tämän vuoksi eurooppalaisia yrityksiä ja EU:ssa toimivia yhdysvaltalaisia yrityksiä saatetaan pyytää siirtämään tietoja Yhdysvaltoihin EU:n ja jäsenvaltioiden lainsäädännön vastaisesti, jolloin ne joutuvat ristiriitaisten oikeudellisten velvoitteiden ristipaineeseen. Tällaisten suorien pyyntöjen aiheuttama oikeudellinen epävarmuus saattaa jarruttaa uusien digitaalipalvelujen, kuten pilvipalvelujen, kehittämistä ja näin haitata tehokkaiden ja edullisempien ratkaisujen tarjoamista kansalaisille ja yrityksille.

## 3. TIETOSUOJAN TEHOKKUUDEN VARMISTAMINEN

Henkilötietojen siirto EU:n ja Yhdysvaltojen välillä on olennainen osa transatlanttisia kauppasuhteita. Tietojenvaihto on myös olennainen osa EU:n ja Yhdysvaltojen turvallisuusyhteistyötä ja ratkaisevan tärkeä osatekijä erityisesti vakavan rikollisuuden ja terrorismin ehkäisemistä ja torjuntaa koskevan yhteisen tavoitteen kannalta. Hiljattain paljastuneet Yhdysvaltojen tiedustelutietojen keruuohjelmat ovat kuitenkin vahingoittaneet tämän yhteistyön perustana olevaa luottamusta. Erityisesti on kärsinyt luottamus tapaan, jolla henkilötietoja käsitellään. Jäljempänä esitetyt toimet ovat tarpeen, jotta luottamus tiedonsiirtoon saataisiin palautettua tavalla, joka edistää digitaalitaloutta, sekä EU:n että Yhdysvaltojen turvallisuutta ja transatlanttisia suhteita yleensäkin.

### 3.1. EU:n tietosuojauudistus

Komission tammikuussa 2012 ehdottama tietosuojalainsäädännön uudistus[16] sisältää keskeisiä henkilötietosuojaa parantavia tekijöitä. Näistä viisi on tältä osin erityisen tärkeitä.

Ensinnäkin asetusehdotuksessa tehdään selväksi, että yritysten, jotka eivät ole sijoittautuneet unioniin, on sovellettava EU:n tietosuojalainsäädäntöä, kun ne tarjoavat tavaroita ja palveluja eurooppalaisille kuluttajille tai seuraavat näiden käyttäytymistä. Tietosuojaa koskeva perusoikeus on siis voimassa yrityksen tai sen tietojenkäsittely-yksikön maantieteellisestä sijainnista riippumatta[17].

Toiseksi asetusehdotuksessa vahvistetaan edellytykset, joiden mukaisesti tietoja voidaan siirtää EU:n ulkopuolelle. Tällaiset kansainväliset siirrot voidaan sallia vain silloin, kun nämä edellytykset, joilla taataan yksilön oikeudet korkeatasoiseen tietosuojaan, täyttyvät[18].

---

16 COM(2012) 10 final: Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta, Bryssel 25.1.2012, ja COM(2012) 11 final: Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus).

17 Komissio panee merkille, että Euroopan parlamentti tuki ja vahvisti tätä asetusehdotuksen 3 artiklaan kirjattua tärkeää periaatetta äänestäessään kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnassa 21. lokakuuta 2013 parlamentin jäsenten Jan-Philipp Albrechtin ja Dimitrios Droutsasin laatimista tietosuojauudistusta koskevista mietinnöistä.

18 Komissio panee merkille, että Euroopan parlamentin kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta ehdotti 21. lokakuuta 2013 pidetyssä äänestyksessään, että tulevaan asetukseen sisällytettäisiin säännös, jonka mukaan ulkomaiset viranomaiset voisivat pyytää EU:ssa kerättyjä

Kolmanneksi EU:n sääntöjen noudattaminen pyritään asetusehdotuksessa varmistamaan säätämällä oikeasuhteisista ja varoittavista seuraamuksista (enintään 2 prosenttia yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta)[19]. Uskottavat seuraamukset lisäävät yritysten halua noudattaa EU:n lainsäädäntöä.

Neljänneksi asetusehdotuksessa on selkeät säännöt tietojen käsittelijöiden (esimerkiksi pilvipalvelujen tarjoajien) velvoitteista ja vastuista, myös turvallisuuden osalta[20]. Kuten Yhdysvaltojen tiedustelutietojen keruuohjelmia koskevat paljastukset ovat osoittaneet, tämä on ratkaisevan tärkeää, koska nämä ohjelmat vaikuttavat pilveen tallennettuihin tietoihin. Pilvitallennustilaa tarjoavat yritykset, joita pyydetään toimittamaan henkilötietoja ulkomaiden viranomaisille, eivät myöskään voi väistää vastuutaan viittaamalla siihen, että ovat tietojen käsittelijöitä eivätkä rekisterinpitäjiä.

Viidenneksi uudistuspaketilla luodaan kattavat säännöt lainvalvonta-alalla käsiteltävien henkilötietojen suojaamiseksi.

Säädöspaketti hyväksyttäneen suunnitelmien mukaisesti vuoden 2014 aikana[21].

### 3.2. Safe harbor -järjestelmän turvallisuuden lisääminen

Safe harbor -järjestelmä on tärkeä osa EU:n ja Yhdysvaltojen kauppasuhteita, ja sitä käyttävät yritykset Atlantin molemmin puolin.

Komission kertomuksessa safe harbor -järjestelmän toiminnasta tuotiin esille joukko järjestelmään liittyviä puutteita. Järjestelmän puutteellinen avoimuus ja heikko noudattamisen valvonta ovat johtaneet siihen, että osa safe harbor -järjestelmään liittyneistä yrityksistä ei käytännössä noudata sen periaatteita. Tällä on kielteinen vaikutus EU:n kansalaisten perusoikeuksiin. Se johtaa myös tilanteeseen, jossa eurooppalaiset yritykset ovat epäedullisessa asemassa verrattuna sellaisiin niiden kanssa kilpaileviin yhdysvaltalaisiin yrityksiin, jotka toimivat järjestelmän puitteissa, mutta eivät käytännössä noudata sen periaatteita. Tämä puute vaikuttaa myös siihen yhdysvaltalaisten yritysten pääosaan, joka soveltaa järjestelmää asianmukaisesti. Safe harbor -järjestelmää voidaan käyttää EU:n kansalaisten henkilötietojen siirtämiseen EU:sta Yhdysvaltoihin myös silloin, kun Yhdysvaltojen tiedusteluviranomaiset velvoittavat yritykset luovuttamaan tietoja tiedustelutietojen keruuohjelmien puitteissa. Jos näitä puutteita ei korjata, EU:n yritykset joutuvat epäedulliseen kilpailuasemaan ja EU:n kansalaisten perusoikeus tietosuojaan vaarantuu.

Euroopan tietosuojaviranomaisten reaktio äskettäisiin valvontaohjelmapaljastuksiin on tuonut selvästi esille safe harbor -järjestelmän puutteet. Safe harbor -päätöksen 3 artiklan mukaan tietosuojaviranomaiset voivat tietyin edellytyksin keskeyttää järjestelmään liittyneille

---

henkilötietoja käyttöönsä vasta saatuaan kansalliselta tietosuojaviranomaiselta tähän ennakkoluvan, paitsi jos pyyntö esitetään keskinäistä oikeusapua koskevan sopimuksen tai muun kansainvälisen sopimuksen perusteella.

19 Komissio panee merkille, että kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta ehdotti 21. lokakuuta 2013 pidetyssä äänestyksessään komission ehdotuksen tiukentamista siten, että sakko voisi olla jopa 5 prosenttia yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta.

20 Komissio panee merkille, että kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta hyväksyi 21. lokakuuta 2013 pidetyssä äänestyksessään tietojen käsittelijöiden velvoitteiden ja vastuiden tiukentamisen erityisesti siltä osin kuin on kyse asetusehdotuksen 26 artiklasta.

21 Lokakuussa 2013 kokoontuneen Eurooppa-neuvoston päätelmissä todetaan seuraavaa: ”On tärkeää edistää kansalaisten ja yritysten luottamusta digitaalitalouteen. EU:n vahvan yleisen tietosuojakehyksen ja kyberturvallisuusdirektiivin ripeä hyväksyminen on oleellista digitaalisten sisämarkkinoiden toteuttamiseksi vuoteen 2015 mennessä.”

yrityksille suunnatut tietovirrat[22]. Saksan tietosuojaviranomaiset ovat päättäneet olla myöntämättä uusia lupia tietojen siirtämiseksi EU:n ulkopuolisiin maihin (esimerkiksi lupia tiettyjen pilvipalvelujen käyttöön). Ne aikovat myös tutkia, olisiko safe harbor -järjestelmään perustuvat tiedonsiirrot syytä keskeyttää[23]. Vaarana on, että tällaiset kansallisen tason toimenpiteet johtavat eroihin järjestelmän kattavuudessa, mikä puolestaan tarkoittaa sitä, että safe harbor -järjestelmä ei enää olisi ensisijainen mekanismi, kun on kyse henkilötietojen siirrosta EU:n ja Yhdysvaltojen välillä.

Komissiolla on direktiivin 95/46/EY nojalla valtuudet keskeyttää safe harbor -päätöksen soveltaminen tai kumota se, jos järjestelmän tarjoaman suojan taso ei enää ole riittävä. Lisäksi komissio voi päätöksen 3 artiklan mukaan kumota päätöksen, lykätä sen soveltamista tai rajoittaa sen soveltamisalaa ja päätöksen 4 artiklan mukaan puolestaan muuttaa päätöstä milloin tahansa sen täytäntöönpanosta saatujen kokemusten perusteella.

Tämän perusteella tarjolla on useita toimintavaihtoehtoja:

- vallitsevan tilanteen säilyttäminen;
- safe harbor -järjestelmän vahvistaminen ja sen toiminnan perusteellinen arviointi;
- safe harbor -päätöksen soveltamisen keskeyttäminen tai päätöksen kumoaminen.

Kun otetaan huomioon safe harbor -järjestelmässä havaitut heikkoudet, on selvää, että sen soveltamista ei voida jatkaa nykyiseen tapaan. Safe harbor -päätöksen kumoaminen vaikuttaisi kuitenkin haitallisesti järjestelmään liittyneiden EU:n ja Yhdysvaltojen yritysten etuihin. Komissio katsookin, että safe harbor -järjestelmää olisi vahvistettava.

Tässä yhteydessä olisi pyrittävä toisaalta korjaamaan avoimuuteen ja noudattamisen valvontaan liittyvät rakenteelliset puutteet ja toisaalta tekemään parannuksia itse safe harbor -periaatteisiin ja kansallisen turvallisuuden perusteella sallittavia poikkeuksia koskevaan järjestelyyn.

Jotta safe harbor -järjestelmä toimisi tarkoitetulla tavalla, Yhdysvaltojen viranomaisten olisi seurattava ja valvottava tehokkaammin ja järjestelmällisemmin sitä, miten järjestelmään liittyneet yritykset noudattavat yksityisyyden suojaa koskevia safe harbor -periaatteita. Järjestelmään kuuluvien yritysten tietosuojakäytäntöjen avoimuutta on parannettava. Lisäksi on syytä varmistaa, että EU:n kansalaisten käytettävissä on kohtuuhintaisia riitojenratkaisujärjestelmiä.

Komissio aloittaa viipymättä Yhdysvaltojen viranomaisten kanssa keskustelut todetuista puutteista. Keinoja tilanteen korjaamiseksi olisi löydettävä kesään 2014 mennessä, ja ne olisi toteutettava mahdollisimman pian. Tämän jälkeen komissio tekee kattavan arvioinnin safe harbor -järjestelmän toiminnasta. Tähän laajempaan tarkasteluprosessiin olisi kuuluttava avoin kuulemismenettely ja keskustelu Euroopan parlamentissa ja neuvostossa sekä keskusteluja Yhdysvaltojen viranomaisten kanssa.

---

[22] Safe harbor -päätöksen 3 artiklassa säädetään tarkemmin ottaen, että tällaiseen keskeytykseen voidaan turvautua tapauksissa, joissa on huomattavan todennäköistä, että järjestelmän 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.

[23] Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, lehdistötiedote 24.7.2013.

On myös tärkeää, että safe harbor -päätöksessä kansallisen turvallisuuden perusteella sallittua poikkeusta käytetään ainoastaan silloin kun se on ehdottoman välttämätöntä ja oikeasuhteista.

### 3.3. Tietosuojatakeiden lujittaminen lainvalvonta-alan yhteistyössä

EU ja Yhdysvallat neuvottelevat parhaillaan tietosuojaa käsittelevästä puitesopimuksesta, joka koskee henkilötietojen siirtoa ja käsittelyä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä. Tällainen sopimus, jossa varmistetaan korkeatasoinen henkilötietojen suoja, vahvistaisi merkittävästi luottamusta Atlantin molemmin puolin. Sopimuksella voitaisiin edistää EU:n kansalaisten tietosuojaa ja oikeuksia ja näin vahvistaa transatlanttista yhteistyötä rikollisuuden ja terrorismin ehkäisemiseksi ja torjumiseksi.

Komissiolle puitesopimuksen neuvottelemista koskevat valtuudet antavan päätöksen mukaan neuvottelujen tavoitteena pitäisi olla EU:n tietosuojasäännöstöä vastaavan korkeatasoisen suojan varmistaminen. Tätä varten olisi sovittava säännöistä ja takeista, jotka koskevat muun muassa tietojen käyttötarkoituksen rajoittamista ja tietojen säilyttämisen ehtoja ja kestoa. Komission olisi neuvottelujen yhteydessä myös saatava sitoumuksia, jotka koskevat täytäntöönpanokelpoisia oikeuksia, muun muassa EU:n kansalaisten oikeussuojakeinoja siinä tapauksessa, että he eivät asu Yhdysvalloissa[24]. Sen lisäksi, että EU ja Yhdysvallat tekevät tiivistä yhteistyötä yhteisiin turvallisuushaasteisiin vastaamiseksi, tarvitaan myös toimia, joilla varmistetaan, että kansalaisilla Atlantin molemmin puolin on samat oikeudet, kun samanlaisia tietoja käsitellään samassa tarkoituksessa. On myös tärkeää määritellä tarkasti kansallisten turvallisuustarpeiden perusteella tehtävät poikkeukset. Tältä osin olisi yhdessä vahvistettava tarvittavat suojatoimet ja rajoitukset.

Neuvottelut tarjoavat mahdollisuuden selventää, että Yhdysvaltojen lainvalvontaviranomaiset eivät voi saada suoraan käyttöönsä yksityisten yritysten hallussa olevia, EU:ssa sijaitsevia henkilötietoja, eikä niitä voida siirtää näille viranomaisille muutoin kuin virallisia yhteistyökanavia käyttäen. Näihin yhteistyökanaviin lukeutuvat keskinäistä oikeusapua koskevat sopimukset ja EU:n ja Yhdysvaltojen alakohtaiset sopimukset, joilla annetaan valtuudet tällaisiin siirtoihin. Muunlaista pääsyä tietoihin ei pitäisi sallia, paitsi jos se tapahtuu selkeästi määritellyissä poikkeustapauksissa ja asia on mahdollista saattaa tuomioistuimen käsiteltäväksi. Yhdysvaltojen olisi annettava tätä koskevia sitoumuksia[25].

---

[24] Ks. Washingtonissa 18. marraskuuta 2013 järjestetyn EU:n ja Yhdysvaltojen oikeus- ja sisäasiainministereiden kokouksen jälkeen annetun yhteisen lehdistötiedotteen asiaa koskeva kohta: ”Haluamme tämän vuoksi edetä nopeasti neuvotteluissa, jotka koskevat tarkoituksenmukaisen ja kattavan tietosuojapuitesopimuksen tekemistä lainvalvonnan alalla. Sopimuksella helpotettaisiin tietojen siirtoa poliisiyhteistyön ja rikosasioissa tehtävän oikeudellisen yhteistyön yhteydessä varmistamalla Yhdysvaltojen ja EU:n kansalaisten henkilötietojen korkeatasoinen suoja. Vakaana tavoitteenamme on ratkaista jäljellä olevat ongelmakohdat, joita molemmat osapuolet ovat ottaneet esille, mukaan lukien oikeussuojakeinoihin liittyvät kysymykset (keskeinen asiakohta EU:n kannalta). Pyrimme saamaan sopimusneuvottelut päätökseen kesään 2014 mennessä.”

[25] Ks. Washingtonissa 18. marraskuuta 2013 järjestetyn EU:n ja Yhdysvaltojen oikeus- ja sisäasiainministereiden kokouksen jälkeen annetun yhteisen lehdistötiedotteen asiaa koskeva kohta: ”Korostamme lisäksi EU:n ja Yhdysvaltojen välisen keskinäistä oikeusapua koskevan sopimuksen arvoa. Pyrimme edelleen määrätietoisesti varmistamaan, että sitä käytetään laajasti ja tehokkaasti todisteiden hankkimiseksi rikosoikeudenkäyntejä varten. Keskusteluja käytiin myös tarpeesta selventää, että lainvalvontaviranomaisten on käytettävä lainmukaisesti hyväksyttyjä kanavia, kun ne haluavat saada käyttöönsä yksityisten tahojen hallussa toisen osapuolen alueella olevia henkilötietoja. Päätimme myös, että keskinäistä oikeusapua koskevan sopimuksen toimintaa on tarpeen tarkastella sopimuksessa esitetyllä tavalla ja että neuvottelemme keskenämme aina, kun se on tarpeen.”

Näiden periaatteiden mukaisella puitesopimuksella saataneen luotua sellainen yleinen kehys, jonka puitteissa voidaan varmistaa korkeatasoinen suoja henkilötiedoille, joita siirretään Yhdysvaltoihin rikollisuuden ja terrorismin ehkäisemiseksi tai torjumiseksi. Jos tiedonsiirtojen luonne sitä edellyttää, voidaan lisäksi tehdä lisäsääntöjä ja -takeita sisältäviä alakohtaisia sopimuksia. Esimerkkinä voisivat tältä osin toimia EU:n ja Yhdysvaltojen väliset PNR- ja TFTP-sopimukset, joissa asetetaan tiukat ehdot tietojen siirtämiselle ja vahvistetaan asianmukaiset takeet EU:n kansalaisten oikeuksien turvaamiseksi.

### 3.4. Eurooppalaisten näkökohtien huomioon ottaminen Yhdysvalloissa meneillään olevassa uudistusprosessissa

Yhdysvaltojen presidentti Barack Obama on ilmoittanut käynnistävänsä maan kansallisten turvallisuusviranomaisten toimien ja alaa koskevan lainsäädännön tarkastelun. Tämä prosessi tarjoaa hyvän tilaisuuden käsitellä niitä huolenaiheita, joita hiljattain paljastuneet Yhdysvaltojen tiedustelutietojen keruuohjelmat ovat nostaneet esille EU:ssa. Tärkeintä olisi ulottaa Yhdysvaltojen kansalaisille ja muille asukkaille annetut takeet koskemaan myös EU:n kansalaisia, vaikka nämä eivät asuisi Yhdysvalloissa, lisätä tiedustelutoiminnan avoimuutta ja parantaa entisestään sen valvontaa. Tällaiset muutokset palauttaisivat luottamuksen EU:n ja Yhdysvaltojen väliseen tiedonvaihtoon ja kannustaisivat eurooppalaisia käyttämään internetin tarjoamia palveluja.

Yhdysvaltojen kansalaisiin ja muihin asukkaisiin sovellettavien takeiden ulottamisesta koskemaan myös EU:n kansalaisia voidaan todeta, että Yhdysvaltojen ja EU:n kansalaisia eri tavoin kohteleviin Yhdysvaltojen valvontaohjelmiin liittyviä oikeusperiaatteita olisi syytä tarkistaa, missä yhteydessä asiaa olisi tarkasteltava myös tarpeellisuuden ja suhteellisuuden näkökulmasta ja pitäen mielessä Yhdysvaltojen ja EU:n tiiviin turvallisuuskumppanuuden, joka perustuu yhteisiin arvoihin, oikeuksiin ja vapauksiin. Tämä vähentäisi Yhdysvaltojen tiedustelutietojen keruuohjelmien kielteisiä vaikutuksia eurooppalaisiin.

Yhdysvaltojen tiedustelutietojen keruuohjelmien oikeudellisesta kehyksestä ja sen tulkinnasta yhdysvaltalaisissa tuomioistuimissa samoin kuin näiden ohjelmien laajuudesta on kerrottava avoimemmin. Tällaisista muutoksista olisi hyötyä myös EU:n kansalaisille.

Yhdysvaltojen tiedustelutietojen keruuohjelmien valvontaa voitaisiin parantaa vahvistamalla ulkomaantiedusteluun liittyviä asioita käsittelevän tuomioistuimen (*Foreign Intelligence Surveillance Court*) roolia ja ottamalla käyttöön yksityishenkilöitä koskevia oikeuskeinoja. Näillä järjestelyillä voitaisiin vähentää eurooppalaisten henkilötietojen käsittelyä tapauksissa, joilla ei ole merkitystä kansallisen turvallisuuden kannalta.

### 3.5. Yksityisyyden suojaa koskevien sääntöjen edistäminen kansainvälisesti

Nykyaikaisten tietosuojamenetelmien esille nostamat kysymykset eivät rajoitu pelkästään tietojen siirtoon EU:n ja Yhdysvaltojen välillä. Henkilötietojen korkeatasoinen suoja olisi taattava kaikille luonnollisille henkilöille. Tietojen keräämistä, käsittelyä ja siirtoa koskevia EU:n sääntöjä olisi edistettävä kansainvälisesti.

Hiljattain on ehdotettu erinäisiä toimia, joilla voitaisiin edistää yksityisyyden suojaa erityisesti internetissä[26]. EU:n olisi varmistettava, että tällaisten toimien yhteydessä otetaan täysimääräisesti huomioon EU:n lainsäädännössä ja verkkoturvallisuusstrategiassa vahvistetut

[26] Ks. tältä osin Saksan ja Brasilian YK:n yleiskokoukselle ehdottama päätöslauselmaluonnos, jossa esitetään toimia yksityisyyden suojan varmistamiseksi niin internetissä kuin sen ulkopuolellakin.

perusoikeuksien, sananvapauden, henkilötietojen ja yksityisyyden suojaamisen periaatteet. Samalla olisi varmistettava, että nämä toimet eivät heikennä kyberavaruuden vapautta, avoimuutta ja turvallisuutta. Tämä käsittää myös demokraattisen ja tehokkaan useita sidosryhmiä kattavan hallintomallin.

Atlantin molemmin puolin käynnissä olevat tietosuojasäännösten uudistukset tarjoavat EU:lle ja Yhdysvalloille myös ainutlaatuisen tilaisuuden toimia esikuvana kansainvälisellä tasolla. Atlantin yli tapahtuvaa ja laajempaakin tietojenvaihtoa hyödyttäisi suuresti se, että Yhdysvaltojen oikeudellista kehystä lujitettaisiin muun muassa saattamalla voimaan kuluttajien tietosuojaa koskeva perusoikeuskirja (*Consumer Privacy Bill of Rights*), jota presidentti Obama esitti helmikuussa 2012 osana kattavaa suunnitelmaa kuluttajien yksityisyyden suojan parantamiseksi. Tiukkojen ja täytäntöönpanokelpoisten tietosuojasääntöjen soveltaminen sekä EU:ssa että Yhdysvalloissa muodostaisi vankan perustan rajat ylittävälle tiedonsiirrolle.

Yksityisyyden suojaa koskevia sääntöjä voitaisiin edistää kansainvälisellä tasolla myös kannustamalla maita liittymään Euroopan neuvoston yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Tähän yleissopimukseen voivat liittyä myös maat, jotka eivät ole Euroopan neuvoston jäseniä[27]. Kansainvälisillä foorumeilla sovittavilla suojatoimilla ja takeilla olisi saavutettava korkeatasoinen suoja, joka vastaa EU:n lainsäädännön vaatimuksia.

## 4. PÄÄTELMÄT JA SUOSITUKSET

Tässä tiedonannossa käsitellyt asiat edellyttävät toimia sekä Yhdysvalloilta että Euroopan unionilta ja sen jäsenvaltioilta.

Atlantin yli tapahtuvaan tietojenvaihtoon liittyvät ongelmat ovat ensinnäkin merkki siitä, että EU:n ja sen jäsenvaltioiden olisi syytä edetä ripeästi ja määrätietoisesti tietosuojalainsäädännön uudistamisessa. Nyt jos koskaan tarvitaan vahvoja tietosuojasääntöjä, jotka ovat selkeät ja täytäntöönpanokelpoiset myös silloin, kun tietoja siirretään ulkomaille. Sen vuoksi EU:n toimielinten olisi jatkettava työtä, jotta EU:n tietosuojauudistus saadaan hyväksyttyä keväällä 2014. Näin varmistetaan, että henkilötiedoilla on tehokas ja kattava suoja.

Atlantin yli tapahtuvan tietojen siirron merkityksen vuoksi on tärkeää, että tiedonsiirron perustana olevissa välineissä otetaan asianmukaisesti huomioon digitaaliajan haasteet ja mahdollisuudet sekä uusi teknologia, esimerkiksi pilvipalvelut. Nykyisillä ja tulevilla järjestelyillä ja sopimuksilla olisi varmistettava korkeatasoisen tietosuojan jatkuvuus transatlanttisessa tietojenvaihdossa.

Vahva safe harbor -järjestelmä hyödyttää niin EU:n ja Yhdysvaltojen kansalaisia kuin yrityksiäkin. Järjestelmää olisi lyhyellä aikavälillä vahvistettava paremman seurannan ja täytäntöönpanon keinoin, ja sen toimintaa olisi tämän pohjalta arvioitava kattavasti. Parannuksia tarvitaan, jotta voitaisiin varmistaa, että safe harbor -päätöksen alkuperäiset tavoitteet – tietosuojan jatkuvuus, oikeusvarmuus ja tietojen vapaa liikkuvuus EU:n ja Yhdysvaltojen välillä – saavutetaan jatkossakin.

[27] Yhdysvallat on jo liittynyt toiseen Euroopan neuvoston yleissopimukseen eli vuoden 2001 yleissopimukseen tietoverkkorikollisuudesta (nk. Budapestin yleissopimus).

Yhdysvaltojen viranomaisten olisi erityisesti tarpeen seurata ja valvoa tehokkaammin sitä, miten oman varmennuksen antaneet yritykset noudattavat yksityisyyden suojaa koskevia safe harbor -periaatteita.

On myös tärkeää, että safe harbor -päätöksessä kansallisen turvallisuuden perusteella sallittua poikkeusta käytetään ainoastaan silloin kun se on ehdottoman välttämätöntä ja oikeasuhteista.

Lainvalvonnan alalla käydään neuvotteluja puitesopimuksesta, jolla pyritään varmistamaan kansalaisille korkeatasoinen tietosuoja Atlantin molemmin puolin. Sopimus vahvistaisi eurooppalaisten luottamusta EU:n ja Yhdysvaltojen väliseen tietojenvaihtoon ja tarjoaisi perustan EU:n ja Yhdysvaltojen turvallisuusyhteistyön ja -kumppanuuden jatkokehittämiselle. Neuvotteluissa olisi saatava sitoumuksia siitä, että eurooppalaisilla on oikeus menettelytakeisiin, myös oikeussuojakeinoihin, vaikka he eivät asuisi Yhdysvalloissa.

Yhdysvaltojen hallinnolta olisi pyrittävä saamaan sitoumukset siitä, että maan lainvalvontaviranomaiset eivät hanki suoraan käyttöönsä yksityisten yritysten hallussa EU:ssa olevia henkilötietoja muutoin kuin virallisia yhteistyökanavia käyttäen. Näihin yhteistyökanaviin lukeutuvat keskinäistä oikeusapua koskevat sopimukset ja EU:n ja Yhdysvaltojen alakohtaiset sopimukset, esimerkiksi PNR- ja TFTP-sopimukset, joilla annetaan valtuudet tällaisiin siirtoihin tiukoin edellytyksin. Muussa tapauksessa tietojen suora käyttöön antaminen sallittaisiin vain, jos se tapahtuu selkeästi määritellyissä poikkeustapauksissa ja asia on mahdollista saattaa tuomioistuimen käsiteltäväksi.

Yhdysvaltojen olisi lisäksi ulotettava Yhdysvaltojen kansalaisille ja muille asukkaille annetut takeet koskemaan myös EU:n kansalaisia, vaikka nämä eivät asuisi Yhdysvalloissa, varmistettava ohjelmien tarpeellisuus ja oikeasuhteisuus ja lisättävä avoimuutta ja valvontaa siltä osin kuin on kyse maan kansallisiin turvallisuusviranomaisiin sovellettavasta lainsäädännöstä.

Tässä tiedonannossa mainituilla aloilla tarvitaan rakentavia toimia molemmin puolin Atlanttia. EU ja Yhdysvallat ovat strategisia kumppaneita, jotka pystyvät yhteistoimin poistamaan suhteidensa nykyiset jännitteet ja palauttamaan luottamuksen EU:n ja Yhdysvaltojen väliseen tiedonsiirtoon. Molempien osapuolten poliittinen ja oikeudellinen sitoutuminen yhteistyön jatkamiseen näillä aloilla on omiaan vahvistamaan transatlanttisia suhteita kokonaisuudessaan.

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]

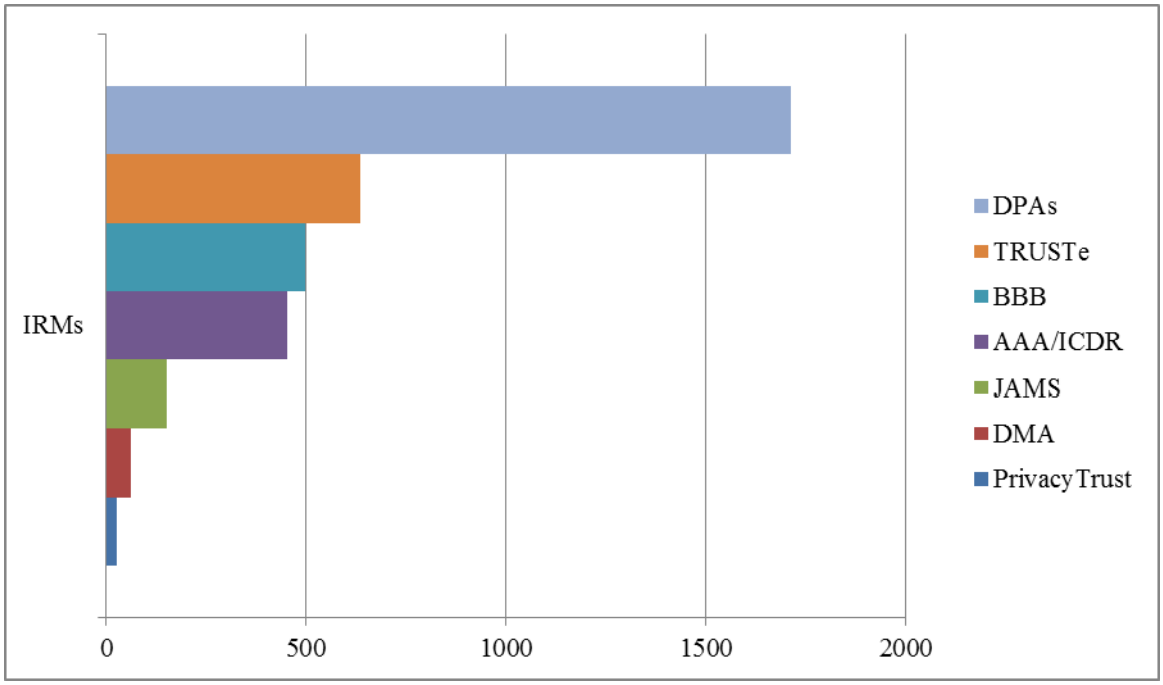
## 6 YKSITYISYYDEN SUOJAA KOSKEVIEN SAFE HARBOR -PERIAATTEIDEN VAHVISTAMINEN

### 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.*

EUROOPAN
KOMISSIO

Bryssel 27.11.2013
COM(2013) 844 final

# KOMISSION KERTOMUS EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

## matkustajarekisteritietojen käsittelyä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen täytäntöönpanon yhteisestä tarkastelusta

**KOMISSION KERTOMUS EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE**

**matkustajarekisteritietojen käsittelyä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen täytäntöönpanon yhteisestä tarkastelusta**

Amerikan yhdysvaltojen ja Euroopan unionin sopimus matkustajarekisteritietojen käytöstä ja siirtämisestä Yhdysvaltojen sisäisen turvallisuuden ministeriölle tuli voimaan 1. heinäkuuta 2012.

Sopimuksessa määrätään, että osapuolet tarkastelevat yhdessä sopimuksen täytäntöönpanoa ensimmäisen kerran vuoden kuluttua sen voimaantulosta ja sen jälkeen säännöllisesti, siten kuin yhdessä sovitaan. Yhteinen tarkastelu toteutettiin 8 ja 9. heinäkuuta 2013 Washingtonissa. Siinä keskityttiin pääasiassa sopimuksen täytäntöönpanoon kiinnittäen erityisesti huomiota matkustajarekisteritietojen, jäljempänä 'PNR-tiedot', siirtotapaan sekä PNR-tietojen edelleensiirtoon sopimuksen asiaa koskevien artiklojen ja sen johdanto-osan 18 kappaleen mukaisesti.

Yhteinen tarkastelu perustuu menetelmään, jonka EU:n ja Yhdysvaltojen edustajat kehittivät vuoden 2004 PNR-sopimuksen ensimmäistä, syyskuussa 2005 suoritettua yhteistä tarkastelua varten. Menetelmän ensimmäisessä vaiheessa Euroopan komissio lähetti Yhdysvaltojen sisäisen turvallisuuden ministeriölle (DHS) kyselylomakkeen ennen yhteistä tarkastelua. DHS vastasi siihen kirjallisesti ennen yhteistä tarkastelua. Toiseksi EU:n edustajat vierailivat DHS:n operaatiokeskuksessa. Kolmanneksi järjestettiin kokous, jossa DHS:n ja sen yksityisyyden suojasta vastaavan osaston, Yhdysvaltojen oikeusministeriön ja ulkoministeriön sekä EU:n edustajat keskustelivat yksityiskohtaisesti sopimuksen täytäntöönpanosta.

Ennen yhteistä tarkastelua DHS:n yksityisyyden suojasta vastaava osasto oli toteuttanut sisäisen tarkastelun, jossa keskityttiin siihen, miten DHS on pannut sopimuksen täytäntöön. Sen tarkoituksena oli selvittää, toimiiko DHS EU:n kanssa tehdyn sopimuksen mukaisesti.

EU:n edustajat totesivat, että DHS soveltaa sopimusta siinä vahvistettujen ehtojen mukaisesti. Se esimerkiksi käyttää tehokkaita suodattimia karsiakseen pois sellaiset tiedot, joilla ei ole kytköstä Yhdysvaltoihin, sekä tiedot, jotka eivät kuulu mihinkään sopimuksen liitteessä kuvatuista 19 luokasta. Arkaluonteisten tietojen häivyttämistä ja poistamista koskevia määräyksiä noudatetaan, ja DHS on ilmoittanut, että se ei ole koskaan tarkastellut arkaluonteisia tietoja operatiivisista syistä.

DHS noudattaa myös matkustajien oikeuksiin liittyviä sitoumuksia, erityisesti tarjoamalla asianmukaista tietoa ja kunnioittamalla matkustajien oikeutta itseään koskeviin tietoihin poikkeuksetta. Tässä yhteydessä olisi kuitenkin kiinnitettävä huomiota jäljempänä esitettyyn neljänteen suositukseen, joka koskee tarvetta lisätä avoimuutta matkustajien käytettävissä olevista muutoksenhakukeinoista.

DHS huolehtii tietojen jakamisesta muiden Yhdysvaltojen virastojen kanssa sopimuksen mukaisesti. Tietoja jaetaan tapauskohtaisesti, tiedonvaihto kirjautuu lokitietoihin ja se perustuu kirjallisiin sopimuksiin. Tietojen jakaminen myös kolmansien maiden kanssa on mahdollisimman vähäistä ja sopimuksen mukaista.

Yleisellä tasolla suositellaan, että DHS:n yksityisyyden suojasta vastaava osasto suorittaa toisen sisäisen tarkastelun ennen seuraavaa yhteistä tarkastelua. Osapuolten mukaan seuraava yhteinen tarkastelu olisi hyvä järjestää vuoden 2015 alkupuoliskolla.

On myös suositeltavaa siirtyä kokonaan tarjontamenetelmään (”push-menetelmä”) mahdollisimman pian ja joka tapauksessa 1. heinäkuuta 2014 mennessä, kuten 15 artiklan 4 kohdassa edellytetään.

Edelleen suositellaan, että Yhdysvallat ja EU edistävät yhteisten standardien, erityisesti IATA:n, lentoyhtiöiden ja viranomaisten kehittämän PNRGOV-standardin, käyttöä. Tässä yhteydessä olisi hyvä, jos IATA:ssa käydyt keskustelut yhteisestä ”push”-standardista johtaisivat yhteiseen tilapäiseen ”push”-standardiin.

Sopimuksen täytäntöönpanosta huolimatta joitakin parannuksia tarvitaan edelleen. Tämä koskee ensiksikin sopimuksen 8 artiklan 1 kohdassa tarkoitetun kuuden kuukauden jakson (jonka jälkeen PNR-tiedoista erotetaan tunnistamisen mahdollistavat tiedot) alkamista. Tällä hetkellä tämän jakson katsotaan alkavan vasta, kun PNR-tietoja viimeisen kerran päivitetään DHS:n automatisoidussa kohdentamisjärjestelmässä (ATS), johon PNR-tiedot tallennetaan, eikä siitä kun tiedot ladataan ATS:ään. Suositellaan, että kuuden kuukauden jakson katsottaisiin alkavan siitä, kun PNR-tiedot ladataan ATS:ään (latauspäivästä käytetään nimitystä *ATS Load Date*) eli päivästä, jolloin tiedot ensimmäisen kerran tallennetaan ATS:ään. Tähänastisessa käytännössä kuuden kuukauden jakson laskenta on viivästynyt, sillä se on alkanut vasta PNR-tietojen viimeisestä päivityksestä ATS:ssä.

Toiseksi olisi kiinnitettävä erityistä huomiota tilapäisen ”pull”-menetelmän käyttöön. Suositellaan, että DHS pitäisi nykyisten lokitietojen lisäksi tarkemmin kirjaa menetelmän käytön syistä kussakin tapauksessa, jotta voitaisiin arvioida paremmin käytön oikeasuhteisuutta ja valvoa käyttöä tehokkaammin, sillä menetelmää on tarkoitettu käytettävän vain poikkeuksellisesti.

Kolmanneksi DHS:ää pyydetään noudattamaan sitoumustaan vastavuoroisuuteen ja oma-aloitteisesti jakamaan yksittäisiä PNR-tietoja ja PNR-tiedoista johdettuja analyyttisiä tietoja EU:n jäsenvaltioiden ja tarvittaessa Europolin ja Eurojustin kanssa.

Neljänneksi suositellaan lisäämään avoimuutta Yhdysvaltojen lainsäädännön mukaisista muutoksenhakukeinoista. Avoimuutta tarvitaan, jotta matkustajilla, jotka eivät ole Yhdysvaltojen kansalaisia tai laillisia asukkaita, olisi mahdollisuus kiistää DHS:n päätökset, jotka liittyvät PNR-tietojen käyttöön, etenkin jos niiden käyttö voi vaikuttaa siihen, että liikenteenharjoittajalle suositellaan, ettei matkustajaa oteta lennolle.

DHS on myös toteuttanut toimia, jotka ylittävät sopimuksen vaatimukset. DHS ilmoittaa Euroopan komissiolle 48 tunnin kuluessa, jos pääsyä arkaluonteisiin PNR-tietoihin on käytetty. DHS on ottanut käyttöön uuden menettelyn, jonka mukaisesti se tarkastelee ATS:n käyttöä neljännesvuosittain sekä kaikkia matkustamiseen liittyviä skenaarioita, analyysejä ja sääntöjä varmistaakseen, että ne ovat oikeasuhteisia ja vaikuttavat mahdollisimman vähän vilpittömässä mielessä liikkuvien matkustajien kansalaisoikeuksiin ja -vapauksiin ja yksityisyyden suojaan, sekä matkustajiin kohdistuvan syrjinnän välttämiseksi.

Siitä huolimatta, että sopimusta arvioidaan yhdessä sen 23 artiklan 1 kohdan mukaisesti neljän vuoden kuluttua sen voimaantulosta, on suoritettu alustava arviointi siitä, vastaako PNR-järjestelmä tarkoitustaan terrorismin ja muiden luonteeltaan kansainvälisten rikosten torjunnassa. Alustavan arvioinnin mukaan PNR-järjestelmä tarjoaa DHS:lle mahdollisuuden tehdä kaikista matkustajista ennakkoarviointi 96 tuntia ennen matkaan lähtöä, jolloin DHS:lle jää riittävästi aikaa kaikkiin taustaselvityksiin ja toimenpiteiden valmisteluun ennen matkustajan saapumista. DHS saa tiedoista tukea myös päättäessään, voidaanko matkustaja ottaa lennolle vai ei. Se tarjoaa DHS:lle myös mahdollisuuden riskinarviointiin erilaisiin skenaarioihin perustuvien kohdentamissääntöjen perusteella, jotta voitaisiin havaita ennalta tuntemattomat, mahdollisesti suuren riskin aiheuttavat henkilöt. Lisäksi se tarjoaa

mahdollisuuden tehdä kytkentöjä matkustajien välillä ja tunnistaa rikollisia, jotka kuuluvat samaan järjestäytyneen rikollisuuden ryhmittymään. DHS:n mukaan PNR-tietoja on käytetty menestyksellä myös sen selvittämiseen, minkälaisia suuntauksia, esimerkiksi reittivalinnan suhteen, rikollisten matkustamiseen liittyy.

Tämän tiedonannon liitteenä on yhteistä tarkastelua koskeva kertomus, joka jakautuu kolmeen osaan. Luvussa 1 esitetään yleiskatsaus tarkastelun taustasta ja tarkoituksesta sekä tarkastelun suoritustavoista. Luvussa 2 esitellään tarkastelun tärkeimmät havainnot ja asiat, joihin DHS:n pitää kiinnittää enemmän huomiota. Tätä lukua täydentää liite A, joka sisältää kyselylomakkeen ja DHS:n vastaukset siihen. Luvussa 3 esitellään tarkastelun yleiset päätelmät. Liitteessä B esitetään tarkastelun suorittaneiden EU:n ja Yhdysvaltojen ryhmien kokoonpano.

EUROOPAN
KOMISSIO

Bryssel 27.11.2013
COM(2013) 843 final

# KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

## Euroopan komission ja Yhdysvaltojen valtiovarainministeriön yhteisestä kertomuksesta, jossa tarkastellaan toimitettujen TFTP-tietojen hyödyllisyyttä rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä Euroopan unionista Yhdysvaltoihin terrorismin rahoituksen jäljittämisohjelman tarkoituksiin tehdyn Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen 6 artiklan 6 kohdan nojalla

**KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE**

# Euroopan komission ja Yhdysvaltojen valtiovarainministeriön yhteisestä kertomuksesta, jossa tarkastellaan toimitettujen TFTP-tietojen hyödyllisyyttä rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä Euroopan unionista Yhdysvaltoihin terrorismin rahoituksen jäljittämisohjelman tarkoituksiin tehdyn Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen 6 artiklan 6 kohdan nojalla

## 1. Oikeusperusta

Euroopan komissio ja Yhdysvaltojen valtiovarainministeriö ovat laatineet yhteisen kertomuksen rahaliikenteen sanomanvälitystietojen käsittelystä ja siirtämisestä Euroopan unionista Yhdysvaltoihin terrorismin rahoituksen jäljittämisohjelman tarkoituksiin tehdyn Euroopan unionin ja Yhdysvaltojen välisen sopimuksen, jäljempänä ’TFTP-sopimus’, nojalla toimitettujen TFTP-tietojen hyödyllisyydestä, jäljempänä ’yhteinen kertomus’, kuten sopimuksen 6 artiklan 6 kohdassa määrätään. Kertomuksessa ”keskitytään erityisesti useita vuosia säilytettävien tietojen ja 13 artiklan mukaisesti suoritetusta yhteisestä tarkastelusta saatujen asianmukaisten tietojen hyödyllisyyteen”.

## 2. Menettelyihin liittyvät näkökohdat

Euroopan komissio ja Yhdysvaltojen valtiovarainministeriö ovat yhdessä päättäneet tämän kertomuksen laatimista koskevista yksityiskohdista TFTP-sopimuksen 6 artiklan 6 kohdan mukaisesti.

Euroopan komissio ja Yhdysvaltojen valtiovarainministeriö aloittivat neuvottelut kertomuksen laatimiseen liittyvien yksityiskohtien, toimivallan ja menettelyjen vahvistamiseksi joulukuussa 2012. EU:n ja Yhdysvaltojen tarkasteluvaltuuskunnat pitivät 25. helmikuuta 2013 Washingtonissa (D.C.) kokouksen, jossa keskusteltiin kertomuksen valmistelusta ja kutsuttiin koolle toinen kokous, joka pidettiin Europolin tiloissa Haagissa 14. toukokuuta 2013. Haagin-kokouksessa EU:n ja Yhdysvaltojen valtuuskunnat tapasivat myös Europolin edustajia, joiden kanssa keskusteltiin kaikkien osapuolten alkupanoksesta ja siitä, miten sen jälkeen edettäisiin.

Euroopan komissio järjesti EU:n puolesta jäsenvaltioiden edustajien kanssa luottamuksellisen kokouksen 13. toukokuuta 2013. Jäsenvaltiot ja Europol ovat toimittaneet kirjallisia selvityksiä, jotka on otettu huomioon kertomuksen laatimisessa. Europol esitti selvityksensä laatimista varten kaikille asianomaisille jäsenvaltioille kyselyn, jossa niiltä pyydettiin tietoja kertomusta varten. Kyselyn tarkoituksena oli kerätä ajantasaista tietoa TFTP-sopimuksen nojalla toimitettavien tietojen hyödyllisyydestä asianomaisten jäsenvaltioiden toimivaltaisten viranomaisten tutkimien tapausten yhteydessä.

Yhdysvaltojen tarkasteluvaltuuskunta arvioi TFTP-sopimuksen nojalla toimitettujen tietojen hyödyllisyyttä haastattelemalla ajanjaksolla 1. helmikuuta – 24. toukokuuta 2013 eri virastoissa työskenteleviä terrorismintutkijoita, tarkastelemalla terrorismintorjuntatapauksia, joissa oli hyödynnetty TFTP-tietoja, ja analysoimalla yli tuhat TFTP-raporttia.

## 3. Soveltamisala

Kertomuksen laatimisessa käytetyt tiedot ovat peräisin Yhdysvaltojen valtiovarainministeriöltä, Europolilta ja EU:n jäsenvaltioilta. Kertomuksessa keskitytään siihen, millä tavoin TFTP-tietoja on käytetty ja mitä hyötyä niistä on ollut terrorismintorjuntatutkimuksissa Yhdysvalloissa ja EU:ssa. Kertomuksessa esitetään useita käytännön esimerkkejä siitä, miten kolme vuotta tai kauemmin säilytetyt TFTP-tiedot ovat edistäneet terrorismintorjuntatutkimuksia Yhdysvalloissa ja EU:ssa jo ennen kuin TFTP-sopimus tuli voimaan 1. elokuuta 2010 ja sen jälkeen. Tämän kertomuksen ohella esimerkkejä TFTP-tietojen hyödyllisyydestä ja merkityksestä on esitetty niiden kahden yhteisen tarkastelun yhteydessä, jotka on tehty helmikuussa 2011 ja lokakuussa 2012 TFTP-sopimuksen 13 artiklan nojalla. Yhdessä nämä tosiseikkoihin ja konkreettisiin tapauksiin perustuvat tiedot antavat merkittävää lisätietoa TFTP-ohjelman toiminnasta ja sen hyödyllisyydestä.

Kertomuksessa tarkastellaan myös sitä, miten Yhdysvaltojen valtiovarainministeriö on tarkastellut tietojen säilyttämisaikoja ja valikoimattomien tietojen poistamista.

Kertomus osoittaa, että TFTP-sopimuksen nojalla toimitetut tiedot, mm. tiedot, joita on säilytetty usean vuoden ajan, ovat olleet erittäin hyödyllisiä terrorismintorjuntatutkimuksissa sekä Yhdysvalloissa että Euroopassa ja muuallakin.

Komissio toimittaa yhteisen kertomuksen Euroopan parlamentille ja neuvostolle tämän tiedonannon liitteenä.

EUROPEISKA
KOMMISSIONEN

Bryssel den 27.11.2013
COM(2013) 846 final

# MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

## Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna

## 1. INLEDNING: DE FÖRÄNDRADE FÖRUTSÄTTNINGARNA FÖR BEHANDLING AV DATA I EU OCH FÖRENTA STATERNA

Europeiska unionen och Förenta staterna är strategiska partner, och detta partnerskap är av största betydelse för att vi ska kunna främja våra gemensamma värderingar, vår säkerhet och vårt gemensamma ledarskap i globala frågor.

Förtroendet för partnerskapet har dock påverkats negativt och behöver återställas. EU, dess medlemsstater och medborgarna har emellertid uttryckt stor oro efter avslöjandena om storskaliga amerikanska program för insamling av underrättelseinformation, särskilt när det gäller skyddet av personuppgifter[1]**.** Massövervakning av privat kommunikation är, oavsett om den drabbar medborgare, företag eller politiska ledare, oacceptabel.

Överföringen av personuppgifter är en viktig och nödvändig del av de transatlantiska förbindelserna. Den utgör en integrerad del av handelsutbytena över Atlanten, också för nya och växande digitala affärsverksamheter, såsom sociala medier eller molntjänster, där stora mängder data överförs från EU till Förenta staterna. De utgör även ett viktigt inslag i samarbetet mellan EU och Förenta staterna i fråga om brottsbekämpning och i samarbetet mellan medlemsstaterna och Förenta staterna på området för nationell säkerhet. För att underlätta dataflödena och samtidigt garantera en sådan hög nivå av uppgiftsskydd som krävs enligt EU-lagstiftningen, har Förenta staterna och EU upprättat en rad avtal och arrangemang.

Handelsrelaterade frågor behandlas i beslut 2000/520/EG[2] (nedan kallat *Safe Harbour-beslutet*). Detta beslut ger en rättslig grund för överföringar av personuppgifter från EU till företag som är etablerade i Förenta staterna och som har anslutit sig till Safe Harbour-principerna om integritetsskydd).

Utbytet av personuppgifter mellan EU och Förenta staterna för brottsbekämpningsändamål, inbegripet förebyggande och bekämpning av terrorism och andra former av allvarlig brottslighet, regleras av ett antal avtal på EU-nivå. Det rör sig om avtalet om ömsesidig rättslig hjälp[3], avtalet om användning och överföring av passageraruppgifter (PNR)[4], avtalet om behandling och överföring av uppgifter om finansiella meddelanden i syfte att bekämpa terrorism (*Terrorism Financing Tracking Programme* –TFTP)[5], och avtalet mellan Europol och Förenta staterna. Dessa avtal behandlar stora säkerhetsrelaterade utmaningar och främjar EU:s och Förenta staterna gemensamma säkerhetsintressen, samtidigt som de garanterar skyddet av personuppgifter. Dessutom håller EU och Förenta staterna på att förhandla fram ett ramavtal (”paraplyavtal”) om dataskydd på området för polissamarbete och straffrättsligt

---

1 I detta meddelande inbegriper hänvisningar till EU-medborgare även registrerade personer som inte är medborgare i EU, men som ändå omfattas av Europeiska unionens dataskyddslagstiftning.

2 Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, 25.8.2000, s. 7).

3 Rådets beslut 2009/820/Gusp av den 23 oktober 2009 om ingående på Europeiska unionens vägnar av avtalet om utlämning mellan Europeiska unionen och Amerikas förenta stater och av avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater (EUT L 291, 7.11.2009, s. 40).

4 Rådets beslut 2012/472/EU av den 26 april 2012 om ingående av avtalet mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter till Förenta staternas Department of Homeland Security (EUT L 215, 11.8.2012, s. 4)

5 Rådets beslut av den 13 juli 2010 om ingående av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP) (EUT L 195, 27.7.2010, s. 3).

samarbete [6]. Syftet är att garantera att personuppgifter som blir föremål för utbyte omfattas av ett gott skydd, och därigenom ytterligare främja samarbetet mellan EU och Förenta staterna i kampen mot brottslighet och terrorism, på grundval av gemensamma värderingar och överenskomna garantier.

Dessa instrument har utformats för en miljö där flödena av personuppgifterna får allt större betydelse.

Å ena sidan har utvecklingen av den digitala ekonomin lett till en exponentiell tillväxt i uppgiftsbehandlingens kvantitet, kvalitet, mångfald och natur. Medborgarnas användning av elektroniska kommunikationstjänster i vardagen har ökat. Personuppgifter har blivit en värdefull tillgång. EU-medborgarnas personuppgifter uppskattades till ett värde av 315 miljarder euro 2011, en siffra som kan komma att öka till nästan en biljon euro till 2020 [7]. Marknaden för analys av stora uppgiftsmängder ökar med 40 % om året i världen som helhet[8]. På samma sätt har den tekniska utvecklingen, till exempel i samband med datormoln, satt perspektiv på begreppet internationell överföring av uppgifter, eftersom gränsöverskridande dataflöden håller på att bli en vardagsrealitet.[9]

Den ökade användningen av elektronisk kommunikation och databehandlingstjänster, däribland molntjänster, har också bidragit till att på ett betydande sätt vidga omfattningen och betydelsen av transatlantiska överföringar av personuppgifter. Faktorer som amerikanska företags centrala ställning i den digitala ekonomin[10], det förhållandet att en stor del av den elektroniska kommunikationen dirigeras över Atlanten och volymen av elektroniska dataflöden mellan EU och Förenta staterna, har fått ännu större betydelse.

Å andra sidan ger moderna metoder för överföring av personuppgifter upphov till nya och viktiga frågeställningar. Detta gäller såväl nya metoder för storskalig bearbetning av konsumentdata som utförs av privata företag för kommersiella ändamål och underrättelsemyndigheters ökade förmåga till storskalig övervakning av kommunikationsuppgifter.

Omfattande amerikanska program för insamling av underrättelseinformation, t.ex. Prism, inkräktar på européers grundläggande rättigheter, särskilt rätten till ett privatliv och rätten till skydd av personuppgifter. Dessa program pekar också på ett samband mellan statlig övervakning och uppgiftsbehandling som utförs av privata företag, särskilt amerikanska internetföretag. Som en följd av detta kan de få ekonomiska konsekvenser. Om medborgare är oroade över den omfattande behandling av deras personuppgifter som utförs av privata företag eller av övervakningen av personuppgifter från underrättelsetjänster vid användning av internettjänster, kan detta påverka deras förtroende för den digitala ekonomin, eventuellt med negativa konsekvenser för tillväxten.

Denna utveckling ställer uppgiftsflödena mellan EU och Förenta staterna i ett nytt perspektiv, och det här meddelandet tar upp de utmaningar som vi måste kunna möta. I meddelandet undersöks det fortsatta arbetet på grundval av slutsatserna i rapporten från EU-ledamöterna i EU:s och Förenta staternas gemensamma tillfälliga arbetsgrupp och meddelandet om Safe Harbour.

---

6 Den 3 december antog rådet beslutet om att bemyndiga kommissionen att förhandla om avtalet. Se IP/10/1661 av den 3 december 2010.

7 Boston Consulting Group, The Value of our Digital Identity, november 2012.

8 McKinsey, Big data: The next frontier for innovation, competition, and productivity, 2011

9 Meddelande om frigörande av de molnbaserade tjänsternas potential i Europa, KOM(2012) 529 slutlig.

10 T.ex. det sammanlagda antalet unika besökare till Microsoft Hotmail, Google Gmail och Yahoo! Antalet e-postmeddelanden från europeiska länder uppgick i juni 2012 till över 227 miljoner, vilket överskuggade alla andra leverantörer. Det samlade antalet unika europeiska besökare på Facebook och Facebook Mobile uppgick i mars 2012 till 196,5 miljoner, vilket gör Facebook till det största sociala nätverket i Europa. Google är den ledande sökmotorn för internet, och används av 90,2 % av världens internetanvändare. Den amerikanska mms-tjänsten What's ap användes i juni 2013 av 91 % av alla iPhone-användare i Tyskland.

Det syftar till att tillhandahålla en effektiv strategi för att återskapa förtroendet och förbättra samarbetet mellan EU och Förenta staterna på dessa områden samt stärka de transatlantiska förbindelserna i bredare bemärkelse.

Detta meddelande grundar sig på antagandet att nivån på skyddet av personuppgifter måste behandlas i sitt rätta sammanhang, utan att det påverkar andra aspekter av förbindelserna mellan EU och Förenta staterna, inbegripet de pågående förhandlingarna om ett transatlantiskt partnerskap för handel och investeringar. Därför är det inte aktuellt att diskutera frågan om uppgiftsskyddsnormer inom ramen för det transatlantiska partnerskapet för handel investeringar, som fullt ut kommer att respektera bestämmelserna om skydd av personuppgifter.

Det är viktigt att notera att även om EU kan vidta åtgärder rörande frågor som omfattas av EU:s behörighet, särskilt för att säkerställa en korrekt tillämpning av EU-rätten[11], är den nationella säkerheten ett område som helt omfattas av varje medlemsstats eget ansvar[12].

## 2. INVERKAN PÅ INSTRUMENT FÖR ÖVERFÖRING AV UPPGIFTER

När det gäller uppgifter som överförs för kommersiella ändamål har principen om Safe Harbour visat sig vara ett viktigt verktyg för överföring av uppgifter mellan EU och Förenta staterna. Dess kommersiella betydelse har ökat allteftersom flödena av personuppgifter har fått en större betydelse i de transatlantiska handelsförbindelserna. Över de senaste 13 åren har systemet med Safe Harbour utvecklats så att det nu omfattar över 3 000 företag, av vilka hälften har anmält sig under de senaste fem åren. Trots detta har farhågorna ökat när det gäller nivån på skyddet av EU-medborgares personuppgifter som överförs till Förenta staterna inom ramen för Safe Harbour-systemet. Det faktum att systemet är frivilligt och bygger på förklaringar har lett till ökat fokus på öppenhet och efterlevnad. Även om en majoritet av de berörda amerikanska företagen tillämpar systemets principer, finns det vissa självcertifierade företag som har valt att avstå. Det förhållandet att vissa självcertifierade företag inte följer Safe Harbour-principerna för skydd av privatlivet innebär att dessa företag får en konkurrensfördel jämfört med europeiska företag som är verksamma på samma marknader.

Safe Harbour-systemet ger möjlighet att införa inskränkningar i uppgiftsskyddet när det nödvändigt med hänsyn med hänsyn till den nationella säkerheten[13], men det har ifrågasatts huruvida den storskaliga insamlingen och behandlingen personuppgifter inom ramen för de amerikanska övervakningsprogrammen är nödvändig och proportionerlig för att ta hänsyn till de nationella säkerhetsintressena. Det framgår också av de resultat som EU:s och Förenta staternas tillfälliga arbetsgrupp har kommit fram till att EU-medborgare inte omfattas av samma rättigheter och rättssäkerhetsgarantier som amerikaner inom ramen för dessa program.

Räckvidden av dessa övervakningsprogram, i kombination med ojämlik behandling av EU-medborgare, medför att den skyddsnivå som erbjuds genom Safe Harbour-systemet måste ifrågasättas. EU-medborgares personuppgifter som sänds till Förenta staterna inom ramen för Safe Harbour är åtkomliga för och kan behandlas ytterligare av amerikanska myndigheter på ett sätt som är oförenligt med de ändamål för vilka uppgifterna ursprungligen samlades in i EU och sedermera överfördes till Förenta staterna. En majoritet av de amerikanska internetföretag som förefaller vara mer direkt berörda av dessa program är certifierade enligt Safe Harbour-systemet.

---

11 Se domstolens dom i mål C-300/11, ZZ mot Secretary of State for the Home Department.

12 Artikel 4.2 i Fördraget om Europeiska unionen.

13 Se t.ex. Safe Harbour-beslutet, bilaga I.

När det gäller utbyte av uppgifter för brottsbekämpande ändamål har befintliga avtal (PNR, TFTP) visat sig vara mycket värdefulla verktyg för att möta gemensamma säkerhetshot med koppling till allvarlig gränsöverskridande brottslighet och terrorism, samtidigt som de innehåller skyddsbestämmelser som garanterar en hög nivå på uppgiftsskyddet[14]. Dessa garantier omfattar även EU-medborgare, och avtalen föreskriver mekanismer för att se över genomförandet och behandla problem i samband med detta. TFTP-avtalet inför också ett system för tillsyn, där EU:s oberoende övervakare kan kontrollera hur uppgifter som omfattas av avtalet blir föremål för åtgärder från Förenta staternas sida.

Mot bakgrund av de farhågor som framförts i EU med avseende på amerikanska övervakningsprogram, har Europeiska kommissionen använt sig av dessa mekanismer för att kontrollera hur avtalen tillämpas. När det gäller PNR-avtalet gjordes en gemensam översyn med deltagande av experter från både EU och Förenta staterna, där man tittade på hur avtalet har tillämpats [15]. Denna översyn gav ingen indikation på att de amerikanska övervakningsprogrammen utsträcker sig till eller påverkar passageraruppgifter som omfattas av PNR-avtalet. När det gäller TFTP-avtalet beslutade kommissionen att inleda formella samråd efter påståenden om att amerikanska underrättelsetjänster fått direkt tillgång till personuppgifter i EU, i strid med avtalet. Vid dessa samråd framkom inget som pekar på en överträdelse av TFTP-avtalet, med fick Förenta staterna att lämna en skriftlig försäkran om att ingen direkt insamling av uppgifter hade ägt rum i strid med bestämmelserna i avtalet.

Den omfattande insamlingen och behandlingen av personuppgifter inom ramen för de amerikanska övervakningsprogrammen föranleder dock en fortsatt mycket ingående övervakning av genomförandet av de PNR och TFTP-avtalen också i framtiden. EU och Förenta staterna därför enats om gå vidare med nästa gemensamma översyn av TFTP-avtalet, som kommer att genomföras under våren 2014. Inom ramen för denna och framtida gemensamma översyner är det viktigt att säkerställa öppenhet om hur tillsynen fungerar och hur den bidrar till att skydda EU-medborgares personuppgifter. Parallellt kommer åtgärder att vidtas för att se till att tillsynssystemet fortsätter att rikta uppmärksamheten på hur uppgifter som överförs till Förenta staterna inom ramen för avtalet behandlas, med fokus på hur uppgifterna delas mellan amerikanska myndigheter.

För det tredje understryker den ökade volymen av behandlade personuppgifter betydelsen av tillämpliga rättsliga och administrativa garantier. Ett av målen med EU:s och Förenta staternas tillfälliga arbetsgrupp var att fastställa vilka skyddsmekanismer som tillämpas för att minimera uppgiftsbehandlingens effekter på EU-medborgarnas grundläggande rättigheter. Skyddsåtgärder är också nödvändiga för att skydda företag. Vissa amerikanska lagar, t.ex. Patriot Act, gör det möjligt för amerikanska myndigheter att direkt begära att företag ger tillgång till uppgifter som lagras i EU. Europeiska företag, och amerikanska företag som finns i EU, kan således åläggas att överföra uppgifter till Förenta staterna i strid med EU-rätten och medlemsstaternas lagstiftning. De hamnar således i kläm mellan motstridiga rättsliga skyldigheter. Den rättsosäkerhet som uppstår till följd att sådana direkta uppmaningar att lämna tillgång till uppgifter kan bli till hinder för utvecklingen av nya digitala tjänster, exempelvis datormolntjänster, vilka annars kan ge effektiva och billiga lösningar för enskilda och företag.

---

[14] Se gemensam rapport från kommissionen och det amerikanska finansdepartementet rörande värdet av uppgifter som tillhandahållits inom ramen för TFTP, i enlighet med artikel 6.6 i avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism

[15] Se kommissionens rapport Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security.

## 3. ETT EFFEKTIVT UPPGIFTSSKYDD

Överföringen av personuppgifter mellan EU och Förenta staterna är ett viktigt inslag i de transatlantiska handelsförbindelserna. Informationsutbyte är också en viktig del av säkerhetssamarbetet mellan EU och Förenta staterna, och dessutom avgörande för förutsättningarna att uppnå det gemensamma målet att förebygga och bekämpa allvarlig brottslighet och terrorism. De senaste avslöjandena om de amerikanska programmen för insamling av underrättelseinformation har haft en negativ inverkan på det förtroende som samarbetet bygger på. Det har särskilt påverkat förtroendet för hur personuppgifter behandlas. Följande åtgärder bör vidtas för att återställa förtroendet för överföringar av personuppgifter, till förmån för den digitala ekonomin, säkerheten i såväl EU som Förenta staterna och de transatlantiska förbindelserna i bredare bemärkelse.

### 3.1 Reformeringen av uppgiftsskyddet i EU

Den uppgiftsskyddsreform som kommissionen föreslog i januari 2012[16]är av stor betydelse för att stärka skyddet av personuppgifter. Fem delar av det föreslagna uppgiftsskyddspaketet är av särskild betydelse.

När det gäller det geografiska tillämpningsområdet klargörs i den föreslagna förordningen att företag som inte är etablerade i EU kommer att vara tvungna att tillämpa EU-lagstiftningen om uppgiftsskydd när de erbjuder varor och tjänster till de europeiska konsumenter eller övervakar dess beteende. Med andra ord kommer den grundläggande rätten till skydd av personuppgifter att respekteras, oberoende av var ett företag eller dess anläggning för behandling av uppgifter finns [17].

När det gäller internationella överföringar fastställer den föreslagna förordningen villkoren för överföring av uppgifter utanför EU. Överföringar kan endast tillåtas om dessa villkor, som garanterar individens rätt till en hög skyddsnivå, är uppfyllda [18].

De förslagna bestämmelserna föreskriver proportionerliga och avskräckande sanktioner (upp till 2 % av ett företags årliga omsättning) för att säkerställa att företag följer EU-lagstiftningen[19]. Förekomsten av trovärdiga sanktioner kommer att öka företagens incitament att följa EU-lagstiftningen.

Den föreslagna förordningen innehåller klara regler om skyldigheter och ansvar för uppgiftsbehandlare, t.ex. leverantörer av molntjänster, även säkerhetsbestämmelser[20]. Som avslöjandena rörande de amerikanska programmen för insamling av underrättelseinformation

---

16 KOM(2012) 10 slutlig: Förslag till Europaparlamentets och rådets direktiv om skyddet av enskilda vid behöriga myndigheters behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, samt fri rörlighet för sådana uppgifter, Bryssel 25.1.2012, samt KOM(2012) 11 slutlig. Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning),

17 Kommissionen noterar att Europaparlamentet bekräftade och understödde denna viktiga princip, som fastställs i artikel 3 i den föreslagna förordningen, i sin omröstning den 21 oktober 2013 om betänkandena om reformen av uppgiftsskyddet från parlamentsledamöterna Jan-Philipp Albrecht och Dimitrios Droutsas i utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor.

18 Kommissionen noterar att Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 föreslog att man i den framtida förordningen skulle införa en bestämmelse som innebär att framställningar från utländska myndigheter om tillgång till personuppgifter som samlats in i EU endast kan beviljas om det finns förhandsgodkännande från en nationell dataskyddsmyndighet, i sådana fall där framställan görs utanför ramen för ett avtal om ömsesidig rättsligt hjälp eller ett annat internationellt avtal.

19 Kommissionen noterar att utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 föreslog att kommissionens förslag skulle skärpas ytterligare genom införande av böter på upp till 5 % av ett företags årliga omsättning i världen.

20 Kommissionen noterar att utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 stödde att registerförarnas skyldigheter och ansvar skulle skärpas, särskilt med avseende på artikel 26 i den föreslagna förordningen.

har visat är detta av avgörande betydelse, eftersom dessa program påverkar uppgifter som lagras i datormoln. Företag som tillhandahåller lagringsutrymme i molnet, och som uppmanas att lämna ut personuppgifter till utländska myndigheter, kommer inte att kunna kringgå sitt ansvar genom att hänvisa till att de är registerförare och inte registeransvariga.
Paketet kommer att leda till att det införs övergripande bestämmelser om skydd av personuppgifter som behandlas i samband med brottsbekämpning.
En överenskommelse om paketet kan förväntas under loppet av 2014[21].

### 3.2 Ett säkrare Safe Harbour-system

Safe Harbour-systemet är ett viktigt inslag i handelsförbindelserna mellan EU och Förensta staterna, som företag på båda sidor om Atlanten förlitar sig på.
I kommissionens rapport om Safe Harbour-systemets funktion konstaterades brister i systemet. Brist på öppenhet och tillsyn har lett till att vissa självcertifierade Safe Harbour-medlemmar inte följer systemets principer i praktiken. Detta har en negativ inverkan på EU-medborgarnas grundläggande rättigheter. Det medför även att europeiska företag har en nackdel jämfört med de konkurrerande amerikanska företag som verkar inom ramen för systemet utan att tillämpa dess principer i praktiken. Bristen påverkar även den majoritet amerikanska företag som tillämpar systemet korrekt. Safe Harbour fungerar också som en kanal för överföring av personuppgifter om EU-medborgare från EU till Förenta staterna av företag som är skyldiga att överlämna uppgifter till amerikanska underrättelsetjänster inom ramen för amerikanska program för insamling av underrättelseinformation. Om inte dessa brister rättas till kommer konkurrensnackdelarna för EU:s företag och den negativa inverkan på den grundläggande rätten till skydd för personuppgifter i EU att kvarstå.
Bristerna i Safe Harbour-systemet har betonats särskilt i samband med de europeiska dataskyddsmyndigheternas reaktioner på de senaste övervakningsavslöjandena. Enligt artikel 3 Safe Harbour-beslutet har dessa myndigheter under vissa förutsättningar rätt att stoppa dataflöden till certifierade företag.[22] Tyska dataskyddsansvariga har beslutat att inte utfärda några nya tillstånd att överföra uppgifter till länder utanför EU (t.ex. för användning av vissa molntjänster). De kommer också att undersöka om dataöverföringar inom ramen för Safe Harbour-systemet bör stoppas.[23] Risken är dock att sådana åtgärder, om de vidtas på nationell nivå, leder till skillnader i tillämpningen, med följden att Safe Harbour skulle upphöra att vara ett kärnverktyg för överföring av personuppgifter mellan EU och Förenta staterna.
Enligt direktiv 95/46/EG har kommissionen rätt att upphäva eller återkalla Safe Harbour-beslutet om systemet inte längre ger en tillräcklig skyddsnivå. I artikel 3 i Safe Harbour-beslutet föreskrivs att kommissionen har rätt att upphäva beslutet helt eller tills vidare eller begränsa dess tillämpningsområde. Enligt artikel 4 får kommissionen möjlighet när som helst ändra beslutet mot bakgrund av erfarenheterna från genomförandet.
Mot bakgrund av detta finns det en rad politiska alternativ som kan övervägas, bland annat följande:

---

21 I sina slutsatser från oktober 2013 konstaterade Europeiska rådet följande: ”Det är viktigt att främja medborgarnas och företagens förtroende för den digitala ekonomin. Ett snabbt antagande av en kraftfull allmän uppgiftsskyddsram för EU samt av it-säkerhetsdirektivet är avgörande för att den inre digitala marknaden ska kunna fullbordas2015”

22 Enligt artikel 3 i Safe Harbour-beslutet kan sådana avbrott särskilt bli aktuella om det finns välgrundad anledning att anta att det föreligger en kränkning av Safe Harbour-principerna och att den berörda genomförandemekanismen inte i tid utmynnar i lämpliga åtgärder för att avgöra ärendet, samt om fortsatt överföring skulle medföra en överhängande risk för att registrerade lider allvarlig skada och de behöriga myndigheterna i EU-medlemsstaten i fråga, med hänsyn till rådande omständigheter, har gjort vad de rimligen har kunnat för att meddela organisationen och ge den tillfälle att vidta åtgärder.

23 Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, pressmeddelande av den 24 juli 2013.

- Bibehålla status quo.
- Stärka ramen för Safe Harbour-systemet och göra en ingående översyn av dess.
- Upphäva Safe Harbour-beslutet helt eller tills vidare.

Med tanke på de konstaterade bristerna är det inte möjligt att fortsätta med den nuvarande tillämpningen av Safe Harbour-beslutet. Ett återkallande av beslutet skulle emellertid inverka negativt på intressena för de företag i EU och Förenta staterna som deltar i systemet. Kommissionen anser att Safe Harbour-systemet i stället bör stärkas.
Förbättringarna bör utöver de strukturella bristerna rörande öppenhet och tillsyn och de materiella Safe Harbour-principerna omfatta tillämpningen av det undantag som kan åberopas med hänvisning till den nationella säkerheten.
För att Safe Harbour ska fungera på det sätt som var avsett krävs att de amerikanska myndigheterna på ett mer effektivt och systematiskt sätt övervakar hur certifierade företag uppfyller sina åtaganden inom ramen för Safe Harbour-systemet. Insyn i de certifierade företagens strategier för integritetsskydd måste förbättras. EU-medborgarna måste också tillförsäkras tillgång till ekonomiskt överkomliga tvistlösningsmekanismer.
Kommissionen kommer å det snaraste att inleda en dialog med de amerikanska myndigheterna för att diskutera de konstaterade bristerna. Till sommaren 2014 bör det finnas förslag till lösningar. Dessa bör genomföras så snart som möjligt. Med utgångspunkt från detta kommer kommissionen att göra en fullständig genomgång av hur Safe Harbour-systemet fungerar. Denna bredare översyn bör inbegripa öppna samråd och debatter i Europaparlamentet och rådet samt diskussioner med de amerikanska myndigheterna.
Det är också viktigt att möjligheten till undantag med hänvisning till den nationella säkerheten som föreskrivs i Safe Harbour-beslutet endast används i den omfattning som är absolut nödvändig och proportionerlig.

### 3.3 Stärkt dataskydd i det brottsbekämpande samarbetet

EU och Förenta staterna förhandlar för närvarande om ett ”paraplyavtal” om överföring och behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete. Ingåendet av ett avtal som ger ett gott skydd för personuppgifter skulle vara ett viktigt bidrag för att stärka förtroendet över Atlanten. Ett bättre skydd för EU-medborgarnas rättigheter skulle bidra till att stärka den del av det transatlantiska samarbetet som syftar till att förebygga och bekämpa brottslighet och terrorism.
Enligt beslutet om att bemyndiga kommissionen att förhandla om paraplyavtalet bör syftet med förhandlingarna vara att garantera en hög skyddsnivå i linje med EU:s regelverk på området för skydd av personuppgifter. Detta bör återspeglas i överenskomna regler och garantier när det gäller bland annat ändamålsbegränsning samt villkor och lagringstid vid lagring av personuppgifter. I samband med förhandlingarna bör kommissionen också utverka åtaganden när det gäller lagstadgade rättigheter, däribland införande av möjligheter till rättslig prövning för EU-medborgare som inte är bosatta i Förenta staterna[24]. Ett nära samarbete mellan EU och Förenta staterna för att åtgärda gemensamma säkerhetsproblem bör

[24] Se relevant avsnitt i det gemensamma pressmeddelande som utfärdades efter mötet mellan EU:s och Förenta staternas justitie- och inrikesministrar den 18 november 2013 i Washington: ”Vi är därför, som en fråga av högsta prioritet, fast beslutna att avancera snabbt i förhandlingarna om ett ändamålsenligt och övergripande paraplyavtal om skydd av personuppgifter på brottsbekämpningens område. Avtalet skulle fungera som grund för att underlätta överföring av uppgifter i samband med polissamarbete och straffrättsligt samarbete genom att säkerställa en hög nivå av skydd för amerikanska medborgares och EU-medborgares personuppgifter. Vi är inriktade på att fortsätta arbetet för att lösa återstående frågor som har tagits upp av båda parter, inklusive frågan i möjlighet till rättslig prövning (som är av avgörande betydelse för EU). Vårt mål är att slutföra förhandlingarna om avtalet före sommaren 2014.”

kombineras med insatser för att se till att medborgare omfattas av samma rättigheter när samma personuppgifter behandlas för samma ändamål, oavsett på vilken sida av Atlanten det sker. Det är också viktigt att undantag baserade på nationella säkerhetsöverväganden är snävt definierade. För detta ändamål är det viktigt att säkerställa säkerhetsmekanismer och begränsningar.

Dessa förhandlingar ger tillfälle att klargöra att personuppgifter som innehas av privata företag i EU inte ska vara åtkomliga för eller kunna överföras till amerikanska brottsbekämpande organ utanför de formella samarbetskanalerna, såsom avtal om ömsesidig rättslig hjälp eller sektorsavtal mellan EU och Förenta staterna. All annan åtkomst bör vara utesluten, såvida det inte är fråga om definierade undantagssituationer där det finns möjlighet till rättslig prövning. Förenta staterna bör göra de åtaganden som krävs i detta hänseende[25].

Ett ”paraplyavtal” som ingåtts på dessa premisser bör ge den allmänna ram som krävs för att garantera en hög skyddsnivå för personuppgifter som överförs till Förenta staterna i syfte att förebygga eller bekämpa brottslighet och terrorism. Sektorsavtal bör, när det är nödvändigt på grund av dataöverföringens natur, innehålla ytterligare regler och skyddsåtgärder. Utgångspunkten vara PNR- och TFTP-avtalen mellan EU och Förenta staterna, som fastställer stränga villkor för överföring av personuppgifter och särskilda skyddsåtgärder för EU-medborgare.

### 3.4 Europeiska farhågor när det gäller den pågående reformprocessen i Förenta staterna

Förenta staternas president Barack Obama har aviserat en översyn av den verksamhet som bedrivs av Förenta staternas nationella säkerhetsmyndigheter, också av den tillämpliga rättsliga ramen. Denna pågående process ger ett utmärkt tillfälle att ta upp den oro som de nya avslöjandena om Förenta staternas program för insamling av underrättelseinformation har väckt i EU. De viktigaste förändringarna skulle vara att utsträcka de skyddsåtgärder som finns tillgängliga för amerikanska medborgare och EU-medborgare bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, skapa ökad insyn i underrättelseverksamhet och ytterligare stärka kontrollen. Sådana förändringar skulle bidra till att återställa förtroendet för datautbyten mellan EU och Förenta staterna och främja européernas användning av internettjänster.

Inför en utvidgning av det skydd som gäller för amerikanska medborgare och EU-medborgare som är bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, är det viktigt att se över de rättsregler om de amerikanska övervakningsprogrammen som innebär att amerikanska medborgare och EU-medborgare behandlas olika, också ur ett nödvändighets- och proportionalitetsperspektiv, med hänsyn till det nära transatlantiska säkerhetspartnerskapet som grundar sig på gemensamma värderingar, rättigheter och friheter. Detta skulle innebära att européerna inte drabbas på samma sätt av amerikanska program för insamling av underrättelseinformation.

Det behövs bättre insyn beträffande den rättsliga ramen för de amerikanska programmen för insamling av underrättelseinformation och hur denna ram tolkas av de amerikanska

---

[25] Se relevant avsnitt i det gemensamma pressmeddelande som utfärdades efter mötet mellan EU:s och Förenta staternas justitie- och inrikesministrar den 18 november 2013 i Washington: ”Vi vill också understryka betydelse av avtalet om ömsesidig rättslig hjälp mellan EU och Förenta staterna. Vi upprepar vårt åtagande att se till att det används på ett brett och effektivt sätt för bevisupptagningsändamål i straffrättsliga förfaranden. Det har också förekommit diskussioner om behovet av att klargöra att personuppgifter som innehas av privata enheter på en annan parts territorium inte bör vara tillgängliga för brottsbekämpande myndigheter utanför de lagstadgade kanalerna. Vi är också eniga om att se över hur avtalet om ömsesidig rättslig hjälp fungerar, såsom var tänkt i avtalet, och att samråda med varandra vid behov.”

domstolarna, men även beträffande den kvantitativa dimensionen av programmen. Även EU-medborgarna skulle ha nytta av sådana förändringar.
Tillsynen över de amerikanska programmen för insamling av underrättelseinformation skulle förbättras genom en förstärkt roll för domstolen för övervakning av utländsk underrättelseinformation och införande av möjligheter till rättslig prövning för enskilda. Dessa mekanismer skulle minska behandlingen av personuppgifter som saknar betydelse för den nationella säkerheten.

### 3.5 Främjande av höga standarder när det gäller skydd av personuppgifter

Frågor rörande moderna metoder för uppgiftsskydd är inte begränsade till dataöverföring mellan EU och Förenta staterna. Var och en har rätt till ett bra skydd för sina personuppgifter. EU:s regler om insamling, behandling och överföring av uppgifter bör främjas internationellt.
Nyligen har en rad initiativ lagts fram för att främja skyddet av privatlivet, särskilt på internet[26]. EU bör se till att sådana initiativ, om de genomförs, tar full hänsyn till de principer rörande skydd av de grundläggande rättigheterna, yttrandefriheten, personuppgifter och privatlivet som fastställs i EU-lagstiftningen och i EU:s som anges i EU:s lagstiftning och i EU:s strategi för it-säkerhet, och inte undergräver friheten, öppenheten och säkerheten i cyberrymden. Detta inbegriper en demokratisk och effektiv styrningsmodell med många inblandade parter.
De pågående reformerna av lagstiftningen om uppgiftsskydd på båda sidorna av Atlanten ger också EU och Förenta staterna en unik möjlighet att etablera standarden internationellt. Datautbyten över Atlanten och längre bort skulle gynnas kraftigt om man stärkte Förenta staternas inhemska rättsliga ram och kunde få igenom den konsumentlagstiftning (Consumer Privacy Bill of Rights) som president Barack Obama aviserade i februari 2012, som en del av en större plan för att förbättra skyddet av konsumenters privatliv. En uppsättning starka och verkställbara bestämmelser om dataskydd i både EU och Förenta staterna skulle utgöra en solid grund för dataflöden över gränserna.
För att främja normer om skydd av privatlivet på ett internationellt plan är det viktigt att främja anslutning till Europarådets konvention om skydd av individer med avseende på automatisk behandling av personuppgifter (”konvention 108”), som är öppen för länder som inte är medlemmar i Europarådet[27]. Skyddsåtgärder och garantier som avtalats i internationella forum bör leda till en högra skyddsnivå i linje med vad EU-lagstiftningen kräver.

## 4. SLUTSATSER OCH REKOMMENDATIONER

De frågor som behandlas i detta meddelande kräver att åtgärder av såväl Förenta staterna och som av EU och dess medlemsstater.
Oron kring det transatlantiska datautbytet är i första hand en väckarklocka som signalerar att EU och dess medlemsstater måste vidta snabba och ambitiösa åtgärder för att driva igenom uppgiftsskyddsreformen. Den visar att det mer än någonsin behövs en stark rättslig ram med tydliga regler som tillämpas även vid överföring av uppgifter till utlandet. EU-institutionerna bör därför fortsätta arbetet för att anta EU:s uppgiftsskyddsreform till våren 2014, och därigenom se till att personuppgifter omfattas av ett effektivt och övergripande skydd.
Med tanke på att dataflödena över Atlanten är av så stor betydelse är det viktigt att de instrument på vilka detta utbyte vilar är utformade på ett sådant sätt att det blir möjligt att möta utmaningarna och tillvarata möjligheterna i den digitala tidsåldern, inklusive ny teknik

[26] Se det utkast till resolution som Tyskland och Brasilien lagt fram för FN:s generalförsamling om skydd av privatlivet såväl på som utanför internet.
Förenta staterna är redan medlem i en annan av Europarådets konventioner, nämligen 2001 års konvention om it-relaterad brottslighet (även kallad *Budapestkonventionen*).

som datormoln. Befintliga och framtida bestämmelser och avtal bör garantera en kontinuerligt hög skyddsnivå när det gäller dataflöden över Atlanten.
Medborgare och företag i EU och Förenta staterna har intresse av ett väl fungerande Safe Harbour-system. Systemet bör stärkas genom bättre övervakning och genomförande på kort sikt och, med detta som utgångspunkt, en bredare översyn av dess funktion. Förbättringar är nödvändiga för att säkerställa att de ursprungliga målen med Safe Harbour-beslutet dvs. kontinuerligt uppgiftsskydd, rättssäkerhet och fria dataflöden mellan EU och Förenta staterna, kan uppfyllas även i fortsättningen.
Förbättringarna bör vara inriktade på behovet av att skapa förutsättningar för de amerikanska myndigheterna att bättre kunna övervaka och kontrollera om och hur självcertifierade företag följer Safe Harbour-principerna om integritetsskydd.
Det är också viktigt att möjligheten till undantag med hänvisning till den nationella säkerheten som föreskrivs i Safe Harbour-beslutet endast används i den omfattning som är absolut nödvändig och proportionerlig.
Inom brottsbekämpningens område bör de pågående förhandlingarna om ett paraplyavtal leda till en hög skyddsnivå för medborgare på båda sidor av Atlanten. Ett sådant avtal skulle stärka européernas förtroende för datautbytena mellan EU och Förenta staterna och utgöra en grund för vidareutveckling av samarbete och partnerskap på säkerhetsområdet. I samband med förhandlingarna är det viktigt att utverka åtaganden om att även européer som inte är bosatta i Förenta staterna ska ha tillgång till rättssäkerhetsgarantier, inklusive möjligheter till rättslig prövning.
Den amerikanska förvaltningen bör lämna åtaganden som säkerställer att amerikanska brottsbekämpande myndigheter inte har tillgång till personuppgifter som innehas av privata aktörer i EU utanför de formella samarbetskanalerna, såsom avtal om ömsesidig rättslig hjälp och sektorsavtal mellan EU och Förenta staterna, t.ex. PNR- och TFTP-avtalen, som under väl avgränsade förutsättningar tillåter sådana överföringar, såvida det inte är fråga om klart definierade undantagssituationer där det finns möjlighet till rättslig prövning.
Förenta staterna bör också utsträcka de skyddsåtgärder som finns tillgängliga för amerikanska medborgare och EU-medborgare bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, se till att programmen motsvarar kraven på nödvändighet och proportionalitet och säkerställa ökad öppenhet och insyn i den rättsliga ram som tillämpas av Förenta staternas säkerhetsmyndigheter.
De frågor som tas upp i detta meddelande kommer att kräva ett konstruktivt engagemang från båda sidor av Atlanten. Som strategiska partner har EU och Förenta staterna tillsammans förmåga att lösa de rådande spänningarna i de transatlantiska förbindelserna och återskapa förtroendet för dataflödena mellan EU och Förenta staterna. Gemensamma politiska och rättsliga åtaganden om närmare samarbete på dessa områden kommer att bidra till att stärka de transatlantiska förbindelserna överlag.

EUROPEISKA
KOMMISSIONEN

Bryssel den 27.11.2013
COM(2013) 847 final

# MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

## om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET**

**om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU**

## 1. INLEDNING

I direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (nedan kallat *dataskyddsdirektivet*) fastställs reglerna för överföring av personuppgifter från EU:s medlemsstater till andra länder utanför EU[1] i den mån sådana överföringar faller inom denna rättsakts tillämpningsområde[2].

Enligt direktivet kan kommissionen konstatera att ett tredjeland sörjer för en adekvat skyddsnivå på grundval av dess nationella lagstiftning eller de internationella åtaganden som landet gjort för att skydda enskildas rättigheter, i vilket fall de specifika begränsningarna för dataöverföring till det berörda landet inte är tillämpliga. Dessa beslut kallas allmänt för ***beslut om adekvat skyddsnivå***.

Den 26 juli 2000 antog kommissionen beslut 2000/520/EG[3] (nedan kallat ***safe harbour-beslutet***) där man erkänner att de principer om integritetsskydd (Safe Harbor Privacy Principles) (nedan kallade *safe harbour-principerna* eller *principerna*) och de frågor och svar (nedan kallade *frågorna och svaren* eller *FoS*) som Förenta staternas handelsministerium utfärdat, säkerställer ett adekvat skydd vid överföring av personuppgifter från EU. Safe harbour-beslutet fattades sedan en kvalificerad majoritet av medlemsstaterna avgett ett yttrande i artikel 29-gruppen respektive artikel 31-kommittén. I enlighet med rådets beslut 1999/468 granskades safe harbour-beslutet först av Europaparlamentet.

Till följd av detta möjliggör det gällande safe harbour-beslutet fri överföring[4] av personuppgifter från EU:s medlemsstater[5] till företag i Förenta staterna som har anslutit sig till principerna under omständigheter där överföringen annars inte skulle uppfylla EU:s krav på en adekvat skyddsnivå, mot bakgrund av de betydande olikheterna mellan integritetsreglerna på bägge sidor av Atlanten.

Det nuvarande safe harbour-systemet bygger på åtaganden och självcertifiering från de medverkande företagens sida. Deltagande i systemet är frivilligt, men reglerna är bindande för dem som ansluter sig. De grundläggande principerna för systemet är följande:

a) De medverkande företagens policy för integritetsskydd ska vara tillgänglig för insyn.

b) Safe harbour-principerna ska införlivas i företagens policy för integritetsskydd.

---

1 I artiklarna 25 och 26 i dataskyddsdirektivet fastställs den rättsliga ramen för överföring av personuppgifter från EU till tredjeländer utanför EES.

2 Ytterligare regler har lagts fast i artikel 13 i rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete i den mån sådana överföringar rör personuppgifter som överförs eller görs tillgängliga av en medlemsstat till en annan medlemsstat, som avser att sedan överföra dessa uppgifter till en tredjestat eller ett internationellt organ i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

3 Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, EGT L 215, 28.8.2000, s. 7.

4 Det ovanstående utesluter inte att andra krav som kan finnas i nationell lagstiftning om genomförande av EU:s dataskyddsdirektiv tillämpas på databehandlingen.

5 Dataöverföringar från de tre stater som är EES-medlemmar påverkas på ett liknande sätt till följd av utvidgningen av direktiv 95/46/EG till EES-avtalet genom beslut nr 83/1999 av den 25 juni 1999, EGT L 296, 23.11.2000, s. 41.

c) Genomförandet ska följas upp, inbegripet av offentliga myndigheter.

Dessa grundprinciper för safe harbour måste ses över mot bakgrund av de **nya omständigheterna** med

a) den exponentiella ökningen av dataflödena, som tidigare hade en stödfunktion men som numera är av central betydelse för den snabba tillväxten i den digitala ekonomin, och de mycket stora förändringarna när det gäller insamling, behandling och användning av data,

b) dataflödenas avgörande betydelse särskilt för den transatlantiska ekonomin,[6]

c) den snabba ökningen av antalet företag i Förenta Staterna som är anslutna till safe harbour-systemet; det finns nu åtta gånger fler sådana företag än 2004 (en ökning från 400 år 2004 till 3 246 år 2013),

d) de nyligen offentliggjorda uppgifterna om de amerikanska övervakningsprogrammen, som ger upphov till nya frågor om den skyddsnivå som safe harbour-systemet ska anses garantera.

Det är mot denna bakgrund som detta meddelande ger en överblick av hur safe harbour-systemet fungerar. Meddelandet **bygger på bevisning** som kommissionen samlat in, det arbete som utfördes 2009 inom EU–US Privacy Contact Group, en oberoende undersökning som utarbetades 2008[7] samt information som inhämtats inom ramen för den ad hoc-arbetsgrupp mellan EU och Förenta staterna (nedan kallad *arbetsgruppen*) som inrättats till följd av avslöjandena om Förenta staternas övervakningsprogram *(se parallellt dokument)*. Meddelandet följer på två **utvärderingsrapporter från kommissionen** som offentliggjordes under inkörningsperioden av safe harbour-systemet, 2002[8] respektive 2004[9].

## 2. SAFE HARBOUR-SYSTEMETS STRUKTUR OCH FUNKTIONSSÄTT

### 2.1. Safe harbour-systemets struktur

Ett amerikanskt företag som vill ansluta sig till safe harbour måste a) i sin allmänt tillgängliga policy för integritetsskydd ange att det ansluter sig till principerna och tillämpar dem i praktiken, och b) lämna in en självcertifiering, dvs. anmäla till Förenta Staternas handelsministerium att det efterlever principerna. Självcertifieringen ska förnyas årligen. Principerna om integritetsskydd (Safe Harbour Privacy Principles) i bilaga I till safe harbour-beslutet innefattar krav på både det materiella skyddet av personuppgifter (principer för dataintegritet, säkerhet, valmöjlighet och vidare överföring) och de registrerades processuella rättigheter (principer för meddelande, tillgång samt genomförande och uppföljning).

---

6 Om tjänster och gränsöverskridande dataflöden skulle störas till följd av att tillämpningen av bindande företagsregler, modeller för avtalsklausuler och safe harbour-systemet avbryts, skulle den negativa effekten på EU:s BNP enligt vissa undersökningar kunna uppgå till mellan -0,8 % och -1,3 % och EU:s export till Förenta staterna minska med -6,7 % på grund av försämrad konkurrenskraft. Se *The Economic Importance of Getting Data Protection Right*, en studie av European Centre for International Political Economy för den amerikanska handelskammaren (US Chamber of Commerce), mars 2013.

7 Konsekvensbedömning utarbetad 2008 för Europeiska kommissionen av *Centre de Recherche Informatique et Droit* (CRID) vid universitetet i Namur.

8 Arbetsdokument från kommissionens avdelningar om tillämpningen av kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, SEK(2002) 196, 13.12.2002.

9 Arbetsdokument från kommissionens avdelningar om genomförandet av kommissionens beslut 520/2000/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, SEK(2004) 1323, 20.10.2004.

När det gäller genomförandet av Safe Harbour-systemet i Förenta Staterna har två amerikanska institutioner en central funktion: handelsministeriet (US Department of Commerce) och den federala konkurrensmyndigheten (US Federal Trade Commission).

**Handelsministeriet** kontrollerar alla safe harbour-självcertifieringar och alla årliga förnyanden av självcertifieringar som det får från företag i syfte att se till att de innehåller allt som krävs för att delta i systemet[10]. Ministeriet uppdaterar kontinuerligt en förteckning över företag som har lämnat in skrivelser om självcertifiering och offentliggör förteckningen och skrivelserna på sin webbplats. Dessutom övervakar det safe harbour-systemets funktionssätt och stryker företag som inte uppfyller kraven från förteckningen.

Den **federala konkurrensmyndigheten** ingriper, inom ramen för sina befogenheter på konsumentskyddsområdet, mot illojala eller bedrägliga metoder i enlighet med avsnitt 5 i *Free Trade Commission Act*. Till konkurrensmyndighetens verkställighetsåtgärder hör utredningar av oriktiga påståenden om att företag är anslutna till safe harbour-systemet och av bristande efterlevnad av safe harbour-principerna av företag som är medlemmar i systemet. I de specifika fall som rör uppföljning av lufttrafikföretags genomförande av safe harbour-principerna är det behöriga organet Förenta staternas transportministerium (US Department of Transportation).[11]

Det gällande safe harbour-beslutet är en del av EU:s lagstiftning som måste tillämpas av medlemsstaternas myndigheter. I beslutet föreskrivs det att EU:s nationella **dataskyddsmyndigheter** har rätt att avbryta överföringar av personuppgifter till safe harbour-certifierade företag i särskilda fall[12]. Kommissionen känner inte till några fall då överföringar skulle ha avbrutits av en nationell dataskyddsmyndighet sedan safe harbour-systemet infördes 2000. Oavsett vilka befogenheter de har enligt safe harbour-beslutet har EU:s nationella dataskyddsmyndigheter behörighet att ingripa för att säkerställa att de allmänna dataskyddsprinciperna i dataskyddsdirektivet från 1995 efterlevs, även i fråga om internationella överföringar.

Som påpekas i det gällande safe harbour-beslutet har **kommissionen befogenhet** – i enlighet med det granskningsförfarande som avses i förordning (EG) nr 182/2011 – att när som helst anpassa beslutet, upphäva det eller begränsa dess tillämpningsområde mot bakgrund av erfarenheterna av dess genomförande. Detta gäller särskilt i händelse av ett systemsammanbrott på Förenta staternas sida, t.ex. om ett organ som ansvarar för att se till att safe harbour-principerna iakttas i Förenta staterna i praktiken inte utför sina uppgifter eller om den skyddsnivå som safe harbour-principerna erbjuder är lägre än kraven i den amerikanska lagstiftningen. Liksom varje annat kommissionsbeslut kan det också ändras av andra skäl eller till och med återkallas.

---

10 Om ett företags certifiering eller förnyade certifiering inte uppfyller kraven för safe harbour meddelar handelsministeriet företaget vilka åtgärder som måste vidtas (t.ex. klargöranden, ändringar i policybeskrivningen) för att företagets certifiering ska kunna slutföras.

11 Enligt avdelning 49 i US Code Section 41712.

12 Mer specifikt kan avbrytande av överföringar krävas i två situationer, varvid
a) det amerikanska myndighetsorganet har fastställt att företaget agerar i strid med safe harbour-principerna, eller
b) det är i hög grad sannolikt att safe harbour-principerna åsidosätts, det finns välgrundad anledning att tro att den berörda tillsynsmekanismen inte vidtar eller inte i tid kommer att vidta åtgärder för att avgöra ärendet, det skulle medföra en överhängande risk för allvarlig skada för de registrerade om överföringen fortsätter, och de behöriga myndigheterna i medlemsstaterna har vidtagit efter omständigheterna rimliga åtgärder för att varna företaget och ge det möjlighet att reagera.

## 2.2. Safe harbour-systemets funktionssätt

Bland de **3 246**[13] **certifierade företagen** finns både små och stora företag[14]. Även om finansiella tjänster och telekommunikationssektorn ligger utanför den federala konkurrensmyndighetens tillsynsbefogenheter och därför inte omfattas av safe harbour är många andra industri- och tjänstesektorer representerade bland de certifierade företagen, inklusive välkända internetföretag och företag inom så vitt skilda områden som informations- och datatjänster, läkemedel, resetjänster och turism, hälso- och sjukvård eller kreditkortstjänster[15]. De flesta av dessa företag är amerikanska företag som tillhandahåller tjänster på EU:s inre marknad. Några av dem är dotterbolag till EU-företag som t.ex. Nokia eller Bayer. 51 % av företagen behandlar data rörande anställda i Europa som överförs till Förenta staterna i personalförvaltningssyfte[16].

Vissa dataskyddsmyndigheter i EU hyser **allt större farhågor** rörande dataöverföring inom ramen för det nuvarande safe harbour-systemet. Några medlemsstaters dataskyddsmyndigheter har kritiserat den mycket vaga formuleringen av principerna och den stora tilltron till självcertifiering och självreglering. Liknande farhågor har tagits upp av näringslivet med hänvisning till snedvridning av konkurrensen på grund av bristande tillsyn.

Det nuvarande safe harbour-systemet bygger på att företagen frivilligt ansluter sig, på de anslutna företagens självcertifiering och på att offentliga myndigheter utövar tillsyn över åtagandena inom ramen för självcertifieringen. I detta sammanhang utgör varje brist på insyn och varje brist i tillsynen ett hot mot själva grunden för safe harbour-systemet.

Eventuella luckor när det gäller insyn och tillsyn på den amerikanska sidan leder till att ansvaret vältras över till europeiska dataskyddsmyndigheter och till de företag som använder systemet. Den 29 april 2010 utfärdade den tyska dataskyddsmyndigheten ett beslut genom vilket företag som överför data från EU till Förenta staterna ålades att aktivt kontrollera att de företag i Förenta staterna som importerar data verkligen efterlever safe harbour-principerna och rekommenderades att ”åtminstone fastställa huruvida importörens safe harbour-certifiering fortfarande är giltig”[17].

Den 24 juli 2013, efter avslöjandena om Förenta staternas övervakningsprogram, gick de tyska dataskyddsmyndigheterna ett steg längre och uttryckte sin oro över ”den stora sannolikheten att principerna i kommissionens beslut överträds”[18]. Det finns fall då dataskyddsmyndigheter (t.ex. den i Bremen) har krävt att ett företag som överför personuppgifter till amerikanska leverantörer ska underrätta dataskyddsmyndigheten om huruvida och på vilket sätt de berörda leverantörerna förhindrar att den nationella säkerhetsmyndigheten (National Security Agency, NSA) får tillgång till uppgifterna. Den

---

13 Den 26 september 2013 uppgick antalet organisationer på safe harbour-förteckningen som var registrerade som ”**för närvarande anslutna**” till **3 246** och antalet ”**för närvarande ej anslutna**” till **935.**

14 Safe harbour-organisationer med högst 250 anställda: **60 %** (1 925 av 3 246). Safe harbour-organisationer med minst 251 anställda: **40 %** (1 295 av 3 246).

15 T.ex. MasterCard arbetar med tusentals banker och är ett tydligt exempel på ett fall där safe harbour-principerna inte kan ersättas med andra rättsliga instrument för överföring av personuppgifter, såsom bindande företagsregler eller avtal.

16 Safe harbour-organisationer vars certifiering omfattar organisationens personaluppgifter (och vilka därigenom har samtyckt till att samarbeta med EU:s dataskyddsmyndigheter och följa deras regler): **51 %** (1 671 av 3 246).

17 Se beslut av Düsseldorfer Kreis av den 28–29 april 2010. Se 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 Europeiska datatillsynsmannen Peter Hustinx uttryckte dock vid en utfrågning i Europaparlamentets LIBE-utskott den 7 oktober 2013 uppfattningen att ”betydande förbättringar har gjorts och de flesta frågor nu är lösta” vad gäller safe harbour: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Se resolutionen från en tysk konferens för dataskyddsombud i vilken det framhävs att underrättelsetjänster utgör ett massivt hot mot datatrafiken mellan Tyskland och länder utanför Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

irländska dataskyddsmyndigheten har meddelat att den nyligen tagit emot två klagomål rörande safe harbour-programmet efter rapporteringen om den amerikanska underrättelsetjänstens program, men att den avvisat dem med motiveringen att överföringen av personuppgifter till ett tredjeland uppfyller kraven i den irländska lagstiftningen om dataskydd. Till följd av ett liknande klagomål har dataskyddsmyndigheten i Luxemburg fastslagit att Microsoft och Skype har iakttagit Luxemburgs dataskyddslagstiftning vid överföring av data till Förenta staterna[19]. Sedan dess har den irländska High Court dock bifallit en begäran om rättslig omprövning enligt vilken den kommer att granska det irländska dataskyddsombudets underlåtenhet att vidta åtgärder med avseende på USA övervakningsprogram. Ett av de två klagomålen ingavs av en grupp studerande, Europe v Facebook (EvF), som också lämnat in ett liknande klagomål mot Yahoo i Tyskland som är under behandling hos de behöriga dataskyddsmyndigheterna.

Dessa varierande reaktioner från olika dataskyddsmyndigheters sida på avslöjandena om övervakningen visar på en reell risk för fragmentisering av safe harbour-systemet och väcker frågan om i vilken utsträckning genomförandet av systemet övervakas.

## 3. INSYN I DE MEDVERKANDE FÖRETAGENS POLICY FÖR INTEGRITETSSKYDD

Enligt FoS 6 i bilaga II till safe harbour-beslutet måste företag som är intresserade av certifiering inom ramen för safe harbour-systemet sända sin policy för integritetsskydd till handelsministeriet och göra den tillgänglig för allmänheten. Den måste innehålla ett åtagande att följa principerna om integritetsskydd. Kravet att självcertifierade företag ska **offentliggöra sin policy för integritetsskydd** och sitt åtagande att följa principerna om integritetsskydd är av avgörande betydelse för genomförandet av systemet.

Otillräcklig tillgång till sådana företags policy för integritetsskydd är till nackdel för de enskilda vars personuppgifter samlas in och behandlas och kan innebära en **överträdelse av principen om meddelande**. I sådana fall kan enskilda personer vars uppgifter överförs från EU vara omedvetna om vilka rättigheter och skyldigheter ett självcertifierat företag har.

Vidare innebär företagens åtagande att respektera principerna om integritetsskydd att **den federala konkurrensmyndigheten har rätt att utöva tillsyn av dessa principer** med avseende på företag som underlåter att efterleva dem, t.ex. genom illojala eller bedrägliga metoder. Bristande insyn i amerikanska företag försvårar konkurrensmyndighetens övervakning och undergräver tillsynens effektivitet.

Under årens lopp har ett betydande antal självcertifierade företag underlåtit att offentliggöra sin policy för integritetsskydd och/eller att göra ett offentligt åtagande att följa principerna om integritetsskydd. Rapporten om safe harbour från 2004 pekar på behovet av att handelsministeriet **intar en mer aktiv hållning när det gäller att kontrollera** om detta krav är uppfyllt.

Sedan 2004 har handelsministeriet utvecklat **nya informationsverktyg** som syftar till att hjälpa företagen att fullgöra sina skyldigheter avseende insyn. Relevant information om systemet finns tillgänglig på handelsministeriets webbplats om safe harbour[20], där företag också kan lägga upp sin policy för integritetsskydd. Handelsministeriet har rapporterat att företag har utnyttjat denna funktion och publicerat sin policy för integritetsskydd på ministeriets webbplats i samband med att de ansökt om att ansluta sig till safe harbour[21]. Dessutom har handelsministeriet 2009–2013 offentliggjort en rad riktlinjer för företag som

[19] Se pressmeddelandet från Luxemburgs dataskyddsmyndighet av den 18 november 2013.

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

[21] https://SafeHarbour.export.gov/list.aspx

vill ansluta sig till safe harbour, t.ex. *Guide to Self-Certification* och *Helpful Hints on Self-Certifying Compliance*[22].

Företagen fullgör skyldigheterna avseende insyn i varierande grad. Vissa företag inskränker sig till att meddela handelsministeriet en beskrivning av deras policy för integritetsskydd som en del av självcertifieringsprocessen, men de flesta offentliggör sin policy på sin egen webbplats vid sidan av att de laddar upp den på handelsministeriet webbplats. Det är dock **inte alltid som policyn presenteras i en användarvänlig och lättläst form**. Länkar till policyn för integritetsskydd fungerar inte alltid som de ska och leder inte heller alltid till rätt webbsidor.

Av beslutet och dess bilagor följer att kravet att företagen bör offentliggöra sin integritetsskyddspolicy **innebär mer än bara anmälan** av självcertifiering till handelsministeriet. Till de krav för certifiering som beskrivs i frågorna och svaren hör en beskrivning av policyn för integritetsskydd och tydlig information om var den finns tillgänglig för allmänheten[23]. Redogörelserna för integritetsskyddspolicyer måste vara tydliga och lätt tillgängliga för allmänheten. De måste innehålla en hyperlänk till handelsministeriet webbplats för safe harbour där förteckningar över alla ”för närvarande anslutna” medlemmar i systemet och en länk till den alternativa instansen för tvistlösning. Ett antal företag anslutna till systemet under perioden 2000–2013 har dock underlåtit att uppfylla dessa krav. I samband med arbetskontakter med kommissionen i februari 2013 medgav handelsministeriet att upp till 10 % av de certifierade företagen kan ha underlåtit att faktiskt publicera en policy för integritetsskydd som innehåller företagets åtagande att iaktta safe harbour-principerna på sin offentliga webbplats.

Färsk statistik visar också på ett ihållande problem med **oriktiga påståenden om anslutning till safe harbour**. Ca 10 % av de företag som påstår sig vara anslutna till safe harbour finns inte upptagna på handelsministeriets förteckningar över för närvarande anslutna medlemmar i systemet[24]. Sådana oriktiga påståenden kommer från både företag som aldrig har medverkat i safe harbour och företag som har anslutit sig till systemet men senare inte årligen förnyat sin självcertifiering hos handelsministeriet. I det sistnämnda fallet tas företaget fortfarande upp på förteckningen på safe harbour-webbplatsen, men med certifieringsstatus ”för närvarande ej anslutet”, vilket innebär att företaget har varit medlem i systemet och därmed är skyldigt att fortsätta att skydda data som redan behandlats. Den federala konkurrensmyndigheten är behörig att ingripa i fall av bedrägliga förfaranden och bristande efterlevnad av safe harbour-principerna (se avsnitt 5.1). Otydligheten när det gäller dessa ”oriktiga påståenden” inverkar menligt på systemets trovärdighet.

Europeiska kommissionen gjorde genom regelbundna kontakter under 2012 och 2013 handelsministeriet uppmärksamt på att det inte räcker med att företagen sänder en beskrivning av sin integritetsskyddspolicy enbart till handelsministeriet för att de ska fullgöra skyldigheterna vad gäller insyn. Redogörelserna för integritetsskyddspolicyn måste göras tillgängliga för allmänheten. Handelsministeriet ombads också att **intensifiera sina regelbundna kontroller av företagens webbplatser** efter kontrollförfarandet i samband med

---

22 Det förstnämnda dokumentet (”Guide”) finns på programmets webbplats: http://export.gov/SafeHarbour/ Dokumentet om ”Helpful Hints” finns på: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Den 12 november 2013 bekräftade handelsministeriet att ”företag som har offentliga webbplatser och som hanterar data om konsumenter/klienter/besökare måste i nuläget ha en policy för integritetsskydd som är förenlig med safe harbour-principerna på deras respektive webbplats” (se dokumentet *U.S.-EU Cooperation to Implement the Safe Harbor Framework* av den 12 november 2013).

24 I september 2013 jämförde det australiensiska konsultföretaget Galexia ”oriktiga påståenden” om safe harbour-medlemskap under 2008 och 2013. Det viktigaste resultatet var att det parallellt med ökningen av antalet medlemmar i safe harbour-systemet mellan 2008 och 2013 (från 1 109 till 3 246) skett en ökning av antalet oriktiga påståenden från 206 till 427. http://www.galexia.com/public/about/news/about_news-id225.html

den första självcertifieringsprocessen eller den årlig förnyelsen av självcertifieringen, och att vidta åtgärder mot de företag som inte uppfyller kraven på insyn.

Som en första reaktion på farhågorna från EU:s sida har **konkurrensmyndigheten sedan mars 2013 gjort det obligatoriskt** för de företag inom safe harbour-systemet som har en offentlig webbplats att göra sin policy för integritetsskydd avseende data om kunder/användare lätt tillgänglig på denna. Samtidigt har handelsministeriet börjat meddela alla företag vars integritetsskyddspolicy inte redan innehåller en länk till handelsministeriets webbplats för safe harbour att de bör lägga till en sådan för att göra den officiella safe harbour-förteckningen och webbplatsen direkt tillgängliga för konsumenter som besöker företagets webbplats. Detta kommer att göra det möjligt för de registrerade i EU att omedelbart, utan ytterligare internetsökningar, kontrollera de åtaganden som ett företag lämnat in till handelsministeriet. Dessutom har handelsministeriet börjat meddela företagen att kontaktuppgifter för deras oberoende instans för tvistlösning bör ingå i deras publicerade integritetsskyddspolicy[25].

**Denna process bör påskyndas** för att säkerställa att alla certifierade företag helt och hållet uppfyller safe harbour-kraven senast i mars 2014 (då fristen för företagens årliga förnyande av certifieringen löper ut, räknat från det att de nya kraven infördes i mars 2013).

Farhågor kvarstår dock när det gäller huruvida alla självcertifierade företag helt och hållet uppfyller kraven på insyn. Uppfyllandet av de åtaganden som gjorts i samband med den ursprungliga självcertifieringen och den årliga förnyelsen av den bör övervakas och undersökas mer strikt av handelsministeriet.

## 4. INTEGRERING AV SAFE HARBOUR-PRINCIPERNA I FÖRETAGENS POLICYER FÖR INTEGRITETSSKYDD

Självcertifierade företag måste iaktta principerna för integritetsskydd i bilaga I till beslutet för att få ansluta sig till och fortsatt kunna åtnjuta fördelarna med safe harbour-systemet.

I rapporten från 2004 fann kommissionen att ett betydande antal **företag inte på ett korrekt sätt hade införlivat safe harbour-principerna** i sin policy för databehandling. Enskilda personer fick t.ex. inte alltid tydlig och lättbegriplig information om de ändamål för vilka uppgifterna behandlades eller gavs inte möjlighet att välja (opt out) om deras uppgifter skulle lämnas ut till en tredje part eller användas till ett ändamål som inte stämde överens med de syften för vilka de ursprungligen samlades in. I kommissionens rapport från 2004 ansågs det att handelsministeriet *borde inta en mer proaktiv hållning när det gäller tillträde till safe harbour-principerna och medvetenhet om grundprinciperna*[26].

Begränsade framsteg har gjorts i detta avseende. Sedan den 1 januari 2009 har varje företag som ansöker om att förnya sin certifieringsstatus inom safe harbour, vilket måste göras årligen, fått sin policy för integritetsskydd utvärderad av handelsministeriet innan certifieringen förnyats. Utvärderingen har emellertid begränsad räckvidd. Det finns **ingen fullständig utvärdering** av nuvarande praxis i de självcertifierade företagen som på något märkbart sätt skulle öka självcertifieringsprocessens trovärdighet.

---

25 Mellan mars och september 2013 har handelsministeriet
• meddelat de 101 företag *som redan hade laddat upp en policy för integritetsskydd som överensstämmer med safe harbour-principerna på webbsidan för safe harbour* att de också måste publicera policyn på deras företagswebbplats,
• meddelat de 154 företag som inte redan gjort det att de bör lägga till en länk till webbplatsen för safe harbour i deras integritetsskyddspolicy,
• meddelat över 600 företag att de bör lägga till kontaktuppgifter för deras oberoende instans för tvistlösning i deras integritetsskyddspolicy.

26 Se sidan 8 i rapporten; SEK(2004) 1323.

Till följd av kommissionens krav på en mer noggrann och systematisk övervakning av de självcertifierade företagen från handelsministeriets sida **ägnar man nu större uppmärksamhet åt nya ansökningar**. Antalet nya ansökningar som inte har godkänts utan har återsänts till företagen för att de ska göra förbättringar i sin policy för integritetsskydd har ökat avsevärt mellan 2010 och 2013: det har fördubblats när det gäller ansökningar om förnyad certifiering och tredubblats när det gäller nya ansökningar om anslutning till safe harbour-systemet[27]. Handelsministeriet har försäkrat kommissionen att all certifiering eller förnyande av certifiering kan slutföras endast om företagets integritetsskyddspolicy uppfyller alla krav, särskilt kravet att den ska innehålla ett åtagande om anslutning till de relevanta safe harbour-principerna och att policyn är tillgänglig för allmänheten. Ett företag är skyldigt att i sin post i safe harbour-förteckningen ange var man kan hitta den relevanta policyn. Företaget måste också på sin webbplats tydligt ange en alternativ instans för tvistlösning och lägga in en länk till safe harbour-självcertifieringen på handelsministeriets webbplats. Det uppskattas dock att över 30 % av safe harbour-medlemmarna inte lämnar någon information om tvistlösning i integritetsskyddspolicyerna på sina webbplatser[28].

En majoritet av de företag som handelsministeriet strukit från safe harbour-förteckningen ströks på de berörda företagens uttryckliga begäran (t.ex. företag som gått samman eller förvärvats, ändrat sitt verksamhetsområde eller lagt ned sin verksamhet). En mindre antal företag som upphört har strukits när de webbplatser som angetts befunnits vara ur bruk och företagens certifieringsstatus varit ”för närvarande ej anslutet” under flera år[29]. Viktigt är att ingen av dessa strykningar förefaller ha gjorts till följd av att handelsministeriets kontroll lett till att man upptäckt problem med bristande överensstämmelse.

Ett företags post i safe harbour-förteckningen fungerar som ett offentligt tillkännagivande och ett protokoll över företagets safe harbour-åtaganden. **Åtagandet att ansluta sig till safe harbour-principerna är inte tidsbegränsat** när det gäller uppgifter som mottagits under den period då företaget omfattas av safe harbour, och företaget måste fortsätta att tillämpa principerna på dessa uppgifter så länge det lagrar, använder eller lämnar ut dem, även om det av någon anledning lämnar safe-harbour-systemet.

Antalet safe harbour-**sökande som inte klarat handelsministeriets administrativa granskning** och därför aldrig förts upp på safe harbour-förteckningen är följande: År **2010** lämnades endast **6 %** (33) av de 513 företag som ansökte om certifiering för första gången utanför safe harbour-förteckningen på grund av att de inte levde upp till handelsministeriets normer för självcertifiering. År **2013** lämnades **12 %** (75) av de 605 företag som ansökte om certifiering för första gången utanför safe harbour-förteckningen på grund av att de inte levde upp till handelsministeriets normer för självcertifiering.

Som ett minimikrav för större öppenhet i tillsynen bör handelsministeriet på sin webbplats ha en förteckning över alla företag som har strukits från safe harbour-förteckningen och ange skälen till certifieringen inte har förnyats. Beteckningen ”för närvarande ej anslutet” i handelsministeriet förteckning över safe harbour-företag bör inte ses enbart som information utan åtföljas av **en tydlig varning** både i ord och grafiskt – om att ett företag för närvarande inte uppfyller kraven för safe harbour.

---

27 Enligt statistik som handelsministeriet lämnade i september 2013 uppmanade ministeriet år 2010 18 % (93) av de 512 företag som ansökte om certifiering för första gången och 16 % (231) av de 1 417 företag som förnyade sin certifiering att göra förbättringar i deras integritetsskyddspolicy och/eller ansökningar avseende safe harbour. Som en uppföljning av kommissionens krav på strikt, noggrann och systematisk kontroll av alla ansökningar uppmanade dock handelsministeriet fram till mitten av september 2013 56 % (340) av de 602 företag som ansökte om certifiering för första gången och 27 % (493) av de 1 809 företag som förnyade sin certifiering att göra förbättringar i deras integritetsskyddspolicy.

28 Enligt Chris Connolly (Galexia) vid utfrågningen i Europaparlamentets LIBE-utskott den 7 oktober 2013.

29 Fram till december 2011 hade handelsministeriet strukit 323 företag från safe harbour-förteckningen: 94 företag hade strukits för att de inte längre var verksamma, 88 till följd av förvärv eller sammanslagningar, 95 på begäran av moderbolaget, 41 till följd av upprepad underlåtenhet att ansöka om förnyad certifiering och 5 av andra skäl.

Dessutom har vissa företag ännu inte helt och hållet införlivat alla safe harbour-principerna. Vid sidan av frågan om insyn, som tas upp i avsnitt 3 ovan, är de självcertifierade företagens policyer för integritetsskydd ofta oklara när det gäller de syften för vilka uppgifter samlas in och rätten att välja huruvida uppgifter kan lämnas ut till tredje man. Detta väcker frågor om förenlighet med principerna om meddelande och valmöjlighet. Meddelande och valmöjlighet är avgörande för att garantera de registrerades kontroll över vad som händer med deras personuppgifter.

Den kritiska första steget i efterlevnadsförfarandet, att införliva safe harbour-principerna i företagens policy för integritetsskydd, säkerställs inte i tillräckligt hög grad. Handelsministeriet bör prioritera att åtgärda detta genom att utveckla en metod för efterlevnad i företagens praktiska verksamhet och deras interaktion med kunder. **Handelsministeriet måste aktivt följa upp att safe harbour-principerna faktiskt integreras i företagens integritetsskyddspolicyer,** snarare än att vidta verkställighetsåtgärder enbart till följd av klagomål från enskilda personer.

## 5. OFFENTLIGA MYNDIGHETERS UPPFÖLJNING AV GENOMFÖRANDET

Ett antal mekanismer finns för att garantera ett effektivt genomförande av safe harbour-systemet och ge enskilda personer möjlighet till klagomål i fall då skyddet av deras personuppgifter påverkas av bristande efterlevnad av principerna om integritetsskydd.

Enligt principen om genomförande och uppföljning måste självcertifierade organisationers policy för integritetsskydd innefatta effektiva mekanismer för att se till att principerna följs. Enligt principen om genomförande och uppföljning såsom den förtydligas i FoS 11, 5 och 6 kan detta krav uppfyllas genom användning av **oberoende rättsmedel** som offentligt har tillkännagjort sin behörighet att handlägga enskilda klagomål avseende underlåtenhet att iaktta principerna. Alternativt kan detta uppnås genom att organisationen åtar sig att samarbeta med **EU:s arbetsgrupp för dataskydd**[30]. Dessutom omfattas självcertifierade företag av den federala konkurrensmyndighetens behörighet enligt avsnitt 5 i *Federal Trade Commission Act*, som förbjuder illojala eller bedrägliga handlingar eller metoder inom handeln eller som påverkar handeln[31].

I rapporten från 2004 uttrycks farhågor när det gäller tillsynen av safe harbour-systemet och anges att den federala konkurrensmyndigheten bör inta en mer proaktiv hållning när det gäller att inleda utredningar och informera enskilda personer om deras rättigheter. Ett annat problemområde var bristen på klarhet i förhållande till konkurrensmyndighetens behörighet att övervaka efterlevnaden av principerna när det gäller personaluppgifter.

Det rättsmedel som ansvarar för personaluppgifter – EU:s arbetsgrupp för dataskydd – har tagit emot ett klagomål avseende personaluppgifter[32]. Denna avsaknad av klagomål gör det omöjligt att dra slutsatser om huruvida systemet i dess helhet fungerar väl. Kontroller på eget initiativ av företagens efterlevnad bör införas för att kontrollera det faktiska genomförandet av

30 EU:s arbetsgrupp för dataskydd är ett organ som är behörigt att undersöka och pröva klagomål från enskilda om påstådda överträdelser av safe harbour-principerna av amerikanska företag som är anslutna till safe harbour-systemet. Företag som är certifierade inom ramen för safe harbour-principerna måste välja mellan att följa ett oberoende rättsmedel eller att samarbeta med EU:s arbetsgrupp för dataskydd för att åtgärda problem som uppstår till följd av underlåtenhet att iaktta safe harbour-principerna. Samarbete med EU:s arbetsgrupp för dataskydd är dock obligatoriskt i de fall då det amerikanska företaget behandlar personaluppgifter som överförs från EU i samband med ett anställningsförhållande. Om företaget åtar sig att samarbeta med EU-arbetsgruppen måste det också åta sig att följa eventuella råd från arbetsgruppen om denna anser att företaget behöver vidta specifika åtgärder för att följa safe harbour-principerna, inklusive korrigerande eller kompenserande åtgärder.

31 Förenta staternas transportministerium utövar en liknande behörighet när det gäller lufttrafikföretag med stöd av avdelning 49 i United States Code Section 41712.

32 Klagomålet kom från en schweizisk medborgare och EU:s arbetsgrupp för dataskydd har därför hänskjutit det till den schweiziska dataskyddsmyndigheten (Förenta staterna har ett särskilt safe harbour-system för Schweiz).

åtaganden om dataskydd. EU:s dataskyddsmyndigheter bör också vidta åtgärder för att öka medvetenheten om arbetsgruppens existens.

Problem har uppmärksammats när det gäller det sätt på vilket alternativa rättsmedel fungerar som tillsynsorgan. Ett antal av dessa organ saknar lämpliga metoder för att åtgärda fall av underlåtenhet att iaktta principerna. Denna brist måste åtgärdas.

### 5.1. Den federala konkurrensmyndigheten (Federal Trade Commission)

Den federala konkurrensmyndigheten kan vidta verkställighetsåtgärder vid överträdelser av företagens safe harbour-åtaganden. När safe harbour-systemet inrättades åtog sig konkurrensmyndigheten att prioritera granskning av alla hänskjutningar från EU-medlemsstaternas myndigheter[33]. Eftersom inga klagomål inkommit under de första tio åren med systemet beslutade konkurrensmyndigheten att försöka identifiera eventuella överträdelser av safe harbour i varje utredning av integritetsskydd och uppgiftsskydd som den genomför. Sedan 2009 har konkurrensmyndigheten vidtagit tio verkställighetsåtgärder mot företag med anledning av safe harbour-överträdelser. Dessa åtgärder ledde i synnerhet till vitesföreläggande – belagda med betydande påföljder – med förbud mot falska uppgifter om integritetsskydd, inbegripet falska uppgifter om efterlevnad av safe harbour-principerna, och krav på heltäckande integritetsskyddsprogram och revisioner under 20 år. Företagen måste godta oberoende bedömningar av deras program för integritetsskydd på begäran av konkurrensmyndigheten. Dessa bedömningar rapporteras regelbundet till konkurrensmyndigheten. Konkurrensmyndighetens beslut förbjuder också dessa företag att ge falska uppgifter om deras praxis för integritetsskydd och deras deltagande safe harbour-systemet eller liknande system för integritetsskydd. Detta var fallet t.ex. i konkurrensmyndighetens utredningar av Google, Facebook och MySpace[34]. År 2012 godtog Google att betala böter på 22,5 miljoner US-dollar för att reda ut misstankar om att företaget hade överträtt en consent order *(*beslut om krav på samtycke). I alla utredningar som rör integritetsskydd undersöker konkurrensmyndigheten på eget initiativ om safe harbour-åtaganden har överträtts.

Den federala konkurrensmyndigheten har nyligen än en gång upprepat sina uttalanden och sitt åtagande att som en prioriterad fråga se över varje hänskjutande från företag som självreglerar sitt integritetsskydd och från EU-medlemsstater som hävdar att ett företag inte efterlever safe harbour-principerna[35]. Konkurrensmyndigheten har fått endast ett fåtal hänskjutanden från europeiska dataskyddsmyndigheter under de tre senaste åren.

Ett transatlantiskt samarbete mellan dataskyddsmyndigheter har börjat växa fram under de senaste månaderna. Till exempel undertecknade den federala konkurrensmyndigheten den 26 juni 2013 ett samförståndsavtal med Irlands dataskyddsombud om ömsesidigt bistånd vid tillsynen av lagstiftning om skydd för personuppgifter inom den privata sektorn. Genom samförståndsavtalet inrättas en ram för ett utökat, mer enhetligt och effektivare samarbete för tillsyn av integritetsskyddet[36].

---

33 Se bilaga V till rådets beslut 2000/520/EG av den 26 juli 2000.

34 Under perioden 2009–2012 slutförde konkurrensmyndigheten tio verkställighetsåtgärder avseende safe harbour-åtaganden: FTC v. Javian Karnani, och 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), Myspace LLC (2012). Se *Federal Trade Commission of Safe Harbour Commitments*: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Se också *Case Highlights*: http://business.ftc.gov/us-eu-Safe-Harbour-framework. De flesta av dessa ärenden rör problem med företag som en gång anslutit sig till safe harbour och sedan fortsatt att utge sig som medlemmar utan att årligen förnya certifieringen.

35 Detta åtagande upprepades än en gång vid ett möte mellan chefen för den federala konkurrensmyndigheten Julie Brill och EU:s dataskyddsmyndigheter (artikel 29-gruppen) i Bryssel den 17 april 2013.

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

I augusti 2013 tillkännagav konkurrensmyndigheten att kontrollerna av företag som kontrollerar stora databaser med personuppgifter skulle skärpas ytterligare. Myndigheten har också upprättat en portal där konsumenterna kan lämna in integritetsskyddsrelaterade klagomål mot amerikanska företag[37].

Den federala konkurrensmyndigheten bör även utöka sina insatser för att undersöka oriktiga påståenden om anslutning till safe harbour. Ett företag som på sin webbplats påstår att det uppfyller kraven för safe harbour men som inte tagits upp på handelsministeriets förteckning över ”för närvarande anslutna” medlemmar vilseleder konsumenterna och missbrukar deras förtroende. Oriktiga påståenden minskar förtroendet för systemet som helhet och bör därför omedelbart tas bort från företagens webbplatser. Företagen bör vara bundna av ett verkställbart krav att konsumenterna inte får vilseledas. Konkurrensmyndigheten bör fortsätta att försöka upptäcka oriktiga påståenden om anslutning till safe harbour, som i fallet Karnani där konkurrensmyndigheten stängde en kalifornisk webbplats för att den innehöll ett oriktigt påstående om safe harbour-registrering och användes för bedrägliga metoder i samband med e-handel riktade mot europeiska konsumenter[38].

Den 29 oktober 2013 meddelade konkurrensmyndigheten att den hade inlett ”många utredningar av safe harbour-efterlevnad under de senaste månaderna” och att fler verkställighetsåtgärder på detta område kan förväntas ”under de kommande månaderna”. Konkurrensmyndigheten bekräftade också att den är ”fast besluten att undersöka hur dess effektivitet kan förbättras” och kommer att ”fortsätta att välkomna alla materiella ledtrådar, såsom det klagomål som inkommit under den senaste månaden från en EU-baserad konsumentorganisation om ett stort antal påstådda safe harbour-överträdelser”[39]. Myndigheten åtog sig också att ”systematiskt övervaka efterlevnaden av beslut inom ramen för safe harbour-systemet, på samma sätt som vi övervakar alla våra beslut[40]

Den 12 november 2013 meddelade den federala konkurrensmyndigheten Europeiska kommissionen att ”**om ett företags integritetsskyddspolicy utlovar safe harbour-skydd, kan inte det faktum att företaget inte har gjort eller bibehållit en registrering i sig innebära att företaget är undantaget från konkurrensmyndighetens tillsyn av att dessa safe harbour-åtaganden efterlevs**”[41].

I november 2013 meddelade handelsministeriet Europeiska kommissionen att ministeriet, ”för att garantera att företag inte gör oriktiga påståenden om anslutning till safe harbour-systemet, i fortsättningen kommer att kontakta safe harbour-deltagare en månad före den dag då deras certifiering ska förnyas för att beskriva vilka åtgärder de måste vidta om de väljer att avstå från att förnya den”. **Handelsministeriet ”kommer att varna företagen** i denna kategori att de måste avlägsna alla hänvisningar till safe harbour-deltagande, inbegripet användning av ministeriets safe harbour-certifieringsmärke, i företagens policyer för integritetsskydd och på deras webbplatser samt **tydligt underrätta dem om att underlåtenhet att göra detta kan göra att företagen blir föremål för verkställighetsåtgärder från den federala konkurrensmyndighetens sida**”[42].

---

37 Konsumenter kan lämna in sina klagomål via den federala konkurrensmyndighetens klagomålsassistent (Complaint Assistant) (https://www.ftccomplaintassistant.gov/) och internationella konsumenter kan lämna in klagomål via webbplatsen econsumer.gov (http://www.econsumer.gov).

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

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

40 Skrivelse från konkurrensmyndighetens ordförande Edith Ramirez till Europeiska kommissionens vice ordförande Viviane Reding.

41 Skrivelse från konkurrensmyndighetens ordförande Edith Ramirez till Europeiska kommissionens vice ordförande Viviane Reding.

42 *U.S.-EU Cooperation to Implement the Safe Harbor Framework* av den 12 november 2013.

För att motverka oriktiga påståenden om safe harbour-anslutning bör de självcertifierade företagens webbplatser alltid innehålla en länk till handelsministeriets safe harbour-webbsida där alla ”för närvarande anslutna” medlemmar förtecknas. På så sätt kan alla registrerade i Europa direkt, utan att behöva göra ytterligare sökningar, kontrollera om ett företag för närvarande är anslutet till safe harbour. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.

Den federala konkurrensmyndighetens fortlöpande övervakning och konsekventa tillsyn av att safe harbour-principerna faktiskt iakttas förblir – vid sidan av de ovannämnda åtgärder som handelsministeriet vidtar – en huvudprioritering för att se till att systemet fungerar korrekt och effektivt. Det är i synnerhet nödvändigt att öka antalet **kontroller och utredningar på eget initiativ av hur företagen efterlever** safe harbour-principerna. Det bör också bli enklare att lämna in klagomål till konkurrensmyndigheten om överträdelser.

### 5.2. EU:s arbetsgrupp för dataskydd

EU:s arbetsgrupp för dataskydd är ett organ som inrättats inom ramen för safe harbour-beslutet. Den har behörighet att handlägga klagomål från enskilda rörande personuppgifter som samlats in inom ramen för ett anställningsförhållande, och ärenden som gäller certifierade företag som har valt detta alternativ för tvistlösning inom safe harbour-systemet (53 % av alla företag). Arbetsgruppen består av representanter för olika dataskyddsmyndigheter i EU.

Hittills har arbetsgruppen mottagit fyra klagomål (två klagomål 2010 och två klagomål 2013). Den hänsköt år 2010 två klagomål till nationella dataskyddsmyndigheter (Förenade kungariket och Schweiz). Det tredje och det fjärde klagomålet behandlas för närvarande. Att klagomålen är så få kan förklaras av att arbetsgruppens befogenheter, som nämnts ovan, huvudsakligen begränsas till vissa typer av data.

Det begränsade antalet ärenden kan också delvis förklaras av bristande kunskap om arbetsgruppens existens. Kommissionen har sedan 2004 gjort information om arbetsgruppen mer synlig på sin webbplats[43].

För ett bättre utnyttjande av arbetsgruppen bör amerikanska företag som har valt att samarbeta med denna och följa dess beslut, när det gäller vissa eller samtliga av de kategorier av personuppgifter som omfattas av deras respektive självcertifieringar, klart och tydligt ange detta i åtagandena i sin policy för integritetsskydd så att handelsministeriet kan kontrollera denna aspekt. Alla dataskyddsmyndigheter i EU bör på sin webbplats skapa en särskild safe harbour-sida för att öka medvetenheten om safe harbour bland europeiska företag och registrerade.

### 5.3. Bättre genomförande och uppföljning

Den bristande insyn och de brister när det gäller genomförande och uppföljning som konstaterats ovan har gett upphov till oro bland företag i Europa när det gäller safe harbour-systemets negativa inverkan på de europeiska företagens konkurrenskraft. Om ett europeiskt företag konkurrerar med ett amerikanskt företag som deltar i safe harbour-systemet, men som

[43] I enlighet med rapporten från 2004 har ett informationsmeddelande i form av frågor och svar om EU:s arbetsgrupp för dataskydd offentliggjorts på kommissionens webbplats (GD Rättsliga frågor) för att informera enskilda och hjälpa dem att lämna in klagomål när de har anledning att tro att deras personuppgifter har behandlats i strid mot safe harbour-reglerna: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Standardblanketten för klagomål finns på http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf

i praktiken inte tillämpar dess principer, har det europeiska företaget en konkurrensnackdel i förhållande till det amerikanska företaget.

Dessutom omfattar den federala konkurrensmyndighetens behörighet illojala eller bedrägliga handlingar eller metoder i handeln och i verksamhet som påverkar handeln. I avsnitt 5 i *Federal Trade Commission Act* fastställs dock undantag till konkurrensmyndigheten befogenheter när det gäller illojala eller bedrägliga handlingar eller metoder bland annat när det gäller **telekommunikation**. Eftersom telekomföretagen inte omfattas av konkurrensmyndighetens tillsyn får de inte lov att ansluta sig till safe harbour-systemet. Med den ökande konvergensen mellan teknik och tjänster är dock många av deras direkta konkurrenter i den amerikanska IKT-sektorn medlemmar i safe harbour-systemet. Det faktum att telekomföretag är uteslutna från datautbyte inom ramen för safe harbour-systemet oroar vissa europeiska telekomoperatörer. Enligt Europeiska sammanslutningen för publika telenätoperatörer (Etno) står detta i tydlig strid med telekommunikationsoperatörernas mest angelägna krav, nämligen behovet av lika villkor[44].

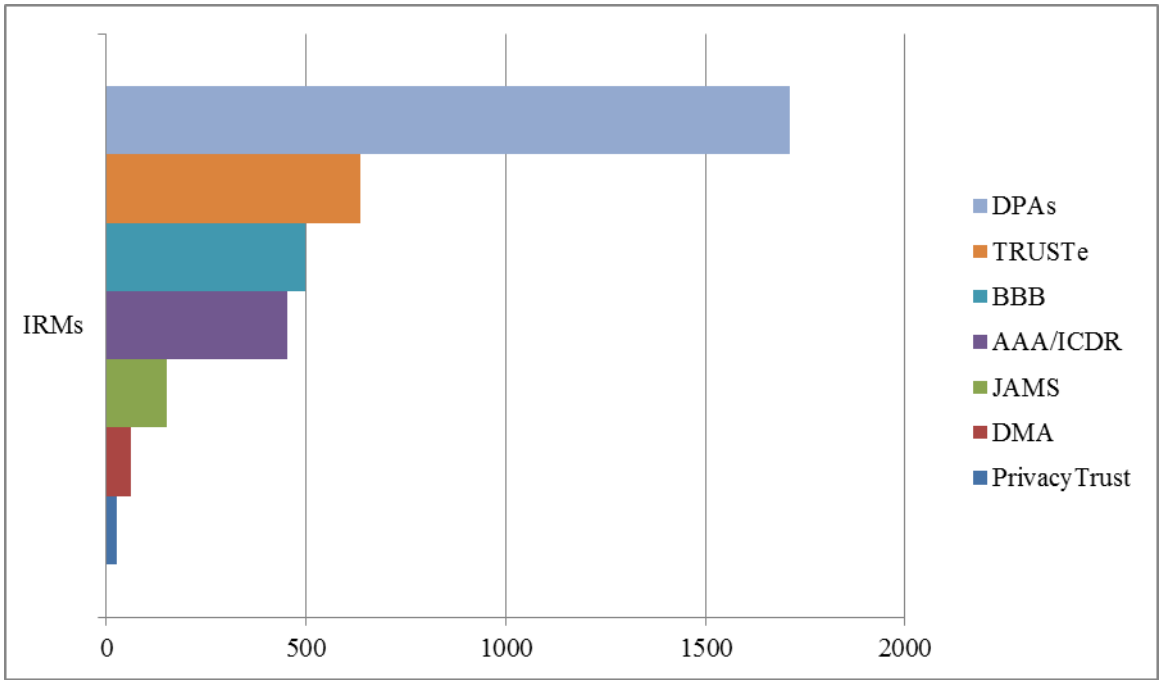
## 6. SKÄRPNING AV SAFE HARBOUR-PRINCIPERNA OM INTEGRITETSSKYDD

### 6.1. Alternativ tvistlösning

Enligt principen om genomförande och uppföljning måste det finnas ”**enkelt tillgängliga och billiga oberoende rättsmedel** genom vilka varje enskilds klagomål och tvister kan handläggas”. Inom ramen för safe harbour-systemet har det inrättats därför ett system för alternativ tvistlösning av en oberoende tredje part[45] för att tillhandahålla snabba lösningar för enskilda. De tre viktigaste organen för tvistlösning är EU:s arbetsgrupp för dataskydd, BBB (Better Business Bureaus) och TRUSTe.

44 *ETNO considerations*, som kommissionen mottog den 4 oktober 2013, tar även upp 1) definitionen av personuppgifter inom safe harbour-systemet, 2) bristen på övervakning av safe harbour, 3) det faktum att amerikanska företag kan överföra data med betydligt färre restriktioner än europeiska företag, vilket innebär en klar diskriminering av europeiska företag och påverkar de europeiska företagens konkurrenskraft. Enligt safe harbour-reglerna måste organisationer tillämpa principerna om meddelande och valmöjlighet för att få lämna uppgifter till en tredje part. Om en organisation vill överföra uppgifter till en tredje part som agerar som förmedlare kan organisationen göra detta, om den först förvissar sig om att tredje part ansluter sig till principerna eller omfattas av direktivet eller på annat sätt garanterar en adekvat skyddsnivå eller om den ingår ett skriftligt avtal med denna tredje part om att denne ska tillhandahålla minst samma integritetsskyddsnivå som krävs i principerna.

45 I EU-direktivet 2013/11/EU om alternativ tvistlösning framhålls vikten av oberoende, opartiska, öppna, effektiva, snabba och rättvisa alternativa tvistlösningsförfaranden.




Användningen av alternativ tvistlösning har ökat sedan 2004 och handelsministeriet har skärpt övervakningen av amerikanska alternativa tvistlösningsorgan för att se till att deras information om klagomålsförfarandet är tydlig, lättillgänglig och begriplig. Än så länge vet man dock inte hur effektivt detta system är, eftersom endast få ärenden hittills behandlats[46].

Även om handelsministeriet har lyckats få ner de avgifter som tas ut av de alternativa tvistlösningsorganen fortsätter två av de sju större tvistlösningsorganen att ta ut avgifter från enskilda som lämnar in klagomål[47]. Dessa anlitas av ungefär 20 % av företagen inom safe harbour-systemet. Dessa företag har valt ett tvistlösningsorgan som tar ut en avgift av konsumenter för att lämna in klagomål. Denna praxis är inte förenlig med safe harbour-principen om genomförande och uppföljning som ger enskilda rätt till tillgång till ”enkelt tillgängliga och billiga oberoende rättsmedel”. I EU är tillgången till oberoende tvistlösningstjänster som tillhandahålls av EU:s arbetsgrupp för dataskydd gratis för alla registrerade.

Den 12 november 2013 bekräftade handelsministeriet att det ”kommer att fortsätta att verka för EU-medborgarnas rätt till integritetsskydd och tillsammans med de alternativa tvistlösningsorganen undersöka om deras avgifter kan sänkas ytterligare”.

När det gäller påföljder förfogar inte alla de alternativa tvistlösningsorganen över de nödvändiga verktygen för att avhjälpa situationer där principerna för integritetsskydd inte har

[46] Exempelvis rapporterade en större tjänsteleverantör (TRUSTe) att man år 2010 mottagit 881 förfrågningar, men att endast tre av dessa ansågs godtagbara och välgrundade, vilket ledde till att de berörda företagen blev tvungna att ändra sin policy för integritetsskydd och sin webbplats. År 2011 var antalet klagomål 879, och i ett ärende blev företaget tvunget att ändra sin policy för integritetsskydd. Enligt handelsministeriet kommer större delen av klagomålen till de alternativa tvistlösningsorganen från konsumenter, till exempel användare som har glömt sitt lösenord och inte kunnat erhålla detta från sin internetleverantör. På kommissionens begäran har handelsministeriet tagit fram nya kriterier för statistikrapportering som ska användas av alla alternativa tvistlösningsorgan. Kriterierna skiljer mellan rena förfrågningar och klagomål och klargör mer utförligt de olika typer av klagomål som mottas. De nya kriterierna måste dock diskuteras ytterligare så att de nya statistikuppgifterna för 2014 omfattar alla alternativa tvistlösningsorgan, är jämförbara och ger den information som behövs för bedömningen av rättsmedlens effektivitet.

[47] International Centre for Dispute Resolution/American Arbitration Association (ICDR/AAA) tar ut 200 US-dollar och JAMS en registreringsavgift på 250 US-dollar. Handelsministeriet meddelade kommissionen att man hade arbetat med AAA, det dyraste tvistlösningsorganet för enskilda, för att utveckla ett särskilt safe harbour-program som minskade kostnaden för konsumenterna från tusentals dollar till ett fast pris på 200 US-dollar.

följts. Dessutom verkar inte alla alternativa tvistlösningsorgan tillämpa offentliggörande av konstaterade fall av bristande efterlevnad som en tillämplig påföljd eller åtgärd.

De alternativa tvistlösningsorganen måste också hänskjuta ärenden till den federala konkurrensmyndigheten om ett företag inte rättar sig efter resultatet av den alternativa tvistlösningen, eller avvisar tvistlösningsorganets beslut, så att konkurrensmyndigheten kan granska och utreda ärendet och, vid behov, vidta verkställighetsåtgärder. Hittills har dock tvistlösningsorganen inte hänskjutit några ärenden till konkurrensmyndigheten[48].

De alternativa tvistlösningsorganen har på sina webbplatser aktuella förteckningar över företag (Dispute Resolution Participants) som använder deras tjänster, vilket gör att konsumenter vid tvist med ett företag enkelt kan kontrollera om en enskild person kan lämna in ett klagomål till ett visst tvistlösningsorgan. Exempelvis förtecknar tvistlösningsorganet BBB alla företag som omfattas av BBB:s tvistlösningssystem. Det finns dock många företag som påstår att de omfattas av ett särskilt tvistlösningssystem men som inte tagits upp av de alternativa tvistlösningsorganen som deltagare i deras system[49].

Förfarandena för alternativ tvistlösning bör vara enkelt tillgängliga, oberoende och billiga för enskilda. Den registrerade bör ha möjlighet att lämna in ett klagomål utan alltför stora hinder. Alla tvistlösningsorgan bör på sina webbplatser offentliggöra statistik om de klagomål som handlagts och särskild information om resultaten av dessa. Tvistlösningsorganen bör också följas upp närmare så att deras information om förfarandet och om hur man lämnar in ett klagomål är tydlig och begriplig, och för att tvistlösning ska bli ett effektivt och tillförlitligt instrument som ger goda resultat. Det bör även upprepas att offentliggörande av konstaterade fall av bristande efterlevnad bör vara en av de obligatoriska påföljderna vid alternativ tvistlösning.

### 6.2. Vidare överföring

Den exponentiella tillväxten av dataflöden gör det nödvändigt att säkerställa kontinuiteten i skyddet av personuppgifter i alla skeden av databehandlingen, särskilt när data överförs av ett safe harbour-anslutet företag till en **tredje part som är registerförare**. Behovet av bättre genomförande och uppföljning av safe harbour gäller därför inte bara medlemmar i safe harbour utan även underleverantörer.

Enligt safe harbour-systemet är vidare överföring till en tredje part som agerar som ”förmedlare” tillåten om företaget – medlem i safe harbour-systemet – ”förvissar sig om att tredje part ansluter sig till principerna eller omfattas av direktivet eller på annat sätt garanterar en adekvat skyddsnivå eller om den ingår ett skriftligt avtal med denna tredje part om att denne skall tillhandahålla minst samma integritetsskyddsnivå som krävs i princip”[50]. Exempelvis kräver handelsministeriet att en leverantörer av molntjänster, som mottar personuppgifter som ska behandlas, ingår ett avtal även om denne uppfyller safe harbour-principerna[51]. Denna bestämmelse är dock inte tydlig i bilaga II till safe harbour-beslutet.

---

48 Se FoS 11.

49 Exempel: Amazon har informerat handelsministeriet om att företaget använder BBB som sitt tvistlösningsorgan. Hos BBB finns dock inte Amazon med på förteckningen över deltagare. Motsatt förhållande gäller för Arsalon Technologies (www.arsalon.net), som tillhandahåller molnvärdtjänster. Detta företag finns med på BBB:s förteckning över företag som deltar i tvistlösning inom safe harbour-systemet, men är för närvarande inte anslutet till safe harbour (den 1 oktober 2013). BBB, TRUSTe och andra alternativa tvistlösningsorgan bör ta bort eller korrigera felaktiga påståenden om certifiering. De bör vara bundna av ett verkställbart krav att endast certifiera företag som är medlemmar i safe harbour.

50 Se kommissionens beslut 2000/520/EG sidan 7 (vidare överföring).

51 Se *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

Eftersom användningen av underleverantörer ökat kraftigt under de senaste åren, särskilt i samband med molntjänster, bör ett företag inom safe harbour-systemet underrätta handelsministeriet när det ingår ett sådant avtal och vara skyldigt att offentliggöra de bestämmelser som rör integritetsskydd[52].

De tre ovannämnda frågorna, nämligen en alternativ tvistlösningsmekanism, förstärkt tillsyn och vidare överföring av data, bör klargöras bättre.

## 7. TILLGÅNG TILL UPPGIFTER SOM ÖVERFÖRS INOM RAMEN FÖR SAFE HARBOUR-SYSTEMET

Under 2013 har information om omfattningen och räckvidden av Förenta staternas övervakningsprogram gett anledning till oro för kontinuiteten i skyddet för personuppgifter som överförts lagligt till Förenta staterna inom ramen för safe harbour-systemet. Det verkar t.ex. som om alla företag som deltar i Prism-programmet och som ger de amerikanska myndigheterna tillgång till uppgifter som lagras och behandlas i Förenta staterna, är safe harbour-certifierade. Detta har gjort safe harbour-systemet till en av de kanaler genom vilken den amerikanska underrättelsetjänsten får möjlighet till att samla in personuppgifter som ursprungligen behandlats i EU.

Enligt bilaga I till safe harbour-beslutet kan efterlevnaden av principerna om integritetsskydd begränsas, om det är befogat med hänsyn till krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller till lagar, myndighetsföreskrifter eller rättspraxis. För att begränsningar och restriktioner för åtnjutande av grundläggande rättigheter ska gälla måste de tolkas restriktivt. De ska vara fastställda i allmänt tillgänglig lag och de måste vara nödvändiga och proportionerliga i ett demokratiskt samhälle. I safe harbour-beslutet specificeras särskilt att sådana begränsningar endast är tillåtna om de är begränsade till**"vad som är nödvändigt"** för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden[53]. Safe harbour-systemet medger visserligen behandling av uppgifter i undantagsfall med hänsyn till den nationella säkerheten, allmänintresset och rättsefterlevnaden, men underrättelseorganens omfattande tillgång till uppgifter som överförts till Förenta staterna i samband med handelstransaktioner var inget som kunde förutses vid antagandet av safe harbour-beslutet.

För att skapa tydlighet och rättslig säkerhet bör dessutom handelsministeriet underrätta Europeiska kommissionen om lagar eller myndighetsföreskrifter som kan inverka på anslutningen till safe harbour-principerna om integritetsskydd[54]. Användningen av undantag bör övervakas noggrant och de får inte användas på ett sätt som undergräver det skydd som

---

52 Detta gäller leverantörer av molntjänster som inte omfattas av safe harbour-systemet. Enligt konsultföretaget Galexia är andelen molntjänsteleverantörer som är medlemmar i safe harbour (och som följer principerna ) relativt hög. Molntjänsteleverantörer har vanligtvis integritetsskydd i flera skikt, som ofta kombinerar direkta avtal med kunderna och den övergripande policyn för integritetsskydd. Med ett eller två viktiga undantag följer molntjänsteleverantörerna inom safe harbour de centrala bestämmelserna för tvistlösning samt för genomförande och uppföljning. I nuläget finns det inga stora molntjänstleverantörer upptagna på förteckningen över företag som använder sig av oriktiga påståenden (enligt Chris Connolly från Galexia vid utfrågningen i LIBE-utskottet om elektronisk massövervakning av EU-medborgare).

53 Se bilaga I i safe harbour-beslutet: "Efterlevnaden av principerna kan begränsas a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses, eller c) om följden av direktivet eller medlemsstaternas lagstiftning är att man tillåter undantag och avvikelser förutsatt att sådana undantag eller avvikelser tillämpas i jämförbara sammanhang. I överensstämmelse med målen om ökat integritetsskydd bör organisationerna sträva efter att genomföra dessa principer öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna av skäl angivna i b ovan kommer att göras regelbundet. Av samma skäl förväntas organisationerna, såvida det finns en valmöjlighet enligt principerna och/eller amerikansk lag, välja en högre skyddsnivå om det är möjligt."

54 Yttrande 4/2000 om den dataskyddsnivå som garanteras genom safe harbor-principerna, antaget av artikel 29-gruppen den 16 maj 2000.

**principerna** innebär[55]. Det är framför allt de amerikanska myndigheternas omfattande tillgång till uppgifter som behandlas av självcertifierade safe harbour-företag som riskerar att undergräva konfidentialiteten vid elektronisk kommunikation.

### 7.1. Proportionalitet och nödvändighet

Som framgår av resultaten från ad hoc-arbetsgruppen mellan EU och Förenta staterna finns det ett antal rättsliga grunder enligt amerikansk lagstiftning som tillåter omfattande insamling och behandling av personuppgifter som lagras eller på annat sätt behandlas av företag som är baserade i Förenta staterna. Sådana uppgifter kan omfatta uppgifter som tidigare överförts från EU till Förenta staterna inom ramen för safe harbour-systemet, och det väcker frågan om safe harbour-principerna fortfarande efterlevs. Storskaligheten i dessa program kan leda till att amerikanska myndigheter får tillgång till och vidarebehandlar uppgifter som överförs inom ramen för safe harbour utöver vad som är absolut nödvändigt och proportionerligt för att skydda den nationella säkerheten enligt undantaget i safe harbour-beslutet.

### 7.2. Begränsningar och möjlighet till prövning

Som framgår av resultaten från ad hoc-arbetsgruppen för dataskydd mellan EU och Förenta staterna gäller garantierna enligt amerikansk lagstiftning främst amerikanska medborgare eller i Förenta staterna lagligen bosatta personer. Dessutom finns det ingen möjlighet för registrerade personer, varken i EU eller i Förenta staterna, att få tillgång till, rätta eller radera uppgifter eller möjlighet till administrativ eller rättslig prövning med avseende på insamling och vidare behandling av personuppgifter som sker inom ramen för amerikanska övervakningsprogram.

### 7.3. Insyn

Företagen uppger inte systematiskt i sin integritetsskyddspolicy när de tillämpar undantag från principerna. Enskilda och företag vet alltså inte vad som sker med deras uppgifter. Detta är särskilt relevant i samband med de amerikanska övervakningsprogrammen i fråga. Detta innebär att de européer vars uppgifter överförs till ett företag i Förenta staterna inom ramen för safe harbour-systemet eventuellt inte får besked från företagen om att det kan beviljas tillgång till deras uppgifter[56]. Detta väcker frågan om safe harbour-principerna för insyn efterlevs. Insyn bör garanteras så långt det är möjligt utan att den nationella säkerheten äventyras. Utöver de befintliga kraven på företagen att i sin integritetsskyddspolicy ange när principerna kan begränsas av lagar, myndighetsföreskrifter eller rättspraxis bör företag också uppmanas att i sin policy för integritetsskydd ange när de tillämpar undantag från principerna för att uppfylla krav i fråga om nationell säkerhet, allmänintresse eller rättsefterlevnad.

## 8. SLUTSATSER OCH REKOMMENDATIONER

Sedan safe harbour-systemet antogs 2000 har det blivit en kanal för flödena av personuppgifter mellan EU och Förenta staterna. Vikten av effektivt skydd vid överföring av personuppgifter har ökat till följd av den exponentiella ökningen av dataflöden som är av central betydelse för den digitala ekonomin, och till följd av de mycket stora förändringarna

[55] Yttrande 4/2000 om den dataskyddsnivå som garanteras genom safe harbor-principerna, antaget av artikel 29-gruppen den 16 maj 2000.

[56] Vissa europeiska företag som är med i safe harbour-systemet tillhandahåller relativt transparent information. Exempelvis anger Nokia, som bedriver verksamhet i Förenta staterna och som är medlem i safe harbour i sin policy för integritetsskydd att *”vi kan komma att pliktas enligt tvingande lag att lämna ut dina personuppgifter till vissa myndigheter eller annan tredje part, till exempel brottsbekämpande myndigheter i de länder där vi eller tredje part som handlar å våra vägnar har verksamhet.”*

när det gäller insamling, behandling och användning av data. Internetföretag som Google, Facebook, Microsoft, Apple och Yahoo har hundratals miljoner användare i Europa och överför personuppgifter för behandling i Förenta staterna i en omfattning som ingen kunde föreställa sig år 2000 då safe harbour inrättades.

På grund av bristande öppenhet och insyn och brister i genomförandet och uppföljningen av safe harbour kvarstår vissa problem som bör åtgärdas:

a) Insynen i safe-harbourmedlemmarnas policy för integritetsskydd.

b) Amerikanska företags faktiska tillämpning av principerna för integritetsskydd.

c) Effektiviteten i genomförande och uppföljning.

Underrättelseorganens **omfattande tillgång till de uppgifter som safe harbour-certifierade företag överför till Förenta staterna** ger dessutom upphov till allvarliga frågor om kontinuiteten för européers dataskyddsrättigheter när deras uppgifter överförs till Förenta staterna.

På grundval av ovanstående har kommissionen kommit fram till följande **rekommendationer**:

**Öppenhet och insyn**

1. *Självcertifierade företag bör offentliggöra sin policy för integritetsskydd.* Det räcker inte att företagen lämnar in en beskrivning av sin policy för integritetsskydd till handelsministeriet. Företagens policy för integritetsskydd bör göras allmänt tillgänglig på företagens webbplatser, på ett klart och tydligt språk.
2. *Självcertifierade företags webbplatser bör alltid innehålla en länk till handelsministeriets safe harbour-webbplats där alla ”för närvarande anslutna” medlemmar förtecknas.* På så sätt kan alla registrerade i Europa direkt, utan att behöva göra ytterligare sökningar, kontrollera om ett företag för närvarande är anslutet till safe harbour. Detta skulle bidra till att öka systemets trovärdighet genom att minska möjligheterna för oriktiga påståenden om att ett företag är anslutet till safe harbour. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.
3. *Självcertifierade företag bör offentliggöra de bestämmelser som rör integritetsskydd i alla avtal som de ingår med underleverantörer, t.ex. om datormolntjänster.* Safe harbour medger vidare överföring från självcertifierade safe harbour-företag till tredje part som agerar som förmedlare, t.ex. leverantörer av molntjänster. Så vitt känt kräver handelsministeriet i dessa fall att självcertifierade företag ska ingå ett avtal. När sådana avtal ingås bör ett safe harbour-företag dock även underrätta handelsministeriet och vara skyldigt att offentliggöra de bestämmelser som rör integritetsskydd.
4. *På handelsministeriets webbplats bör alla företag som inte för närvarande är anslutna till systemet tydligt anges.* Beteckningen ”för närvarande ej anslutet” i handelsministeriets förteckning över safe harbour-medlemmar bör åtföljas av en tydlig varning om att företaget för närvarande inte uppfyller kraven för safe harbour. Ett ”för närvarande ej anslutet” företag är dock skyldigt att fortsätta att tillämpa safe harbour-kraven för de uppgifter som det mottagit inom ramen för safe harbour.

**Tvistlösning**

5. *Den policy för integritetsskydd som företagen publicerar på sina webbplatser bör omfatta en länk till det alternativa tvistlösningsorganet och/eller EU:s arbetsgrupp.* Detta gör det möjligt för registrerade i Europa att omedelbart kontakta tvistlösningsorganet eller EU:s arbetsgrupp om det uppstått problem. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.

6. Alternativ tvistlösning bör vara lätt tillgänglig och billig. Vissa organ för alternativ tvistlösning inom ramen för safe harbour-systemet fortsätter att ta ut avgifter från enskilda – vilket kan bli mycket kostsamt för en enskild användare — för handläggning av klagomål (200–250 US-dollar). I Europa däremot kostar det inget att vända sig till den arbetsgrupp för dataskydd som inrättats för att lösa klagomål inom ramen för safe harbour.

7. *Handelsministeriet bör mer systematiskt övervaka tvistlösningsorganen i fråga om insyn i och tillgängligheten till den information som de tillhandahåller om det förfarande de tillämpar och deras uppföljning av klagomål.* Detta gör tvistlösning till ett effektivt och tillförlitligt instrument som ger goda resultat. Det bör även upprepas att offentliggörande av konstaterade fall av bristande efterlevnad bör vara en av de obligatoriska påföljderna vid alternativ tvistlösning.

**Genomförande och uppföljning**

8. *Efter certifiering eller förnyande av certifiering av företag inom ramen för safe harbour bör en viss andel av dessa företag bli föremål för en utredning (som omfattar mer än bara en kontroll av att de formella kraven följs) av att de i praktiken följer sin policy för integritetsskydd.*

9. *Om bristande efterlevnad konstateras till följd av ett klagomål eller en utredning bör företaget bli föremål för en särskild uppföljningsutredning efter ett år.*

10. *Vid misstanke om att ett företag brister i efterlevnaden eller vid icke avgjorda klagomål bör handelsministeriet informera den behöriga europeiska dataskyddsmyndigheten.*

11. *Oriktiga påståenden om anslutning till safe harbour bör fortsätta att utredas.* Ett företag som på sin webbplats påstår att det uppfyller kraven för safe harbour men som inte tagits upp på handelsministeriets förteckning över ”för närvarande anslutna” medlemmar vilseleder konsumenterna och missbrukar deras förtroende. Oriktiga påståenden minskar förtroendet för systemet som helhet och bör därför omedelbart tas bort från företagens webbplatser.

**De amerikanska myndigheternas tillgång**

12. *Självcertifierade företags policy för integritetsskydd bör innehålla uppgifter om i vilken utsträckning den amerikanska lagstiftningen tillåter offentliga myndigheter att samla in och behandla de uppgifter som överförts inom ramen för safe harbour. Framför allt bör företag uppmanas att i sin policy för integritetsskydd ange i vilka*

*fall de tillämpar undantag till principerna för att uppfylla krav i fråga om nationell säkerhet, allmänintresse eller rättsefterlevnaden.*

13. *Det är viktigt att undantaget avseende nationell säkerhet enligt safe harbour-beslutet endast används i en omfattning som är absolut nödvändig eller proportionerlig.*

EUROPEISKA
KOMMISSIONEN

Bryssel den 27.11.2013
COM(2013) 844 final

# RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

## om en gemensam översyn av genomförandet av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av passageraruppgifter till Förenta staternas Department of Homeland Security

**RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET**

**om en gemensam översyn av genomförandet av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av passageraruppgifter till Förenta staternas Department of Homeland Security**

Det nu gällande avtalet mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter (*Passenger Name Records*, nedan kallade *PNR*) till Förenta staternas Department of Homeland Security trädde i kraft den 1 juli 2012.

I avtalet föreskrivs att en första gemensam översyn ska göras ett år efter avtalets ikraftträdande och därefter med jämna mellanrum enligt en gemensam överenskommelse. Den gemensamma översynen genomfördes den 8 och 9 juli 2013 i Washington. Det främsta syftet med översynen var att undersöka genomförandet av avtalet, med särskilt beaktande av metoden för överföring av PNR-uppgifter och vidareöverföringen av PNR-uppgifter, i enlighet med de relevanta artiklarna i avtalet och i överensstämmelse med skäl 18 i avtalet.

Den gemensamma översynen bygger på det förfarande som EU:s och Förenta staternas grupper utarbetade för den första gemensamma översynen av 2004 års avtal om passageraruppgifter, vilken ägde rum i september 2005. Den första delen av detta förfarande bestod i ett frågeformulär som Europeiska kommissionen sände till Förenta staternas Department of Homeland Security (nedan kallat *DHS*) före den gemensamma översynen. DHS lämnade skriftliga svar på frågeformuläret före den gemensamma översynen. Den andra delen av förfarandet bestod i att EU-gruppen besökte en av DHS driftcentraler. Den tredje delen bestod i ett möte mellan företrädare för DHS, Förenta staternas justitieministerium, Förenta staternas utrikesministerium, EU-gruppen och DHS dataskyddskontor, där genomförandet av avtalet diskuterades ingående.

Före den gemensamma översynen gjorde DHS dataskyddskontor en intern översyn av hur DHS genomfört avtalet. Översynen gjordes för att fastställa om DHS följer alla normer och representationer i avtalet med EU.

EU-gruppen konstaterade att DHS tillämpar avtalet i enlighet med de villkor som där anges. Bland annat använder DHS effektiva filter för att filtrera bort data utan koppling till Förenta staterna och PNR-uppgifter som faller utanför de 19 kategorier som beskrivs i bilagan till avtalet. Reglerna för avidentifiering och radering av känsliga uppgifter respekteras och DHS har uppgett att man aldrig har tagit fram känsliga uppgifter för operativa ändamål.

DHS genomför också sina åtaganden i fråga om passagerarnas rättigheter, särskilt när det gäller att tillhandahålla lämplig information till passagerare och att tillämpa rätten till insyn i personuppgifter utan några undantag. Detta bör dock ses i förhållande till den fjärde rekommendationen nedan, enligt vilken det behövs större insyn i passagerarnas möjligheter till rättslig prövning.

DHS hanterar utbyte av uppgifter med andra interna organ i enlighet med avtalet. Utbyte sker från fall till fall på grundval av skriftliga överenskommelser, och registreras. Utbyte av uppgifter med tredjeländer tolkas strikt och sker också i enlighet med avtalet.

Som en allmän rekommendation bör DHS dataskyddskontor åter göra en intern översyn av avtalet innan nästa gemensamma översyn äger rum. Förenta staterna och EU föreslår att nästa gemensamma översyn ska anordnas under första halvåret 2015.

Det rekommenderas också att så snabbt som möjligt, och i varje fall senast den 1 juli 2014, övergå till sändmetoden i enlighet med artikel 15.4 i avtalet.

Det rekommenderas vidare att Förenta staterna och EU ska samarbeta för att främja användningen av gemensamma standarder för sändning, särskilt PNRGOV-standarden som utvecklats av IATA, flygbolag och myndigheter. I detta sammanhang skulle det vara välkommet om diskussionerna i IATA om en gemensam sändmetod också ledde till en gemensam standard för tillfällig sändning.

Vissa förändringar krävs emellertid i fråga om genomförandet av avtalet. Först och främst gäller detta början av den sexmånadersperiod efter vilken PNR-uppgifterna ska göras anonyma i enlighet med artikel 8.1 i avtalet. För närvarande räknas denna period från och med den dag då PNR-uppgifterna senast uppdaterades i DHS profileringssystem *Automated Targeting System* (ATS), där uppgifterna lagras, och inte den dag då PNR-uppgifterna lades in i ATS. Rekommendationen är att sexmånadersperioden ska räknas från och med den dag då PNR-uppgifter läggs in i ATS (den så kallade *ATS Load Date*), dvs. den dag då uppgifterna lagras i ATS, istället för att tillämpa nuvarande praxis, som försenar tillämpningen av sexmånadersperioden (till den sista uppdateringen av PNR-uppgifterna i ATS).

För det andra bör särskild uppmärksamhet ägnas användningen av den tillfälliga direktåtkomstmetoden. DHS rekommenderas att utöver sin nuvarande registrering bättre dokumentera orsakerna till varför den tillfälliga direktåtkomstmetoden används i varje enskilt fall. Detta skulle leda till en bättre bedömning av proportionaliteten och möjliggöra en effektivare granskning av metodens användning, som är tänkt att vara ett undantag från regeln.

För det tredje uppmanas DHS att respektera sitt åtagande att säkerställa ömsesidighet och aktivt dela enskilda PNR-uppgifter och analytisk information som härrör från PNR-uppgifter med EU:s medlemsstater och i förekommande fall med Europol och Eurojust.

För det fjärde rekommenderas en större insyn i de förfaranden för rättslig prövning som fastställs i Förenta staternas lagstiftning. Sådan insyn skulle göra det möjligt för passagerare som inte är amerikanska medborgare eller lagligt bosatta i Förenta staterna att få till stånd en prövning av DHS beslut om användning av PNR-uppgifter, särskilt i fall där användningen av sådana uppgifter kan bidra till att lufttrafikföretag rekommenderas att neka passagerare ombordstigning.

Slutligen genomför DHS också åtgärder som går utöver vad som föreskrivs i avtalet. DHS avser att göra en anmälan till Europeiska kommissionen inom 48 timmar efter det att man fått tillgång till känsliga PNR-uppgifter. DHS har infört ett nytt förfarande för att en gång i kvartalet se över och granska genomförandet av ATS. DHS granskar också möjliga resmål samt analyser och regler som rör dessa för att inverkan på resenärer med ärligt uppsåt och deras medborgerliga rättigheter, medborgerliga friheter och integritet ska bli så liten som möjligt samt för att undvika diskriminering av resenärer.

Utan hinder av artikel 23.1 om en gemensam utvärdering av avtalet fyra år efter dess ikraftträdande, framgår av en preliminär bedömning av huruvida PNR-uppgifterna fullgör syftet att stödja kampen mot terrorism och andra brott av gränsöverskridande natur att DHS tack vare PNR-uppgifterna kan göra en bedömning av samtliga passagerare upp till 96 timmar före avgång och därigenom få tillräckligt med tid för att genomföra alla säkerhetsprövningar före en passagerares ankomst, samt förbereda eventuella åtgärder. Förfarandet ligger också till grund för DHS beslut om huruvida en passagerare ska få gå ombord på ett flygplan eller inte. Dessutom ger det DHS möjlighet att genomföra riskbedömningar på grundval av regler baserade på olika scenarier i syfte att identifiera ”okända” potentiella högriskpersoner. PNR-

uppgifter kan också användas för att göra kopplingar mellan passagerare och identifiera brottslingar som tillhör samma grupp organiserade brottslingar. Enligt DHS har PNR-uppgifter också framgångsrikt använts för att undersöka hur brottslingar beter sig när de reser, exempelvis genom bättre förståelse för vilka rutter de använder.

Den gemensamma översynsrapport som bifogas detta meddelande är indelad i tre kapitel. Kapitel 1 ger en bakgrund till översynen och presenterar syftet med och förfarandemässiga aspekter av arbetet. I kapitel 2 presenteras de viktigaste resultaten från den gemensamma översynen och de punkter som DHS bör åtgärda. Detta kapitel kompletteras av bilaga A, som innehåller frågeformuläret och DHS svar. I kapitel 3 presenteras de allmänna slutsatserna av arbetet. Bilaga B visar hur de grupper från EU och Förenta staterna som utförde översynen är sammansatta.

EUROPEISKA
KOMMISSIONEN

Bryssel den 27.11.2013
COM(2013) 843 final

# MEDDELANDE FRÅN KOMMISSIONEN MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

## om den gemensamma rapporten från kommissionen och amerikanska finansdepartementet om värdet av de uppgifter som tillhandahållits genom TFTP enligt artikel 6 i avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism

**MEDDELANDE FRÅN KOMMISSIONEN MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET**

**om den gemensamma rapporten från kommissionen och amerikanska finansdepartementet om värdet av de uppgifter som tillhandahållits genom TFTP enligt artikel 6 i avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism**

## 1. Rättslig grund

I enlighet med artikel 6.6 i avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (nedan kallat *avtalet*) har Europeiska kommissionen och Förenta staternas finansdepartement utarbetat föreliggande gemensamma rapport om vilket värde uppgifter tillhandahållna genom programmet har i spårandet av finansieringen av terrorism (nedan kallat *TFTP* eller *programmet*) ”med särskild betoning på värdet av uppgifter som lagras i flera år och relevanta upplysningar som erhållits via den gemensamma översyn som utförts i enlighet med artikel 13.”

## 2. Förfarandefrågor

Föreliggande rapports uppbyggnad har fastställts gemensamt av Europeiska kommissionen och amerikanska finansdepartementet, i enlighet med artikel 6.6.

Europeiska kommissionen och amerikanska finansdepartementet inledde i december 2012 diskussioner om former, uppdrag och metod för rapporten. Den 25 februari 2013 träffades EU:s och USA:s utvärderingsgrupper i Washington, D.C. för att diskutera rapporten och kallade till ett andra mötet i Europols lokaler i Haag den 14 maj 2013. Under mötet i Haag träffade EU:s och USA:s experter även Europols representanter för diskussioner av samtliga parters initiala bidrag och därjämte kommande steg.

För EU:s del höll kommissionen den 13 maj 2013 ett hemligt möte med företrädare för medlemsstaterna. Medlemsstaterna och Europol har lämnat skriftliga bidrag som har beaktats och medtagits i utarbetandet av föreliggande rapport. Europol tog för detta ändamål fram ett frågeformulär för alla berörda medlemsstater för insamlingen av relevant information som utgjorde dess bidrag till rapporten. Syftet med frågeformuläret var att skapa överblick över tillhandahållna TFTP-uppgifters mervärde i specifika fall som utretts av behöriga myndigheter i berörda medlemsstater.

Mellan den 1 februari och den 24 maj 2013 intervjuade USA:s bedömningsgrupp terrorutredare i en rad olika organ, granskade fall av terrorism där TFTP använts och analyserade över 1 000 TFTP-rapporter för att bedöma värdet av TFTP-baserad information.

## 3. Tillämpningsområde

Underlaget till rapporten har tagits fram av USA:s finansdepartement, Europol och medlemsstaterna. Rapporten är koncentrerad på hur TFTP-uppgifter har använts och vilket värde de har för terrorutredningar i USA och EU. Rapporten innehåller ett flertal konkreta exempel på hur TFTP-uppgifter, bl.a. uppgifter som lagras i tre år eller längre, har varit värdefulla i terrorundersökningar i USA och EU, före och efter avtalets ikraftträdande den 1 augusti 2010. Jämte föreliggande rapport lades andra exempel på TFTP-uppgifternas användbarhet och värde fram vid de två gemensamma översyner som, i enlighet med artikel 13 i avtalet, gjordes i februari 2011 och oktober 2012. Sammantaget illustrerar denna faktabaserade och konkreta information mycket tydligare än tidigare TFTP:s funktion och mervärde.

I rapporten beskrivs likaledes vilken bedömning amerikanska finansdepartementet gör av lagringsperioderna och radering av icke framtagna uppgifter.

Rapporten visar att tillhandahållna TFTP-uppgifter, bl.a. flerårigt lagrade uppgifter, har haft ett mycket stort värde i kampen mot terrorism i USA, Europa och annorstädes.

I anslutning till föreliggande meddelande överlämnar kommissionen den bilagda gemensamma rapporten till Europaparlamentet och rådet.

**COUNCIL OF THE EUROPEAN UNION**

**Brussels, 27 November 2013**

**16987/13**

**JAI 1078**
**USA 61**
**DATAPROTECT 184**
**COTER 151**
**ENFOPOL 394**

**NOTE**

| | |
|---|---|
| from: | Presidency and Commission Services |
| to: | COREPER |
| Subject: | Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection |

Delegations will find attached the Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection.

**Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection**

## 1. AIM AND SETTING UP OF THE WORKING GROUP

In June 2013, the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data was revealed. The programmes concern in particular the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of US information and communications technology companies in the EU market, the transatlantic routing of electronic data flows, and the volume of data flows across the Atlantic, significant numbers of individuals in the EU are potentially affected by the US programmes.

At the EU-US Justice and Home Affairs Ministerial Meeting in June 2013, and in letters to their US counterparts, Vice-President Reding and Commissioner Malmström expressed serious concerns regarding the impact of these programmes on the fundamental rights of individuals in the EU, particularly the fundamental right to protection of personal data. Clarifications were requested from the US authorities on a number of aspects, including the scope of the programmes, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, as well as the different levels of protection and procedural safeguards that apply to US and EU persons.

Further to a COREPER meeting of 18 July 2013, an ad hoc EU-US Working Group was established in July 2013 to examine these matters. The purpose was to establish the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens.

Further to that COREPER meeting, a "second track" was established under which Member States may discuss with the US authorities, in a bilateral format, matters related to their national security, and the EU institutions may raise with the US authorities questions related to the alleged surveillance of EU institutions and diplomatic missions.

On the EU side, the ad hoc Working Group is co-chaired by the Commission and the Presidency of the Council. It is composed of representatives of the Presidency, the Commission services, the European External Action Service, the incoming Presidency, the EU Counter-Terrorism Co-ordinator, the Chair of the Article 29 Working Party, as well as ten experts from Member States, having expertise in the area of data protection and law enforcement/security. On the US side, the group is composed of senior officials from the Department of Justice, the Office of the Director of National Intelligence, the State Department and the Department of Homeland Security.

A preparatory meeting took place in Washington, D.C. on 8 July 2013. Meetings of the Group took place on 22 and 23 July 2013 in Brussels, on 19 and 20 September 2013 in Washington, D.C., and on 6 November 2013 in Brussels.

The findings by the EU co-chairs of the ad hoc EU-US Working Group are presented in this report. The report is based on information provided by the US during the meetings of the ad hoc EU-US working group, as well as on publicly available documents, including classified documents disclosed in the press but not confirmed by the US. Participants on the EU side had an opportunity to submit comments on the report. The US was provided with an opportunity to comment on possible inaccuracies in the draft. The final report has been prepared under the sole responsibility of the EU-co chairs.

The distinction between the EU-US Working Group and the bilateral second track, which reflects the division of competences between the EU and Member States and in particular the fact that national security remains the sole responsibility of each Member State, set some limitations on the discussion in the Working Group and the information provided therein. The scope of the discussions was also limited by operational necessities and the need to protect classified information, particularly information related to sources and methods. The US authorities dedicated substantial time and efforts to responding to the questions asked by the EU side on the legal and oversight framework in which their Signal Intelligence capabilities operate.

## 2. THE LEGAL FRAMEWORK

The US provided information regarding the legal basis upon which surveillance programmes are based and carried out. The US clarified that the President's authority to collect foreign intelligence outside the US derives directly from his capacity as "commander in chief" and from his competences for the conduct of the foreign policy, as enshrined in the US constitution.

The overall US constitutional framework, as interpreted by the US Supreme Court is also sufficiently relevant to make reference to it here. The protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause"[1] extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment[2].

Two legal authorities that serve as bases for the collection of personal data by US intelligence agencies are: Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) (as amended by the 2008 FISA Amendments Act, 50 U.S.C. § 1881a); and Section 215 of the USA PATRIOT Act 2001 (which also amended FISA, 50 U.S.C. 1861). The FISA Court has a role in authorising and overseeing intelligence collection under both legal authorities.

---

1 "Probable cause" must be shown before an arrest or search warrant may be issued. For probable cause to exist there must be sufficient reason based upon known facts to believe a crime has been committed or that certain property is connected with a crime. In most cases, probable cause has to exist prior to arrest, search or seizure, including in cases when law enforcement authorities can make an arrest or search without a warrant.

2 According to the US Supreme Court, foreigners who are not residing permanently in the US can only rely on the Fourth Amendment if they are part of the US national community or have otherwise developed sufficient connection with the US to be considered part of that community: US v. Verdugo-Urquidez – 494 U.S. 259 (1990), pp. 494 U.S. 264-266.

The US further clarified that not all intelligence collection relies on these provisions of FISA; there are other provisions that may be used for intelligence collection. The Group's attention was also drawn to Executive Order 12333, issued by the US President in 1981 and amended most recently in 2008, which sets out certain powers and functions of the intelligence agencies, including the collection of foreign intelligence information. No judicial oversight is provided for intelligence collection under Executive Order 12333, but activities commenced pursuant to the Order must not violate the US constitution or applicable statutory law.

## 2.1. Section 702 FISA (50 U.S.C. § 1881a)

### *2.1.1. Material scope of Section 702 FISA*

Section 702 FISA provides a legal basis for the collection of "foreign intelligence information" regarding persons who are "reasonably believed to be located outside the United States." As the provision is directed at the collection of information concerning non-US persons, it is of particular relevance for an assessment of the impact of US surveillance programmes on the protection of personal data of EU citizens.

Under Section 702, information is obtained "from or with the assistance of an electronic communication service provider". This can encompass different forms of personal information (e.g. emails, photographs, audio and video calls and messages, documents and internet browsing history) and collection methods, including wiretaps and other forms of interception of electronically stored data and data in transmission.

The US confirmed that it is under Section 702 that the National Security Agency (NSA) maintains a database known as PRISM. This allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube.

The US also confirmed that Section 702 provides the legal basis for so-called "upstream collection"; this is understood to be the interception of Internet communications by the NSA as they transit through the US [1] (e.g. through cables, at transmission points).

Section 702 does not require the government to identify particular targets or give the Foreign Intelligence Surveillance Court (hereafter 'FISC') Court a rationale for individual targeting. Section 702 states that a specific warrant for each target is not necessary.

The US stated that no blanket or bulk collection of data is carried out under Section 702, because collection of data takes place only for a specified foreign intelligence purpose. The actual scope of this limitation remains unclear as the concept of foreign intelligence has only been explained in the abstract terms set out hereafter and it remains unclear for exactly which purposes foreign intelligence is collected. The EU side asked for further specification of what is covered under "foreign intelligence information," within the meaning of FISA 50, U.S.C. §1801(e), such as references to legal authorities or internal guidelines substantiating the scope of foreign intelligence information and any limitations on its interpretation, but the US explained that they could not provide this as to do so would reveal specific operational aspects of intelligence collection programmes. "Foreign intelligence information", as defined by FISA, includes specific categories of information (e.g. international terrorism and international proliferation of weapons of mass destruction) as well as "information relating to the conduct of the foreign affairs of the US." Priorities are identified by the White House and the Director of National Intelligence and a list is drawn up on the basis of these priorities.

Foreign intelligence could, on the face of the provision, include information concerning the political activities of individuals or groups, or activities of government agencies, where such activity could be of interest to the US for its foreign policy[2]. The US noted that "foreign intelligence" includes information gathered with respect to a foreign power or a foreign territory as defined by FISA, 50 USC 1801.

---

1 Opinions of the Foreign Intelligence Surveillance Court (FISC) of 3 October 2011 and of 30 November 2011.

2 50 U.S.C. §1801(e) (2) read in conjunction with §1801(a) (5) and (6).

On the question whether "foreign intelligence information" can include activities that could be relevant to US economic interests, the US stated that it is not conducting any form of industrial espionage and referred to statements of the President of the United States[1] and the Director of National Intelligence[2]. The US explained that it may collect economic intelligence (e.g. the macroeconomic situation in a particular country, disruptive technologies) that has a foreign intelligence value. However, the US underlined that information that is obtained which may provide a competitive advantage to US companies is not authorised to be passed on to those companies.

Section 702 provides that upon issuance of an order by FISC, the Attorney General and the Director of National Intelligence may authorize jointly the targeting of persons reasonably believed to be located outside the US to acquire foreign intelligence information. Section 702 does not require that foreign intelligence information be the sole purpose or even the primary purpose of acquisition, but rather "a significant purpose of the acquisition". There can be other purposes of collection in addition to foreign intelligence. However, the declassified FISC Opinions indicate that, due to the broad method of collection applied under the upstream programme and also due to technical reasons, personal data is collected that may not be relevant to foreign intelligence[3].

---

1 Speaking at a press conference in Stockholm on 4 September 2013, President Obama said: "when it comes to intelligence gathering internationally, our focus is on counterterrorism, weapons of mass destruction, cyber security -- core national security interests of the United States".

2 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 September 2013: "What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line"; full statement available at: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

3 According to the FISC Declassified Opinion of 3 October 2011, "NSAs 'upstream collection' of Internet communications includes the acquisition of entire 'transactions'", which "may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection" (p. 5). The FISC further notes that "NSA's upstream collection devices have technological limitations that significantly affect the scope of collection" (p. 30), and that "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from or about a tasked selector" (p. 31). It is stated in the FISC Declassified Opinion that "the portions of MCTs [multi communication transactions] that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT" (p. 57).

*2.1.2. Personal scope of Section 702 FISA*

Section 702 FISA governs the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". It is aimed at the targeting of non-US persons who are overseas.

This is confirmed by the limitations set forth in Section 702 (b) FISA which exclusively concern US citizens or non-US persons within the US[1]. More specifically, acquisition of data authorised under Section 702 may not:

(i) intentionally target any person known at the time of acquisition to be located in the US;

(ii) intentionally target a person believed to be located outside the US if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the US;

(iii) intentionally target a US person reasonably believed to be located outside the US;

(iv) intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the US.

In addition, pursuant to the same provision, acquisition of data must be "conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States", that prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause".

As far as US persons are concerned, the definition of "foreign intelligence information" requires that the information to be collected is *necessary* to the purpose pursued[2]. Concerning non-US persons, the definition of "foreign intelligence information" only requires the information to be *related* to the purpose pursued[3].

---

1 "US person" is defined in 50 U.S.C. §1801(i) as a US citizen, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are US citizens or permanent residents, or a corporation incorporated in the US but not including a corporation or association that is a foreign power.

2 50 U.S.C. §1801(e).

3 Ibid.

As discussed below, collection under Section 702 is subject to targeting and minimisation procedures that aim to reduce the collection of personal data of US persons under Section 702, as well as the further processing of personal data of US persons incidentally acquired under Section 702. While, according to the US, non US persons may benefit from some requirements set out in the minimization procedures[1], there are no targeting or minimisation procedures under Section 702 that specifically aim to reduce the collection and further processing of personal data of non-US persons incidentally acquired.

*2.1.3. Geographical scope of Section 702 FISA*

Section 702 does not contain limitations on the geographical scope of collection of foreign intelligence information.

Section 702 (h) provides that the Attorney General and the Director of National Intelligence may direct an "electronic communication service provider" to provide immediately all information, facilities or assistance necessary. This encompasses a wide range of electronic communication services and operators, including those that may have personal data pertaining to individuals in the EU in their possession:

(i) any service which provides users with the ability to send or receive wire or electronic communications (this could include e.g. email, chat and VOIP providers)[2];

(ii) any "remote computing" service, i.e. one which provides to the public computer storage or processing services by means of an electronic communications system[3];

(iii) any provider of telecommunications services (e.g. Internet service providers)[4]; and

---

1 Declassified minimization procedures (2011) used by the NSA in connection with acquisitions of foreign intelligence information pursuant to Section 702 FISA. See Section 3 (a)

2 FISA s.701 (b)(4)(B); 18 U.S.C. § 2510.

3 FISA s.701 (b) (4) (C); 18 U.S.C. § 2711.

4 FISA s.701 (b) (4) (A); 47 U.S.C. § 153.

(iv) any other communication service provider who has access to wire or electronic communications either as they are transmitted or as they are stored[1].

Declassified FISC opinions confirm that US intelligence agencies have recourse to methods of collection under Section 702 that have a wide reach, such as the PRISM collection of data from internet service providers or through the "upstream collection" of data that transits through the US[2].

The EU asked for specific clarifications on the issue of collection of or access to data not located or not exclusively located in the US; data stored or otherwise processed in the cloud; data processed by subsidiaries of US companies located in the EU; and data from Internet transmission cables outside the US. The US declined to reply on the grounds that the questions pertained to methods of intelligence collection.

### 2.2. Section 215 US Patriot Act (50 U.S.C. § 1861)

Section 215 of the USA-Patriot Act 2001 is the second legal authority for surveillance programmes that was discussed by the ad hoc EU-US working group. It permits the Federal Bureau of Investigation (FBI) to make an application for a court order requiring a business or another entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities[3]. The order is secret and may not be disclosed. However, the US Office of the Director of National Intelligence declassified and made public some documents related to Section 215, including documents revealing the legal reasoning of the FISC on Section 215.

---

1 FISA s.701 (b) (4) (D).

2 See declassified letters of 4 May 2002 from DOJ and ODNI to the Chairman of the US senate and House of Representatives' Select Committee on Intelligence, p. 3-4 of annexed document.

3 Section 215 further specifies that production of information can relate to an investigation on international terrorism or clandestine intelligence activities concerning a US person, provided that such investigation of a US person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

The US confirmed that this provision serves as the basis for a programme of intelligence collection via orders obtained by the FBI from the FISC directing certain telecommunications service providers to provide specified non-content telephony "meta-data". For that programme, the information is stored by the NSA and queried only for counter-terrorism purposes.

That programme is limited to the collection of call detail records, or telephony "meta-data" maintained by specified telecommunications service providers. These records cover information such as telephone numbers dialled and the numbers from which calls are made, as well as the date, time and duration of calls, but do not include the content of the calls, the names, address or financial information of any subscriber or customer, or any cell site location information. According to the explanations provided by the US, this means that the intelligence agencies cannot, through this programme, listen to or record telephone conversations.

The US explained that Section 215 allows for "bulk" collection of telephony meta-data maintained by the company to whom the order is addressed. The US also explained that, although the collection is broad in scope, the further processing of the meta-data acquired under this programme is limited to the purpose of investigation of international terrorism. It was stated that the bulk records may not be accessed or queried by intelligence agencies for any other purpose.

An order for data under Section 215 can concern not only the data of US persons, but also of non-US persons. Both US and EU data subjects, wherever located, fall within the scope of the telephony meta-data programme, whenever they are party to a telephone call made to, from or within the US and whose meta-data is maintained and produced by a company to whom the order is addressed.

There are limitations on the scope of Section 215 generally: when applying for an order, the FBI must specify reasonable grounds to believe that the records sought are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person, or to protect against international terrorism or clandestine intelligence activities. In addition, US persons benefit under Section 215 from a further protection unavailable to non-US persons, as Section 215 specifically excludes from its scope "investigation of a United States person […] conducted solely upon the basis of activities protected by the first amendment to the Constitution", i.e. activities protected by the freedom of religion, the freedom of speech or of the press, as well as the freedom of assembly and to petition the Government for redress for grievances.

## 2.3. Executive Order 12333

The US indicated that Executive Order 12333 serves as the basis for other surveillance programmes, the scope of which is at the discretion of the President. The US confirmed that Executive Order 12333 is the general framework on intelligence gathering inside and outside the US. Although the Executive Order requires that agencies operate under guidelines approved by the head of the agency and the Attorney General, the Order itself does not set any restriction to bulk collection of data located outside the US except to reiterate that all intelligence collection must comply with the US Constitution and applicable law. Executive Order 12333 also provides a legal basis to disseminate to foreign governments information acquired pursuant to Section 702[1].

The EU requested further information regarding the scope and functioning of Executive Order 12333 and the guidelines and supplemental procedures whose adoption is provided for under the Executive Order. The EU requested information in particular with regard to the application of Executive Order 12333 to bulk data collection, its impact on individuals in the EU and any applicable safeguards. The US explained that the part that covers signals intelligence annexed to the relevant regulation setting forth procedures under 12333 is classified, as are the supplementary procedures on data analysis, but that the focus of these procedures is on protecting information of US persons. The US indicated that the limitations on intelligence collection under Executive Order 12333 are not designed to limit the collection of personal data of non-US persons. For example, on the question whether collection of inbox displays from email accounts and/or collection of contact lists are authorised, the US representatives replied that they were not aware of a prohibition of such practices.

The US confirmed that judicial approval is not required under Executive Order 12333 and that there is no judicial oversight of its use, except in limited circumstances such as when information is used in a legal proceeding. Executive oversight is exercised under Executive Order 12333 by the Inspector-Generals of each agency, who regularly report to the heads of their agencies and to Congress on the use as well as on breaches of Executive Order 12333. The US was unable to provide any quantitative information with regard to the use or impact on EU citizens of Executive Order 12333. The US did explain, however, that the Executive Order states that intelligence agencies should give "special emphasis" to detecting and countering the threats posed by terrorism, espionage, and the proliferation of weapons of mass destruction[2].

---

[1] See Declassified minimization procedures, at p. 11.

[2] See Executive Order 12333, Part 1.1 (c).

The US further confirmed that in the US there are other legal bases for intelligence collection where the data of non-US persons may be acquired but did not go into details as to the legal authorities and procedures applicable.

## 3. COLLECTION AND FURTHER PROCESSING OF DATA

In response to questions from the EU regarding how data is collected and used under the surveillance programmes, the US stated that the collection of personal information based on Section 702 FISA and Section 215 Patriot Act is subject to a number of procedural safeguards and limitative conditions. Under both legal authorities, according to the US, privacy is protected by a multi-layered system of controls on what is collected and on the use of what is collected, and these controls are based on the nature and intrusiveness of the collection.

It appeared from the discussions that there is a significant difference in interpretation between the EU and the US of a fundamental concept relating to the processing of personal data by security agencies. For the EU, data acquisition is synonymous with data collection and is a form of processing of personal data. Data protection rights and obligations are already applicable at that stage. Any subsequent operation carried out on the data collected, such as storage or consultation by human eyes, constitutes further processing. As the US explained, under US law, the initial acquisition of personal data does not always constitute processing of personal data; data is "processed" only when it is analysed by means of human intervention. This means that while certain safeguards arise at that moment of acquisition, additional data protection safeguards arise at the time of processing.

### 3.1. Section 702 FISA

#### *3.1.1. Certification and authorization procedure*

Section 702 does not require individual judicial orders or warrants authorizing collection against each target. Instead, the FISC approves annual certifications submitted in writing by the Attorney General and the Director of National Intelligence. Both the certifications and the FISC's orders are secret, unless declassified under US law. The certifications, which are renewable, identify categories of foreign intelligence information sought to be acquired. They are therefore critical documents for a correct understanding of the scope and reach of collection pursuant to Section 702.

The EU requested, but did not receive, further information regarding how the certifications or categories of foreign intelligence purposes are defined and is therefore not in a position to assess their scope. The US explained that the specific purpose of acquisition is set out in the certification, but was not in a position to provide members of the Group with examples because the certifications are classified. The FISC has jurisdiction to review certifications as well as targeting and minimization procedures. It reviews Section 702 certification to ensure that they contain all required elements and targeting and minimization procedures to ensure that they are consistent with FISA and the Fourth Amendment to the US Constitution. The certification submitted to FISC by the Attorney General and the Director of National Intelligence must contain all the required elements under Section 702 (i), including an attestation that a significant purpose of the acquisition is to obtained foreign intelligence information. The FISC does not scrutinise the substance of the attestation or the need to acquire data against the purpose of the acquisition, e.g. whether it is consistent with the purpose or proportionate, and in this regard cannot substitute the determination made by the Attorney General and the Director of National Intelligence. Section 702 expressly specifies that certifications are not required to identify the specific facilities, places, premises, or property to which an acquisition of data will be directed or in which it will be conducted.

On the basis of FISC-approved certifications, data is collected by means of directives addressed to electronic communications services providers to provide any and all assistance necessary. On the question of whether data is "pushed" by the companies or "pulled" by the NSA directly from their infrastructure, the US explained that the technical modalities depend on the provider and the system they have in place; providers are supplied with a written directive, respond to it and are therefore informed of a request for data. There is no court approval or review of the acquisition of data in each specific case.

According to the US,[1] under Section 702, once communications from specific targets that are assessed to possess, or that are likely to communicate, foreign intelligence information have been acquired, the communications may be queried. This is achieved by tasking selectors that are used by the targeted individual, such as a telephone number or an email address. The US explained that there are no random searches of data collected under Section 702, but only targeted queries. Query terms include names, email addresses, telephone numbers, or keywords. When query terms are used to search databases, there is no requirement of reasonable suspicion neither of unlawful activity nor of a specific investigation. The applicable criterion is that the query terms should be reasonably believed to be used to return foreign intelligence information. The US confirmed that it is possible to perform full-text searches of communications collected, and access both content information and metadata with respect to communications collected.

The targeting decisions made by NSA in order to first acquire communications are reviewed after-the-fact by the Department of Justice and the Office of the Director of National Intelligence; other instances of oversight exist within the executive branch. There is no judicial scrutiny of the selectors tasked, e.g. their reasonableness or their use. The EU requested further information on the criteria on the basis of which selectors are defined and chosen, as well as examples of selectors, but no further clarifications were provided.

[1] See also Semi-Annual Assessment of Compliance with the Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, declassified by the Director of National Intelligence on 21 August 2013 (http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf), Annex A, p. A2.

The collection of data is subject to specific "minimisation" procedures approved by the FISC. These procedures explicitly apply to information incidentally collected of, or concerning, US persons. They primarily aim to protect the privacy rights of US persons, by limiting the collection, retention, and dissemination of incidentally acquired information to, from or about US persons. There is no obligation to minimize impact on non-US persons outside the US. However, according to the US, the minimisation procedures also benefit non-US persons, since they are aimed at limiting the collection to data reasonably relevant to a foreign intelligence purpose[1]. An example provided by the US in Section 4 of the Minimisation Procedures, which contains attorney-client protections for anyone under indictment in the United States, regardless of citizenship status.

The collection of data is also subject to specific "targeting" procedures that are approved by the FISC. These "targeting" procedures primarily aim to protect the privacy rights of US persons, by ensuring that, in principle, only non-US persons located abroad are targeted. However, the US refers to the fact that the targeting procedures contain factors for the purpose of assessing whether a target possesses and/or is likely to communicate foreign intelligence information[2].

The US did not clarify whether and how other elements of the minimisation and targeting procedures apply in practice to non-US persons, and did not state which rules apply in practice to the collection or processing of non-US personal data when it is not necessary or relevant to foreign intelligence. For example, the EU asked whether information that is not relevant but incidentally acquired by the US is deleted and whether there are guidelines to this end. The US was unable to provide a reply covering all possible scenarios and stated that the retention period would depend on the applicable legal basis and certification approved by FISC.

Finally, the FISC review does not include review of potential measures to protect the personal information of non-US persons outside the US.

---

1 Ibid, at p. 4, Section 3 (b) (4); but see also the declassified November 2011 FISC Opinion which found that measures previously proposed by the government to comply with this requirement had been found to be unsatisfactory in relation to "upstream" collection and processing; and that new measures were only found to be satisfactory for the protection of US persons.

2 See declassified NSA targeting procedures, p 4.

*3.1.2. Quantitative indicators*

In order to assess the reach of the surveillance programmes under Section 702 and in particular their impact on individuals in the EU, the EU side requested figures, e.g. how many certifications and selectors are currently used, how many of them concern individuals in the EU, or regarding the storage capacities of the surveillance programmes. The US did not discuss the specific number of certification or selectors. Additionally, the US was unable to quantify the number of individuals in the EU affected by the programmes.

The US confirmed that 1.6% of all global internet traffic is "acquired" and 0.025% of it is selected for review; hence 0.0004% of all global internet traffic is looked at by NSA analysts. The vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports[1]. Communications data makes up a very small part of global internet traffic. The US did not confirm whether these figures included "upstream" data collection.

*3.1.3. Retention Periods*

The US side explained that "unreviewed data" collected under Section 702 is generally retained for five years, although data collected via upstream collection is retained for two years. The minimisation procedures only state these time limits in relation to US-persons data[2]. However, the US explained that these retention periods apply to all unreviewed data, so they apply to both US and non-US person information.

---

1 See Cisco Visual Networking Index, 2012 (available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf)

2 See Declassified minimisation procedures, at p.11, Section 7; and the declassified November 2011 FISC Opinion, at page 13-14: "The two-year period gives NSA substantial time to review its upstream acquisitions for foreign intelligence information but ensures that non-target information that is subject to protection under FISA or the Fourth Amendment [i.e. information pertaining to US persons] is not retained any longer than is reasonably necessary... the Court concludes that the amended NSA minimization procedures, as NSA is applying them to ["upstream collection" of Internet transactions containing multiple communications], are "reasonably designed ... to minimize the ... retention[] ... of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

If the data is deemed to be of foreign intelligence interest, there is no limitation on the length of retention. The US did not specify the retention period of data collected under Executive Order 12333.

The EU asked what happens to "non-responsive" information (i.e. data collected that does not respond to query on the basis of a query term). The US responded that it is not "collecting" non-responsive information. According to the US, information that is not reviewed pursuant to a query made to that database normally will "age off of the system". It remains unclear whether and when such data is deleted.

### *3.1.4. Onward transfers and sharing of information*

The US indicated that the collected data are stored in a secure database with limited access for authorised staff only. The US however also confirmed that in case data collected under Section 702 reveal indications of criminal conduct, they can be transferred to or shared with other agencies outside the intelligence community, e.g. law enforcement agencies, for purposes other than foreign intelligence and with third countries. The minimisation procedures of the recipient agency are applicable. "Incidentally obtained" information (information not relevant to foreign intelligence) may also be shared if such information meets the standard under the applicable procedures.
On the use of private contractors, the US insisted that all contractors are vetted and subject to the same rules as employees.

### *3.1.5. Effectiveness and added value*

The US stated that in 54 instances, collection under Sections 702 and 215 contributed to the prevention and combating of terrorism; 25 of these involved EU Member States. The US was unable to provide figures regarding Executive Order 12333. The US confirmed that out of the total of 54 cases, 42 cases concerned plots that were foiled or disrupted and 12 cases concerned material support for terrorism cases.

*3.1.6. Transparency and remedies ex-post*

The EU asked whether people who are subject to surveillance are informed afterwards, where such surveillance turns out to be unjustified. The US stated that such a right does not exist under US law. However, if information obtained through surveillance programmes is subsequently used for the purposes of criminal proceedings, the protections available under US criminal procedural law apply.

*3.1.7. Overarching limits on strategic surveillance of data flows*

The EU asked whether surveillance of communications of people with no identified link to serious crime or matters of state security is limited, for example in terms of quantitative limits on the percentage of communications that can be subject to surveillance. The US stated that no such limits exist under US law.

**3.2. Section 215 US Patriot Act**

*3.2.1. Authorization procedure*

Under the Section 215 programme discussed herein, the FBI obtains orders from the FISC directing telecommunications service providers to provide telephony meta-data. The US explained that, generally, the application for an order from the FISC pursuant to Section 215 must specify reasonable grounds to believe that the records are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person or to protect against international terrorism or clandestine intelligence activities. Under the telephony metadata collection programme, the NSA, in turn, stores and analyses these bulk records which can be queried only for counterterrorism purposes. The US explained that the information sought must be "relevant" to an investigation and that this is understood broadly, since a piece of information that might not be relevant at the time of acquisition could subsequently prove to be relevant for an investigation. The standard applied is less stringent than "probable cause" under criminal law and permits broad collection of data in order to allow the intelligence authorities to extract relevant information.

The legal standard of relevance under Section 215 is interpreted as not requiring a separate showing that every individual record in the database is relevant to the investigation. It appears that the standard of relevance is met if the entire database is considered relevant for the purposes sought.[1] While FISC authorization is not required prior to the searching of the data by the NSA, the US stated that Court has approved the procedures governing access to the meta-data acquired and stored under the telephony meta-data programme authorised under Section 215. A small number of senior NSA officials have been authorised to determine whether the search of the database meets the applicable legal standard. Specifically, there must be a "reasonable, articulable suspicion" that an identifier (e.g. a telephone number) used to query the meta-data is associated with a specific foreign terrorist organisation. It was explained by the US that the "reasonable, articulable suspicion" standard constitutes a safeguard against the indiscriminate querying of the collected data and greatly limits the volume of data actually queried.

The US also stressed that they consider that constitutional privacy protections do not apply to the type of data collected under the telephony meta-data programme. The US referred to case-law of the US Supreme Court[2] according to which parties to telephone calls have no reasonable expectation of privacy for purposes of the Fourth Amendment regarding the telephone numbers used to make and receive calls; therefore, the collection of meta-data under Section 215 does not affect the constitutional protection of privacy of US persons under the Fourth Amendment.

*3.2.2. Quantitative indicators*

The US explained that only a very small fraction of the telephony meta-data collected and retained under the Section 215-authorised programme is further reviewed, because the vast majority of the data will never be responsive to a terrorism-related query. It was further explained that in 2012 less than 300 unique identifiers were approved as meeting the "reasonable, articulable suspicion" standard and were queried. According to the US, the same identifier can be queried more than once, can generate multiple responsive records, and can be used to obtain second and third-tier contacts of the identifier (known as "hops"). The actual number of queries can be higher than 300 because multiple queries may be performed using the same identifier. The number of persons affected by searches on the basis of these identifiers, up to third-tier contacts, remains therefore unclear.

---

1 See letter from DOJ to Representative Sensenbrenner of 16 July 2013 (http://beta.congress.gov/congressional-record/2013/7/24/senate-section/article/H5002-1)

2 U.S. Supreme Court, *Smith v. Maryland*, 442 U.S. 735 (1979):

In response to the question of the quantitative impact of the Section 215 telephony meta-data programme in the EU, for example how many EU telephone numbers calling into the US or having been called from the US have been stored under Section 215-authorised programmes, the US explained that it was not able to provide such clarifications because it does not keep this type of statistical information for either US or non-US persons.

### *3.2.3. Retention periods*

The US explained that, in principle, data collected under Section 215 is retained for five years, with the exception for data that are responsive to authorized queries. In regard to data that are responsive to authorized queries, the data may be retained pursuant to the procedures of the agency holding the information, e.g. the NSA or another agency such as the FBI with whom NSA shared the data. The US referred the Group to the "Attorney General's Guidelines for Domestic FBI Operations"[1] which apply to data that is further processed in a specific investigation. These Guidelines do not specify retention periods but provide that information obtained will be kept in accordance with a records retention plan approved by the National Archives and Records Administration. The National Archives and Records Administration's General Records Schedules do not establish specific retention periods that would be appropriate to all applications. Instead, it is provided that electronic records should be deleted or destroyed when "the agency determines they are no longer needed for administrative, legal, audit or other operational purposes".[2] It follows that the retention period for data processed in a specific investigation is determined by the agency holding the information or conducting the investigation.

---

1 Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf, p. 35.

2 Available at: http://www.archives.gov/records-mgmt/grs/grs20.html: "The records covered by several items in this schedule are authorized for erasure or deletion when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. NARA cannot establish a more specific retention that would be appropriate in all applications. Each agency should, when appropriate, determine a more specific disposition instruction, such as "Delete after X update cycles" or "Delete when X years old," for inclusion in its records disposition directives or manual. NARA approval is not needed to set retention periods for records in the GRS that are authorized for destruction when no longer needed."

*3.2.4. Onward transfers and sharing of information*

The EU asked for details with regards to sharing of data collected under Section 215 between different agencies and for different purposes. According to the US, the orders for the production of telephony meta-data, among other requirements, prohibit the sharing of the raw data and permit NSA to share with other agencies only data that are responsive to authorized queries for counterterrorism queries. In regard to the FBI's handling of data that it may receive from the NSA, the US referred to the "Attorney General's Guidelines for Domestic FBI Operations"[1]. Under these guidelines, the FBI may disseminate collected personal information to other US intelligence agencies as well as to law enforcement authorities of the executive branch (e.g. Department of Justice) for a number of reasons or on the basis of other statutes and legal authorities[2].

## 4. OVERSIGHT AND REDRESS MECHANISMS

The US explained that activities authorised by Section 702 FISA and Section 215 Patriot Act are subject to oversight by the executive, legislative and judicial branches.

The oversight regime and the balance between the roles of each of the branches in overseeing the surveillance programmes differ according to the legal basis of collection. For instance, because judicial oversight is limited in relation to Section 702 and collection under Executive Order 12333 is not subject to judicial oversight, a greater role is played by the executive branch in these cases. Oversight regarding whether collection on a foreign target is in keeping with Section 702 would appear to take place largely with the Department of Justice and the Office of the Director of National Intelligence as the responsible departments of the executive branch.

---

1 Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf.

2 Attorney General's Guidelines for Domestic FBI Operations, p. 35-36, provide that "[t]he FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements".

### 4.1. Executive oversight

Executive Branch oversight plays a role both prior to the collection of intelligence and following the collection, with regard to the processing of the intelligence. The National Security Division of the Department of Justice oversees the implementation of its decisions on behalf of the US intelligence community. These attorneys, together with personnel from the Office of the Director of National Intelligence, review each tasking under FISA 702 (checking justification for a valid foreign intelligence purpose; addressing over-collection issues, ensuring that incidents are reported to the FISC) and the request for production under Section 215 Patriot Act. The Department of Justice and the Office of the Director of National Intelligence also submit reports to Congress on a twice-yearly basis and participates in regular briefings to the intelligence committees of both the House of Representatives and the Senate to discuss FISA-related matters.

Once the data is collected, a number of executive oversight mechanisms and reporting procedures apply. There are internal audits and oversight controls (e.g. the NSA employs more than 300 personnel who support compliance efforts). Each of the 17 agencies that form the intelligence community, including the Office of the Director of National Intelligence has a General Counsel and an Inspector General. The independence of certain Inspectors General is protected by a statute and who can review the operation of the programmes, compel the production of documents, carry out on-site inspections and address Congress when needed. Regular reporting is done by the executive branch and submitted to the FISC and Congress.

As an example, the NSA Inspector-General in a letter of September 2013 to Congress referred to twelve compliance incidents related to surveillance under Executive Order 12333.In this context, the US drew the Group's attention to the fact that since 1 January 2003 nine individuals have been investigated in relation to the acquisition of data related to non-US persons for personal interests. The US explained that these employees either retired, resigned or were disciplined.

There are also layers of external oversight within the Executive Branch by the Department of Justice, the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board.

The Director of National Intelligence plays an important role in the definition of the priorities which the intelligence agencies must comply with. The Director of National Intelligence also has a Civil Liberties Protection Officer who reports directly to the Director.

The Privacy and Civil Liberties Oversight Board was established after 9/11. It is comprised of four part-time members and a full-time chairman. It has a mandate to review the action of the executive branch in matters of counterterrorism and to ensure that civil liberties are properly balanced. It has investigation powers, including the ability to access classified information.

While the US side provided a detailed description of the oversight architecture,[1] the US did not provide qualitative information on the depth and intensity of oversight or answers to all questions about how such mechanisms apply to non-US persons.

### 4.2. Congressional oversight

Congressional oversight of intelligence activities is conducted through the Intelligence Committee and the Judiciary Committee of both Senate and the House, which employ approximately 30 to 40 staff. The US emphasised that both Committees are briefed on a regular basis, including on significant FISC opinions authorising intelligence collection programmes, and that there was specific re-authorisation of the applicable laws by Congress, including the bulk collection under Section 215 Patriot Act[2].

### 4.3. Judicial oversight: FISC role and limitations

The FISC, comprised of eleven Federal judges, oversees intelligence activities that take place on the basis of Section 702 FISA and Section 215 Patriot Act. Its proceedings are *in camera* and its orders and opinions are classified, unless they are declassified. The FISC is presented with government requests for surveillance in the form of authorisations for collection or certifications, which can be approved, sent back for improvement, e.g. to be modified or narrowed down, or refused. The number of formal refusals is very small. The US explained that the reason for this is the amount of scrutiny of these requests by different layers of administrative control before reaching the FISC, as well as the iterative process between the FISC and the administration prior to a FISC decision. According to the US, FISC has estimated that at times approximately 25% of applications submitted are returned for supplementation or modification.

---

1 See Semi-Annual Assessment of Compliance.

2 In addition, the Congressional committees are provided with information from the FISC regarding its procedures and working methods; see, for example, the letters of FISA Court Presiding Judge Reggie Walton to Senator Leahy of 29 July 2013 and 11 October 2013.

What exactly is subject to judicial oversight depends on the legal basis of collection. Under Section 215, the Court is asked to approve collection in the form of an order to a specified company for production of records. Under Section 702, it is the Attorney General and the Director of National Intelligence that authorise collection, and the Court's role consists of confirmation that the certifications submitted contain all the elements required and that the procedures are consistent with the statute. There is no judicial oversight of programmes conducted under Executive Order 12333.

The limited information available to the Working Group did not allow it to assess the scope and depth of oversight regarding the impact on individuals in the EU. As the limitations on collection and processing apply primarily to US persons as required by the US Constitution, it appears that judicial oversight is limited as far as the collection and further processing of the personal data of non-US persons are concerned.

Under Section 702, the FISC does not approve government-issued directives addressed to companies to assist the government in data collection, but the companies can nevertheless bring a challenge to a directive in the FISC. A decision of the FISC to modify, set aside or enforce a directive can be appealed before the FISA Court of Review. Companies may contest directives on grounds of procedure or practical effects (e.g. disproportionate burden or departure from previous orders). It is not possible for a company to mount a challenge on the substance as the reasoning of the request is not provided.

FISC proceedings are non-adversarial and there is no representation before the Court of the interests of the data subject during the consideration of an application for an order. In addition, the US Supreme Court has established that individuals or organisations do not have standing to bring a lawsuit under Section 702, because they cannot know whether they have been subject to surveillance or not[1]. This reasoning would apply to both US and EU data subjects. In light of the above, it appears that individuals have no avenues for judicial redress under Section 702 of FISA.

[1] *Clapper v Amnesty International*, Judgment of 26 February 2013, 568 U. S. (2013)

## 5. SUMMARY OF MAIN FINDINGS

(1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702.

(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:

i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if *necessary* to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it *relates* to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.

ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.

iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

(3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).

(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333.

(5) Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.

(6) Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 and Section 702. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under Section 702. The FISC operates *ex parte* and *in camera*. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch.

Annexes: Letters of Vice-President Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship and Commissioner Cecilia Malmström, Commissioner for Home Affairs, to US counterparts

Ref. Ares(2013)1935546 - 10/06/2013

European Commission

**Viviane REDING**
Vice-President of the European Commission
Justice, Fundamental Rights and Citizenship

Rue de la Loi, 200
B-1049 Brussels
T. +32 2 298 16 00

*Brussels, 10 June 2013*

*Dear Attorney General,*

*I have serious concerns about recent media reports that United States authorities are accessing and processing, on a large scale, the data of European Union citizens using major US online service providers. Programmes such as PRISM and the laws on the basis of which such programmes are authorised could have grave adverse consequences for the fundamental rights of EU citizens.*

*The respect for fundamental rights and the rule of law are the foundations of the EU-US relationship. This common understanding has been, and must remain, the basis of cooperation between us in the area of Justice.*

*This is why, at the Ministerial of June 2012, you and I reiterated our joint commitment to providing citizens of the EU and of the US with a high level of privacy protection. On my request, we also discussed the need for judicial remedies to be available to EU citizens when their data is processed in the US for law enforcement purposes.*

*It is in this spirit that I raised with you already last June the issue of the scope of US legislation such as the Patriot Act. It can lead to European companies being required to transfer data to the US in breach of EU and national law. I argued that the EU and the US have already agreed formal channels of cooperation, notably a Mutual Legal Assistance Agreement, for the exchange of data for the prevention and investigation of criminal activities. I must underline that these formal channels should be used to the greatest possible extent, while direct access of US law enforcement authorities to the data of EU citizens on servers of US companies should be excluded unless in clearly defined, exceptional and judicially reviewable situations.*

*Mr Eric H. Holder, Jr.*
*Attorney General of the United States Department of Justice*
*950 Pennsylvania Avenue, NW*
*Washington, DC 20530-0001*
*United States of America*

[redacted]

*Trust that the rule of law will be respected is also essential to the stability and growth of the digital economy, including transatlantic business. It is of paramount importance for individuals and companies alike. In this context, programmes such as PRISM can undermine the trust of EU citizens and companies in the Safe Harbour scheme which is currently under review in the EU legislative process.*

*Against this backdrop, I would request that you provide me with explanations and clarifications on the PRISM programme, other US programmes involving data collection and search, and laws under which such programmes may be authorised.*

*In particular:*

1. *Are PRISM, similar programmes and laws under which such programmes may be authorised, aimed only at the data of citizens and residents of the United States, or also – or even primarily – at non-US nationals, including EU citizens?*

2. *(a) Is access to, collection of or other processing of data on the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, limited to specific and individual cases?*

   *(b) If so, what are the criteria that are applied?*

3. *On the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, is the data of individuals accessed, collected or processed in bulk (or on a very wide scale, without justification relating to specific individual cases), either regularly or occasionally?*

4. *(a) What is the scope of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised? Is the scope restricted to national security or foreign intelligence, or is the scope broader?*

   *(b) How are concepts such as national security or foreign intelligence defined?*

5. *What avenues, judicial or administrative, are available to companies in the US or the EU to challenge access to, collection of and processing of data under PRISM, similar programmes and laws under which such programmes may be authorised?*

6. *(a) What avenues, judicial or administrative, are available to EU citizens to be informed of whether they are affected by PRISM, similar programmes and laws under which such programmes may be authorised?*

   *(b) How do these compare to the avenues available to US citizens and residents?*

7. *(a) What avenues are available, judicial or administrative, to EU citizens or companies to challenge access to, collection of and processing of their personal data under PRISM, similar programmes and laws under which such programmes may be authorised?*

   *(b) How do these compare to the avenues available to US citizens and residents?*

*Given the gravity of the situation and the serious concerns expressed in public opinion on this side of the Atlantic, you will understand that I will expect swift and concrete answers to these questions on Friday 14 June, when we meet at the EU-US Justice Ministerial. As you know, the European Commission is accountable before the European Parliament, which is likely to assess the overall trans-Atlantic relationship also in the light of your responses.*

*Yours sincerely,*

ARES (2013) 2309322

**VIVIANE REDING**
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

**CECILIA MALMSTRÖM**
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

*Brussels, 19 June 2013*

*Dear Secretary,*

*On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.*

*At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.*

*In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.*

*We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.*

*We look forward to your reply.*

*Yours sincerely,*

*Viviane Reding*

*Cecilia Malmström*

*Secretary Janet Napolitano*
*Department of Homeland Security*
*U.S. Department of Homeland Security*
*Washington, D.C. 20528*
*United States of America*

*European Commission – rue de la Loi 200, B-1049 Brussels*
*eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu*

ARES (2013) 2309328

**VIVIANE REDING**
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

**CECILIA MALMSTRÖM**
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

*Brussels, 19 June 2013*

*Dear Attorney General,*

*On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.*

*At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.*

*In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.*

*We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.*

*We look forward to your reply.*

*Yours sincerely,*

*Viviane Reding* *Cecilia Malmström*

*Mr Eric H. Holder, Jr.*
*Attorney General of the United States Department of Justice*
*950 Pennsylvania Avenue, NW*
*Washington, DC 20530-0001*
*United States of America*

*European Commission – rue de la Loi 200, B-1049 Brussels*
*eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu*