Tampereen yliopisto

Pia Rautiainen

HENKILÖTIETOJEN SIIRTO EU:STA YHDYSVALTOIHIN JA REKISTERINPITÄJÄN LISÄSUOJATOIMENPITEET

Johtamisen ja talouden tiedekunta

Pro Gradu -tutkielma

Maaliskuu 2021

TIIVISTELMÄ

Pia Rautiainen: Henkilötietojen siirto EU:sta Yhdysvaltoihin ja rekisterinpitäjän lisäsuojatoimenpiteet
Pro gradu -tutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma
Kevät 2021

Henkilötietojen ja yksityisyyden suojilla on vahva perusoikeusasema EU:ssa, joiden merkitys on kasvanut globaalin digitaalitalouden kehityksen myötä entisestään. Yritykset siirtävät osana päivittäisiä ja välttämättömiä liiketoimintojaan suuria määriä henkilötietoja EU-alueen ulkopuolelle, jolloin henkilötietoja on suojattava myös kolmansissa maissa.

Unionin tasoisen tietojen suojan ulottaminen Yhdysvaltoihin on ollut erityisen haastavaa, sillä Yhdysvalloissa rekisteröidyn yksityisyydelle ei anneta samanlaista säädösperusteista suojaa kuin EU:ssa. EU:n ja Yhdysvaltojen välillä onkin jo jonkin aikaa pyritty löytämään ratkaisuja, joiden avulla yritykset voisivat siirtää tietoja Yhdysvaltoihin EU-standardien mukaisesti.

EUT mitätöi vuonna 2020 jo toisen tiedonsiirtosopimusjärjestelyn EU:n ja Yhdysvaltojen välillä, sillä kuten edeltäjänsä, tämäkään sopimus ei taannut riittävää suojaa EU-kansalaisia koskeville henkilötiedoille Yhdysvalloissa. Viimeisimmän mitätöintipäätöksensä yhteydessä EUT arvioi eri tiedonsiirtomenetelmistä nimenomaan vakiolausekkeiden riittävyyttä tietojen ja yksityisyyden suojan takaajana. EUT päätyi siihen, etteivät vakiolausekkeet automaattisesti takaa riittävää suojaa Yhdysvaltoihin siirretyille henkilötiedoille, sillä ne eivät sido Yhdysvaltain tiedusteluviranomaisia. Jatkossa yritysten on arvioitava, vaatiiko tiedonsiirto vakiolausekkeiden lisäksi lisäsuojatoimenpiteitä, jotta unionin tasoinen suoja voidaan varmistaa Yhdysvaltoihin siirretyille henkilötiedoille.

Tutkielmassa tarkastellaan vakiolausekkeita käyttävien rekisterinpitäjien lisäsuojatoimenpiteitä sekä arvioidaan niiden riittävyyttä henkilötietojen ja yksityisyyden suojan toteutumisen suhteen Yhdysvalloissa.

Avainsanat: henkilötietojen suoja, yksityisyyden suoja, henkilötietojen siirto, vakiolausekkeet, lisäsuojatoimenpiteet

Sisällysluettelo

Lähteet

Kirjallisuus

Aalto-Setälä, Minna & Viitaila, Mikko. 2018. Tietosuojaopas yrityksille. Tietosuoja pähkinänkuoressa. Helsinki: Keskuskauppakamari.

Alderman, Ellen & Kennedy, Caroline. (1995). The right to privacy. New York.

Atallah, Max. (2020). Henkilötietojen siirtäminen kolmansiin maihin post Schrems II – Uudet suositukset. 19.11.2020.

Blume, Peter. (2002). Protection of Informational Privacy. Copenhagen.

Brownsword, Roger. (2009). Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. Springer

De Hert, P. – Gutwirth, Serge: Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Teoksessa S. Gutwirth et al. (toim.), Reinventing Data Protection? Springer Science+Business Media B.V. 2009, 3–44.

González Fuster, Gloria & Gutwirth, Serge. (2013). Opening up personal data protection: A conceptual controversy. The computer law and security report, 2013–10, Vol.29 (5), 531–539. Elsevier.

Hanninen, Minna, Laine, Elli, Rantala, Kati & Rusi, Mari. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

Himma, Kenneth Einar. (2007). Privacy Versus Security: Why Privacy is Not an Absolute Value or Right. San Diego Law Review, Vol. 44, s. 857–920.

Husa, Jaakko, Mutanen, Anu Kaarina & Pohjolainen, Teuvo. (2008). Kirjoitetaan juridiikkaa: ohjeita oikeustieteellisten kirjallisten töiden laatijoille. Helsinki. Talentum.

Hirvonen, Ari. (2011). Mitkä metodit? Opas oikeustieteen metodologiaan. hirvonen_mitka_metodit.pdf (helsinki.fi)

Koillinen, Mikael. (2013). Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2. Edilex.

Kulk, Stefan & Zuiderveen Borgesius, Frederik. (2014). Google Spain v. González: Did the Court Forget about Freedom of Expression? European Journal of Risk Regulation, Is. 3, s. 389–398.

Li, Lily. (2018). US Privacy Laws in a Global Context: Predictions for the Next Year. Computer and Internet Lawyer; Frederick Vol. 35, Iss. 9, (Sep 2018), s. 39–42.

Lynskey, Orla. (2014). Deconstructing Data Protection: The Added-Value of a Right to Data Preotection in the EU Legal Order. International and Comparative Law Quarterly, Vol. 63.

Lynskey, Orla. (2015). The Foundations of EU Data Protection Law. Oxford.

Neuvonen, Riku. (2014). Yksityisyyden suoja Suomessa. Helsinki. Kauppakamari.

Rickless, Samuel. (2008). The Right to Privacy Unveiled.

Scheinin Martin. (1991). Ihmisoikeudet Suomen oikeudessa. Jyväskylä.

Saarenpää, Ahti. (2016a). Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan. Lapin yliopisto. Oikeusinformatiikan instituutin kotisivut. Artikkelit ja julkaisut. Artikkelin kirjoitusaikaa ei saatavilla. Saatavilla internetissä: https://www.ulapland.fi/loader.aspx?id=35185384-e21d-406b-96cc-1abe9705623d (viimeksi katsottu 22.10.2020)

Sharma, Sanjay, & Menon, Pranav. 2020. Data privacy and GDPR handbook. John Wiley & Sons Inc..

Sloan, Robert & Richard Warner, Richard. 2013. Beyond Notice and Choice: Privacy, Norms, and Consent. Article in SSRN Electronic Journal March 2013. DOI: 10.2139/ssrn.223909

Smith, W. Zachary. (2014). Privacy and security post-Snowden: surveillance law and policy in the United States and India.

Twining, William. (2009). General Jurisprudence. Understanding Law from a Global Perspective. Cambridge.

Tzanou, Maria. (2011). The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement. Doctoral Thesis, EUI. Firenze 2009.

Vanto, Jarno J. (2011). Henkilötietolaki käytännössä. WSOYpro Oy.

Viljanen, Veli-Pekka. (2001). Perusoikeuksien rajoitusedellytykset. Helsinki: WSOY.

Wright, David & De Hert, Paul. (2012). Part of the Law, Governance and Technology Series book series (LGTS, volume 6). Springer Science+Business Media B.V.

Muut lähteet

Aarnio, Reijo. (2020). Valvontako petti. Tietosuojavaltuutetun toimisto. 30.10.2020.

BusinessEurope, European Roundtable for Industry, et al, Schrems II Impact Survey Report. Saatavilla osoitteessa:Schrems II - Impact survey report | BusinessEurope (viimeksi katsottu 7.2.2020)

COM. (2017). 10 Ehdotus. Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). COM (2017) 10 final. 10.1.2017.

Coos, Andrada. (2018). EU vs US: What Are the Differences Between Their Data Privacy Laws? Saatavilla osoitteessa: https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ (viimeksi katsottu 17.11.2020)

Euroopan komissio. Opas EU:n ja Yhdysvaltojen Privacy Shield -järjestelyyn. file:///C:/Users/aprau/Downloads/eu-us_privacy_shield_guide_fipdf%20(3).pdf (viimeksi katsottu 14.9.2020)

Euroopan tietosuojaneuvosto. (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Saatavilla osoitteessa: edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)Viimeksi katsottu. 31.1.2021.

Euroopan tietosuojaneuvosto. (2020). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. Saatavilla osoitteessa: Recommendations 02/2020 on the

European Essential Guarantees for surveillance measures | European Data Protection Board (europa.eu)Viimeksi katsottu. 31.1.2021.

Euroopan tietosuojaneuvosto. (2020). Euroopan tietosuojaneuvoston 42. täysistunto: Kahden uuden vakiolausekeluonnoksen esittely ja Euroopan tietosuojaneuvoston sähköisen viestinnän tietosuoja-asetusta koskevan lausunnon hyväksyminen. Saatavilla osoitteessa: https://edpb.europa.eu/news/news/2020/european-data-protection-board-42nd-plenary-session-presentation-two-new-sets-sccs_fi Viimeksi katsottu 21.12.2020.

Euroopan tietosuojaneuvosto. (2020). Euroopan tietosuojaneuvoston 41. täysistunto: Euroopan tietosuojaneuvosto antaa suosituksia täydentävistä suojatoimista Schrems II -tuomion jälkeen. Saatavilla osoitteessa: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_fi. Viimeksi katsottu: 25.12.2020.

Euroopan tietosuojaneuvosto. (2020). Euroopan tietosuojaneuvoston 37. täysistunto: Rekisterinpitäjiä ja henkilötietojen käsittelijöitä koskevat ohjeet, ohjeet käyttäjien kohdentamisesta sosiaalisen median palveluissa, Euroopan unionin tuomioistuimen Schrems II -tuomion jälkeen tehtyjä valituksia. Saatavilla osoitteessa: https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_fi. Viimeksi katsottu 21.12.2020.

Euroopan Unionin neuvosto 6339/18. Sähköisen todistusaineiston parempi saatavuus yli rajojen. 26.2.2018 Saatavilla osoitteessa: https://data.consilium.europa.eu/doc/document/ST-6339-2018-INIT/fi/pdf. Viimeksi katsottu 21.12.2020.

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 35/2017.

Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act). (2020).

Fondia. (2020). Tärkeitä muutoksia liittyen henkilötietojen siirtämiseen USA:han. https://fondia.com/fi/blogsandnews/tarkeita-muutoksia-liittyen-henkilotietojen-siirtamiseen (viimeksi katsottu 16.10.2020)

Gray, Stacey. (2020). California´s Prop 24, the ”California Privacy Rights Act,” passed. Whats´s next? Viimeksi katsottu 14.11.2020.

Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta 309/1993 vp.

Hallituksen esitys Eduskunnalle sosiaaliturva- ja vakuutuslainsäädännön muuttamiseksi EU:n yleisen tietosuoja-asetuksen johdosta HE 87/2019 vp.

Henkilötietojen siirto kahden rekisterinpitäjän välillä 2001/497/EC

Henkilötietojen siirto kahden rekisterinpitäjän välillä 2004/915/EC

Henkilötietojen siirto rekisterinpitäjän ja henkilötietojen käsittelijän välillä 2010/87/EU

Hill, Kashmir (2012). Max Schrems: The Austrian Thorn In Facebook's Side. 7.2.2012. Forbes. Saatavilla osoitteessa: Max Schrems: The Austrian Thorn In Facebook's Side (forbes.com) Viimeksi katsottu 14.2.2021.

Ihmisoikeuskeskus 2018. https://1586428.168.directo.fi/@Bin/1c7e2a9c2eacb576b92947e865d23cab/1603883297/application/pdf/6325135/Ihmisoikeussanasto_Ihmisoikeuskeskus_julkaistu%202018.pdf (Viimeksi katsottu 28.10.2020)

Junttila, Harri. (2020). Kalifornia katsoi Eurooppaa – ja taisi lähteä perään. Tekniikka ja Talous. 36. 6.11.2020.

Julkisasiamiehen ratkaisuehdotus asiassa C-311/18. 2019, nro. 165/19. Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems.

Euroopan unionin lehdistötiedote nro 91/20. (2020). Unionin tuomioistuin toteaa, että EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä annettu päätös 2016/1250 on pätemätön. Saatavilla osoitteessa: Unionin tuomioistuin toteaa, että EU:n ja Yhdysvaltojen välisen Privacy Shield järjestelyn tarjoaman tietosuojan tason riittävyydestä annettu päätös 2016/1250 on pätemätön (europa.eu) Viimeksi katsottu: 15.2.2021.

Leuan, Jolly. (2017). Data protection in the United States: overview. Thomson Reuters. Practical Law.

Lindfors, Heidi. (2004). Empiirinen tutkimus oikeustieteessä. Oikeuspoliittisen tutkimuslaitoksen tiedonantoja. 64. Helsinki.

Ortamo, Simo. (2019). Kolmekymppinen itävaltalaisjuristi on piikki Facebookin lihassa – tiistaina alkava oikeudenkäynti voi myllätä tuhansien yhtiöiden bisneksen. 9.7.2019. Yle. Saatavilla osoitteessa: Kolmekymppinen itävaltalaisjuristi on piikki Facebookin lihassa – tiistaina alkava oikeudenkäynti voi myllätä tuhansien yhtiöiden bisneksen | Yle Uutiset | yle.fi Viimeksi katsottu. 14.2.2021.

Perustuslakivaliokunnan mietintö 25/1994 vp. hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta.

Punke, Michael. (2019). Tebatti: Cloud Act ei avaa viranomaisille vapaata pääsyä pilvipalveluihin. 10.6.2019. Talouselämä. Saatavilla osoitteessa: https://www.talouselama.fi/uutiset/tebatti-cloud-act-ei-avaa-viranomaisille-vapaata-paasya-pilvipalveluihin/f9fee4c3-57d0-4ac8-b10d-b000be5a415c. Viimeksi katsottu 21.12.2020.

Schechner, Sam & Glazer, Emily. (2020). The Wall Street Journal. Ireland to Order Facebook to Stop Sending User Data to U.S.. https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980 Viimeksi katsottu 17.9.2020.

Sajari, Petri. (2015). Henkilötietojen siirto Yhdysvaltoihin voi olla rikos. Helsingin Sanomat. 8.10.2015.

Simola, Anna-Eliina. (2018). EU:n tietosuojalainsäädännön vaikutus kolmansissa maissa. Helsingin yliopisto.

Tietosuojaneuvosto. (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Tietosuojavaltuutetun toimisto. 2014. Safe Harbor tiensä päässä? 1.12.2014. Saatavilla osoitteessa: Safe Harbor tiensä päässä? - Tietosuojavaltuutetun toimisto Viimeksi katsottu 9.2.2021.

Tietosuojavaltuutetun toimisto. Mikä on henkilötieto? https://tietosuoja.fi/mika-on-henkilotieto (viimeksi katsottu 21.10.2020)

Tietosuojavaltuutetun toimisto. Pseudonymisoidut ja anonymisoidut tiedot. Saatavilla osoitteessa: https://tietosuoja.fi/pseudonymisointi-anonymisointi Viimeksi katsottu: 22.12.2020.

Tietosuojavaltuutetun toimisto (2020). EU-tuomioistuin kumosi päätöksen Privacy Shieldin tarjoaman tietosuojan riittävyydestä. Saatavilla osoitteessa: https://tietosuoja.fi/-/eu-tuomioistuin-kumosi-paatoksen-privacy-shieldin-tarjoaman-tietosuojan-riittavyydesta Viimeksi katsottu 17.9.2020.

Tietosuojavaltuutetun toimisto. Komission hyväksymät vakiolausekkeet. Saatavilla osoitteessa: https://tietosuoja.fi/komission-hyvaksymat-vakiolausekkeet. Viimeksi katsottu 21.12.2020.

Tietosuojavaltuutetun toimisto. Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle. Saatavilla osoitteessa: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle. Viimeksi katsottu 21.12.2020.

Tietosuojavaltuutetun toimisto. Henkilötietojen käsittely. Saatavilla osoitteessa: https://tietosuoja.fi/henkilotietojen-kasittely. Viimeksi katsottu 18.12.2020.

Tietosuojavaltuutetun toimisto. 2020. Tietojen siirrot kolmansiin maihin: suosituksia siirtovälineitä täydentävistä suojatoimista ja luonnokset komission uusista vakiolausekkeista. Saatavilla osoitteessa: https://tietosuoja.fi/-/tietojen-siirrot-kolmansiin-maihin-suosituksia-siirtovalineita-taydentavista-suojatoimista-ja-luonnokset-komission-uusista-vakiolausekkeista. Viimeksi katsottu 18.12.2020.

Tietosuojavaltuutetun toimisto. Euroopan tietosuojaneuvoston ohjeita. Saatavilla osoitteessa: Euroopan tietosuojaneuvoston ohjeet - Tietosuojavaltuutetun toimisto. Viimeksi katsottu 25.2.2021.

Turunen, Turkka. 2019. Tebatti: Yhdysvaltojen tietosuojalaki voi tuottaa vakavaa päänvaivaa suomalaisyrityksille. Talouselämä 27.5.2019. Saatavilla osoitteessa: https://www.talouselama.fi/uutiset/tebatti-yhdysvaltojen-tietosuojalaki-voi-tuottaa-vakavaa-paanvaivaa-suomalaisyrityksille-aikapommi-tikittaa-en-luottaisi-sokeasti-yhdenkaan-suurvallan-viranomaisten-vilpittomyyteen/415c627d-3cce-4af0-881e-e21cff455f8b. Viimeksi katsottu 21.12.2020.

Palaute. 2020. Vakiosopimuslausekkeet henkilötietojen siirtämisestä EU:n ulkopuolisiin maihin (täytäntöönpanosäädös). Saatavilla osoitteessa: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries Viimeksi katsottu: 21.12.2020.

Wahlberg, Frida & Kasanen, Hannu. (2020). Irlannin tietosuojaviranomainen haastaa Facebookin henkilötietojen siirron Yhdysvaltoihin. https://www2.deloitte.com/fi/fi/pages/risk/articles/Irlannin-tietosuojaviranomainen-haastaa-Facebookin.html. Viimeksi katsottu 22.10.2020.

Yhdysvaltain kauppakamari. (2020). U.S. Chamber of Commerce Response to the European Data Protection Board's Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with EU Level of Protection of Personal Data. Saatavilla osoitteessa: us_chamber_submission_edpb_supplementary_measures_final.pdf. Viimeksi katsottu. 31.1.2021.

Your Europe, 2020. Yleinen tietosuoja-asetus (GDPR). Saatavilla osoitteessa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm. Viimeksi katsottu. 21.12.2020.

Oikeustapaukset

EIT Niemietz v. Saksa, no. 13710/88, 16.12.1992.
EIT Klass ym. v. Saksa, tuomio 6.9.1978.
EIT Kennedy v. Yhdistynyt kuningaskunta, 26839/05, 18.5.2010.
EUT C-362/14 Schrems.
EUT C-311/18 Facebook Ireland ja Schrems.
EUT S. ja Marper v. Yhdistynyt Kuningaskunta (4.12.2008, suuri jaosto).
EUT C-112/00 Eugen Schmidberger, Internationale Transporte und Planzuge v. Itävallan tasavalta, 2003.
EUT C-92/09 (9.11.2010, suuri jaosto) Volker und Markus Schecke GbR.
EUT C-70/10 Scarlet Extended.
EUT C-26/62 Van Gend en Loos.
EUT C-6/64 Costa v. ENEL.
EUT C-106/77 Simmenthal.
U.S.LEXIS 1977:42, Supreme court 429 U.S. 589 (1966), Whalen vs. Roe.

Lyhenteet

BCR	Binding Corporate Rules, yrityksiä sitovat säännöt
EEG	European Essential Guarantees, valvontatoimien olennaiset eurooppalaiset takeet
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
ENISA	Euroopan Unionin kyberturvallisuusvirasto
E.O.	Executive order, toimeenpanoasetus
ETA	Euroopan talousalue
EU	Euroopan Unioni
EUT	Euroopan Unionin tuomioistuin
FISA	Foreign Intelligence Surveillance Act, ulkomaisen tiedustelun valvontalaki
FISC	Yhdysvaltain Foreign Intelligence Surveillance Court, ulkomaisen tiedustelun valvontatuomioistuin
ISO	International Organization for Standardization
NSA	National Security Agency, kansallinen turvallisuusvirasto
PL	Perustuslaki
PPD	Presidential Policy Directive, presidentin määräys
SCC	Standard Contractual Clauses, vakiolausekkeet

1 Johdanto

1.1 Tutkimuksen taustaa

Henkilötietojen ja yksityisyyden suojilla on vahva perus- ja ihmisoikeusasema EU:ssa. Vuonna 2018 voimaan tulleella tietosuoja-asetuksella (2016/679) EU halusi vahvistaa EU-kansalaisten henkilötietojen suojaa entisestään, ja asetti henkilötietojen suojan globaaliksi tavoitteekseen. Henkilötietoja kerätään ja käytetään monenlaisten liiketoimintojen yhteydessä. Eurooppalaisia henkilötietoja voidaan kerätä esimerkiksi silloin, kun kuluttaja ostaa tavaroita tai palveluja verkossa, hyödyntää sosiaalista mediaa tai tallentaa tietojaan pilvipalveluun. Tietoja voidaan käsitellä myös rajat ylittävällä tavalla esimerkiksi silloin, kun henkilö työskentelee tytäryrityksessä, joka on sijoittautunut EU:n alueelle ja emoyhtiö, joka käsittelee työntekijöiden tietoja, on sijoittautunut Yhdysvaltoihin.[1] Globaalin digitaalitalouden vuoksi ei riitä, että henkilötiedot on suojattu vain EU-alueella, vaan kattavan suojan toteutuminen edellyttää, että tiedot on suojattu kaikkialla missä niitä käsitellään ja säilytetään[2].

EU:n korkean tietosuojavaateen toteutuminen on ollut erityisen haastavaa Yhdysvalloissa; siinä missä EU:ssa yksilön yksityisyys on perustuslaillinen oikeus, harjoitetaan Yhdysvalloissa kansallisen turvallisuuden nimissä kohdentumatonta sähköistä valvontaa, jonka kohteeksi ovat joutuneet myös EU-kansalaisten henkilötiedot[3]. EU:n ja Yhdysvaltojen välillä onkin jo pidemmän aikaa pyritty löytämään ratkaisuja, joiden avulla eurooppalaisia henkilötietoja voitaisiin siirtää Yhdysvaltoihin EU-standardien mukaisesti.

Vuonna 2000 EU ja Yhdysvallat solmivat ensimmäisen tietojensiirtoa koskevan Safe Harbor -sopimusjärjestelyn, jonka tarkoitus oli mahdollistaa yritysten väliset tiedonsiirrot EU-alueelta Yhdysvaltoihin. Käytännössä järjestelmä toimi siten, että yhdysvaltalaiset yhtiöt liittyivät Safe Harboriin ja sitoutuivat noudattamaan sen ehtoja[4]. Vuoden 2011 elokuusta lähtien asianajaja ja aktivisti Maximillian Schrems teki 23 kantelua Irlannin tietosuojaviranomaiselle Facebook Irelandista liittyen hänen yksityisyyteensä ja tietosuojaansa. Lopulta yhden kantelun perusteella Irlannin ylempi piirituomioistuin High Court pyysi ennakkoratkaisua EUT:lta, sillä Schrems oli

[1] Opas EU:n ja Yhdysvaltojen Privacy Shield -järjestelyyn.
[2] Simola 2018, 2.
[3] EUT C-311/18, kohta 191.
[4] Tietosuojavaltuutetun toimisto 2014.

onnistunut tuomaan kyseisessä kantelussaan esiin Safe Harbor -sopimuksen puutteet henkilötietojen suojaamisessa. Tämän seurauksena, vuonna 2015 EUT mitätöi Safe Harborin niin sanotussa Schrems I -tuomiossaan.[5]

Vuonna 2016 EU ja Yhdysvallat solmivat uuden tiedonsiirtosopimusjärjestelyn (Privacy Shield), jonka tarkoitus oli vastata Safe Harborin jättämään haasteeseen eli taata Yhdysvaltoihin siirretyille EU-kansalaisia koskeville henkilötiedoille riittävän korkeatasoinen suoja[6]. Vuonna 2020 EUT kuitenkin päätti mitätöidä (Schrems II) Privacy Shield -sopimuksen, Schremsin osoittaessa tähänkin sopimukseen liittyvät yksityisyyshuolet. EUT katsoi Schrems II -tuomiossaan, ettei Yhdysvallat noudattaneet EU:n mukaisia tietosuojastandardeja yksityisyydensuojasta[7]. Schrems II -tapauksen vaikutukset ulottuvat kaikkiin eurooppalaisiin yrityksiin, jotka jollain tapaa siirtävät eurooppalaisia henkilötietoja Yhdysvaltoihin[8]. Ennen EUT:n mitätöintipäätöstä Privacy Shield salli henkilötietojen siirron EU:sta yhdysvaltalaiselle yritykselle, mikäli yritys noudatti henkilötietojen käsittelyssä määriteltyjä tietosuojasäännöksiä. Privacy Shield -järjestelyn ohella yritykset pystyivät hyödyntämään myös muita siirtomekanismeja, kuten esimerkiksi komission hyväksymiä vakiolausekkeita (standard contractual clauses, SCC).

Yritykset ovat käyttäneet komission hyväksymiä vakiolausekkeita merkittävästi Yhdysvaltoihin tehtyjen tietosiirtojen yhteydessä.[9] Osin tästä syystä, EUT jätti Schrems II -tuomiossaan vakiolausekkeet voimaan. Vakiolausekkeisiin sisältyy kuitenkin sama riski kuin Safe Harbor ja Privacy Shield -sopimuksiin: ne eivät takaa riittävää suojaa henkilötiedoille. EUT korosti antamassaan ratkaisussaan, että yritysten laajasti käyttämät vakiolausekkeet eivät automaattisesti itsessään takaa siirron lainmukaisuutta, vaan rekisterinpitäjän eli yritysten, on *tapauskohtaisesti* arvioitava tarvetta lisäsuojatoimenpiteille (supplementary measures) henkilötietojen asianmukaisen suojan takaamiseksi Yhdysvalloissa. Mikäli tietojen siirrossa ei voida varmistua riittävistä lisäsuojatoimenpiteistä, tulisi rekisterinpitäjän tai viimekädessä tietosuojaviranomaisen keskeyttää tai kieltää tietojen siirto.[10]

Vuoden 2020 marraskuussa, pian EUT:n päätöksen jälkeen, Euroopan tietosuojaneuvosto määritteli suositukset lisäsuojatoimenpiteitä sekä valvontatoimien olennaisista eurooppalaisista takeista.

[5] EUT C-362/14.
[6] Simola 2018, 69.
[7] Tietosuojavaltuutetun toimisto.
[8] Fondia 2020.
[9] Opas EU:n ja Yhdysvaltojen Privacy Shield -järjestelyyn.
[10] EUT C-311/18, kohta 31.

Suositusten tarkoituksena on auttaa rekisterinpitäjiä (tietojen viejä) ja henkilötietojen käsittelijöitä (tietojen tuoja) yksilöimään ja toteuttamaan asianmukaisia täydentäviä suojatoimia, jos ne ovat tarpeen sen varmistamiseksi, että siirrettävät tiedot saavat olennaisilta osin unionin tasoisen suojan Yhdysvalloissa[11]. Tietosuojaneuvoston suositukset ovat kuitenkin ohjeellisia, jolloin yhtä, kaikkien rekisterinpitäjien sovellettavissa olevaa lisäsuojatoimenpidelistaa ei ole olemassa. On siis ensisijaisesti rekisterinpitäjän vastuulla arvioida, tarvitseeko sen valittujen siirtomenetelmien lisäksi käyttää vielä täydentäviä menetelmiä.

1.2 Tutkimusaiheen rajaus, tutkimuskysymys ja menetelmät

Tutkielman aiheena on vakiolausekkeita käyttävien rekisterinpitäjien lisäsuojatoimenpiteet henkilötietojen siirrossa Yhdysvaltoihin. Tutkimuskysymys on määritelty seuraavasti:

1. Miten vakiolausekkeita ja lisäsuojatoimenpiteitä käyttävä rekisterinpitäjä voi siirtää eurooppalaisia henkilötietoja Yhdysvaltoihin, jotta se varmistaa unionin tasoisen suojan siirretyille tiedoille?

Rekisterinpitäjillä tarkoitetaan ihmistä tai organisaatiota, joka määrittelee mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään, kun taas henkilötietojen käsittelijöillä tarkoitetaan ihmistä tai organisaatiota, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.[12] Tämä tutkielma painottuu ensisijaisesti EU:ssa sijaitseviin rekisterinpitäjiin eli tietojen viejien vastuuseen siirtäessään tietoja Yhdysvalloissa sijaitsevalle henkilötietojen käsittelijälle eli tietojen tuojalle. Koska rekisterinpitäjän velvoitteet ulottuvat myös henkilötietojen käsittelijöihin, tullaan tutkielmassa huomioimaan olennaisilta osin myös henkilötietojen käsittelijät. Yleisenä rajauksena on vielä selvyyden vuoksi todettava, että tutkielmassa käsiteltävät EU-säädökset, ohjeistukset ja suositukset koskevat kaikkia kolmansia maita, jotka eivät Euroopan komission mukaan takaa riittävää unionin tasoista suojaa siirretyille henkilötiedoille. Tämä tutkielma keskittyy tarkastelemaan aihetta ainoastaan EU:n ja Yhdysvaltojen välisen suhteen kannalta. Siirtomenetelmien osalta tutkielman kohde on rajattu vakiolausekkeisiin ja lisäsuojatoimenpiteisiin ja muita tiedonsiirtomekanismeja sivutaan ainoastaan niiltä osin kuin se on tutkielman kannalta tarpeellista.

Tutkielma on oikeustieteellinen, joka kuuluu ensisijaisesti EU-oikeuden alaan, sen käsitellessä tietojen siirtoa Yhdysvaltoihin EU:n tietosuojasäännösten asettamien vaatimusten valossa.

[11] Euroopan tietosuojaneuvosto 41. täysistunto, 2020.
[12] Tietosuojavaltuutetun toimisto.

Tutkielmalla on myös vahva sopimusoikeudellinen elementti, ennen kaikkea tutkielmassa käsiteltävien vakiolausekkeiden, mutta osin myös lisäsuojatoimenpiteiden luonteen vuoksi. Yksityisyyden ja henkilötietojen suojan määrittelyjen vuoksi tutkielman lähestymistapa on alussa oikeusteoreettinen, mikä tarkoittaa oikeuden yleisten kysymysten tutkimista antaen kokonaiskuvan oikeudesta ja sen käsitteistä[13].

Tämän tutkielman tutkimusmenetelmä on oikeusdogmaattinen, jonka keskeisin tehtävä on pyrkiä selvittämään, mikä on voimassaolevan oikeuden sisältö käsiteltävänä olevassa tutkimusongelmassa eli toisin sanoen kuinka voimassaolevan oikeusjärjestyksen mukaan tulisi todellisissa käytännön tilanteissa toimia. Selvitän tutkielmassani mitä lisäsuojatoimenpiteillä tarkoitetaan ja miten ne suhteutuvat vakiolausekkeisiin. Lisäksi tarkastelen miten tietosuojaneuvoston suositukset ja keskeinen lainsäädäntö vaikuttavat rekisterinpitäjän vastuuseen silloin, kun se siirtää henkilötietoja Yhdysvaltoihin ja tavoittelee unionin tasoista suojaa siirretyille tiedoille. Tarkastelen lisäksi lainopin avulla rekisterinpitäjän vastuun määräytymistä suhteessa henkilötietojen käsittelijään ja valvontaviranomaiseen.

Lainopin toisena merkittävänä tehtävänä on voimassa olevan oikeuden systematisointi eli jäsentäminen, mikä on avuksi oleellisten säännösten etsimisessä ja kokonaiskuvan hahmottamisessa oikeudellisista järjestelyistä sekä niiden välisistä suhteista.[14] Jotta tietosuojalainsäädännön vaikutuksia rekisterinpitäjän velvoitteisiin ekstraterritoriaalisissa tiedon siirroissa voidaan arvioida kattavasti, tulee sitä koskevan lain sisältöä jäsentää. Tässä käytetään apuna EUT:n ratkaisuja, erityisesti Schrems II -tapausta.

1.3 Tutkielman rakenne ja lähdeaineisto

Hyödynnän tutkielmassani lähteinä lainsäädäntöä, EUT:n ratkaisuja, komission, julkiasiamiehen ja tietosuojaneuvoston mietintöjä ja suosituksia sekä oikeuskirjallisuutta. Erityisesti henkilötietojen siirtoa koskevien lisäsuojatoimenpiteiden osalta aineisto painottuu tietosuojaneuvoston antamiin suosituksiin ja ohjeistuksiin sekä EUT:n tietosuojalainsäädäntöä koskevaan tulkintaan.

Tutkielma koostuu viidestä pääluvusta, joista ensimmäisessä käydään läpi tutkielman taustaa, tutkimuskysymys, aiheen rajaus, tutkimusmenetelmä, lähdeaineisto sekä tutkimuksen rakenne pääpiirteittäin. Tutkielman toisessa pääluvussa käydään läpi mitä henkilötietojen ja yksityisyyden

[13] Hirvonen 2011, 27.
[14] Husa, Mutanen & Pohjolainen 2008, 19–21.

suojalla tarkoitetaan ja miten ne suhteutuvat toisiinsa. Henkilötietojen ja yksityisyyden suojan lähempi arviointi sääntelyn ohella on tärkeää, jotta lukijalle muodostuu kattava kuva näiden käsitteiden monimuotoisuudesta. Tarkastelen toisessa luvussa myös yksityisyyttä ja henkilötietojen suojaa koskevaa sääntelyä niin EU:ssa kuin Yhdysvalloissa. Johtuen kuitenkin Yhdysvaltojen yksityisyyden suojaa koskevien lakien runsaasta määrästä sekä niiden erilaisuudesta keskenään, tulen ainoastaan tarkastelemaan tutkimusaiheen kannalta keskeisimpiä lakeja. Yleisesti toisen luvun tarkoitus on tuoda kattavasti esiin EU:n ja Yhdysvaltojen erilainen oikeuskäsitys ja sääntely koskien henkilötietojen ja yksityisyyden suojaa, sillä tällä on ollut merkittävä vaikutus nykyisen tiedonsiirtoja koskevan tilanteen muodostumiseen EU:n ja Yhdysvaltojen välillä.

Kolmas pääluku keskittyy vakiolausekkeisiin eurooppalaisten henkilötietojen siirtomenetelmänä sekä eri siirtoperusteiden kuvaamiseen. Luonnollisesti osana vakiolausekkeiden tarkastelua, tulen käymään läpi EUT:n Schrems II -ratkaisua, jonka tarkoitus on hahmottaa vakiolausekkeiden riittävyyttä tiedonsiirtomekanismina. Luvun lopussa käyn vielä pääpiirteittäin läpi Euroopan komission uusia vakiolausekeluonnoksia ja niihin liittyviä haasteita rekisterinpitäjien kannalta.

Neljäs pääluku keskittyy kokonaisuudessaan tietosuojaneuvoston lisäsuojatoimenpidesuosituksiin. Luvussa käydään läpi lisäsuojatoimenpiteitä, arvioidaan lisäsuojatoimenpiteiden ja vakiolausekkeiden välistä suhdetta, lisäsuojatoimenpiteiden yritysvaikutuksia sekä lisäsuojatoimenpiteitä täydentäviä suosituksia valvontatoimien olennaisista eurooppalaisista takeista. Lopuksi tutkielman neljännessä eli viimeisessä pääluvussa teen yhteenvedon, jossa tuon tutkielmassa esitetyt merkittävät seikat yhteen ja esitän johtopäätökseni, jolla vastaan esittämääni tutkimuskysymykseen.

2 Henkilötietojen ja yksityisyyden suoja

2.1 Yksityisyys ja yksityisyyden suoja

Yksityisyydestä tuli 2010-luvulla tietourkintojen ja tietoverkkojen kehityksen ja vakoilun vuoksi yksi oikeustieteen avainsanoista[15]. Yksityisyys ja erityisesti sen suoja on muodostunut yhä tärkeämmäksi, osin ihmisten valveutuneisuuden myötä ja osin siksi, että yksityisyyden merkitys on huomioitu entistä vahvemmin myös lainsäädännöllisesti. Luomme päivittäin huomaamattamme laajoja määriä henkilökohtaista tietoa, kun käytämme erilaisia teknologiapalveluja, kuten Facebookia, Twitteriä ja Whatsappia. Maksamme tällaisten palvelujen käyttämisestä näkymätöntä hintaa, sillä jokainen palvelun käyttökerta jättää digitaalisen jäljen altistaen palveluja käyttävien tiedot sähköiselle valvonnalle.[16] Tämä herättää väistämättä huolen omasta yksityisyyden suojasta. Oikeus yksityisyyteen tulisi olla yksilön valinta, samoin kuin sen, miten, ja missä joku taho hyödyntää yksilön itseään koskevia ja vapaaehtoisesti luovuttamia henkilötietojaan[17].

Yksityisyyttä ei voi määritellä yksiselitteisesti ja tarkasti[18] sen monimuotoisuuden[19] vuoksi. Yleisellä ja laajalla tasolla suurin osa meistä ymmärtää yksityisyyden kuitenkin oikeudeksi, joka suojaa meitä ulkopuolisten tarkkailulta ja puuttumiselta yksityisiksi kokemiimme asioihin. Oikeusteoriassa yksityisyyttä voidaan tarkastella itsemääräämisoikeutemme muotoutumiseen liittyvänä suhdekäsitteenä, jossa yksilöllä tulisi lähtökohtaisesti olla oikeus suhteessa johonkin, mikä on itsemääräämisoikeuden ydin. Oikeusteoreettinen lähestymistapa yksityisyydenkäsitteeseen yksilön oikeuden lähtökohtaisuudesta ilmentää nimenomaisesti sitä, että oikeus yksityisyyteen ei ole ehdoton[20].

Yksityisyyttä ei ole määritelty Yhdysvaltain perustuslaissa, mutta perustuslain 4. lisäys (Fourth Amendment) suojaa kuitenkin kansalaisia, heidän omaisuuttaan ja kotiaan perusteettomasti tehtyjä kotietsintöjä tai takavarikkoja vastaan.[21] Vaikka yksityisyys ei esiinnykään perustuslaissa käsitteenä, on sitä koskevaa tulkintaa esitetty Yhdysvaltain korkeimman oikeuden päätöksessä Whalen vs. Roe[22]. Päätöksessään korkein oikeus katsoi, että yksilöllä on perustuslaillinen oikeus riippumattomaan päätöksentekoon sekä oikeus estää henkilökohtaisten asioiden julkistaminen. Yleisesti tätä päätöstä

[15] Neuvonen 2014, 11.
[16] Sharma, Sanjay 2020, 1.
[17] Sharma, Sanjay 2020, 8.
[18] Neuvonen 2014, 21, Rickless 2007, 773.
[19] Tzanou 2013, 23, Wright & De Hert 2012, IX ja Gonzáles Fuster – Gutwirth 2013, 537.
[20] Saarenpää 2016a, 1–2
[21] Alderman ja Kennedy 1995, 10–11.
[22] Supreme court 429 U.S. 589 (1966), Whalen vs. Roe.

on tulkittu siten, että henkilöä koskevien tietojen käyttöä voidaan rajoittaa, mikäli se vaarantaa jonkin muun Yhdysvaltain perustuslaissa suojatun oikeuden käytön[23]. Yksilön oikeus ei siis tässäkään ole ehdoton, vaan se tulee suhteuttaa toisen oikeuden käytön tosiasialliseen vaarantumiseen.

Yksityisyyden määrittelemättömyys on sen heikkous, sillä vaatimus lainsäädännön täsmällisyydestä ja selkeydestä ei voi toteutua yksityisyyden kaltaisen suhdekäsitteen kohdalla. Samalla sen määrittelemättömyys on kuitenkin sen vahvuus, sillä lainsäädäntö sopeutuu yhteiskunnan muutoksiin dynaamisesti.[24] Yksityisyyden käsitteen perustelua ei tulisi viedä liian kauas perus- ja ihmisoikeuksista, sillä tämä voi johtaa tilanteeseen, jossa yhteys oikeustieteeseen katkeaa. Yksityisyyden suojaa tulisikin tarkastella väljillä käsitteillä. Tukea tälle lähestymistavalle antavat EIT, joka on tulkinnut yksityisyyden käsitettä laajasti[25] sekä Euroopan ihmisoikeussopimus (63/1999) ja Suomen perustuslaki (731/1999), jotka molemmat turvaavat käsitteellisesti yksityiselämän suojan, mutta joihin kuuluu samalla muitakin oikeuksia. Tämän lisäksi Euroopan perusoikeuskirja (2012/C 326/02) turvaa oikeudet eri tavoin kuin EIS tai perustuslaki. Täten on perusteltua, että yksityisyyden tarkka rajaaminen ei ole tarkoituksenmukaista[26] ja kokonaisuutena arvioiden, yksityisyyden kattavaksi tarkoitettu hetkellinen määrittely on jopa erheellistä.[27]

Yksi tuoreimpia, yksityisyyden käsitteeseen kohdistuneita ”väljää” tulkintalinjaa noudattaneita, on EUT Schrems II -tuomiossaan. EUT katsoi, että yksilöä koskeviin henkilötietoihin pääsy niiden säilyttämistä tai käyttöä varten vaikuttaa Euroopan perusoikeuskirjan 7 artiklassa taattuun yksityiselämän kunnioittamista koskevaan perusoikeuteen. Tällainen tietojen käsittely kuuluu myös perusoikeuskirjan 8 artiklan henkilötietojen suojaa koskevaan soveltamisalaan, koska se merkitsee kyseisessä artiklassa tarkoitettua henkilötietojen käsittelyä, jolloin sen on ehdoitta täytettävä myös kyseisestä artiklasta juontuvat tietojen suojan vaatimukset. Lisäksi henkilötietojen siirtäminen esimerkiksi viranomaiselle, merkitsee puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin siirrettyjen tietojen myöhemmästä käytöstä riippumatta. Sama koskee henkilötietojen säilyttämistä sekä pääsyä kyseisiin tietoihin niiden käyttämiseksi viranomaisissa riippumatta siitä, ovatko kyseessä olevat yksityiset tiedot arkaluonteisia vai eivät tai onko sille, jonka tiedoista on kyse, mahdollisesti aiheutunut haittaa tietoihin puuttumisesta.[28]

[23] Smith 2014,184.
[24] Saarenpää 2016a, 1–2.
[25] Niemietz vs. Saksa, kohta 29.
[26] Neuvonen 2014 28–29
[27] Saarenpää 2016a, 1–2.
[28] EUT C-311/18, kohdat 170–171.

2.2 Henkilötiedot ja henkilötietojen suoja

Yksityisyyteen sisältyy persoonallisuuden suoja, anonymiteetti, liikkumisvapaus, oikeus olla suojassa julkisuudelta sekä yksilöä koskevien tietojen suoja eli henkilötietojen suoja[29].

Tietosuoja-asetuksen artiklan 4 kohdan 1 mukaan henkilötiedoilla tarkoitetaan:

> kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Kuten asetuksesta käy ilmi, henkilötiedon käsitettä on tulkittava laajasti[30]. Henkilötietoja ovat esimerkiksi nimi, henkilötunnus tai jokin muu tunnusomainen tekijä, jonka perusteella yksilö on mahdollista tunnistaa joko suoraan tai välillisesti esimerkiksi yhdistämällä jokin yksittäinen tieto johonkin toiseen tietoon[31]. Henkilötietojen suoja käsittää persoonallisuuden sekä itsemääräämisoikeuden, jotka pyrkivät luomaan yksilöille laajat vaikutusmahdollisuudet siihen, kuka, miten ja missä käsittelee heitä koskevia henkilötietoja[32]. Henkilötietoja tarvitaan erilaisten palvelujen tarjoamiseen, väestön hallinnointiin ja kaupankäynnin mahdollistamiseen. Samalla näiden palvelujen käyttäminen edellyttää luopumista osasta omaa yksityisyyttään, jolloin keskiöön asettuvat ne ehdot, joiden perusteella henkilötietoja saa käsitellä, luovuttaa tai yhdistää toisiin henkilötietoihin. Toisin sanoen oikeuksiin, joilla pyritään suojaamaan henkilötietojen luvatonta käyttöä.

Henkilötietojen suoja jakaantuu kahteen osa-alueeseen, henkilötietojen suojaan ja tietoturvaan. Henkilötietojen suoja määrittelee henkilötiedot ja niiden käsittelyn edellytykset, ja tietoturva puolestaan tietojen käsittelyn konkreettisen viitekehyksen.[33] Henkilötietojen suojan sekä tietoturvan vaatimukset, joita rekisterinpitäjän on noudatettava, määrittyvät tietosuojalainsäädännön artiklan 5 kohdan 1 mukaisten oikeudellisten tietosuojaperiaatteiden kautta. Periaatteet edellyttävät, että henkilötietojen käsittely on lainmukaista, rekisteröidyn kannalta läpinäkyvää, minkä lisäksi henkilötietoja saa kerätä ainoastaan tiettyä laillista tarkoitusta varten, jolloin henkilötietojen käsittelyn tarpeen on oltava myös oikeassa suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Asetus sallii kuitenkin poikkeuksen tähän siltä osin, kun henkilötietoja käsitellään yleisen edun

[29] Neuvonen 2014, 29.
[30] Vanto 2011, 22–28.
[31] Tietosuojavaltuutetun toimisto.
[32] Neuvonen 2014, 60.
[33] Neuvonen 2014, 61–64.

mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten. Poikkeuskin kuitenkin edellyttää, että asetuksen mukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi.

2.3 Henkilötietojen ja yksityisyyden suojat perus- ja ihmisoikeutena

Perusoikeuksien rajoittamisten tulee olla suhteellisuudentajuisia, vankkoja ja yhteiskunnallisen tarpeen kautta perusteltuja sekä ihmisoikeussopimusten mukaan hyväksyttäviä[34], mikä ilmentää kyseisten oikeuksien yhteiskunnallista painoarvoa. Perusoikeudet voidaan katsoa olevan eräänlaisia parannuksia Euroopan ihmisoikeussopimuksen (EIS) määrittelemästä ihmisoikeuksien vähimmäistasosta, minkä lisäksi perus- ja ihmisoikeuksilla on EIS:n määrittelemien ja EIT:n antamien ihmisoikeuksiin liittyvien tulkintojen myötä selkeä tulkintayhteys.[35] Perus- ja ihmisoikeudet turvaavat yksilön yksityisyyden suojaa, joista merkittävin on yksityiselämän suoja, joka on määritelty Suomen perustuslaissa (PL 10 §), EIS:ssa (artikla 8) sekä Euroopan perusoikeuskirjassa (art. 7).

Henkilötietojen suoja on muotoutunut EU:n perusoikeudeksi perinteistä perusoikeusdialektiikkaa rikkovasti, sillä henkilötietojen suojaa koskevat periaatteet on ensin muotoiltu aineellisessa lainsäädännössä, josta ne on myöhemmin siirretty perusoikeussopimuksen myötä perus- ja ihmisoikeustasolle. Tulkinnan painoarvo on täten perusoikeustason sijaan tietosuojaa koskevissa laeissa. Henkilötietojen suojan perusoikeusluonne tulee esiin siinä, että Euroopan unionin alueella tietosuoja-asetuksella on horisontaalisia ulottuvuuksia, mikä ilmenee yksityisen rekisterinpitäjän laissa säädettyinä velvollisuuksina tämän käsitellessä yksilöä koskevia henkilötietoja. Kyseinen suoja voi toteutua myös vertikaalisti eli suojata valtion puuttumiselta yksityisyyteen. Kun asiaa tarkastellaan Schrems II -tapauksen kannalta, on ilmeistä, että Yhdysvalloissa yksilöt kokevat puutteellista henkilötietojen suojaa. Tämä on merkittävä ero eurooppalaiseen oikeuskäsitykseen, jossa henkilötietojen suoja sekä yksityiselämän kunnioittaminen ovat perusoikeuksia. Tästä samasta perustelusta johdettuna EUT katsoi tuomiossaan, että tiedusteluviranomaisten eurooppalaisiin tietoihin pääsy ja tietojen käsittely merkitsee sekä yksityiselämän kunnioittamista että henkilötietojen suojaa (art. 8) koskeviin oikeuksiin puuttumista.[36]

[34] HE 309/1993 vp s. 29–30, PeVM 25/1994 vp, 5 ja EUT:n tuomio C-112/00, kohta 80.
[35] Neuvonen 2014, 34.
[36] Neuvonen 2014, 61 ja ks. myös luku 2.2.

Oikeus yksityisyyteen on kirjattu YK:n ihmisoikeusjulistuksen (10.12.1948) 12 artiklaan, mikä kertoo yksityisyyden yleismaailmallisesti tunnustetusta luonteesta ihmisoikeutena. Tämän lisäksi valtioiden kansalliset lait suojaavat yksityiselämää. Yleensä juuri YK:n ihmisoikeusjulistuksen koetaan olevan universaali lista arvoista ja oikeuksista, jotka ovat kaikkialla maailmassa hyväksyttyjä ja joita halutaan suojata[37]. Ihmisoikeusjulistuksen lisäksi lähes kaikki maailman valtiot ovat ratifioineet Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (8/1976) eli KP-sopimuksen, jonka 17 artiklassa oikeus yksityisyyteen on vahvistettu kansainväliseksi sopimusvelvoitteeksi. Niin Yhdysvallat kuin useat Euroopan maat jakavat täten ainakin lähtökohtaisesti samat länsimaiset arvot ja periaatteet, kun oikeus yksityisyyteen on hyväksytty ihmisoikeudeksi YK:n näkemyksen mukaisesti. Tätä lähtökohtaa tukee myös se, että Yhdysvaltojen ihmisoikeussopimus on laadittu Euroopan ihmisoikeussopimusta mallintaen[38], jolloin Yhdysvaltain sopimuksen artikla 11 sääntelee oikeutta yksityisyyteen hyvin pitkälti samoin kuin eurooppalainen vastinparinsa. Kansainvälisen oikeuden sinänsä vahva asema Yhdysvaltojen oikeusjärjestyksessä ei kuitenkaan näy ihmisoikeussopimusten noudattamisessa, sillä todellisuudessa Yhdysvallat on liittynyt ainoastaan muutamiin kansainvälisiin ihmisoikeussopimuksiin. Tosin, on huomioitava, että Yhdysvalloissa kansainvälistä ihmisoikeussääntelyä hyödynnetään valtionsisäisen perustuslain ja lainsäädännöntulkinnan apukeinona.[39]

Kansainväliset sopimukset ja ihmisoikeusjulistukset puhuvat yksilön oikeudesta yksityisyyteen, mutta henkilötietojen suojaa ei mainita. Tämä johtuu siitä, että oikeus henkilötietojen suojaan hahmotetaan kansainvälisessä ihmisoikeusajattelussa yksityisyyteen kuuluvaksi alakategoriaksi[40]. Näin ollen, vaikka ihmisoikeuksia koskevissa dokumenteissa ei ole erillisiä henkilötietojen suojaa koskevia kohtia, on henkilötietojen suoja myös ihmisoikeus. Euroopassa tätä näkemystä tukee erityisesti se, että Euroopan neuvosto on laatinut erillisen sopimuksen henkilötietojen suojasta tukemaan nimenomaisesti sen ihmisoikeusasemaa.[41] Henkilötietojen suojan nostaminen ihmisoikeusasemaa nauttivaksi oikeudeksi korostaa Yhdysvaltojen ja EU:n toisistaan eriävää oikeuskäsitystä yksityisyydestä entisestään.

[37] Twining 2009, 124.
[38] Ihmisoikeuskeskus 2018, 32.
[39] Scheinin 1991, 82.
[40] Lynskey 2014, 569–570, ks. myös kappale 2.2.
[41] Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data.

2.4 Henkilötietojen ja yksityisyyden suojien absoluuttisuus

Perusoikeuden rajoittaminen tarkoittaa perusoikeuksien soveltamisalaan kuuluvan oikeuden kaventamista tai perusoikeussäännöksen suojaamaan yksilön oikeusasemaan puuttumista julkisen vallan toimenpiteillä. Kun esimerkiksi yksilön oikeutta yksityisyyteen rajoitetaan kajoamalla henkilötietojen suojaan, yksilö ei voi käyttää perusoikeuttaan täysimääräisesti. Perusoikeudet eivät siis ole absoluuttisia eli ehdottomia, niiden painoarvosta huolimatta. Jotta voidaan puhua perusoikeusrajoituksesta ylipäätään, tarvitsee rajoituksen kohteena olevan oikeuden kuulua perusoikeussäännöksen soveltamisalaan.[42] Vaikka mikään perusoikeus ei ole absoluuttinen[43], voidaan tulkinnallisena lähtökohtana kuitenkin pitää sitä, että epäselvissä tapauksissa perusoikeuden soveltamisala tulee ymmärtää laajasti[44].

EU:n perusoikeuskirjan 52 artiklan mukaan siinä tunnustettujen oikeuksien ja vapauksien käyttämistä on mahdollista rajoittaa, mutta ainoastaan lailla ja siten, että rajoituksilla kunnioitetaan kyseisten oikeuksien ja vapauksien keskeistä sisältöä. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan määrätä vain, kun ne ovat välttämättömiä ja vastaavat tosiasiallisesti EU:n mukaisia yleisen edun tavoitteita suojella yksilöiden oikeuksia ja vapauksia. Sama toistuu, joskin kohdennetummin, tietosuoja-asetuksen johdannon kohdassa neljä. Siinä määritellyn mukaan, henkilötietojen suoja ei ole absoluuttinen, vaan sitä tulee tarkastella suhteessa sen tehtävään yhteiskunnassa, minkä lisäksi sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin, kuten EUT on oikeuskäytännössäänkin tuonut esiin[45]. Näin ollen, koska yksityisyys, ja sen myötä henkilötietojen suoja, eivät ole absoluuttisia oikeuksia, voidaan niitä rajoittaa, mutta ainoastaan laillisin ja välttämättömin perustein.

Syyt siihen miksi perusoikeudet eivät voi olla absoluuttisia johtuu suoraan käytännön seikoista; individualismista huolimatta yksilö on aina osa yhteiskuntaa, jolloin hänen on käytännössä mahdotonta saavuttaa täysimääräistä yksityisyyttä[46]. Esimerkiksi henkilötietojen käsittely on usein välttämätöntä monissa yhteiskunnan eri toiminnoissa[47]. Yksilö ei voi täten itsenäisesti määrittää hänen yksityisyyden suojan piiriä, sillä oikeuden ja sen normien tulee yhdenvertaisuuden nimissä olla kaikille samat.

[42] Viljanen 2001, 14–16.
[43] Himma 2007, 862–863.
[44] Viljanen 2001, 14–16.
[45] Esim. C-92/09, kohdat 48 ja 50.
[46] Blume 2002, 16.
[47] Simola 2018, 27.

Perusoikeuksien rajoittamisia koskevat välttämättömät perusteet voivat täyttyä niiden välisissä ristiriitatilanteissa eli kollisioissa. Esimerkiksi kansallinen turvallisuus voi olla välttämätön peruste rajoittaa yksilön yksityisyyttä ja henkilötietojen suojaa. Samalla, kun yksityisyyden tulisi luoda piiri, johon siihen kutsumattomilla ei ole pääsyä, mahdollistaa se kyseenalaisten toimien salaamisen. Joskus yhteiskunnassa voidaankin päätyä tilanteeseen, jossa henkilön yksityisyyden piiriin on tunkeuduttava valvonnan kautta kansallisen turvallisuuden takaamiseksi ja vaaran ehkäisemiseksi. Viranomaiset voivat hyödyntää tällä tavoin saamiaan henkilötietoja ja päätellä niiden perusteella yksilöiden toiminnasta.[48]

Schrems II -tapauksessa voidaan hahmottaa nimenomaan kansallisen turvallisuuden ja yksilön yksityisyyden välinen kollisiotilanne; Yhdysvallat rajoittavat EU-kansalaisten yksityisyyttä koskevia oikeuksia harjoittamalla laaja-alaista valvontaa kansallisen turvallisuuden nimissä. EU puolestaan kokee kyseisen valvonnan suhteellisuusperiaatteen vastaisesti, jossa tavoiteltuun päämäärään nähden yksityisyyttä rikotaan yli välttämättömyyden. Hyvin pelkistäen tätä kollisiotilannetta voidaan kuvata vielä siten, että Yhdysvalloissa kansallinen turvallisuus on etusijalla yksityisyyteen nähden, kun taas EU:ssa yksilön yksityisyyden ja henkilötietojen suojaaminen on kansalliseen turvallisuuteen nähden merkittävämpi. Tilanne ei toki ole näin yksinkertainen, sillä kuten edellä on kuvattu, perusoikeuksien rajoittamisten on perustuttava vankkoihin yhteiskunnallisiin seikkoihin, jotka eivät mene yli välttämättömyyden. Tältä kannalta katsoen Yhdysvaltojen yksityisyyttä rajoittavat toimet ovat perusteltuja. Toisaalta rajoitusten on oltava oikeassa suhteessa tavoiteltuun päämäärän, joka puolestaan puoltaa EU:n kantaa, jossa yli välttämättömyyden menevää puuttumista henkilötietojen suojaan ei saisi tapahtua. Tämä oli myös EUT:n yksi keskeisimmistä viesteistä Schrems II:ssa.

Toimien välttämättömyys nykyisessä laajuudessaan, yksilön yksityisyyden kustannuksella, haastaa perus- ja ihmisoikeuksien välisen tulkintayhteyden, jossa perusoikeuksien rajoittamisen tulisi tapahtua ihmisoikeusmyönteisesti. Vaikka yhteiskunnan turvallisuuden takaaminen on lähtökohtaisesti ymmärrettävä ja vankka peruste henkilötietojen käsittelylle tai keräämiselle, on ongelmana kyseisten rajoitusten eli valvonnan kohdentumattomuus, jolloin se ylittää tarpeellisuuden rajan.

2.5 Yksityisyyden ja henkilötietojen suojien välinen suhde

Yksityisyyden suojan määrittely ja kansainväliset sopimukset osoittavat, että yksityisyyden suojassa on kyse suhteesta johonkin muuhun oikeuteen. Oikeudellinen käsitteistö lähestyy asiaa siten, että

[48] Simola 2018, 29.

oikeus yksityisyyteen antaa jollekin oikeuden ja samalla jollekin velvollisuuden kunnioittaa tätä oikeutta, ja täten mahdollisuuden oikeuden toteutumiseen.[49]

Kuten edellä on tuotu esiin, yksityisyydellä mielletään olevan vahva liityntä henkilötietojen suojaan. Tätä perinteistä ajattelua näiden käsitteiden välisestä suhteesta on kuitenkin haastettu erilaisilla hahmotustavoilla. Tässä luvussa keskitytään tarkastelemaan seuraavaa kolmea vaihtoehtoista tapaa:

a) henkilötietojen suojan voidaan katsoa olevan osa yksityisyyden suojaa, jolloin se on yksityisyyden alakategoria, kuten esimerkiksi kansainvälinen ihmisoikeusajattelu asian tulkitsee,

b) henkilötietojen suoja ja yksityisyyden suoja voidaan nähdä toisistaan erillisinä, mutta samalla toisiaan täydentävinä oikeuksina ja

c) henkilötietojen suoja voidaan hahmottaa itsenäisenä oikeutena[50], jota tukee esimerkiksi Euroopan neuvoston laatima erillinen sopimus henkilötietojen suojasta.

On selvää, että tietyntasoinen liityntä henkilötietojen suojan ja yksityisyyden välillä on olemassa. Yksityisyysaspektia ei voida kokonaan erottaa henkilötietojen suojasta, jo pelkästään siitä syystä, että henkilötietojen suoja on kehittynyt nimenomaan yksityisyydestä. Tästä huolimatta, EU:n perusoikeuskirjassa nämä oikeudet on säännelty omissa artikloissaan. Oikeuksien erottelu kuvastaa niiden erillisyyttä ja poikkeusta kansainvälisiin dokumentteihin, joissa henkilötietojen suoja mielletään yksityisyyden jatkeeksi.[51] Vaikka oikeudet onkin eroteltu EU:n perusoikeuskirjassa, on EIT kuitenkin katsonut oikeuskäytännössään, että EIS:n artiklan 8 takaama oikeus yksityisyyteen tulee käsittää laajasti[52], minkä vuoksi se on sisällyttänyt siihen myös henkilötietojen suojan. Tämä tulkinta käy ilmi erityisesti tapauksessa S. ja Marper v. Yhdistynyt Kuningaskunta,[53] jossa EIT esitteli yksityiselämän käsitettä koskevia tulkintojaan laaja-alaisesti viitatessaan aiempiin ratkaisuihinsa. EUT:n tulkintalinja ratkaisuissaan, kuten esimerkiksi Schrems II:ssa, on sama kuin EIT:n; henkilötietojen suoja on osa yksityisyyttä eikä erillinen oikeus[54]. Tätä tulkintaa on helppo ymmärtää, sillä henkilötietojen suoja ja yksityisyyden suoja edustavat hyvin pitkälle samoja tavoitteita, jopa paikoin niin paljon, että on syntynyt päällekkäisyyksiä[55]. Joka tapauksessa, tämä linja ei ole täysin

[49] Neuvonen 2014, 30.
[50] Lynskey 2015, 90.
[51] Lynskey 2014, 569–570.
[52] Gonzáles Fuster – Gutwirth 2013, 537.
[53] S. ja Marper v. Yhdistynyt Kuningaskunta (suuri jaosto), kohdat 66–67.
[54] Lynskey 2015, 90; 2014, 573 ja C-92/09 kohta 47.
[55] Lynskey 2014, 588.

rikkoutumaton, sillä esimerkiksi EUT:n antamassa ratkaisussa C-70/10 EUT ei punninnut henkilötietosuojan ja yksityisyyden välistä suhdetta lainkaan[56].

Tietosuoja voi pitää sisällään asioita, joita ei voi katsoa kuuluvan yksityisyyden suojan piiriin, ja mikäli kaikki tietosuojasta katsottaisiin kuuluvan yksityisyyden suojan alle, tarkoittaisi se silloin sitä, että suojan kohteena olevien henkilötietojen ala kapenisi[57]. Henkilötietojen suoja antaa yksilöille yksityisyyden suojaa tehokkaammat ja täsmällisemmät keinot minimoida omiin tietoihinsa kohdistuvaa haitallista käsittelyä ja se antaa myös yksilöille oikeuden päättää itseään koskevien tietojen siirrosta eli se sallii yksilöille tiedollisen itsemääräämisoikeuden[58]. Lisäksi tietosuojan kannalta katsoen on riittävää, että tieto on liitettävissä yksilöön, kun taas yksityisyyden suojaan kuuluu yksilön yksityiselämään vaikuttavien toimintojen arviointi[59]. Yksityisyyden suojan ja henkilötietojen suojan välinen side voi pahimmillaan muodostua jopa uhaksi, koska henkilötietojen suojan laaja-alaisuuden on katsottu perustuvan ajatukselle, jossa kaikki tiettyyn yksilöön liitettävissä oleva tieto on väärinkäytettävissä oleva tieto.[60] Henkilötietojen suoja on näin ollen myös selkeästi itsenäinen oikeus.

Henkilötietojen suojan ja yksityisyyden suojan välistä oikeudellista suhdetta on mahdotonta määritellä tyhjentävästi. On ilmeistä, että näillä kahdella oikeudella on yhteneväisyyksiä, mutta myös eroavaisuuksia, jolloin ne voidaan ennen kaikkea hahmottaa toisiaan täydentävinä. Niin tuomioistuintulkinnan, kansainvälisten dokumenttien ja näiden oikeuksien sisällön kannalta katsoen henkilötietojen suojan ja yksityisyyden suojan välistä suhdetta ei voi lähestyä yksioikoisesti tulkitsemalla niitä vain osin limittäisiksi. Niiden välisen kytköksen ohella niillä on oma itsenäinen alue, johon liittyen erityisesti henkilötietojen suoja voi tarjota täsmällisiä oikeuksia turvatakseen yksilön tiedollisen itsemääräämisoikeuden itseään koskevien tietojen osalta. Nämä oikeudet ovat usein EUT:n ja EIT:n oikeuskäytännönkin perusteella toisiinsa liittyviä ja näin myös osin toisiaan täydentäviä. Henkilötietojen suojalle tulee kuitenkin antaa sen oma merkitysarvonsa ja nähdä se yksityisyyden suojasta erillisenä oikeutena, jolla on oma vahva oikeudellinen toiminta-alueensa. Se mikä kaipaa edelleen laajempaa arviointia ja tarkennusta, on näiden oikeuksien välinen erillisyys

[56] EUT C-70/10 kohdat 50–51.
[57] Koillinen 2013, 180–183 ja Brownsword 2009, 95.
[58] Lynskey 2014, 588–591.
[59] Tzanou 2011, 38.
[60] De Hert – Gurtwith 2009, 25.

toisistaan, sillä muutoin riski henkilötietojen suojan lisäarvosta ja potentiaalista yksilöiden suojana jää toteutumatta sen jäädessä yksityisyyden varjoon.[61]

2.6 Yksityisyyden ja henkilötietojen suojien sääntely

Euroopan neuvosto selvitti 1970-luvun alussa EIS:n suojan riittävyyttä henkilötietojen käsittelylle. Tämän selvityksen seurauksena annettiin päätöslauselmia, joilla täsmennettiin EIS:n 8 artiklan soveltuvuutta henkilötietojen käsittelyssä. Vuonna 1980 OECD hyväksyi yksityisyyden ja henkilötietojen suojaa koskevan tietosuojasuosituksen ja vuonna 1985 tuli voimaan Euroopan neuvoston tietosuojasopimus (36/1992). Henkilötietojen suojan kehitykselle merkittävimmät tekijät ovat kuitenkin olleet EU:n henkilötietodirektiivi (95/46/EY) sekä televiestinnän tietosuojadirektiivi (97/66/EY), nykyinen sähköisen viestinnän tietosuojadirektiivi).[62] Vuonna 2016 tuli voimaan EU:n yleinen tietosuoja-asetus, jolla korvattiin henkilötietodirektiivi. Tietosuoja-asetuksen mukaan, sen tarkoitus on suojella erityisesti luonnollisten henkilöiden oikeutta henkilötietojen suojaan (art. 1:2). Tietosuojauudistuksellaan EU halusi viestiä sen entistä vahvemmasta roolista yksityisyyden suojelijana, jota ovat tukeneet myös EUT:n tulkintalinjat, yhtenä tuoreimmista Schrems II.

Vuoden 2001 New Yorkissa tapahtuneen terrori-iskun jälkeen, monet maat muuttivat suhtautumistaan yksityisyyden suojan rajoituksiin liittyen. Erityisesti Yhdysvalloissa tämä näkyi siten, että tiedustelupalvelu lisäsi kansalaistensa sähköisen viestinnän seuraamista[63], minkä vuoksi myös EU-kansalaiset ovat päätyneet Yhdysvaltain viranomaisten laittoman sähköisen valvonnan kohteeksi[64]. Yhdysvalloissa ei ole liittovaltion tasolla EU:hun verrattavaa yhtä johdonmukaista yksityisyyttä koskevaa lainsäädäntöä, vaan Yhdysvalloissa yksityisyyttä säännellään kompleksisesti sektori- ja alakohtaisesti[65]. Yksilön oikeutta tietojen yksityisyyteen ei nimenomaisesti tunnusteta Yhdysvaltojen perustuslaissakaan[66], joka länsieurooppalaiseen perusoikeuskäsitykseen verrattuna on jo pelkästään sisällön puolesta varsin suppea.

Kaiken kaikkiaan Yhdysvaltojen lainsäädäntöä leimaa liittovaltiorakenne, jossa normien välisissä ristiriitatilanteissa liitovaltion laki syrjäyttää osavaltion lain (VI artiklan 2 §).[67] Osavaltiot ovat osin tämän takia laatineet omia yksityisyyttä koskevia lakeja, joista uusimpia on Kaliforniassa hyväksytty

[61] Lynskey, 2014, 596.
[62] Neuvonen 2014, 18.
[63] Neuvonen 2014, 15–19.
[64] EUT C-311/18, kohta 191.
[65] Li 2018, 39.
[66] Sharma, Sanjay 2020, 18 ja 60.
[67] Scheinin 1991, 70

lakialoite digitaalisen yksityisyydensuojan tiukentamisesta.[68] Pelkistetysti voidaan todeta, että kun EU pyrkii vahvistamaan asemaansa henkilötietoja koskevan yksityisyyden suojelijana, toimitaan Yhdysvalloissa pirstalemaisesti ilman selkeää yhtenäistä linjaa henkilötietojen ja yksityisyyden suojaamisessa. EU:n ja Yhdysvaltojen erilainen oikeuskäsitys yksityisyyden tärkeydestä tuleekin esiin jo pelkkiä keskeisiä lakeja tarkastellessa; tietosuoja-asetus painottaa yksityisyyden tärkeyttä ja yksilön oikeuksia, kun taas Yhdysvaltojen lainsäädäntö keskittyy enemmän tietoturvan, yksityisten tiedostojen, asiakirjojen ja yleisesti datan suojeluun, josta yksityisyys ja yksilön oikeudet jäävät usein ulkopuolelle. Ongelmana Yhdysvalloissa on ennen kaikkea lakien määrä ja niiden eroavaisuudet osavaltioiden välillä.[69]

2.6.1 Sääntely EU:ssa

Henkilötietolainsäädännön kokonaisuus on kasvanut merkittävästi 1990-luvun alusta lähtien EU:n ja sen jäsenmaiden tasolla[70], minkä vuoksi EU:ssa on tietosuoja-asetuksen lisäksi useita muita asetuksia ja direktiivejä, joilla säännellään niin henkilötietoja kuin yksityisyyttäkin. Sääntelyä löytyy muun muassa viranomaisten tietojenkäsittelydirektiivistä (2016/680/EU) sekä sähköisen viestinnän tietosuojadirektiivistä (58/2002/EY)[71]. EU:n yleisessä tietosuoja-asetuksessa on vahvistettu säännöt koskien henkilötietojen käsittelyä ja niiden vapaata liikkuvuutta (art. 1:1). Asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei (art. 1:3).

EU:n asetukset ovat jäsenvaltioissa suoraan sovellettavaa oikeutta, kuten EU:n toiminnasta tehdyn sopimuksen (SEUT) 288 artiklan toisessa kappaleessa todetaan: ”Asetus pätee yleisesti. Se on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.” Tietosuoja-asetus vaikuttaa näin ollen kaikissa EU:n jäsenvaltioissa ilman implementointia, minkä lisäksi sillä on välitön oikeusvaikutus. EU-oikeuden etusijaperiaate mahdollistaa suoran sovellettavuuden ja välittömän oikeusvaikutuksen tosiasiallisen toteutumisen.[72] Vaikka EU on selkeästi ottanut henkilötietojen suojassa lainsäädännöllisesti järeämmän keinon käyttöön eli säätänyt henkilötiedoista direktiivin sijaan asetuksella, on tietosuoja-asetuksessa jätetty myös liikkumavaraa jäsenvaltiolle.

[68] Gray 2020, Junttila 2020 ja Li 2018, 40.
[69] Coos 2018.
[70] Neuvonen 2014, 15.
[71] Tämä direktiivi tullaan lähitulevaisuudessa korvaamaan sähköisen viestinnän tietosuoja-asetuksella, ks. COM (2017) 10.
[72] Ks. EUT:n ratkaisut C-26/62, C-6/64 ja C-106/77 EU-oikeuden etusijasta, suorasta sovellettavuudesta, välittömästä oikeusvaikutuksesta ja EU.

Jäsenvaltioiden harkintamarginaali eli mahdollisuus säätää poikkeuksia tietosuoja-asetuksesta kansalliseen lakiin, näkyy muun muassa tietosuoja-asetuksen artiklassa 23, joka koskee rekisteröidyn oikeuksia sekä artiklassa 46, joka koskee henkilötietojen siirtoa asianmukaisia suojatoimia soveltaen. Osa artikloista puolestaan asettaa tarkemman sääntelyvelvoitteen jäsenvaltioille[73]. Tietosuoja-asetus on siis paikoin suoraan sovellettavaa sekä tietyntasoisen direktiivinomaisen liikkumavaran sallivaa oikeutta[74].

Suomessa sekä oikeus yksityisyyteen että henkilötietojen suoja on huomioitu jo edellä esiin tuodun perustuslain 10 §:n säännöksessä. Sen mukaan

> Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Suomen tietosuojalaki (1050/2018), joka kumosi vanhan henkilötietolain (523/1999), täydentää ja täsmentää niin tietosuoja-asetusta kuin perustuslakia. Tietosuojalaista voidaan poiketa yksityisyyttä ja henkilötietoja koskevilla erityislaeilla[75], kuten esimerkiksi yksityisyyden suojasta työelämässä (759/2004) ja viranomaisten toiminnan julkisuudesta (ns. julkisuuslaki 621/1999) sekä sähköisen viestinnän palveluista (ns. tietoyhteiskuntakaari, 917/2014) annetuilla laeilla.

2.6.2 Sääntely Yhdysvalloissa

Yhdysvalloissa on liittovaltion ja valtion lakien ja asetusten muodostama kokonaisuus, joka pitää sisällään niin lainsäädännöllisiä päällekkäisyyksiä kuin ristiriitoja. Tämän lisäksi valtion virastot ja teollisuuden alat ovat kehittäneet suuntaviivoja, jotka ovat osa ”itseääntelykehystä”, ja joita pidetään yleisesti hyväksyttyinä parhaina käytänteinä ilman lainvoimaa. Yksityisyyttä sääntelevät lait perustuvat sektorikohtaiseen (sector-specific) lähestymistapaan, jossa ne kohdistuvat ainoastaan tietyntyyppisten toimialojen ja henkilötietojen suojeluun. Esimerkiksi terveys- ja potilastietoja sääntelee The Health Insurance Portability and Accountability Act (HIPAA) ja taloudellisten tietojen keräystä, käyttöä ja julkistamista The Financial Services Modernization Act (Gramm-Leach-BlileyAct (GLB).[76] Yhdysvalloissa on myös laaja kuluttajansuojalaki, mikä ei varsinaisesti ole

[73] Ks. liikkumavarataulukko OMML 35/2017, 48–57.
[74] HE 87/2019, 6.
[75] HE 9/2018 vp, 1.
[76] Li 2018, 40.

yksityisyyttä suojaava, mutta jonka tarkoitus on estää epäoikeudenmukaisuuksia ja harhaanjohtavia käytäntöjä henkilötietojen käsittelyssä.[77]

Vuonna 2003 Kalifornia sääti ensimmäisenä osavaltiona oman tietosuojarikkomuksia koskevan lain (The California Data Protection Act), jota uusin lakialoite (The California Privacy Rights Act) tiukentaa edelleen. Kalifornian ensimmäisen tietosuojalain jälkeen useat muut osavaltiot seurasivat perässä, jonka seurauksena on muodostunut epäjohdonmukainen kokonaisuus erilaisia yksityisyyttä sääntteleviä lakeja. Esimerkiksi Kaliforniassa laki edellyttää, että tietosuojarikkomuksen luonne on kuvattava asianosaiselle, eli se mitä tapahtui ja millaisia vaikutuksia sillä on kyseisen henkilölle, kun taas Massachusettsissa laki nimenomaisesti kieltää tällaisen tiedon julkistamisen asukkailleen.[78] Nämä lainsäädännölliset puitteet ovat johtaneet kasvaviin hallinnollisiin haasteisiin yritysten parissa, kun yritykset joutuvat huomioimaan useita eri säännöksiä, jotka vaihtelevat niin osavaltio kuin sektoritasolla, mutta myös liittovaltion tasolla[79].

Yhdysvalloissa liittovaltion tasoista yksityisyyttä sääntelevää lakia on tähän asti vastustettu. Vuonna 2012 Obaman hallinto vei eteenpäin suunnitelmaa laista (Consumer Privacy Bill of Rights), joka olisi pitänyt sisällään yleiset standardit liittyen henkilötietojen keräämiseen, säilytykseen ja tietoturvaan, mutta tämä suunnitelma koki täystyrmäyksen jo heti alkuun. Trumpin hallinto ei innostunut tietosuojaan liittyvien lakien eteenpäin viemisestä lainkaan, vaan päinvastoin se mitätöi Federal Communications Commission (FCC) -säännöt, jotka sääntelivät laajasti yritysten toimintatapoja käsitellessään henkilötietoja.

Schrems II -tuomiossa EUT nosti esiin yhdysvaltalaisten viranomaisten sääntelemättömät toimintatavat koskien EU-kansalaisten henkilötietojen käsittelyä, sekä tästä johtuvan EU-kansalaisten oikeussuojakeinojen tehottomuuden. Vaikka EU-kansalaisten käytettävissä on useita oikeussuojakeinoja tilanteessa, jossa he ovat joutuneet laittoman sähköisen valvonnan kohteeksi kansallisen turvallisuuden nimissä, ei tämä kuitenkaan koskea tiettyjä Yhdysvaltain tiedusteluviranomaisten käytössä olevia oikeudellisia perusteita, kuten toimeenpanoasetusta E.O. 12333:a. Lisäksi sekä EU-kansalaisten että yhdysvaltalaisten mahdollisuudet kanteen nostamiseen ovat vähäiset, sillä kanteet jätetään tutkimatta, mikäli asianomistajat eivät pysty osoittamaan kanneoikeuttaan.[80] Yhdysvaltojen lainsäädännön puutteellisuus kansalaisten yksityisyyden

[77] Leuan 2018.
[78] Li 2018, 40.
[79] Sharma & Menon 2020, 12.
[80] EUT C-311/18, johdanto-osan kohta 115.

suojelijana näkyy viranomaisten toiminnoissa, jotka voivat suoraan rajoittaa yksilöiden perustavanlaatuisia oikeuksia.

Vuonna 2018 Yhdysvalloissa tuli voimaan Clarifying Lawful Overseas Use of Data Cloud Act (Cloud Act). Cloud Act muutti vuoden 1986 Stored Communications Act -lakia siten, että nykyään Yhdysvaltain lainvalvontaviranomaiset voivat tuomioistuimen luvalla määrätä Yhdysvaltoihin sijoittautuneen palveluntarjoajan luovuttamaan sähköpostitilinsä sisällön, vaikka tilin tiedot olisivatkin varastoitu Yhdysvaltojen ulkopuolella sijaitsevalle palvelimelle eli arkikielen mukaan pilveen. Viranomaisten mahdollisuudet hankkia tietoja muuttuivat siis olennaisesti. Lisäksi säädöksessä on vaatimuksia, joiden nojalla Yhdysvaltain hallinto voi tehdä toimeenpanosopimuksia, jotka sallivat yhdysvaltalaisille palveluntarjoajille sisältötietojen toimittamisen ulkomaalaiselle hallitukselle ilman keskinäisen oikeusavun pyyntöä. Säädös pitää sisällään myös kohteliaisuuslausekkeen (comity clause), jonka kautta Cloud Act -säädös sallii palveluntarjoajille mahdollisuuden pyytää yhdysvaltalaista tuomioistuinta kumoamaan tai muuttamaan ulkomaille varastoitua tietoa koskevan määräyksen, mikäli tieto liittyy muuhun kuin yhdysvaltalaiseen ja jos määräyksen noudattaminen johtaisi siihen, että palveluntarjoajat joutuisivat rikkomaan lakia maassa, jonka kanssa Yhdysvallat on tehnyt toimeenpanosopimuksen.[81]

Cloud Actin voimaantulo on luonnollisesti herättänyt keskustelua sen suhteesta EU:n tietosuoja-asetuksen vaateisiin. Osa Cloud Actin ja tietosuoja-asetuksen välistä suhdetta tulkitsevista katsoo EU:n tietosuoja-asetuksen ja Cloud Actin olevan konfliktissa. Heidän mukaansa Cloud Actista voi aiheuta hyvinkin vakavia tilanteita yrityksille, joita tietosuoja-asetus lähtökohtaisesti kieltää luovuttamasta henkilötietoja EU:n ulkopuolelle. Cloud Actista huolestuneet uskovat myös, että henkilötietojen luovuttaminen Cloud Actin velvoitteiden mukaisesti voisi tuoda eurooppalaisille yrityksille jopa miljoonien sakot sekä mainehaitan, yritysten riitauttamismahdollisuuksien ollessa lähestulkoon olemattomat. Kaiken kaikkiaan pilvipalvelun ei katsota voivan täyttää sekä tietosuoja-asetuksen että Cloud Actin vaatimuksia, vaan ensimmäiseksi mainitun velvoitteiden täyttäminen on mahdollista ainoastaan siten, etteivät yhdysvaltalaisyritykset pääse luovuttamaan henkilötietoja eteenpäin edes varmistustensa kautta.[82]

Vastakkaista näkemystä edustavat katsovat, että Cloud Act -laki vain päivittää pienen osan edellä mainitusta Stored Communications Actista. Cloud Act rajoittuu auttamaan viranomaisia kansainvälisen rikollisuuden ja terrorismin ehkäisemisessä, jolloin se ei anna Yhdysvaltojen

[81] Euroopan Unionin neuvosto 6339/18.
[82] Turunen 2019.

viranomaisille vapautta käyttää pilveen tallennettua tietoa rajoitteetta. Se ei myöskään palvele ainoastaan Yhdysvaltojen etuja, vaan lakia sovelletaan kaikkiin digitaalisen viestinnän palveluihin, jotka noudattavat jo muutoinkin Yhdysvaltojen lakeja, olivatpa palvelut sitten Yhdysvalloissa tai jossain muussa maassa. Lisäksi pystyäkseen velvoittamaan palveluntarjoajat luovuttamaan tietoja, tulee viranomaisilla olla perusteltu syy pyytää tietoja, minkä lisäksi tietojen on liityttävä suoraan rikokseen, josta päättää lopulta tuomioistuin.[83]

Cloud Actin ja tietosuoja-asetuksen välisestä suhteesta ei ainakaan toistaiseksi tule olla kovin huolissaan, sillä vaikka kyseinen säädös velvoittaakin yhdysvaltalaiset palveluntarjoajat luovuttamaan sisältötietoja, on niiden nimenomaan liityttävä olennaisesti rikostutkintaan. Lisäksi, kun hallitukset laativat keskenään toimeenpanosopimuksia, tulee näiden sopimusten sisältää ehtoja, joilla pyritään takaamaan riittävät suojatoimet, jotka rajoittavat Yhdysvaltojen kansalaisiin liittyvien tietojen saatavuutta.[84] Nimenomaan näillä suojatoimilla on huomioitu EU:n tietosuojastandardit.

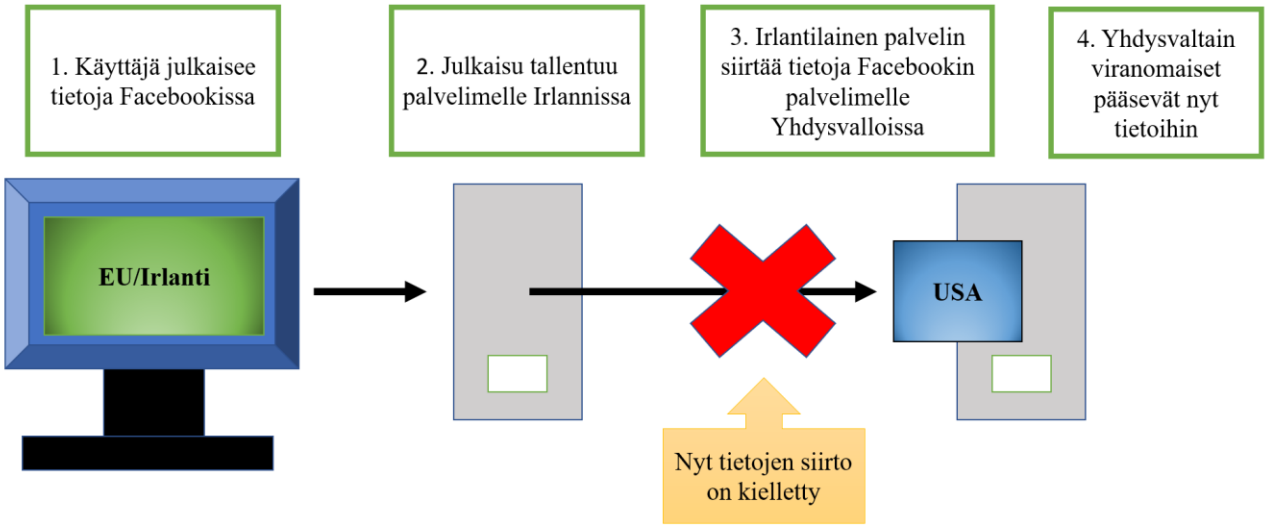
[83] Punke 2019.
[84] Euroopan Unionin neuvosto 6339/18.

3 Vakiolausekkeet henkilötietojen siirtomekanismina

3.1 Henkilötietojen siirto EU:sta Yhdysvaltoihin

Henkilötietojen siirtämisen käsite on laaja. Sitä on tietojen konkreettisen siirtämisen ja lähettämisen lisäksi esimerkiksi pääsyn salliminen rekisterinpitäjän sisämarkkinoilla sijaitsevaan tietokantaan EU:n tai Euroopan talousalueen ulkopuolella toimivalle taholle.[85] Schrems II:ssa oli kyse konkreettisesta vakiolausekkeiden ja Privacy Shield -järjestelyn avulla tehdyistä tietosiirroista Facebook Irelandin ja Facebook Inc.:n välillä. Schremsin perusteet kanteeseen saivat alkunsa vuonna 2013, kun Schrems pyysi Facebook-yhtiötä lähettämään häntä koskevat tiedot, joita hän tarvitsi yliopiston kurssitehtävään liittyen. Koska EU-kansalaisilla on EU:n tietosuoja-asetuksen artiklan 15 mukaan oikeus saada tietää mitä tietoja yritys säilyttää hänestä, lähetti Facebook Schremsille kaikki tiedot hänen Facebook-toiminnoistaan. Lähetetty tiedosto sisälsi kaiken kaikkiaan 1200 sivua tietoa, jopa sellaista, joita käyttäjä olettaa poistettavan.

Schremsin kanteeseen johtaneita syitä voidaan hahmottaa seuraavan kuvion avulla:



KUVIO 1: Schrems II ja henkilötietojen siirtotapahtuma EU:sta Yhdysvaltoihin[86].

Kun Schrems käytti Facebookia, tallentuivat häntä koskevat tiedot EU:ssa sijaitsevalle palvelimelle, josta Facebook Ireland halusi siirtää tiedot tuolloin voimassa olleiden vakiolausekkeiden ja Privacy Shield -järjestelyä hyödyntäen sen emoyhtiön palvelimelle Yhdysvaltoihin. Kun tiedot siirtyvät Yhdysvaltoihin, voivat EU-kansalaisia koskevat tiedot päätyä kyseisen maan tiedusteluviranomaisten sähköisen valvonnan kohteeksi. Schrems ei ensinnäkään halunnut, että Facebook Ireland siirtää häntä

[85] Aalto-Setälä & Viitaila 2018, 30.
[86] Sajari, 2015.

koskevia henkilötietoja Yhdysvaltoihin, sillä Schremsin mielestä henkilötietojen siirto vakiolausekkeilla ja Privacy Shield -sopimuksella eivät suojelleet EU-kansalaisia Yhdysvaltain tiedusteluviranomaisten valvonnalta. Toisekseen henkilötietojen siirto Yhdysvaltojen kaltaiseen maahan on lähtökohtaisesti kielletty, koska kyseinen maa ei takaa samantasoista yksityisyydensuojaa kuin EU. [87] Näin ollen, kun henkilötietoja siirretään EU:sta Yhdysvaltoihin, tietosuoja-asetuksen takaama henkilötietojen suojan taso heikkenee aiheuttaen mahdollisia riskejä rekisteröidyn yksityisyydelle. Nimenomaan tämän Schrems onnistui näyttämään toteen sekä Schrems I, että II kanteissaan.

Rekisteröidyn yksityisyyteen kohdistuvien riskien minimoimiseksi tietosuoja-asetuksessa määritellään edellytyksiä niille perusteille, joilla henkilötietoja voidaan siirtää EU:sta Yhdysvaltoihin. Henkilötietojen käsittelyn tulee olla 1) sallittua EU-maassa kyseisessä tilanteessa ja 2) siirron on myös täytettävä tietosuoja-asetuksen luvun V edellytykset. Kyseisissä edellytyksissä on määritelty siirtomekanismien lisäksi siirtoa koskeva yleinen periaate, kielletyt siirrot ja luovutukset, kansainvälinen yhteistyö henkilötietojen suojaamiseksi sekä erityistilanteita koskevat poikkeukset (art. 44–50). Tietojen siirron Yhdysvaltoihin tulee siis täyttää molemmat (1 ja 2) edellytykset.[88] Siirtoa koskevien yleisten vaatimusten lisäksi tietosuoja-asetuksessa on määritelty yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. Vaatimuksia sovelletaan sekä eurooppalaisiin organisaatioihin, jotka käsittelevät henkilötietoja EU:ssa, että EU:n ulkopuolisiin organisaatioihin, joka käsittelevät EU-kansalaisten henkilötietoja[89], kuten esimerkiksi Facebook Inc.

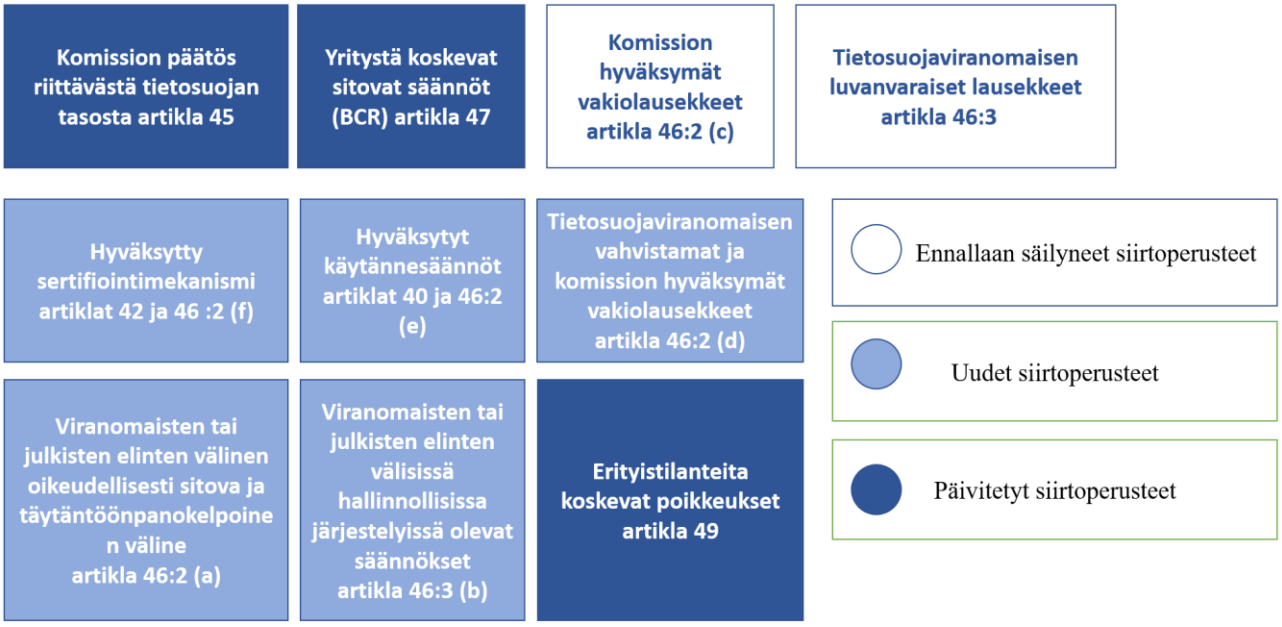
Siirretyt henkilötiedot voivat kulkea useiden eri organisaatioiden läpi. Tällaisessa prosessissa toimii kaksi pääasiallista profiilia, jotka hoitavat henkilötietojen käsittelyä; rekisterinpitäjä, joka päättää henkilötietojen käsittelytarkoituksesta ja -tavasta ja henkilötietojen käsittelijä, joka säilyttää ja käsittelee tiedot rekisterinpitäjän puolesta.[90] Schrems II -tapauksessa Facebook Ireland on rekisterinpitäjä ja Facebook Inc. henkilötietojen käsittelijä. Tietosuoja-asetuksen soveltamisen haasteellisuus tulee esiin juuri Schrems II:n kaltaisessa tapauksessa, jossa EU-alueen ulkopuolinen organisaatio toimii Yhdysvalloissa eli maassa, jossa yksityisyyden suoja ja sitä koskeva sääntely eivät vastaa EU:n tasoa.

[87] Ortamo, 2019 ja Hill, 2012.
[88] Tietosuojavaltuutetun toimisto.
[89] Your Europe, Yleinen tietosuoja-asetus. 2020.
[90] Your Europe. Yleinen tietosuoja-asetus. 2020.

EU:n kannalta katsoen on varsin perusteltua, että Yhdysvaltoihin tehtyjä tietosiirtoja halutaan pyrkiä suojelemaan vakiolausekkeita tehostavilla lisäsuojatoimenpiteillä rekisteröidyn oikeuksien turvaamiseksi. EUT korosti Schrems II -tuomiossaan rekisterinpitäjän vastuuta siitä, että siirrossa käytetään menetelmiä, jotka täyttävät EU:n tavoitteen korkean tietojen suojan tasosta Yhdysvaltoihin siirretyille tiedoille. Rekisterinpitäjän on samalla myös varmistettava, että henkilötietojen käsittelijät, jotka käsittelevät tietoja sen lukuun, noudattavat samoja suojatoimia kuin rekisterinpitäjä. Tällä pyritään varmistamaan, että käsittelyssä varmistetaan rekisteröidyn oikeuksien suojelu (tietosuoja-asetus, johdanto-osa kohta 81 ja art. 28).

3.2 Henkilötietojen siirtoperusteet

Uuden tietosuoja-asetuksen myötä siirtoperusteiden määrä kasvoi, osaa siirtoperusteista päivitettiin ja osa säilyi ennallaan. Seuraavaan kuvioon on koostettu nämä vaikutukset kuhunkin tietosuoja-asetuksen mukaiseen henkilötietojen siirtoperusteeseen:



KUVIO 2: Henkilötietojen siirtoperusteet[91].

Siirtoperusteista säilyivät ennallaan tietosuojaviranomaisen luvanvaraiset sopimuslausekkeet (art. 46:3(a)) sekä komission hyväksymät vakiolausekkeet (art. 46:2(c)), jotka EUT jätti Schrems II -tuomiossaan voimaan. Tuomion myötä komissio on jo ehtinyt laatia uudet vakiolausekeluonnokset, jotta ne olisivat yhteneväiset tietosuojaneuvoston laatimien lisäsuojatoimenpidesuositusten kanssa.

[91] Tietosuojavaltuutetun toimisto.

Päivitettyjä siirtoperusteita olivat artiklat 45, 47 ja 49, joista ensimmäinen on Yhdysvaltoihin tehtyjen siirtojen osalta keskeisin. Artikla 45 koskee komission arviota kolmannen maan, kolmannen maan alueen, yhden tai useamman tietyn sektorin tai kansainvälisen järjestön tietosuojan tasosta. Mikäli tietosuojan taso katsotaan riittäväksi, ei siirrolle tarvita erityistä lupaa. Tällöin maa, sen alue, järjestö tai sektori kuuluu komission vastaavuuspäätöksen piiriin. Mikäli tietosuojan taso katsotaan riittämättömäksi, komissio ei anna vastaavuuspäätöstä. Yhdysvallat kuuluvat niihin maihin, joista komissio ei ole antanut vastaavuuspäätöstä, jolloin siirto on toteutettava muita 46 artiklan mukaisia siirtoperusteita hyödyntäen, kuten esimerkiksi hyödyntämällä vakiolausekkeita ja lisäsuojatoimenpiteitä.

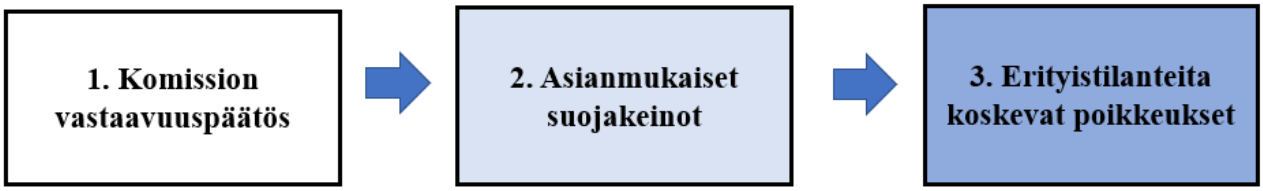
Kaksi muuta päivityksen kohteena ollutta artiklaa olivat yritystä koskevat sitovat säännöt (art. 47) sekä erityistilanteita koskevat poikkeukset (art. 49). Yritystä koskevilla sitovilla säännöillä tarkoitetaan tietosuoja-asetuksen mukaan oikeudellisesti sitovia sääntöjä, joita sovelletaan kaikkiin asianomaisiin konsernin tai yritysryhmän jäseniin (art. 47:1 a)). Erityistilanteita koskevat poikkeustilanteet tarkoittavat puolestaan tiedonsiirtotilanteita, joista ei ole tehty 45 artiklan 3 kohdan mukaista tietosuojan tason riittävyyttä koskevaa päätöstä eikä 46 artiklassa tarkoitettuja asianmukaisia suojatoimia ole toteutettu (art. 49:1).

Uuden tietosuoja-asetuksen myötä kokonaan uusia siirtoperusteita olivat tietosuojaviranomaisen vahvistamat ja komission hyväksymät vakiolausekkeet (art. 46:2(d)), hyväksytty sertifiointimekanismi (art. 42, art. 46:2(f)), hyväksytyt käytännesäännöt (art. 40, art. 46:2(e)), viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline (art. 46:2(a)) sekä näiden tahojen välisissä hallinnollisissa järjestelyissä olevat säännökset (art. 46:3(b)). Uusia siirtoperusteita olivat myös rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön rekisterinpitäjän, henkilötietojen käsittelijän tai vastaanottajan väliset sopimuslausekkeet tai säännökset, jotka sisällytetään viranomaisten tai julkisten elinten välisiin hallinnollisiin järjestelyihin ja joihin sisältyy rekisteröityjen täytäntöönpanokelpoisia ja tehokkaita oikeuksia.[92]

[92] Tietosuojavaltuutetun toimisto.

3.3 Siirtoperusteiden etusijajärjestys

Lähtökohtaisesti henkilötietoja voidaan siirtää EU-alueen ulkopuolelle usealla eri tavalla, mutta siirtomekanismi ja siirron ylipäätään toteutuminen riippuu siirtoperusteesta ja niitä koskevasta etusijajärjestyksestä:



KUVIO 3: Siirtoperusteiden etusijajärjestys.[93]

Kun henkilötietoja aiotaan siirtää Yhdysvaltoihin, on ensin selvitettävä, voidaanko siirto toteuttaa komission vastaavuuspäätöksen (art. 45) perusteella, sillä komission vastaavuuspäätös on ensisijainen siirtoperuste, eikä siirrolle tällöin tarvita erityistä lupaa. Näissäkin tilanteissa siirtojen on kuitenkin noudatettava tietosuojalainsäädännön vaateita sekä ennen siirtoa, siirron aikana, että sen jälkeen. Tällä hetkellä komission voimassa olevat vastaavuuspäätökset on annettu seuraavista maista: Andorra, Argentiina, Färsaaret, Guernsey, Israel, Mansaari, Japani, Jersey, Uusi-Seelanti, Sveitsi ja Uruguay, minkä lisäksi komissio on antanut osittaiset vastaavuuspäätökset Kanadasta.

Komission velvoitteisiin kuuluu tarkastella vastaavuuspäätöksiään vähintään neljän vuoden välein. Kun komissio arvioi tällöin esimerkiksi Yhdysvaltojen pääsyä komission vastaavuuspäätöksen piiriin, tulee arvio toteuttaa objektiivisin perustein, jossa huomioidaan erityiset henkilötietojen käsittelytoimet ja Yhdysvalloissa sovellettavien oikeusnormien soveltamisala ja voimassa oleva lainsäädäntö. Käytännössä Yhdysvaltojen olisi tarjottava takeet niistä toimenpiteistä, joilla se varmistaa riittävän tietosuojan tason, joka vastaa merkittäviltä osin unionin suojan tasoa. Yhdysvaltojen olisi myös toteutettava tehokas ja riippumaton tietosuojavalvonta, joka tekee yhteistyötä EU:n jäsenvaltioiden tietosuojaviranomaisten kanssa sekä varmistettava rekisteröidyille tehokkaat oikeussuojakeinot (tietosuoja-asetus, johdanto-osa, kohta 104). EUT:n Schrems I ja II-tuomiot ovat osoittaneet, ettei Yhdysvallat voi kuulua komission vastaavuuspäätöksen piiriin, sillä tietosuojan taso tai rekisteröityjen oikeussuojakeinot eivät vastaa unionin edellyttämää. Vaikka

[93] Tietosuojavaltuutetun toimisto.

komissio ei ole antanutkaan vastaavuuspäätöstä Yhdysvalloista, tulee rekisterinpitäjien kuitenkin seurata komission vastaavuuspäätöksen ajantasaisuutta.

Koska siirtoa Yhdysvaltoihin ei voida tehdä vastaavuuspäätöksen perusteella, on rekisterinpitäjän selvitettävä, voidaanko henkilötietoja siirtää asianmukaisilla suojakeinoilla (art. 46) eli siirtoperusteilla. Mikäli henkilötietoja ei voida siirtää yhdelläkään 46 artiklassa kuvatuista siirtoperusteista voidaan vielä selvittää, olisiko henkilötietoja mahdollista siirtää erityistilanteita koskevan poikkeuksen (art. 49) perusteella. Siirto on tällöin mahdollinen, mikäli jokin seuraavista edellytyksistä täyttyy:

a) rekisteröity on antanut suostumuksensa siirtoon sen jälkeen, kun hänelle on ilmoitettu, että siirrosta voi aiheuta hänelle riskejä,

b) siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen voimaan saattamiseksi,

c) siirto on tarpeen rekisterinpitäjän ja toisen tahon välisen sopimuksen tekemiseksi,

d) siirto on tarpeen tärkeää yleistä etua koskevien syiden vuoksi,

e) siirto on tarpeen oikeuskanteeseen liittyvän seikan vuoksi,

f) siirto on tarpeen rekisteröidyn etujen suojaamiseksi,

g) siirto tehdään rekisteristä, jonka tarkoituksena on yleisesti saatavilla olevien tietojen antaminen yleisölle

Nimensä mukaisesti kyseessä on poikkeuksellinen siirtotilanne, joka on viimesijainen tiedonsiirtoperuste. Tietojen siirron tulisi siis aina ensisijaisesti perustua joko komission tekemään tietosuojan riittävyyttä koskevaan päätökseen tai tietosuoja-asetuksen 46 artiklan mukaisiin asianmukaisiin suojatoimiin. Mikäli siirto Yhdysvaltoihin ei olisi mahdollista jollain 46 artiklan mukaisista siirtomenetelmistä tai erityistilanteita koskevan poikkeuksen perusteella, voitaisiin henkilötietoja siirtää Yhdysvaltoihin ainoastaan silloin, kun siirto ei ole toistuva, se koskee rajallista määrää rekisteröityjä, se on tarpeen rekisterinpitäjän etujen toteuttamiseksi, joita rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä, ja rekisterinpitäjä on arvioinut kaikki tiedonsiirtoon liittyvät seikat ja toteuttanut tämän arvioinnin perusteella henkilötietojen suojaa koskevat asianmukaiset suojatoimet. Sen lisäksi, että tällainen siirto edellyttää rekisterinpitäjän ilmoitusta siirrosta valvontaviranomaiselle, rekisterinpitäjän on toimitettava rekisteröidylle rekisterinpitäjän

yhteystiedot, ja tapauskohtaisesti myös tietosuojavastaavan yhteystiedot, henkilötietojen käsittelyn tarkoitus ja oikeusperuste (art. 49:1).

3.4 Rekisterinpitäjän vastuu

Kun tietoja siirretään Yhdysvaltoihin vakiolausekkeiden ja lisäsuojatoimenpiteiden avulla, tulee rekisterinpitäjän noudattaa kaikissa toimissaan tietosuoja-asetuksen asettamia velvoitteita. Rekisterinpitäjän vastuu tietojen käsittelyn suhteen on siis laaja. Tämä näkyy rekisterinpitäjään kohdistuvina tietosuojaperiaatteiden noudattamisena (art. 5) sekä velvollisuutena toteuttaa tarvittavia teknisiä ja organisatorisia toimenpiteitä, joilla se voi varmistaa ja osoittaa, että tietojen käsittelyssä noudatetaan näitä kyseisiä periaatteita (art. 24 ja art. 25:1). Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan

a. henkilötietojen pseudonymisointia ja salausta,
b. kykyä taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus,
c. kykyä palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa,
d. menettelyä, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi sekä
e. henkilötietojen käsittelyn seuraamista ja valvontaa (art. 32).

Rekisterinpitäjän vastuulla on myös tarkistaa ja päivittää näitä toimenpiteitä tarpeen mukaan (art. 24:1).

Rekisterinpitäjien tulee huomioida tietojen siirroissa tietosuoja-asetuksen vaatimukset mahdollisimman varhaisessa vaiheessa[94]. Tämä tarkoittaa sitä, että rekisterinpitäjien tulee määrittää selkeät käsittelytavat ja toimenpiteet, joilla tietosuoja-asetuksen vaateet saadaan sisällytettyä tehokkaasti osaksi henkilötietojen käsittelyprosessia (25:1) kokonaisuudessaan. Rekisterinpitäjien on myös varmistettava, että yritys käsittelee vain tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja ei saateta rajoittamattoman yleisön saataville ilman rekisteröidyn myötävaikutusta. (art. 25).

[94] Aalto-Setälä & Viitaila 2018, 26.

Vakiolausekkeiden tehtävänä on, Schrems II -tuomion jälkeen yhdessä lisäsuojatoimenpiteiden kanssa, pyrkiä varmistamaan, että tietosuoja-asetuksen yleisiä rekisterinpitäjää velvoittavia periaatteita sekä sisäänrakennettua ja oletusarvoista tietosuojaa koskevia määrityksiä (tietosuoja-asetus, johdanto-osa, kohta 108) noudatetaan Yhdysvaltoihin tehdyissä tietosiirroissa. Lisäksi vakiolausekkeiden tulisi samaisten tietosiirtojen yhteydessä mahdollistaa rekisteröityjen oikeussuojakeinojen, kuten korvausvaadeoikeuden saatavuus.

Kun rekisterinpitäjä on aikeissa siirtää tietoja Yhdysvaltoihin, tulisi sen huomioida käsittelyn luonne, laajuus, asiayhteys sekä rekisteröityjen oikeuksiin kohdistuvat riskit suhteessa vakiolausekkeisiin. Rekisterinpitäjän on lisäksi osoitusvelvollisuutensa puitteissa kirjattava (art. 30) kaikki henkilötietojen käsittelyprosesseista eli mitä tarkoitusta varten henkilötietoja käsitellään, mitä henkilötietoja käsitellään ja miten ne on suojattu. Myös ostopalveluna hankittavien palvelujen, kuten pilvipalvelujen käyttö, tiedot niistä henkilötiedoista, joita palvelujentarjoajat säilyttävät organisaation puolesta sekä mitä palveluissa säilytettäville henkilötiedoille tapahtuu sopimuksen päättyessä, on dokumentoitava.

Toisin kuin tietosuojaneuvoston laatimien lisäsuojatoimenpiteiden, tietosuoja-asetuksen lähestymistapa on riskiperusteinen. Tällä tarkoitetaan sitä, että rekisterinpitäjän velvoitteet ja suojatoimet tulee suhteuttaa siihen, millainen riski henkilötietojen käsittelystä voi aiheutua rekisteröidylle (art. 35). Yrityksen tulee täten käyttää henkilötietojen käsittelyyn riskienhallinnan keinoja. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat ensisijaisesti velvollisia arvioimaan henkilötietojen käsittelyyn liittyvät riskit eli tekemään arvioinnin käsittelyn vaikutuksista sekä asettamaan tunnistetuille riskeille vaadittavat hallintatoimet. Vaikutusten arviointi on pakollinen henkilötietojen käsittelylle silloin, kun suunnitteluvaiheessa on ilmeistä, että toimiin liittyy yksilöiden oikeuksien tai vapauksien kannalta merkittäviä riskejä.[95] Myös EUT:n tuomio edustaa tietosuoja-asetuksen riskiperusteistä lähestymistapaa, jossa rekisterinpitäjän on siirron arvioinnin perusteella ilmenneiden riskien mukaisesti otettava käyttöön lisäsuojatoimenpiteitä vakiolausekkeiden tueksi, taatakseen siirron EU-sääntöjenmukaisuuden.

Tietosuojaneuvoston lisäsuojatoimenpidesuosituksiin ei sisälly samanlaista riskien arviointimahdollisuutta, vaan suositukset on muotoiltu siten, että EU:sta Yhdysvaltoihin tehtyjen siirtojen kohdalla riskitaso on samanlainen siirron luonteesta riippumatta. Tämä tarkoittaa sitä, että esimerkiksi kansainväliseen konserniin kuuluvien yritysten välillä tehty työntekijää koskeva

[95] Aalto-Setälä & Viitaila 2018, 25–27.

tiedonsiirto edellyttää samantasoista suojausmenetelmää kuin siirto, jossa riskit ovat huomattavasti korkeammat.

Rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava aina, kun tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin tai kun keskeiset tehtävät muodostuvat käsittelytoimista, jotka luonteensa vuoksi edellyttävät laajamittaista ja säännöllistä rekisteröityjen seurantaa. (art. 37). Tietosuojavastaavan nimittäminen ei koske tuomioistuimia, ja yksityisellä sektorillakin ainoastaan tiettyjen toimijoiden on nimettävä tietosuojavastaava. Tietosuojavastaava on otettava riittävän varhaisessa vaiheessa mukaan kaikkiin organisaation tietosuojaa koskeviin kysymyksiin (art. 38). Hänelle on annettava tehtävän hoitoon riittävät resurssit ja pääsy kaikkiin henkilötietoihin ja niihin liittyviin käsittelytoimiin. Tietosuojavastaava valvoo, että lainsäädäntöä noudatetaan (art. 39), ja tämän vuoksi hän on avainasemassa, kun arvioidaan henkilötietojen käsittelyyn liittyviä riskejä, sillä hänen tulee tuntea sekä tietosuoja-asetuksen vaatimukset että organisaation toiminta.[96]

Vaikka tietosuoja-asetuksen velvoitteet rekisterinpitäjille ovat varsin kattavat, kasvaa samassa suhteessa haasteet valvoa näiden toimien noudattamista. Esimerkiksi Schremsille kävi ilmi Facebookin hänelle toimittaman tiedoston myötä, että Facebook rikkoo tietosuojaperiaatteen vaatimusta henkilötietojen säilytyksen rajoittamisesta (art. 5:1 e)). Laaja tiedosto sisälsi sellaistakin käyttäjätietoa, joka tulisi poistaa käsittelyn tarkoituksen toteuttamisen kannalta tarpeettomana[97]. Vaikka Facebook noudattikin tietosuojasäädöksiä sen suhteen, että sen tulee sallia rekisteröidylle pääsy sitä koskeviin tietoihin (art. 15), se toi samalla julki sen osin EU-standardien vastaisen toiminnan.

3.5 Henkilötietojen käsittelijän vastuu

Henkilötietojen käsitelijöinä toimii laaja-alainen joukko erilaisia palveluntarjoajia niin IT-, markkinointi- kuin terveydenhuoltoalueelta, joilla voi olla pääsy rekisterinpitäjän henkilötietoihin erilaisista syistä. Esimerkiksi terveydenhuoltoalalla toimiessaan yritys voi käsitellä näytteitä rekisterinpitäjän lukuun. Työajan seurantalaitteiden, biometristen laitteiden tai lääkinnällisten laitteiden valmistajia ei kuitenkaan katsota henkilötietojen käsittelijöiksi, mikäli niillä ei ole pääsyä henkilötietoihin.

[96] Aalto-Setälä & Viitaila 2018, 24–25.
[97] Hill 2012.

Jos käsittely on määrä suorittaa rekisterinpitäjän lukuun, rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi, jotta käsittely täyttää tietosuoja-asetuksen vaatimukset rekisteröidyn oikeuksien suojelusta (art. 28, kohta 1). Lisäksi henkilötietojen käsittelijän suorittamaa käsittelyä tulee määrittää esimerkiksi sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään (art. 28 kohta 3) ja rekisterinpitäjää velvoittaviin tietosuojavaateisiin. Vakiolausekkeet eivät saisi olla esteenä rekisterinpitäjälle tai henkilötietojen käsittelijälle sisällyttämästä vakiolausekkeita laajoihin sopimuskokonaisuuksiin, kuten esimerkiksi henkilötietojen käsittelijän toisen henkilötietojen käsittelijän kanssa tekemään siirtosopimukseen. Vakiolausekkeiden käytön ei tulisi myöskään olla esteenä muiden lausekkeiden lisäämiselle tai muiden suojatoimenpiteiden hyödyntämiselle, kunhan nämä eivät ole millään tavoin ristiriidassa vakiolausekkeiden kanssa eivätkä ne vaikuta rekisteröidyn oikeuksiin. Rekisterinpitäjiä ja henkilötietojen käsittelijöitä jopa suositellaan tietosuoja-asetuksessa ottamaan käyttöön lausekkeita täydentäviä sopimuksellisia lisätoimenpiteitä, jos niillä voidaan parantaa Yhdysvaltoihin siirrettyjen henkilötietojen suojan tasoa (tietosuoja-asetus, johdanto-osa 109).

Tietosuoja-asetus edellyttää, että henkilötietojen käsittelijä tiedottaa rekisterinpitäjää sellaisista olennaisista asioista, joita tämä voi tarvita rekisteröityjen oikeuksien toteuttamiseksi (art. 28:3 a)). Käytännössä tällaisia ilmoitusvelvollisuuden täyttäviä asioita voisivat olla esimerkiksi Yhdysvaltojen lainsäädännölliset muutokset, jotka estäisivät henkilötietojen käsittelijää sitoutumasta sopimuksellisiin velvoitteisiin. Mikäli henkilötietojen käsittelijä ei voisi sitoutua vakiolausekkeisiin, tarkoittaisi se tietosuojalainsäädännön rikkomusta[98], jolloin tietojen siirto Yhdysvaltoihin tulisi keskeyttää.

Sama velvoite on johdettavissa myös seuraavaan henkilötietojen käsittelijää koskevaan velvoitteeseen; henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän kirjallista ennakkolupaa. Henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista. Tiedonannon tarkoitus on antaa rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia (art. 28 kohta 2). Mikäli alkuperäisen henkilötietojen käsittelijän alihankkija ei täytä tietosuojavelvollisuuksiaan, alkuperäinen henkilötietojen käsittelijä

[98] EUT C-311/18, johdanto-osa, kohta 31.

on edelleen täysimääräisesti vastuussa alihankkijan velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.[99]

Yritykset voivat käsitellä henkilötietoja toisen lukuun, mutta samaan aikaan se voi olla itsekin rekisterinpitäjä sellaisten henkilötietojen käsittelyssä, joita se käsittelee omasta puolestaan, eikä asiakkaina olevien rekisterinpitäjien puolesta. Henkilötietojen käsittelijä voi käsitellä henkilötietoja ainoastaan rekisterinpitäjän tarkoituksiin, jolloin henkilötietojen käsittelijä ei voi ryhtyä käsittelemään rekisterinpitäjän lukuun käsiteltäviä tietoja omiin tarkoituksiinsa. Se milloin yritys on rekisterinpitäjä ja milloin yritys on henkilötietojen käsittelijä, voidaan hahmottaa seuraavien esimerkkien avulla:

a) Yritys X tarjoaa yrityksille Z ja Y asiakasrekisteriin perustuvaa markkinointiviestien välityspalvelua. Koska yritys X käsittelee viestien lähettämiseen tarvittavia asiakastietoja yritysten Z ja Y puolesta, on yritys X henkilötietojen käsittelijä.

b) Yritykset Z ja Y ovat rekisterinpitäjiä suhteessa loppuasiakkaisiinsa, markkinointiviestien toimittaminen mukaan lukien. Yritys X on rekisterinpitäjä suhteessa työllistämäänsä henkilökuntaan sekä asiakkaidensa eli yritysten Z ja Y koskevien henkilötietojen käsittelyn kautta.[100]

Jos tietojen käsittelyn kohteena olevalle henkilölle aiheutuu asetuksen vastaisista tietojen käsittelytoimista aineellista tai aineetonta vahinkoa, hänellä on oikeus saada korvaus rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut asetuksen vastaisesta käsittelystä riippumatta siitä, kuka säännöksiä on rikkonut, kun taas henkilötietojen käsittelijä on vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti sitä koskevia lainsäädännöllisiä velvoitteita tai jos se on toiminut rekisterinpitäjän ohjeiden vastaisesti. Rekisterinpitäjä tai henkilötietojen käsittelijä voi vapautua vastuusta ainoastaan, jos he voivat osoittaa, etteivät ole millään tavoin vastuussa aiheutuneesta vahingosta.

Mikäli samaan tietojenkäsittelyyn osallistuu useampi kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä, kukin heistä on vastuussa koko vahingosta suhteessa rekisteröityyn. Näin varmistetaan se, että rekisteröity saa korvauksen. Korvauksen suorittaneella rekisterinpitäjällä tai henkilötietojen

[99] Aalto-Setälä & Viitaila 2018, 31.
[100] Tietosuojavaltuutetun toimisto.

käsittelijällä on puolestaan regressio-oikeus suhteessa toisiin henkilötietojen käsittelyyn osallistuneisiin tahoihin, mikä tarkoittaa sitä, että rekisterinpitäjä ja henkilötietojen käsittelijä voivat periä muilta niiden osuuden korvauksesta, joka vastaa kunkin vastuuta aiheutuneesta vahingosta (art. 82).

3.6 Valvontaviranomaisten vastuu

Rekisterinpitäjät ja henkilötietojen käsittelijät ovat ensisijaisesti vastuussa siitä, että vakiolausekkeiden perusteella tehdyissä ekstraterritoriaalisissa tiedonsiirroissa toteutuu EU:n mukainen suoja, ja toissijaisesti vastuussa ovat valvontaviranomaiset[101]. Ennen kaikkea tämä vastuu näkyy niin rekisterinpitäjän kuin valvontaviranomaisten velvollisuutena keskeyttää EU-säädösten vastainen siirto. Tähän liittyen Irlannin High Court esitti ennakkoratkaisukysymyksen EUT:lle Schrems II -asiassa:

Jos siirron kohdemaassa tietojen tuojaan sovelletaan tarkkailulainsäädäntöä, joka on valvontaviranomaisen mukaan ristiriidassa vakiolausekkeiden tai EU-säädöksen kanssa, onko valvontaviranomaisen keskeytettävä tietojensiirrot, vai onko näiden valtuuksien käyttö rajattu vain poikkeuksellisiin tapauksiin vai voiko valvontaviranomainen käyttää harkintavaltaansa ja olla keskeyttämättä tietojensiirtoa?[102]

EUT:n mukaan, valvontaviranomaisten ensisijainen tehtävä on valvoa tietosuoja-asetuksen soveltamista ja täytäntöönpanoa. Tämän tehtävän toteuttamisella on erityinen merkitys, kun henkilötietoja siirretään EU-alueen ulkopuolelle. Tällainen siirto voi nimittäin vaikeuttaa rekisteröityjen mahdollisuuksia hyödyntää oikeussuojakeinojaan erityisesti silloin, kun tavoitteena on estää henkilötietojen päätyminen laittoman käytön tai luovuttamisen kohteeksi. EUT nosti esiin vielä sen, että valvontaviranomaiset eivät välttämättä pysty ulottamaan valvontatoimiaan EU-rajojen ulkopuolelle.[103] Näin ollen, toimivaltaisen valvontaviranomaisen tulee keskeyttää tai kieltää vakiolausekkeisiin perustuva ekstraterritoriaalinen henkilötietojen siirto, jos valvontaviranomainen katsoo kaikkien siirtoon vaikuttavien olosuhteiden valossa, ettei siirto noudata kyseisiä lausekkeita kohdemaassa. Tässä kohtaa on vielä erikseen korostettava, että valvontaviranomaiset eivät siis saa estää siirtoa viittaamalla vain suojan tason riittämättömyyteen, vaan ne voivat toimia valtuuksiensa puitteissa ainoastaan, jos siirrettyjä tietoja ei ole esimerkiksi suojattu asianmukaisesti[104].

[101] EUT C-311/18, ennakkoratkaisukysymysten tarkastelu, kohta 134.
[102] EUT C-311/18, kohta 68 ennakkoratkaisukysymys 8.
[103] EUT C-311/18, kohta 108.
[104] EUT C-311/18, kohta 118.

Schrems II -tuomio ulottuu Facebookin lisäksi kaikkiin muihinkin kansainvälisiin yrityksiin. Tämä tarkoittaa sitä, että esimerkiksi Facebook Irelandin on jatkossa keskeytettävä vakiolausekkeisiin perustuvat tietojen siirrot, jotka eivät noudata joko kyseisiä lausekkeita tai EU-säädöksiä. Toissijaisesti siirron keskeyttää valvontaviranomainen.

Kaikkia valvontaviranomaisia velvoittaa yhdenmukaisuusmekanismi, jonka mukaan asetuksen yhdenmukaisen soveltamisen edistämiseksi valvontaviranomaisten on tehtävä yhteistyötä toistensa ja tarvittaessa komission kanssa (art. 63). Jokaisen valvontaviranomaisen tulee lisäksi myötävaikuttaa asetuksen yhdenmukaiseen soveltamiseen kaikkialla unionissa ja jokaisen jäsenvaltion on varmistettava, että rekisteröityjen perusoikeuksien ja -vapauksien suojaamista valvoo riippumaton taho (art. 51, kohdat 1 ja 2).

Tietosuoja-asetuksessa edellytetään, että komissio ja valvontaviranomaiset toteutettavat Yhdysvaltojen suhteen asianmukaiset toimet, joilla kehitetään kansainvälisiä yhteistyökeinoja, jotta henkilötietojen suojaamista koskevan lainsäädännön tosiasiallista täytäntöönpanoa voidaan edistää. Asianmukaisia toimia toteuttamalla tulee tarjota keskinäistä kansainvälistä apua henkilötietojen suojaa koskevan lainsäädännön täytäntöönpanossa esimerkiksi ilmoituksella, lähettämällä valituksia käsiteltäväksi, antamalla tutkinta-apua ja vaihtamalla tietoja. Lisäksi edellytetään, että keskeiset sidosryhmät saadaan mukaan keskusteluun ja toimintaan, joilla edistetään sekä kansainvälistä yhteistyötä niin henkilötietojen suojaa koskevan lainsäädännön kuin henkilötietojen suojaa koskevien käytänteiden osalta (art. 50).

Valvontaviranomainen toimii täysin riippumattomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan. Valvontaviranomaisiin ei saa vaikuttaa ulkopuolelta suoraan eikä välillisesti heidän hoitaessaan tehtäviään, eivätkä he saa pyytää eivätkä ottaa ohjeita miltään taholta. Valvontaviranomaisten on siis pidättäydyttävä kaikesta toiminnasta, joka ei sovi yhteen heidän tehtäviensä hoitamisen kanssa (art. 52, kohdat 1–2). Valvontaviranomaisten tehtävät on lueteltu tietosuoja-asetuksen artiklassa 57. Tehtäviin kuuluu muun muassa yleisen tietoisuuden lisääminen henkilötietojen käsittelyyn liittyvistä riskeistä, neuvonta, rekisterinpitäjien ja henkilötietojen käsittelijöiden tietämyksen edistäminen koskien heidän velvoitteitaan, rekisteröityjen tekemien valitusten tutkiminen, yhteistyö eri tahojen kanssa, tutkimusten tekeminen asetuksen soveltamiseen liittyen, tieto- ja viestintäteknologian sekä kauppatapojen asiaan liittyvän kehityksen seuraaminen. Lisäksi valvontaviranomaiset hyväksyvät vakiosopimuslausekkeita, jotka ovat eri lausekkeita kuin komission hyväksymät ja Schrems II -asiassa käsitellyt lausekkeet, kannustavat sertifiointimekanismien käyttöönottoon ja osallistuvat tietosuojaneuvoston toimintaan sekä rekisterin pitämiseen asetuksen rikkomisista (art. 57).

Artiklassa 58 on vielä määritelty valvontaviranomaisen valtuudet, jotka on jaettu tutkintavaltuuksiin (kohta 1), korjaaviin toimivaltuuksiin (kohta 2) ja hyväksymis- ja neuvontavaltuuksiin (kohta 3). Valtuuksiinsa perusten, valvontaviranomainen voi esimerkiksi määrätä rekisterinpitäjän ja henkilötietojen käsittelijän antamaan kaikki tehtäviensä suorittamiseksi tarvittavat tiedot tai varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen säännösten vastaisia. Valvontaviranomainen voi myös antaa rekisterinpitäjälle neuvoja 36 artiklassa tarkoitetun ennakkokuulemismenettelyn mukaisesti.

3.7 Vakiolausekkeet ja niiden hyödyt ja haitat

Komissio on laatinut päätöksen 2010/87, joka pitää sisällään vakiolausekkeet koskien henkilötietojen siirtoa rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Kyseisillä vakiolausekkeilla tarkoitetaan komission hyväksymiä sopimuksellisia lausekkeita (art. 46:2 (c)), joilla Irlannissa sijaitseva Facebookin tytäryhtiö siirsi sen emoyhtiölle Yhdysvaltoihin käyttäjiä koskevia tietoja. Schrems II:ssa oli siis kyse näistä vakiolausekkeista ja ennen kaikkea niiden riittävyydestä unionin tasoisen suojan takaajana Yhdysvaltoihin siirretyille tiedoille.

Vuonna 2013 Maximillian Schrems teki Irlannin tietosuojavaltuutetulle kantelun, jossa hän vaati, että tämä kieltää Facebook Irelandia siirtämästä häntä koskevia henkilötietoja Facebookin Inc.:lle Yhdysvaltoihin tuolloin voimassa olleen komission 2000/520[105] päätöksen eli niin sanotun Safe Harbor -sopimuksen perusteella. Schrems katsoi, että Yhdysvalloissa voimassa olevat oikeusnormit ja -käytännöt eivät takaa sinne siirretyille henkilötiedoille riittävää suojaa viranomaisten suorittamalta sähköiseltä valvonnalta. Tietosuojavaltuutettu päätti kuitenkin hylätä kantelun vedoten Safe Harbor -sopimukseen, jossa komissio oli todennut, että Yhdysvallat takaavat riittävän tietosuojan tason. Schrems vei asian Irlannin ylempään piirituomioistuimeen High Courtiin, joka pyysi ennakkoratkaisua EUT:lta. EUT:n Schrems I -tuomion mukaan komission 2000/520 päätös oli pätemätön.[106] Jo ennen Schrems II -asiaa oli siis ilmeistä, että EU:n ja Yhdysvaltojen välillä solmittu tiedonsiirtosopimusjärjestely ei takaa riittävää suojaa Yhdysvaltoihin siirretyille eurooppalaisille tiedoille.

[105] 2000/520/EY: Komission päätös, 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.
[106] EUT lehdistötiedote, nro 91/20.

Schrems I -tuomion jälkeen, Facebook päätyi hyödyntämään siirroissaan uutta Privacy Shield -sopimusjärjestelyä sekä vakiosopimuslausekkeita. Uuden sopimusjärjestelyn osalta Schrems I toistui Schrems II -asiassa, sillä jo toistamiseen mitätöinnin kohteeksi päätyi tiedonsiirtojärjestely, joka ei suojannut EU-kansalaisten tietoja Yhdysvaltain EU-säädösten vastaisilta toimilta. Lisäksi Schrems II -tuomiossa kiinnitettiin erityistä huomioita vakiolausekkeisiin. Näiden osalta EUT korosti rekisterinpitäjien vastuuta siitä, että jatkossa vakiolausekkeiden avulla tehdyissä siirroissa on tapauskohtaisen arvioinnin mukaisesti hyödynnettävä lisäsuojatoimenpiteitä, jotta Yhdysvalloissa vallitsevaa puutteellista tietojen suojaa voidaan parantaa. Vaikka komission hyväksymissä vakiolausekkeissa (2010/87) todetaan, että vakiosopimuslausekkeet antavat riittävät takeet yksityisyyden ja yksilöiden perusoikeuksien ja -vapauksien suojaamiseksi (art. 1), katsoi EUT Schrems II -asiassa käsiteltyjen seikkojen perusteella, etteivät vakiolausekkeet voi antaa riittäviä takeita rekisteröidyn oikeuksien suojaamiseksi, sillä ne eivät sido Yhdysvaltain tiedusteluviranomaisia.

Komission mukaan, vakiolausekkeilla tehdyissä siirroissa valvontaviranomaisilla on keskeinen tehtävä sen varmistamisessa, että henkilötietoja suojataan riittävästi sen jälkeen, kun ne on siirretty Yhdysvaltoihin. Niissä poikkeustapauksissa, joissa tietojen viejä kieltäytyy antamasta tietojen tuojalle tarvittavia asianmukaisia ohjeita muodostavat rekisteröidyn oikeuksille vakavan ja välittömän vaaran. Tällöin vakiolausekkeiden olisi mahdollistettava se, että valvontaviranomaiset voivat tarkastaa tietojen tuojien ja niiden alihankkijoina toimivien käsittelijöiden toimintaa ja tarvittaessa tehdä näitä tahoja velvoittavia päätöksiä. Komission mukaan valvontaviranomaisilla on lisäksi oltava oikeus kieltää tai lykätä lausekkeisiin perustuva tietojen siirto niissä tapauksissa, joissa sopimusperusteisella siirrolla on todennäköinen ja merkittävä haittavaikutus niihin velvoitteisiin, joilla rekisteröidyn tiedoille annetaan riittävä tietosuoja.[107]

Komission 2010/87 päätöksessä määritellyt vakiolausekkeet poikkeavat selkeästi EUT:n Schrems II -tuomiosta sekä tietosuojaneuvoston lisäsuojatoimenpidesuositusten linjauksista, jossa ensisijainen vastuu siirtomenetelmien kattavuudesta unionin suojan takaajana sekä siirron keskeytysvastuusta on rekisterinpitäjillä ja vasta toissijaisesti valvontaviranomaisella[108]. Tältä osin on ymmärrettävää, että komissio halusi tehdä kiireellisesti muutoksia vakiolausekkeisiin. Vakiolausekkeiden merkittävin

[107] 2010/87, johdanto, kohdat 11 ja 12
[108] EUT C-311/18, kohta 134.

haaste siirrettyjen tietojen suojan toteutumiselle Yhdysvalloissa on niiden sitomattomuus, jota komission päivitystoimet eivät voi poistaa. Toisaalta juuri tähän haasteeseen on pyritty löytämään ratkaisuja tietosuojaneuvoston laatimilla lisäsuojatoimenpidesuosituksilla. Lisäsuojatoimenpiteiden tarkoitus olisi siis kyetä muodostamaan suojaa siirretyille tiedoille silloin, kun tietojen viejä tai tuoja on tunnistanut tarpeen tällaiselle. EUT:n ja tietosuoja-asetuksen mukaisesti, tarve tulisi käydä ilmi siirtoon kohdistuneen riskiarvioinnin myötä. Mikäli tietojen viejä ja tuoja eivät voi toteuttaa riittäviä lisätoimenpiteitä unionin tasoisen suojan varmistamiseksi, siirto ei saa toteuttaa.[109]

Vakiolausekkeiden vertailukohtana pidetään usein yrityksiä sitovia sääntöjä (art. 47). Nämä oikeudellisesti sitovat säännöt velvoittavat niin yritysryhmään kuuluvia yrityksiä kuin näiden työntekijöitäkin (art. 47 kohta 1–1 (a)), jotka toimivaltainen tietosuojaviranomainen vahvistaa tietosuoja-asetuksen 63 artiklassa säädetyn yhdenmukaisuusmekanismin mukaisesti. Vaikka vakiolausekkeita käytetään tiedonsiirroissa enemmän kuin yrityksiä sitovia sääntöjä, ovat yritykset jättäneet käyttämättä vakiolausekkeita silloin, kun se ei ole ollut pakollista. Yksinkertaisesti vakiolausekkeiden koetaan luovan tietojen viejälle ja tuojalle lisää vastuita ja velvollisuuksia, joita EU-alueen ulkopuolella ei samassa laajuudessa edellytetä, kuten yritysten tai viranomaisten henkilötietojen käsittelyä koskeva puutteellinen lainsäädäntö Yhdysvalloissa on osoittanut.

[109] EUT C-311/18, kohdat 134 ja 135.

Vakiolausekkeiden hyötyjä ja haittoja voidaan hahmottaa seuraavan taulukon avulla:

TAULUKKO 1: Vakiolausekkeiden hyödyt ja haitat.[110]

Hyödyt	Haitat
Nopea käyttöönotto.	Joustamattomuuden ja yksilöllisyyden puute.
Ei merkittävää tarvetta ehtojen uudelleenneuvotteluille.	Korvaa sopimusneuvotteluperusteisen riskinjaon.
Varmuus ehtojen lainmukaisuudesta.	Tietosuojasäännösten mukaan toimiminen on laadittu liian täsmällisten ehtojen muotoon, mikä aiheuttaa hallinnollisia esteitä.
Luo sopimuksellisen perustan kansainvälisille tiedonsiirroille.	Vakiolausekkeet eivät sovi yritysten välillä tehtyihin säännöllisiin tiedonsiirtoihin yhtä hyvin kuin esimerkiksi yrityksiä sitovat säännöt (BCR).
Voidaan käyttää tilanteissa, joissa tietojen käsittelyyn osallistuu useampi eri taho.	Vastuu ja riski on usein suurempi EU-alueella sijaitsevalla osapuolella.

Vakiolausekkeiden etuja ovat niiden ketterä käyttöönotto ja se, että ne eivät vaadi merkittävää uudelleenneuvottelua. Lisäksi ne takaavat ehtojen lainmukaisuuden, luovat sopimuksellisen perustan kansainvälisille tiedonsiirroille ja ovat sopivia tiedonsiirtotilanteisiin, joihin osallistuu useampi eri käsittelijä. Vakiolausekkeiden haittapuoli on niiden joustamattomuus, jolloin ne voidaan kokea liian jäykiksi ja osapuolten neuvottelumahdollisuuksia heikentäviksi. Vakiolausekkeet voidaan kokea myös liian täsmällisinä, jolloin yritysten liikkumavara sopimusneuvotteluissa kapenee entisestään. Lisäksi vakiolausekkeiden haittapuoleksi voi muodostua niiden epätasapainoisesti jakautunut vastuu, jossa EU:hun sijoittautuneella toimijalla on huomattavasti suurempi riski kuin toisella osapuolella. Vakiolausekkeet eivät myöskään sovi säännöllisin väliajoin tehtäviin tiedonsiirtoihin yhtä hyvin, kuin esimerkiksi yrityksiä sitovat säännöt.

3.8 Schrems II

Koska EUT oli tuominnut Schrems I -asiassa komission Safe Harbor -päätöksen (2000/520) pätemättömäksi, kumottiin tietosuojavaltuutetun Schremsin kanteluun annettu hylkäävä päätös ja asia

[110] Sharma & Menon 2020, 169.

palautettiin takaisin kyseisen tietosuojavaltuutetun tutkittavaksi. Tietosuojavaltuutettu kehotti Schremsiä muotoilemaan kantelunsa uudelleen. Uudelleen muotoillussa kantelussaan Schrems väitti, että Yhdysvallat ei tarjoa riittävää suojaa Yhdysvaltoihin siirretyille tiedoille. Tämän vuoksi Schrems vaati, että hänen henkilötietojensa siirrot EU-alueelta Yhdysvaltoihin, jotka Facebook Ireland toteutti nyt komission päätöksen 2010/87 mukaisten vakiolausekkeiden ja Privacy Shield -sopimuksen perusteella, tulisi jatkossa kieltää tai lykätä.

Tietosuojavaltuutetun asiaan liittyvän tutkinnan perusteella kävi ilmi, että Yhdysvaltoihin tehdyissä tietosiirroissa oli vaarana, että kyseisen maan tiedusteluviranomaiset käsittelivät EU-kansalaisten henkilötietoja perusoikeuskirjan kanssa yhteensopimattomalla tavalla. Lisäksi selvisi, ettei EU-kansalaisille anneta perusoikeuskirjan mukaisia oikeussuojakeinoja Yhdysvalloissa, eikä tätä puutetta voitu korjata komission hyväksymillä vakiolausekkeilla, sillä ne antoivat rekisteröidyille ainoastaan sopimukseen perustuvia oikeuksia, jotka eivät sitoneet Yhdysvaltain viranomaisia millään lailla.[111] Tietosuojavaltuutettu katsoi, että Schremsin kantelun käsittely riippui erityisesti päätöksen 2010/87 pätevyydestä, minkä vuoksi se saattoi High Courtissa vireille menettelyn, jotta High Court esittäisi asiasta ennakkoratkaisukysymyksen EUT:lle.

High Court kysyi ennakkoratkaisupyynnössään seuraavaa: sovelletaanko tietosuoja-asetusta sellaisiin henkilötietojen siirtoihin, jotka perustuvat päätöksessä 2010/87 määriteltyihin vakiolausekkeisiin, mikä on asetuksen edellyttämä tietosuojan taso tällaisen siirron kohdalla, ja mitä velvollisuuksia valvontaviranomaisilla on tällaiseen siirtoon liittyen? Lisäksi High Court esitti kysymyksen sekä päätöksen 2010/87 että päätöksen 2016/1250 eli niin sanotun Privacy Shield -sopimuksen pätevyydestä.[112]

3.8.1 Julkiasiamiehen ratkaisuehdotus

Julkisasiamies antoi asiaan oman riippumattoman ja EUT:ta sitomattoman oikeudellisen ratkaisuehdotuksensa. Julkisasiamies katsoi, että pääasiassa on kyse ainoastaan siitä, onko päätös 2010/87, jonka sisältämiin vakiolausekkeisiin Facebook on vedonnut siirtojen tueksi, pätevä. Näin

[111] EUT C-311/18.
[112] EUT lehdistötiedote, nro 91/20.

ollen, julkiasiamiehen mukaan pääasian oikeusriidan ratkaisu ei edellyttänyt, että EUT ottaisi kantaa Privacy Shield -päätöksen pätevyyteen.

Julkiasiamies ei löytänyt Schrems II -tapausta koskevien kysymysten tarkastelussa seikkoja, jotka voisivat vaikuttaa päätöksen 2010/87 pätevyyteen. Julkiasiamiehen mukaan unionin oikeutta sovelletaan siirron kohteena olevaan maahan, kun siirto tehdään kaupallisessa tarkoituksessa, vaikka kyseisen maan viranomaiset voivat käsitellä siirrettyjä tietoja kansalliseen turvallisuuteen liittyvissä tarkoituksissa. Julkiasiamies totesi lisäksi, että tietosuoja-asetuksen ekstraterritoriaalisia siirtoja koskevien säännösten tavoitteena on varmistaa henkilötietojen suojan rikkoutumaton korkea taso riippumatta siitä, tapahtuuko tietojensiirto tietosuojan riittävyydestä tehdyn päätöksen vai viejän toteuttamien asianmukaisten suojatoimien perusteella. Suojan tulee vastata tasoltaan olennaisesti EU:n tietosuoja-asetusta, jonka vuoksi komission hyväksymissä vakiosopimuslausekkeissa on vahvistettu yleinen mekanismi, jota sovelletaan kaikkiin ekstraterritoriaalisiin siirtoihin ja jota kaikkien tietojen viejien tulee tämänkaltaisissa siirroissa noudattaa.

Julkisasiamies tarkasteli vielä lähemmin päätöksen 2010/87 pätevyyttä perusoikeuskirjan kannalta. Hän katsoi, ettei komission päätös ole pätemätön, siitäkin huolimatta, että siinä esitetyt vakiolausekkeet eivät sido kohdemaan viranomaisia tai että ne voivat asettaa tietojen tuojalle lausekkeiden kanssa yhteensopimattomia velvollisuuksia. Se, onko päätös 2010/87 perusoikeuskirjan mukainen, riippuu sellaisten mekanismien olemassaolosta, joilla voidaan varmistaa, että vakiosopimuslausekkeisiin perustuvia siirtoja lykätään tai ne kielletään, jos näitä lausekkeita ei voida noudattaa. Julkiasiamiehen mukaan päätös 2010/87 on perusoikeuskirjan mukainen, sillä päätös velvoittaa rekisterinpitäjiä ja viime kädessä valvontaviranomaisia keskeyttämään tai lykkäämään siirtoa, silloin, kun siirron kohteena olevan maan lainsäädäntö ja vakiolausekkeet ovat keskenään ristiriidassa.[113]

3.8.2 EUT:n ratkaisu

EUT päätti jättää vakiolausekkeet voimaan Schrems II -tuomiossaan, mikä vastasi julkisasiamiehen näkemystä. Samalla EUT kuitenkin mitätöi Privacy Shield -sopimuksen (2016/1250) pätemättömänä ja nosti esiin vakiolausekkeiden riittämättömyyden siirron kohteena olevien henkilötietojen suojan takaamisessa Yhdysvalloissa. Näiltä osin EUT:n tuomio poikkesi julkiasiamiehen linjauksista.

Tietosuoja-asetus edellyttää, että tietoja voidaan siirtää Yhdysvaltoihin, ilman komission päätöstä kohdemaan riittävästä tietosuojan tasosta, ainoastaan silloin, jos kyseinen rekisterinpitäjä tai

[113] Julkisasiamiehen ratkaisuehdotus asiassa C-311/18.

henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on tehokkaita muutoksenhakukeinoja. EUT:n tuomioistuin arvioi Schrems II -päätöksessään, että vaikka EU-kansalaisten käytettävissä on useita oikeussuojakeinoja tilanteessa, jossa he ovat joutuneet Yhdysvaltain tiedusteluviranomaisten laittoman sähköisen valvonnan kohteeksi kansallisen turvallisuuden nimissä, on kuitenkin ilmeistä, ettei tämä koske kaikkia Yhdysvaltojen tiedusteluviranomaisten käytössä olevia oikeusperustoja, kuten toimeenpanoasetusta 12333.

Vaikka periaatteessa EU-kansalaisten käytettävissä on oikeussuojakeinoja esimerkiksi silloin, kun kyse on ulkomaisen tiedustelun valvontalain (Foreign Intelligence Surveillance Act, FISA) mukaisesta valvonnasta, ovat käytettävissä olevat kanneperusteet vähäiset. Tätä tulkintaa tukee ensinnäkin epäsuorasti se, että myös yhdysvaltalaisten kanteet jätetään tutkimatta, mikäli he eivät pysty osoittamaan oikeuttaan kanteen nostamiseen. Toisekseen tätä tulkintaa tukee suoraan se, että unionin kansalaisilla ei ole käytettävissään samoja oikeussuojakeinoja kuin Yhdysvaltojen kansalaisilla Yhdysvaltojen viranomaisten käsitellessä heidän henkilötietojaan, koska Yhdysvaltojen perustuslain (Constitution of the United States) neljäs lisäys, joka Yhdysvaltojen oikeudessa muodostaa tärkeimmän suojan lainvastaista valvontaa vastaan, ei ole sovellettavissa unionin kansalaisiin.[114] Lisäksi Yhdysvaltojen tuomioistuinvalta ei ulotu koskemaan Yhdysvaltain kansallisen turvallisuusviraston (National Security Agency, NSA) toimeenpanoasetukseen 12333 perustuvia tehtäviä, mikä samalla tarkoittaa sitä, että myöskään tältä osin EU-kansalaisilla ei ole käytettävissä oikeussuojakeinoja.

Siitäkin huolimatta, että komissio on katsonut, että Yhdysvallat takaa riittävän suojan henkilötiedoille, joita on siirretty EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa EU:sta Yhdysvaltoihin niille yrityksille, jotka ovat antaneet oman varmennuksensa, katsoi EUT, että Yhdysvaltojen lainsäädännössä ei kuitenkaan varmisteta unionin kansalaisille sellaista suojan tasoa, joka olennaisilta osin vastaisi EU:n tietosuoja-asetuksessa määriteltyä tietojen suojan tasoa, sillä Privacy Shield -järjestelyn oikeusasiamies ei ole perusoikeuskirjan 47 artiklassa tarkoitettu tuomioistuin. Toisaalta EUT huomioi, että Yhdysvaltojen oikeusjärjestyksen mukaan, Yhdysvaltojen viranomaisten mahdollinen puuttuminen niiden EU-kansalaisten perusoikeuksiin, joiden tietoja siirretään Privacy Shield -järjestelyn puitteissa Yhdysvaltoihin, tulee rajoittaa siihen, mikä on välttämätöntä oikeutetun tavoitteen saavuttamiseksi. EUT mukaan, tällaista perusoikeuksiin puuttumista vastaan on olemassa tehokkaita oikeussuojakeinoja.[115]

[114] EUT C-311/18.
[115] EUT C-311/18, johdanto-osan kohdat 115, 136, 140.

Toimeenpanoasetuksesta 12333 EUT totesi, että se mahdollistaa NSA:n pääsyn tietoihin, joita ollaan siirtämässä Yhdysvaltoihin. Toimeenpanoasetus 12333 mahdollistaa myös näiden tietojen keräämisen ja säilyttämisen jo ennen kuin niihin sovelletaan Yhdysvalloissa FISA:n säännöksiä. EUT täsmensi vielä, että toimeenpanoasetus 12333:een perustuvia toimintoja ei säännellä lailla. Siltä osin kuin kyse on tiedustelutoiminnalle asetetuista rajoituksista EU-kansalaisiin, sovelletaan Presidential policy directive 28:aa (PPD-28), jossa todetaan ainoastaan, että tiedustelutoiminnan on oltava ”mahdollisimman räätälöityä” (as tailored as feasible). Näiden seikkojen perusteella EUT katsoi, että Yhdysvallat harjoittaa valikoimatonta tietojen käsittelyä takaamatta suojaa, mikä vastaisi perusoikeuskirjan yksityis- ja perhe-elämän kunnioittamista (art. 7) ja henkilötietojen suojaa (art. 8) koskevissa artikloissa taattua suojaa. Tältä osin EUT vahvisti myös Irlannin tietosuojavaltuutetun tulkinnan. Koska Yhdysvaltoihin siirretyt eurooppalaiset henkilötiedot eivät ole samanlaisen suojan piirissa kuin EU:ssa, tulee rekisterinpitäjien arvioida tarvetta lisäsuojatoimenpiteille niiltä osin kuin tietosuojaa koskevat vakiolausekkeet eivät luonteensa vuoksi voi tarjota yli sopimusvelvollisuuksien meneviä suojatoimia.

EUT pohti Schrems II -päätöksessään vielä sitä, voidaanko komission päätöstä 2010/87 rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä tehtävistä tiedonsiiroista pitää pätevänä, koska kyseiset lausekkeet eivät ole luonteeltaan Yhdysvaltain viranomaisia sitovia eivätkä ne näin ollen korjaa puutteellista suojan tason Yhdysvalloissa. Pohdinnassaan EUT päätyi siihen, että Yhdysvaltojen lainsäädäntö voi olla perusteena tietojen siirron kieltämiselle tai lykkäämiselle, vaikka siirto toteutettaisiinkin vakiolausekkeiden ja niitä täydentävien menetelmien perusteella. Tällä EUT viittasi siihen, että kyseisen maan lainsäädäntö voi asettaa tietojen tuojalle lausekkeiden ja muiden toimenpiteiden kanssa ristiriidassa olevia velvoitteita. Vakiolausekkeiden tehokkuus sopimusmekanismina perustuu täten siihen, että vastuu suojan varmistamisesta Yhdysvaltoihin siirretyille tiedoille on ensisijaisesti EU:ssa sijaitsevalla rekisterinpitäjällä tai sen henkilötietojen käsittelijällä ja toissijaisesti valvontaviranomaisilla. Käytännössä tämä tarkoittaa sitä, että rekisterinpitäjän tai sen henkilötietojen käsittelijän on ennakoivasti jokaisen siirron kohdalla arvioitava ja tarvittaessa yhteistyössä siirron vastaanottajan kanssa tarkistettava, varmistetaanko Yhdysvalloissa siirretyille henkilötiedoille asianmukainen unionin tasoinen suoja. [116]

3.9 Euroopan komission uudet vakiolausekkeet

Euroopan tietosuojaneuvosto käsitteli vuoden 19.11.2020 pidetyssä täysistunnossaan Euroopan komission ehdotuksia kahdesta vakiolausekeluonnoksesta, joista toinen koskee rekisterinpitäjien ja

[116] EUT C-311/18, pääasia ja ennakkoratkaisukysymykset, kohdat 63, 64, 67, 133 ja 134.

henkilötietojen käsittelijöiden välisiä sopimuksia ja toinen tiedonsiirtoja kolmansiin maihin. Lisäksi tietosuojaneuvosto antoi lausunnon valmisteilla olevasta sähköisen viestinnän tietosuoja-asetuksesta eli niin sanotusta ePrivacy-asetuksesta sekä tietosuojaviranomaisten tulevasta roolista. Rekisterinpitäjien ja henkilötietojen käsittelijöiden välisiä sopimuksia koskevat vakiolausekeluonnokset ovat täysin uusia, jotka komissio on laatinut yleisen tietosuoja-asetuksen 28 artiklan 7 kohdan ja asetuksen (EU) 2018/1725 29 artiklan 7 kohdan mukaisesti. Näillä vakiolausekkeilla on EU:n laajuinen vaikutus, joiden tulisi varmistaa rekisterinpitäjien ja henkilötietojen käsittelijöiden välisten sopimusten yhdenmukaistaminen kaikkialla EU:ssa.

Komission uusien vakiolausekkeiden on tarkoitus korvata direktiivin 95/46/EY perusteella hyväksytyt kansainvälisiä siirtoja koskevat nykyiset vakiolausekkeet. Uudet lausekkeet on laadittu siksi, että ne vastaisivat paremmin yleisen tietosuoja-asetuksen vaatimuksia sekä EUT:n Schrems II -asiassa antamaa tuomiota. Päivitetyissä vakiolausekkeissa on pyritty ottamaan paremmin huomioon sellaisten uusien ja monimutkaisempien käsittelytoimien laaja-alainen käyttö, joihin osallistuu useita tietojen tuojia ja viejiä.

Komissio on pyytänyt Euroopan tietosuojaneuvostolta ja Euroopan tietosuojavaltuutetulta yhteistä lausuntoa molempien vakiolausekekokonaisuuksien luonnoksista[117]. Lisäksi vakiolausekkeet olivat avoinna yleiselle kommentoinnille 10.12.2020 saakka ja lähes 150 organisaatiota jätti mielipiteensä uudelleen muotoiltujen lausekkeiden sisällöstä. Organisaatioiden kommentit koskivat muun muassa vakiolausekeluonnosten kohtaa 19, joka koskee tietojen siirtämistä ja käsittelyä. Sen mukaan käsittelyn tulee olla sallittua ainoastaan silloin, kun kolmannen maan lainsäädäntö ei estä tietojen tuojaa sitoutumasta vakiolausekkeisiin. Tähän liittyen kohtaa 19 on pyydetty muokkaamaan EUT:n ja tietosuojaneuvoston linjaa vastaavaksi. Kommenteissa on esitetty, että tietosiirrot voitaisiin toteuttaa, vaikka kohdemaan lainsäädäntö olisikin ristiriidassa EU:n tietosuojavaateiden kanssa, kunhan siirrossa käytetään riittäviä lisäsuojamenetelmiä, kuten tietojen salausta.

Tärkeäksi kohdaksi kommenteissa muodostui myös vakiolausekeluonnosten kohta 24, joka koskee siirtymäaikaa. Luonnosten siirtymäajaksi on asetettu yksi vuosi, minkä lisäksi yritysten edellytetään ottavan uudet vakiolausekeluonnokset osaksi kaikkia tiedonsiirtosopimuksiaan aina, kun sopimuksiin tehdään olennaisia muutoksia. Useat kommentit viittaavat siihen, että yritykset kokevat siirtymäajan liian lyhyeksi, ottaen huomioon, että organisaatioiden tulisi neuvotella uudelleen kaikki sopimukset, myös kolmansia osapuolia koskevat, mikäli ne sisältävät vakiolausekkeet. Tämä voi asettaa pienet ja keskisuuret yritykset haastavaan asemaan, niiden joutuessa neuvottelemaan sopimuksia uusiksi isojen

[117] Tietosuojavaltuutetun toimisto 2020.

toimijoiden kanssa. Lisäksi komissiota on pyydetty täsmentämään mitä vakiolausekeluonnosten ”olennainen” ja ”epäolennainen” sopimusmuutos termeillä tarkalleen ottaen tarkoitetaan. Kommenteissa myös kysytään miksi tietojen viejän tulisi sopimusmuutostilanteessa laatia tiedonsiirtosopimukset kokonaan uudelle perustalle, kun kyse on pääasiassa tehokkaampien tietoturvamenetelmien lisäämisestä sopimukselle. Kaiken kaikkiaan, edellytys sopimuksen pysymisestä muuttumattomana koetaan liian jäykäksi ehdoksi. Esiin on nostettu myös vakiolausekkeiden ja tietosuojaneuvoston laatimien lisäsuojatoimenpidesuositusten osin päällekkäisyys, sillä vakiolausekeluonnosten koetaan sisällön perusteella vain toistavan lisäsuojatoimenpidesuosituksia. Lisäksi on kommentoitu lausekkeiden potentiaalisia haittavaikutuksia eurooppalaisen digitaalitalouden kehittymiselle sekä sitä, että lausekkeista puuttuu tietosuoja-asetuksen mukainen riskiperusteinen lähestymistapa ja oikeasuhteisuus tavoiteltuun päämäärään nähden.[118]

Uusien vakiolausekkeiden kompastuskiveksi voi koitua liiallinen kiire. Komissiolle luodaan painetta useasta suunnasta, kun eri organisaatiot niin EU-alueella kuin Yhdysvalloissa, odottavat kuumeisesti ratkaisuja, joilla yritykset voisivat siirtää tietoja ilman liiallista hallinnollista taakkaa. Toistaiseksi vaikuttaa siltä, että komission laatimien uusien lausekkeiden todellinen lisäarvo yrityksille jää heikoksi. Vakiolausekeluonnosten edellytys siitä, että siirto voidaan toteuttaa ainoastaan, jos kolmannen maan lainsäädäntö ei estä tietojen tuojaa sitoutumasta lausekkeisiin on vaikea sovittaa EU:n ja Yhdysvaltojen välisiin tietosiirtoihin. Yhdysvaltojen lait eivät sääntele omiin tai EU-kansalaisiin kohdistuvia tiedusteluviranomaisten valvontatoimia, vaan viranomaiset voivat harjoittaa sähköistä valvontaa vapaasti ja tunkeutua EU-kansalaisten yksityisyyttä koskeviin oikeuksiin ilman seuraamuksia.

Komission vakiolausekeluonnosten sisällön istuttaminen nykyiseen tilanteeseen tarkoittaisi sitä, ettei tietosiirtoja voida tehdä, ei ainakaan EU-säädösten mukaisesti. Uusien vakiolausekeluonnosten osalta on myös huolestuttavaa, että yritysten edellytetään ottavan uudet lausekkeet osaksi liiketoimintojaan varsin lyhyen siirtymäajan puitteissa. Yrityksillä on valtavat määrät sopimuksia, joiden läpikäyminen ja päivittäminen tuntuu mahdottomalta määritellyn siirtymäajan puitteissa. Vakiolausekkeille on paikkansa, mutta ennen kuin ne velvoittavat yrityksiä ja organisaatioita, tulisi ne olla huolella laaditut, jotta ne vastaisivat yritysten todelliseen tarpeeseen. On olemassa riski, että vakiolausekeluonnokset muodostuvat vain hallinnolliseksi lisäsuojatoimenpiteitä toistavaksi taakaksi, jotka yritykset haluavat kiertää kaukaa. Toisaalta tämä voi kannustaa yrityksiä käyttämään muita siirtomekanismeja, joka

[118] Palaute vakiosopimuslausekkeiden säädösluonnoksesta, 2020.

puolestaan kaventaa vakiolausekkeiden oikeudellista alaa. Kuten EUT totesi Schrems II -tuomiossaan, vakiolausekkeiden pyrkimys on ainoastaan tarjota EU:hun sijoittautuneille rekisterinpitäjille tai henkilötietojen käsittelijöille sopimukseen perustuvia suojatoimia, joita voidaan soveltaa yhtenäisesti kaikissa EU:n ulkopuolisissa maissa, riippumatta siirron kohteena olevan maan tietosuojan tasosta. Tarvittaessa näitä suojatoimia rekisterinpitäjä tai henkilötietojen käsittelijä voivat täydentää muilla menetelmillä.[119] Tältä kannalta katsoen, EUT:n mukaan yrityksille tulisi sallia niiden riskiperusteiseen lähestymistapaan nojaava sopimuksellinen liikkumavara, jossa suojatoimien tietojen viejää ja tuojaa koskevia edellytyksiä ei ole laadittu liian kapea-alaisesti.

[119] EUT C-311/18, kohta 133.

4 Lisäsuojatoimenpiteet

Lisäsuojatoimenpiteiden todellisen tarpeen voi katsoa konkretisoituineen Schrems II -tuomion myötä EUT:n korostaessa vakiolausekkeiden riittämättömyyttä unionin tasoisen suojan varmistajana. Tuomion jatkotoimena perustettiin työryhmä, joka laati lisäsuojatoimenpiteitä koskevat suositukset, jotka ovat olleet julkisen kuulemisen kohteena, mutta joita ei vielä ole hyväksytty käytäntöön[120]. Suositusten tarkoitus on auttaa tietojen viejiä tunnistamaan ja arvioimaan täydentävien toimenpiteiden tarpeellisuutta silloin, kun he siirtävät tietoja vakiolausekkeita tai muita 46 artiklan mukaisia mekanismeja käyttäen[121] Yhdysvaltoihin, jossa tietosuojan taso ei vastaa EU:n tasoa.

Tietosuojaneuvoston laatimiin lisäsuojatoimenpidesuosituksiin sisältyy etenemissuunnitelma tietojen viejien selvitystyötä varten, joka on jaettu kuuteen eri vaiheeseen. Suosituksiin sisältyy lisäksi luettelo lisäsuojamenetelmistä, jotka on jaettu teknisiin, sopimusoikeudellisiin ja organisatorisiin toimiin sekä tyypillisimpiin ekstraterritoriaalisia henkilötietojen siirtotilanteita koskeviin esimerkkeihin.[122]

4.1 Etenemissuunnitelma ja rekisterinpitäjän arviointi- ja osoitusvelvollisuus

Suositusten myötä tietojen viejille on muodostunut tietosuoja-asetuksessa määriteltyä vaikutusten arviointia (art. 35) laajempi vastuu tehdä kattavan selvitystyön tekemisestä aikoessaan siirtää eurooppalaisia henkilötietoja Yhdysvaltoihin. Tämä näkyy suosituksissa erityisesti siten, että tietojen viejien tulisi huomioida arvioinnissaan kaikki siirtoon vaikuttavat olosuhteet[123]. EUT totesi Schrems II -päätöksessä, että mikäli komission vastaavuuspäätöstä ei ole tehty (46:1), rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja EU-alueen ulkopuolelle, eli tässä tapauksessa Yhdysvaltoihin, ainoastaan silloin, jos rekisteröityjen saatavilla on riittäviä oikeussuojakeinoja ja kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, kuten käyttänyt vakiolausekkeita (46:2). Näiden molempien, asianmukaisten suojatoimenpiteiden ja rekisteröityjen oikeussuojakeinojen on varmistettava, että EU-kansalaisten, joiden henkilötietoja siirretään Yhdysvaltoihin, saavat olennaisilta osin unionin tasoisen suojan. Jotta tämä suoja toteutuu, on suojan arvioinnissa huomioitava muun muassa EU:hun sijoittautuneen tietojen viejän ja Yhdysvaltoihin sijoittautuneen tietojen tuojan välillä sovitut sopimusmääräykset. Lisäksi arvioinnissa

[120] Tietosuojavaltuutetun toimisto.
[121] Euroopan tietosuojaneuvoston 37. täysistunto, 2020.
[122] Atallah, 2020.
[123] Euroopan tietosuojaneuvoston suositukset 01/2020, 2.

tulee ottaa huomioon maan oikeusjärjestelmä siltä osin kuin kyse on kohdemaan viranomaisten mahdollisesta pääsystä siirrettyihin henkilötietoihin.[124]

Tehdyn arvioinnin tarkoitus on siis selvittää, voidaanko siirto Yhdysvaltoihin toteuttaa siten, että se täyttää EU-oikeuden sille asettamat vaateet eli toisin sanoen varmistaa, ettei Yhdysvaltain lainsäädäntö asetus siirrossa hyödynnettävien siirtovälineiden kanssa ristiriitaan. Täten on myös mahdollista, että tehty arviointi osoittaa, ettei siirron kohteena oleville tiedoille voida taata riittävää suojaa Yhdysvalloissa, jolloin siirtoa ei saa aloittaa tai mikäli se on jo aloitettu, tulee se EU-säännösten vastaisena keskeyttää.[125]

Tietojen viejän tulisi jatkuvaluonteisesti, sopimuksellisia, teknisiä ja organisatorisia toimenpiteitä hyödyntäen pyrkiä takaamaan unionin tasoinen suoja siirretyille tiedoille sekä myös konkreettisesti osoittamaan, että se on toimillaan pyrkinyt tähän tavoitteeseen. Tällä tietosuojaneuvosto viittaa rekisterinpitäjän osoitusvelvollisuuteen (tietosuoja-asetus, art. 5). Schrems II -tuomiossaan EUT korosti, että tietojen viejien ja tuojien vastuulla on varmistaa, että tietojen käsittely vastaa EU:n tietosuojalainsäädäntöä.[126] Näin ollen, tietojen viejää velvoittavat yleiset periaatteet tulisi sitouttaa sopimuksella myös tietojen tuojaa koskeviksi. Periaatteiden mukaan siirroissa tulisi varmistua, että

a) henkilötietoja käsitellään lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi,

b) käyttötarkoitussidonnaisuusperiaatteen mukaisesti henkilötietoja kerätään tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä käsitellä myöhemmin näiden tarkoitusten kanssa,

c) tietojen minimointiperiaatteen mukaisesti, henkilötiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään,

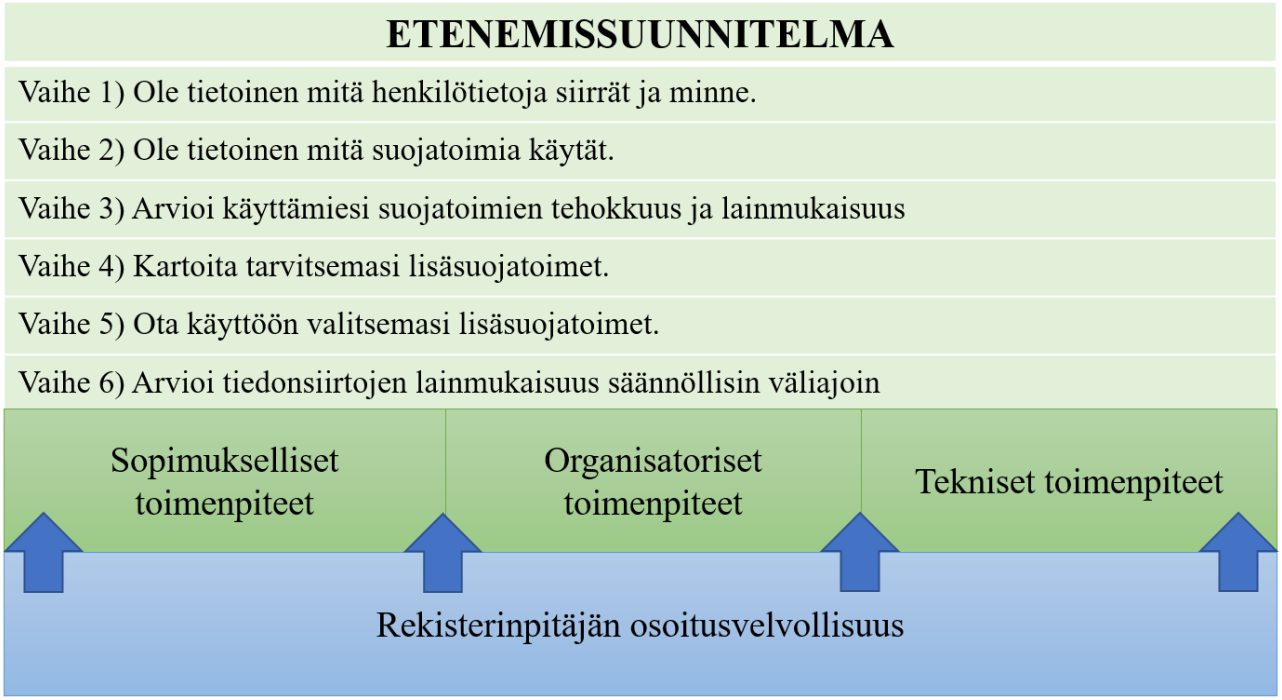
d) henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Tätä varten rekisterinpitäjän tulee toteuttaa kaikki mahdolliset, mutta kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat tai virheelliset henkilötiedot poistetaan tai oikaistaan,

e) henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten,

[124] EUT C-311/18, kohta 203.
[125] EUT C-311/18, kohdat 141 ja Euroopan tietosuojaneuvoston suositukset 01/2020, 3.
[126] EUT C-311/18, kohta 142, Euroopan tietosuojaneuvoston suositukset 01/2020, 7.

f) henkilötietoja käsitellään siten, että henkilötietojen asianmukainen turvallisuus varmistetaan, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (art. 5).

Etenemissuunnitelma konkretisoi rekisterinpitäjän osoitusvelvollisuutta, sillä sen tulee dokumentoida arviointinsa huolellisesti ja perusteellisesti[127]. Etenemissuunnitelma sisältää kuusi vaihetta, joita seuraamalla EU:ssa sijaitsevan tietojen viejän on tarkoitus selvittää, tarvitseeko kyseessä olevassa siirrossa hyödyntää lisäsuojatoimenpiteitä ja jos tarvitsee millaisia.



KUVIO 4: Lisäsuojatoimenpiteet ja rekisterinpitäjän osoitusvelvollisuus.

Ensimmäisessä vaiheessa tietojen viejien tulee kartoittaa kaikki tiedonsiirrot eli tietojen viejien tulee olla tietoisia, minne henkilötietoja siirretään. Tämän lisäksi tietojen viejän on varmistettava, että tiedonsiirto on asianmukainen ja oikeasuhtainen suhteessa siihen tarkoitukseen, minkä vuoksi tietoja siirretään Yhdysvaltoihin. *Toisessa vaiheessa* rekisterinpitäjän tulee tuntea käyttämänsä siirtotyökalut eli mitä 46 artiklan siirtomenetelmistä tietojen viejä aikoo käyttää. *Kolmannessa vaiheessa* tietojen viejien tulee arvioida valitsemiensa suojatoimien tehokkuutta ja lainmukaisuutta. Kun siirron kohteena on Yhdysvaltojen kaltainen maa, jonka tietosuojan tason riittävyydestä ei ole tehty komission vastaavuuspäätöstä, tulisi tietojen viejän kompensoida tätä puutteellisuutta

[127] Euroopan tietosuojaneuvoston suositukset 01/2020, johdanto, 2–3.

asianmukaisten toimenpiteiden, kuten vakiolausekkeiden ja lisäsuojatoimenpiteiden avulla. Tämä tarkoittaa esimerkiksi tietojen viejän ja tuojan välisen sopimussuhteen kannalta katsoen sitä, että tietojen viejää velvoittavat tietosuoja-asetuksesta johdetut velvoitteet tulisi sitoa myös Yhdysvalloissa sijaitsevaa tietojen tuojaa. Käytännössä tietojen viejän tulee siis selvittää, mahdollistaako Yhdysvaltojen lainsäädäntö sen, että siirron vastaanottaja voi noudattaa komission päätöstä 2010/87 tietosuojaa koskevista vakiolausekkeista. Tietojen viejän tulisi ensisijaisesti keskittyä niihin oikeusnormeihin, jotka voivat heikentää siirrettävien tietojen suojaa[128] eli rekisteröidyn oikeutta yksityisyyteen. Vastuu on myös tietojen tuojalla, sillä sen tulee ilmoittaa tietojen viejälle, mikäli se ei jostain syystä voi sitoutua lausekkeisiin johtuen.[129]

EUT:n mukaan Yhdysvaltojen viranomaiset saavat unionista Yhdysvaltoihin siirrettyjä henkilötietoja ja käyttävät näitä tietoja FISA:n 702 §:n nojalla perustettujen PRISM- ja UPSTREAM-tarkkailuohjelmien puitteissa sekä toimeenpanoasetuksen 12333:n perusteella[130]. Yhdysvaltojen takaaman tietosuojan taso on kyseenalaistettu nimenomaan sillä perusteella, että FISA:n 702 §:ään ja toimeenpanoasetukseen 12333 perustuvista tarkkailuohjelmista johtuvia puuttumisia eivät koske vaatimukset, joilla suhteellisuusperiaatteen asettamissa rajoissa varmistetaan EU:n perusoikeuskirjan mukaisten yksityiselämän art. 7) ja henkilötietojen suojaa (art. 8) koskevien oikeuksien suoja. Toisin sanoen, Yhdysvaltain tiedusteluviranomaisten harjoittama valvonta rikkoo perusoikeuskirjan mukaisiin perusoikeuksien rajoittamisiin ulottuvaa välttämättömyyden vaatimusta suhteessa tavoiteltuun vaarantaen EU-kansalaisten oikeutta yksityisyyteen.

Mikäli kolmas vaihe on osoittanut, että tietojen viejän valitsemat siirtomenetelmät eivät ole riittäviä takaamaan unionin tasoista suojaa, tulee sen *neljännessä vaiheessa* tunnistaa tarvitsemansa lisäsuojatoimenpiteet[131]. Toisaalta Yhdysvaltoihin vakiolausekkeilla tehtyjen siirtojen kohdalla lisäsuojatoimenpiteet ovat EUT:n Schrems II -tuomiossa todetun mukaisesti tarpeellisia lausekkeiden heikon tietojen suojaamiskyvyn vuoksi, tosin kunkin siirron luonteesta riippuen. Kolmannen vaiheen voisi kuitenkin katsoa olevan Yhdysvaltojen kohdalla tarpeeton niin kauan kuin maan tiedustelulainsäädäntö sallii valikoimattoman sähköisen valvonnan, sillä vakiolausekkeet eivät kykene estämään tiedusteluviranomaisten pääsyä EU-kansalaisia koskeviin tietoihin.

[128] Euroopan tietosuojaneuvoston suositukset 01/2020, 12.
[129] EUT C-311/18, kohta 142, Euroopan tietosuojaneuvoston suositukset 01/2020, 7.
[130] EUT C-311/18, kohta 165.
[131] Euroopan tietosuojaneuvoston suositukset 01/2020, 15.

Tukeakseen tarpeellisten ja olennaisten lisäsuojatoimenpiteiden tunnistamista, tietojen viejä voi ennen siirtoa ja yhteistyössä Yhdysvalloissa sijaitsevan tietojen tuojan kanssa, selvittää seuraavia siirtoon liittyviä seikkoja:

- siirrettävien tietojen tallennusmuoto
- tietojen luonne
- tietojen käsittelyketjun pituus ja kompleksisuus
- mahdollisuus, että tietoja siirretään edelleen joko kolmannen maan sisällä tai muihin kolmansiin maihin.

Tietojen viejä voi myös yhdistää sopimuksellisia, organisatorisia kuin teknisiäkin toimenpiteitä, ja pyrkiä tällä tavoin tehostamaan katkeamattoman suojan saavuttamista Yhdysvaltoihin tehdyissä tietosiirroissa. [132]

Viidennessä vaiheessa tietojen viejän tulee ottaa käyttöön kaikki valitsemansa lisäsuojamenetelmät. Sen ei tarvitse pyytää varmistusta valituille lisämenetelmille valvontaviranomaiselta, kunhan käyttöön otetut lisäsuojatoimenpiteet eivät ole ristiriidassa vakiolausekkeiden kanssa ja ne ovat riittäviä takaamaan tietosuoja-asetuksen mukaisen suojan siirrettäville henkilötiedoille. Mikäli tietojen viejä päätyy muuttamaan vakiolausekkeita itse tai sen jo ennalta lisäämät lisämenetelmät ovat ristiriidassa vakiolausekkeiden kanssa, ei sen tulkita enää noudattavan vakiosopimuslausekkeita. Tällöin tietojen viejän on haettava tietosuojavalvontaviranomaiselta lupaa, jolla viitataan tietosuoja-asetuksen 46:3 artiklan alakohtaan a), jonka mukaan viranomaisen luvalla asianmukaisia suojatoimia voivat olla myös tietojen viejän ja tuojan väliset sopimuslausekkeet. *Kuudennessa eli viimeisessä vaiheessa* edellytetään vielä, että tietojen viejä arvioi säännöllisin väliajoin suojan riittävyyttä sekä tarkkailee kaikkia suojaan vaikuttavia olosuhteita.[133]

4.2 Esimerkkejä lisäsuojatoimista

Tietosuojaneuvoston lisäsuojatoimenpiteitä koskevan dokumentin liitteessä kaksi on laadittu esimerkinomainen lista teknisistä, sopimuksellisista, ja organisatorisista lisäsuojatoimista. Ohjeistuksessa todetaan, että lista ei ole tyhjentävä. Tämän voi tulkita tukevan tietosuoja-asetuksen johdanto-osan 109 kohdassa todettua, jonka mukaan rekisterinpitäjän käyttämät vakiolausekkeet, eivät saisi estää rekisterinpitäjää lisäämästä muita lausekkeita tai toteuttamasta muita suojatoimia.

[132] Euroopan tietosuojaneuvoston suositukset 01/2020, 16.
[133] Euroopan tietosuojaneuvoston suositukset 01/2020, 2 ja 17–19.

Tätä viestiä EUT toi esiin myös Schrems II -tuomiossaan, jossa se totesi, että rekisterinpitäjiä olisi kannustettava tarjoamaan lisäsuojaa, joilla täydennetään tietosuojaa koskevia vakiolausekkeita[134], ja johon viitataan myös etenemissuunnitelman vaiheessa 5.

4.2.1 Tekniset toimenpiteet

Teknisten menetelmien merkityksellisyys Yhdysvaltojen kohdalla nousee esiin juuri FISA:n 702 §:een ja toimeenpanoasetus 12333:een perustuvien tarkkailuohjelmien myötä. Näiden oikeussäännösten lisäksi Yhdysvaltojen PPD-28 mahdollistaa ”valikoimattoman” tietojen keruun mikä tarkoittaa sitä, että tietoja kerätään laaja-alaisesti signaalitiedustelun avulla, jossa tiedusteluyhteisöllä ei ole käytössään tiettyyn kohteeseen liittyvää tunnistetta. Tietojen keruuta ei siis voida kohdentaa nimenomaiseen kohteeseen.[135] Näin ollen, FISA 702 §, toimeenpanoasetus 12333 ja PPD-28 yhdessä, eivät täytä niitä vähimmäisvaatimuksia, jotka EU-oikeudessa liittyvät suhteellisuusperiaatteeseen. Koska tarkkailuohjelmia ei mainittujen säännösten perusteella voida rajata vain välttämättömään[136], ovat EU:n todelliset keinot unionin tasoisen suojan takaamisessa Yhdysvalloissa vähäiset. Lisäsuojatoimenpiteillä on haastavaa yrittää vaikuttaa toisen maan lainsäädäntöön, vaikkakin sillä voi olla rajoitteita luova vaikutus viranomaisten yrityksiin päästä eurooppalaisiin tietoihin.

Tietosuojaneuvoston laatimia esimerkkejä teknisistä menetelmistä ovat:

1. tietojen tallennus varmuuskopiointia varten,
2. tiedon pseudonymisointi,
3. tiedon salaus silloin, kun tiedot ainoastaan kulkevat kolmannen maan kautta,
4. suojattu vastaanottaja, jolla pyritään varmistamaan, että tieto on suojattu siirron alusta loppuun asti. Viestin saa auki ainoastaan tietojen tuoja, jolla on salausavain.
5. Jaettu käsittely tai useamman tahon tietojen käsittely, tarkoittaa tilannetta, jossa tietojen viejä haluaa, että kaksi toisistaan riippumatonta ja eri oikeudenkäyttöalueilla sijaitsevaa käsittelijää käsittelevät tietoja. Ennen siirtoa tietojen viejä hajauttaa tiedon ennen siirtoa siten, ettei tietoja voida kohdentaa tiettyyn rekisteröityyn ilman lisätietoja. [137]

Edellä kuvattuihin tarkkailuohjelmia sääntéleviin normeihin perustuen ja suositusten sisältöä tulkiten, EU-kansalaisia koskevien tietojen siirtyessä Yhdysvaltoihin, tietojen tulisi olla aina salattu tai

[134] EUT C-311/18, kohta 132.
[135] EUT C-311/18, kohta 49.
[136] EUT C-311/18, kohta 184.
[137] Euroopan tietosuojaneuvoston suositukset 01/2020, 22–27.

pseudonymisoitu, jotta suoja olisi mahdollisimman kattava. Suosituksissa edellytetään lisäksi, että salausavaimen tulisi sijaita EU:ssa tai jollain toisella toimialueella, joka takaa riittävän tietojen suojan. Käytännössä tällainen vaatimus tarkoittaa suhteettoman korkeaa teknistä vaatimusta tietojen viejille[138], huomioiden tietosiirtojen erilaisen luonteen ja tästä johdetun vaihtelevan riskitason.

Tietosuojaneuvosto on esittänyt myös kuvaukset tietojensiirtotilanteista, jotka mahdollistavat Yhdysvaltain viranomaisten välittömän pääsyn tietoihin:

6. Tietosiirto pilvipalveluiden tarjoajille, jotka edellyttävät selkeässä muodossa oleviin henkilötietoihin pääsyä.
7. Liiketoimintatarkoituksessa myönnetty etäkäyttöoikeus tietoihin.[139]

Kohdat 6 ja 7 ovat nimenomaan sellaisia, joiden mukaan useat eri yritykset toimivat EU:n ja Yhdysvaltojen välillä. Esimerkiksi silloin, kun työtekijöitä koskevia tietoja siirretään EU:n ja Yhdysvaltojen välillä, toteutetaan se hyvin usein kohtien 6 ja 7 mukaisesti. Näin määriteltynä vaikuttaa kovin ilmeiseltä, että tietosuojaneuvosto katsoo ainoastaan teknisten menetelmien olevan riittävä lisäsuojatoimenpide takaamaan Yhdysvaltoihin siirretyille EU-kansalaisia koskeville henkilötiedoille unionin tasoinen suoja.[140] Niin sanottu yhden mallin -periaate, jossa kaikki siirrot tulisi suojata teknisin menetelmin on mahdotonta sovittaa yritysten nykyisiin toimintamalleihin.

4.2.2 Sopimusoikeudelliset toimenpiteet

Sopimusoikeudelliset toimenpiteet koostuvat yleensä yksipuoleisista, kaksipuoleisista tai monipuoleisista sopimusoikeudellisista velvoitteista ja ne sitovat EU:hun sijoittautunutta rekisterinpitäjää ja Yhdysvaltoihin sijoittautunutta henkilötietojen siirron vastaanottajaa, jos he ovat tehneet näiden velvoitteiden mukaisen sopimuksen. Tietosuojaneuvosto on koostanut suosituksiin esimerkkejä täydentävistä sopimuslausekkeista, joita ovat läpinäkyvyyttä, teknisiä menetelmiä ja erityisiä toimenpiteitä koskevat velvoitteet ja rekisteröidyn oikeuksien suojaamista koskevat velvoitteet. Tietojen viejä voi sopimuksella sitouttaa tietojen tuojan näihin kaikkiin. *Teknisillä menetelmillä* sopimusvelvoitteena tarkoitetaan sitä, että tietojen viejien tulisi sopia tiedonsiirtoja koskevissa sopimuksissaan teknisistä menetelmistä, silloin kuin tietojen viejä on tunnistanut tarpeen tällaisille.[141] Yhdysvaltoihin tehtyjen siirtojen osalta tulee kuitenkin huomioida teknisten

[138] Yhdysvaltojen kauppakamari 2020.
[139] Euroopan tietosuojaneuvoston suositukset 01/2020, 28.
[140] Yhdysvaltojen kauppakamari 2020.
[141] Euroopan tietosuojaneuvoston suositukset 01/2020, 28–30.

menetelmien, jopa oletusarvoinen käyttöönotto, mikä tavallaan mitätöi tarpeen tietojen viejän itsenäiseltä arvioinnilta.

Läpinäkyvyysvelvoitteilla puolestaan tarkoitetaan sitä, että tietojen viejä voi lisätä liitteitä sopimukseen, jotka sisältävät tietojen tuojan parhaansa mukaan laatimia ja antamia tietoja Yhdysvaltain viranomaisten pääsystä henkilötietoihin. Tietojen viejä voi velvoittaa tietojen tuojaa myös

- listaamaan Yhdysvaltain lait ja säännökset, jotka sitovat tietojen viejää,
- antamaan tietoja ja tilastoja perustuen tietojen tuojan kokemuksiin tai raportteihin eri lähteistä, mikäli viranomaisten tietoihin pääsyä sääntelevää lakia ei ole,
- osoittamaan mitkä menetelmät on otettu käyttöön estääkseen viranomaisten tietoihin pääsy,
- antamaan yksityiskohtaiset tiedot koskien kaikkia viranomaisten pyyntöjä päästä tietoihin ja
- erittelemään, missä määrin tietojen tuoja voi lain mukaan olla luovuttamatta siirrettyjä tietoja Yhdysvaltain viranomaisille.

Tietosuojaneuvosto korostaa tietojen tuojan todistustaakkaa siitä

- ettei tietojen tuoja ole tarkoituksellisesti luonut mahdollisuutta viranomaisille päästä tietoihin,
- ettei se ole tarkoituksellisesti luonut tai muuttanut liiketoimintaprosessejaan tavalla, joka sallisi tietoihin pääsyn viranomaisille,
- ettei Yhdysvaltain laki tai käytäntö edellytä tietojen tuojaa luomaan keinoja päästä tietoihin, kuten esimerkiksi luovuttamaan salausavaimen.[142]

Erityisiä toimenpiteitä koskevilla sopimusvelvoitteilla tietosuojaneuvosto ohjeistaa tietojen viejää sitouttamaan tietojen tuojan arvioimaan Yhdysvaltain lainsäädäntöä suhteessa viranomaisten pyyntöihin päästä tietoihin. Viimeinen täydentävä sopimuslauseke koskee *rekisteröidyn oikeuksien suojaamista* mikä edellyttää EU:ssa rekisteröidyn henkilön etukäteistä suostumusta, ennen kuin häntä koskevia tietoja voidaan siirtää Yhdysvaltoihin[143].

4.2.3 Organisatoriset toimenpiteet

Täydentävät organisatoriset toimenpiteet voivat koostua sisäisistä käytännöistä, organisatorisista menetelmistä ja standardeista, joita tietojen viejät voivat soveltaa itse sekä ulottaa näitä myös tietojen tuojiin. Organisatoriset menetelmät voivat parantaa siirrettävien tietojen suojan johdonmukaisuutta

[142] Euroopan tietosuojaneuvoston suositukset 01/2020, 28–30.
[143] Euroopan tietosuojaneuvoston suositukset 01/2020, 32–35.

sekä tietojen viejien tietoisuutta Yhdysvaltoihin tehtäviin tietosiirtoihin liittyvistä riskeistä. On ilmeistä, etteivät organisatoriset menetelmät voi suoraan taata tietojen siirron EU-sääntöjenmukaisuutta, mutta niitä voidaan hyödyntää sopimuksellisia ja teknisiä menetelmiä täydentävinä.

Organisatorisiin menetelmiin kuuluvilla sisäisillä käytänteillä voidaan hallinnoida ekstraterritoriaalisia tietojen siirtoja. Käytännössä siirtojen hallinnoinnilla tarkoitetaan sisäisten prosessien ja standardoitujen menetelmien laadintaa tilanteisiin, joissa Yhdysvaltain viranomaiset ovat esittäneet virallisen pyynnön tietoihin pääsystä. Organisaatioiden muita käytänteitä voivat olla koulutukset, joissa huomioidaan Yhdysvaltain lait, joille tietojen tuoja on alisteinen. Koulutusten yhteydessä tietosuojaneuvosto viittaa EU:n tietosuojaa koskevien edellytysten huomioimiseen, erityisesti EU:n perusoikeuskirja artiklaan 52:1, jonka mukaan perusoikeuskirjassa tunnustettuja oikeuksia ja vapauksia voidaan rajoittaa vain välttämättömin perustein.[144] Organisatorisiin menetelmiin kuuluvat myös läpinäkyvyys ja osoitusvelvollisuus, jotka yhdessä edellyttävät, että kaikki siirrettäviin tietoihin kohdistuneet viranomaispyynnöt sekä niihin annetut vastaukset, kuten pyyntöjä käsittelevän työryhmän arviointi, tulee tallentaa. Näiden kirjausten tulisi olla tietojen viejän käytettävissä, jonka puolestaan tulisi tarvittaessa antaa ne rekisteröidylle, jonka tiedoista on kyse.

Tietojen minimointi on johdettu suoraan tietosuoja-asetuksen rekisterinpitäjän osoitusvelvollisuudesta (art. 5). Tietojen minimoinnilla tietosuojaneuvosto viittaa tietojen käytön rajoittamiseen esimerkiksi silloin, kun tietoihin on myönnetty vain rajattu käyttöoikeus, kuten etäkäyttö. Tällöin tietoja ei tulisi olla välttämätöntä siirtää lainkaan tai siirto voisi rajoittua vain osaan tiedoista. Organisatorisiin menetelmiin kuuluvat myös standardien soveltaminen ja parhaat käytännöt, joilla tietosuojaneuvosto tarkoittaa tarkasti määriteltyjä käytäntöjä, jotka koskevat tietoturvaa ja yksityisyyttä. Nämä käytännöt perustuvat EU-sertifiointeihin tai kansainvälisiin standardeihin (International Organization for Standardization, ISO) ja parhaisiin käytäntöihin (Euroopan Unionin kyberturvallisuusvirasto, ENISA).[145] Organisatoriset toimenpiteet vastaavat sisällöllisesti hyvin pitkälti niitä toimenpiteitä, joita organisaatiot ovat ottaneet käyttöön uuden tietosuoja-asetuksen ja ennen kaikkea siinä määriteltyjen rekisterinpitäjää koskevien velvoitteiden myötä. Yleisesti arvioiden, organisatorisilla menetelmillä tarkoitetaan henkilöstön sitouttamista, prosessien laatimista ja tiedottamista, joilla ekstraterritoriaalisia tietojensiirtotilanteita voidaan hallita kokonaisuuksina.

[144] Euroopan tietosuojaneuvoston suositukset 01/2020, 35–37.
[145] Euroopan tietosuojaneuvoston suositukset 01/2020, 36–37, Euroopan tietosuojaneuvoston 41. täysistunto 2020 ja EUT C-311/18, kohdat 135 ja 137.

4.3 Valvontatoimien olennaiset eurooppalaiset takeet

Yhdysvaltain lainsäädäntöön kohdistuvassa arvioinnissaan, tietojen viejien tulisi huomioida myös Euroopan tietosuojaneuvoston suosituksia valvontatoimien olennaisista eurooppalaisista takeista (European Essential Guarantees), jotka täydentävät lisäsuojatoimenpidesuosituksia. Takeiden tarkoitus on auttaa tietojen viejiä arvioimaan, voidaanko esimerkiksi Yhdysvaltain tiedustelulakien yksityisyyden ja henkilötietojen suojia koskeviin oikeuksiin valvontatarkoituksissa pitää oikeutettuna[146]. Käytännössä takeiden tulisi selkeyttää rekisterinpitäjien ymmärrystä valitsemiensa siirtomenetelmien lainmukaisuudesta ja tehokkuudesta etenemissuunnitelman vaiheen 3 mukaisesti[147]. Tietosuojaneuvosto on halunnut painottaa tehdyn arvioinnin kattavuutta, jotta se huomioisi mahdollisimman laajasti erilaiset lainsäädännölliset siirtoon vaikuttavat tekijät. Silloin, kun viranomaisten pääsyä siirrettyihin henkilötietoihin sääntelevää lakia ei ole, on tietojen viejän selvitettävä muut siirron kannalta olennaiset ja objektiiviset seikat, mikäli siirtoa halutaan jatkaa.[148]

Neljästä takeesta ensimmäiset kaksi edellyttävät, että a) käsittely perustuu selkeään ja täsmälliseen tietoihin pääsyä koskeviin sääntöihin ja b) tietojen käsittelyn välttämättömyys eli perusoikeuskirjan (art. 52, kohta 1) mukaisen yksityisyyden ja henkilötietojen suojaa koskevien oikeuksien rajoittamiset ovat suhteellisuusperiaatteen mukaisia.[149] Irlannin High Court esitti EUT:lle ennakkoratkaisukysymyksen Schrems II -asiassa, joka koski yksilölle perusoikeuskirjan 47 artiklassa taattua oikeussuojakeinoa. High Court kysyi, kunnioittaako Yhdysvaltojen tarjoama tietojen suojan taso oikeutta silloin, kun yksilön tietosuojaoikeuksia loukataan? High Court jatkoi, että mikäli EUT:n vastaus kysymykseen on myöntävä, ovatko ne rajoitukset, joita Yhdysvaltojen lainsäädännössä asetetaan yksilön oikeussuojakeinoa koskevalle oikeudelle Yhdysvaltojen kansallisen turvallisuuden nimissä, suhteellisuusperiaatteen kanssa yhteneväisiä siten, kuin perusoikeuskirjan 52 artiklassa tarkoitetaan? Ja ovatko ne sellaisia, että ne eivät ylitä sitä, mikä on tarpeen demokraattisessa yhteiskunnassa kansallisen turvallisuuden perusteella? EUT antoi vastauksensa kysymykseen, ja totesi, että on ilmeistä, ettei Yhdysvaltain lainsäädäntö täytä suhteellisuusperiaatteen mukaisia vähimmäisvaatimuksia[150]. Yhdysvallat loukkaavat toimillaan yksilön tietosuojaoikeuksia yli välttämättömyyden. Tältä osin, Yhdysvallat eivät noudata kahta ensimmäistä tietosuojaneuvoston määrittelemää taetta.

[146] Tietosuojavaltuutetun toimisto.
[147] Euroopan tietosuojaneuvoston suositukset 02/2020, 5.
[148] Euroopan tietosuojaneuvoston suositukset 01/2020, 3.
[149] Euroopan tietosuojaneuvoston suositukset 02/2020, 8 ja EUT C-311/18, kohdat 173, 174 ja 180.
[150] EUT C-311/18, kohdat 178, 180, 184.

Kolmas tae edellyttää c) riippumatonta valvontamekanismia. EIT on korostanut useaan kertaan, että erityisesti salaisen tarkkailutoimenpiteen perusteltavuutta arvioidessaan se ottaa huomioon kaiken valvonnan toimenpiteestä ”määrättäessä”, sitä ”toteutettaessa” ja sen ”lakattua”. Ensimmäisessä näistä kolmesta vaiheesta EIT edellyttää, että toimenpide on riippumattoman elimen hyväksymä.[151] Schrems II -tuomiossaan EUT huomioi, että Yhdysvaltain FISC-tuomioistuin ei anna lupaa yksittäisille valvontatoimenpiteille, vaan se ainoastaan hyväksyy valvontaohjelmia ja valvoo, vastaavatko nämä tarkkailuohjelmat tavoitteeseen hankkia ulkomaantiedustelutietoja. Sen valvonta ei täten ulotu koskemaan sitä, onko henkilöt kohdennettu asianmukaisesti ulkomaantiedustelutietojen hankkimiseksi.[152] Tämä osoittaa Yhdysvaltojen sähköisen valvonnan laajuutta, jossa valvontatarkoituksissa tehtyjä pyyntöjä päästä tietoihin ei valvota, jolloin on todennäköistä, että valvontaa kohdistuu myös sellaisiin tietoihin, jotka eivät välttämättä ole tiedusteluviranomaisten mielenkiinnon kohteena, mutta joihin voidaan kuitenkin kohdistaa valvontaa. Schrems II -tuomion valossa, Yhdysvaltojen ei voi katsoa täyttävän myöskään kolmannen takeen vaateita.

Viimeinen tae koskee d) yksilöiden saatavilla olevia muutoksenhakukeinoja, jolla on yhteys erityisesti kahteen ensimmäiseen takeeseen. Tae edellyttää, että jokaisella on oltava käytettävissään tehokkaat oikeussuojakeinot. Perusoikeuskirjan 47 artiklan ensimmäisessä kohdassa edellytetään, että jokaisella EU-kansalaisella, jonka oikeuksia ja vapauksia on loukattu, on oltava 47 artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa. Säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, ei ole tehokasta oikeussuojaa koskevan perusoikeuden mukainen. EUT totesi Schrems II:ssa, etteivät oikeusnormit[153], joihin tarkkailuohjelmien käyttö perustuu, anna EU-rekisteröidyille oikeuksia, joihin voitaisiin vedota Yhdysvaltojen viranomaisia vastaan tuomioistuimissa. Tämän perusteella EUT tulkitsi, ettei rekisteröidyillä ole käytettävissään tehokkaita oikeussuojakeinoja.[154]

Takeiden arviointi vaatii osaavaa tulkintaa, sillä arviointi olennaisen lainsäädännön ja valvontamenetelmien välisestä suhteesta tulee tehdä kaikki tilanteeseen vaikuttavat olosuhteet huomioiden[155]. Edellä käydyn perusteella on kuitenkin ilmeistä, ettei vakiolausekkeilla tehtyjä siirtoja Yhdysvaltoihin voida takeiden mukaan pitää riittävän tehokkaina. Tämä tarkoittaa sitä, että rekisterinpitäjien tulisi kyetä korjaamaan tämä puutteellisuus lisäsuojatoimenpiteillä. Kuten edellä on käsitelty, organisatoriset tai sopimukselliset lisäsuojamenetelmät eivät ole riittäviä takaamaan EU-

[151] Euroopan tietosuojaneuvoston suositukset 02/2020, 8 ja EIT Klass ym. v. Saksa, kohdat 55–56.
[152] Euroopan tietosuojaneuvoston suositukset 02/2020, 8 ja EUT C-311/18, kohdat 178–179.
[153] FISA 702 §, toimeenpanoasetus 12333 ja PPD-28.
[154] Euroopan tietosuojaneuvoston suositukset 02/2020, 8 ja EUT C-311/18, kohta 186, Schrems, C-362/14, kohta 95.
[155] Klass ja muut. v. Saksa, kohta 42; Kennedy v. Yhdistynyt kuningaskunta (18.5.2010), kohta 153.

kansalaisille yksityisyyden suojaa heitä koskevien tietojen siirryttyä Yhdysvaltoihin, jolloin ainoaksi tehokkaaksi menetelmäksi voi valikoitua tekniset menetelmät.

4.4 Lisäsuojatoimenpiteiden ja vakiolausekkeiden välisen suhteen arviointia

EUT:n Schrems II -tuomio loi lisäsuojatoimenpiteille oman oikeudellisen liikkuma-alan, jossa ne tarvittaessa tukevat vakiolausekkeita tietojen siirtovälineenä. Lisäsuojatoimenpiteet rakentuvat täten vakiolausekkeiden puutteellisuudelle, jolloin ne ovat vahvasti vakiolausekkeisiin sidottuja. EUT:n mukaan lisäsuojatoimenpiteitä tulee käyttää vakiolausekkeiden lisänä silloin, kun tapauskohtainen riskiarviointi on osoittanut, että vakiolausekkeiden tarjoama suoja Yhdysvaltoihin siirretyille tiedoille ei ole riittävä. Vaikka tietosuojaneuvosto mainitsee suosituksissaan EUT:n linjauksen[156], edellytetään lisäsuojatoimenpidesuosituksissa, että niitä tulee käyttää aina, kun tietoja siirretään Yhdysvaltojen kaltaiseen maahan, jossa henkilötietojen suojan taso ei vastaa unionin tasoa tai muussa tapauksessa siirtoa ei saa tehdä tai se tulee keskeyttää. Laajentamalla lisäsuojatoimenpiteiden käyttö jokaiseen siirtoon kaventaa organisaatioiden mahdollisuuksia tapauskohtaiseen arviointiin merkittävästi.

Riippumatta lisäsuojatoimenpiteiden vahvasta sidonnaisuudesta vakiolausekkeisiin, niillä on mitä ilmeisemmin myös itsenäinen rooli, sillä ne tarjoavat vakiolausekkeita olennaisesti täsmällisemmät ja konkreettisemmat toimenpiteet siirrettyjen tietojen suojaamiselle. Vakiolausekkeiden roolina on toimia eräänlaisena sopimuksellisena perustana, jonka päälle yritykset voivat rakentaa lisäsuojatoimenpiteistä siirretyille tiedoille tarvitsemansa suojausmenetelmänsä. Lisäsuojatoimenpiteet voivat olla joko prosessuaalisia eli organisatorisia, sopimuksellisia tai konkreettisia suojausmekanismeja eli teknisiä tai kaikki näitä yhdessä. Tietosuojaneuvoston mukaan, prosessuaaliset menetelmät voivat auttaa tietosiirtojen hallinnoinnissa, kasvattaa henkilökunnan tietoisuutta siirroista ja niiden riskeistä sekä sitouttaa tietojen tuojaa EU-säädöksistä johdettuihin velvoitteisiin. Näillä toimenpiteillä ei kuitenkaan voi estää Yhdysvaltain tiedusteluviranomaisten pääsyä EU-kansalaisia koskeviin tietoihin. Niiden suojaustaso on täten hyvin samankaltainen kuin vakiolausekkeiden. Lisäsuojatoimenpiteiden todellisen suojausarvon suhteessa vakiolausekkeisiin voikin katsoa piilevän nimenomaan sen teknisissä menetelmissä. Teknisten suojausmenetelmien, kuten salauksen avulla, tiedostoja on mahdollista suojata ulkopuolisten pääsyltä sopimuksellisia ja organisatorisia menetelmiä tehokkaammin, joskaan nekään eivät ole täysin aukottomia.

Riski tiedusteluviranomaisten pääsystä EU-kansalaisia koskeviin henkilötietoihin on siis lisäsuojamenetelmistäkin huolimatta olemassa. Tämä ei kuitenkaan tarkoita sitä, etteikö näille

[156] Euroopan tietosuojaneuvoston suositukset 01/2020, 2.

menetelmille olisi paikkansa. Päinvastoin yritykset tarvitsevat suuntaviivoja, joiden puitteissa siirtoja Yhdysvaltoihin voidaan tehdä. Näiden suuntaviivojen tulisi kuitenkin olla oikeasuhteisia asetettuun tavoitteeseen nähden. Nykymuodossaan lisäsuojatoimenpiteiden voikin tulkita noudattavan niin sanottua yhden mallin -periaatetta, jossa jokainen siirto on suojattava samalla tavoin, riippumatta tietojen luonteesta tai siirron riskitasosta ylipäätään. Kun yritykset siirtävät tietoja EU:sta Yhdysvaltoihin, tulisi tiedot suojata vain siinä määrin, kuin yritysten laatima riskiarviointi on osoittanut tarpeelliseksi. Muussa tapauksessa niin vakiolausekkeet kuin lisäsuojatoimenpiteet voivat päätyä olemaan siirtomenetelmiä, joita halutaan välttää niiden muodostaessa yrityksille kestämättömän hallinnollisen taakan.

Lisäsuojatoimenpiteiden ja uusien vakiolausekeluonnosten välinen suhde on ennen kaikkea toisiaan täydentävä, joka uusien vakiolausekkeiden myötä on siirtymässä osin jopa toisiaan toistavaan muotoon. Nykyisiin lausekkeisiin nähden lisätoimenpiteiden tarpeellisuus on jokseenkin korostetumpaa. Mikäli lisäsuojatoimenpiteet nähdään vain osana vakiolausekkeita ja mikäli lausekkeet ja lisäsuojatoimenpiteet ovat toistensa toisintoa, on riski, ettei niiden todellista potentiaalia päästä hyödyntämään kokonaisvaltaisesti. Tästä syystä näiden toimenpiteiden erilliset luonteet tietoa suojaavina mekanismeina vaatisivat tarkempaa arviointia. Vakiolausekkeiden tulisi muodostaa perusta tiedonsiirrolle, jota lisäsuojatoimenpiteet tarpeellisilta osin täydentävät. Mikäli vakiolausekkeet vastaavat sisällöllisesti lisäsuojatoimenpiteitä, ei lisäsuojamenetelmille jää enää täydennettävää muutoin kuin teknisinä menetelminä. Tämä kaventaisi lisäsuojatoimenpiteiden vakiolausekkeista erillistä oikeudellista toiminta-aluetta. Näin ollen, vaikka vakiolausekkeet ovat sopimuksellisia ja sitomattomia klausuuleja, joiden välitön siirrettyjen tietojen suojaamiskyky on heikko, antavat ne merkityksellisen lähtökohdan tietojen siirroille, joita eri organisaatiot voivat hyödyntää. Jotta kummankaan, niin vakiolausekkeiden kuin lisäsuojatoimenpiteiden asema ei toisen myötä kapenisi, tulisi niitä muotoilla niille ominaiseen suuntaan, jossa niitä ei pyritäkään asettamaan täysiin samaan muottiin.

Vakiolausekkeet täyttävät oman sopimuksellisen tehtävänsä niiden velvoittaessa EU:hun sijoittautunutta tietojen viejää ja Yhdysvalloissa toimivaa tietojen tuojaa. Vakiolausekkeiden ainoa EU-kansalaisten yksityisyyden takaamisen kannalta olennaisin heikkous piilee kuitenkin nimenomaan sen sopimuksellisessa ydintehtävässä; se ei voi sitoa sopimukseen kuulumatonta osapuolta, kuten Yhdysvaltain tiedusteluviranomaista. Jos vakiolausekkeiden pääasiallinen ongelma on niiden sitomaton ja paikoin lisäsuojatoimenpiteitä toistava luonne, on lisäsuojatoimenpiteiden ongelma niiden yhden mallin -periaatteen soveltaminen yritysten tekemiin tietosiirtoihin. Nykyisessä

muodossaan tämä tarkoittaisi sitä, että jopa konsernien väliset sisäiset tietosiirrot, joita tapahtuu toistuvasti, tulisi suojata teknisin toimenpitein.

Lisäsuojatoimenpiteille on Schrems II -tuomion jälkeen annettu entistä vahvempi rooli täsmällisempinä ja osin tietoturvallisempina tiedonsiirtomenetelminä. Tästä huolimatta lisäsuojatoimenpiteet ja vakiolausekkeet tulevat pysymään vahvasti toisiinsa kytköksissä, sillä vakiolausekkeiden merkitys ja hyöty itsenäisenä siirtomenetelmänä rakentuu pääosin tiedonsiirtoon osallistuvien tahojen sopimuksellisen yhteistyön tunnustamiselle, kun taas lisäsuojatoimenpiteet ovat enemmänkin sopimuksen kohteena olevan tiedon suojaamismekanismeja organisaatioiden toimintavoista teknisiin toteutuksiin. Vaikka vakiolausekkeet omaavatkin heikomman sitovuuden menetelmänä, ovat ne kokonaisuutena arvioiden merkitysarvoltaan vahvemmassa ja itsenäisemmässä asemassa suhteessa täydentäviin menetelmiin. Vakiolausekkeet ja lisäsuojatoimenpiteet ovat erottamaton osa toisiaan, jotka tavoittelevat samaa asiaa: korkean tason suojaa yksityisyydelle ja henkilötietojen käsittelylle. Päällimmäisin pyrkimys onkin velvoittaa rekisterinpitäjä tunnistamaan ne menetelmät, joilla tietoja voidaan suojata tehokkaasti ja siirtää niitä tietojen viejää ja tuojaa velvoittavan sopimuksen puitteissa Yhdysvaltoihin. Kuten todettua, näiden siirtomenetelmien erillisyys vaatii kuitenkin jatkotarkastelua, jotta molempien potentiaali tulisi hyödynnettyä täysimääräisesti.

4.5 Lisäsuojatoimenpiteiden yritysvaikutukset

Useimmille EU-alueella toimiville organisaatioille ekstraterritoriaaliset tiedonsiirrot ovat keskeinen osa päivittäisiä toimintoja. Yrityksiä on eri kokoisia ja eri sektoreilta, jotka siirtävät tietoja joko osana kansainvälistä yritystoimintaa tai tutkimusta. Näistä organisaatioista yli 85 %:ia siirtää tietoja vakiolausekkeilla, joista 90 %:ia tapahtuu yritysten välillä. Nämä tietovirrat ovat elintärkeitä, jotka mahdollistavat arviolta 550 miljardin euron arvosta digitaalisia palveluja, joita EU vie muualle maailmaan. Globaalin tietojen siirtämisten avulla on ollut mahdollista myös maailmanlaajuinen tutkimustyö COVID-19-pandemian torjumiseksi.[157]

Lisäsuojatoimenpiteillä on Schrems II -tuomion myötä pyritty siihen, että tietojen viejät arvioivat Yhdysvaltojen oikeusjärjestelmän sallimia mahdollisuuksia tiedusteluviranomaisille päästä siirrettyihin eurooppalaisiin henkilötietoihin. Toisaalta arvioinnin tarkoitus on myös selvittää, toteutuvatko EU-kansalaisten oikeudet samalla tavalla, jos tietoja käsiteltäisiin EU:ssa. Arviointi painottuu kuitenkin enemmän lainsäädännön tulkintaan kuin siihen, kuinka ilmeistä on, että

[157] Yhdysvaltain kauppakamari 2020.

siirretyille tiedoille aiheutuu todellista haittaa.[158] Tietojen viejien Yhdysvaltojen lainsäädännön vaikutusten arviointi suhteessa vakiolausekkeiden tehokkuuteen tietojen siirrossa[159] on laaja-alainen tehtävä, joka koostuu monista erilaisista muuttuvista tekijöistä. Tästä syystä on myös todennäköistä, että kaikkia siirtoon vaikuttavia tekijöitä ei kyetä huomioimaan, jolloin riski tehdyn arvioinnin epäluotettavuudesta kasvaa. Rekisterinpitäjille sekä henkilötietojen käsittelijöille asetettu tehtävä on vähintäänkin haasteellinen. Tämän lisäksi on epäselvää, missä määrin valvontaviranomaiset tulevat auttamaan rekisterinpitäjiä ja henkilötietojen käsittelijöitä varmistamaan, että tietosuojan taso toteutuu Yhdysvaltoihin siirrettyjen tietojen osalta. Tietosuojaviranomaisten valvontamenetelmiä ei ole tarkennettu suosituksissa, vaan viranomaisten keinot määräytyvät, ainakin toistaiseksi, tietosuoja-asetuksen mukaan (art. 57), jotka on laadittu linjaan tietosuojalainsäädännön riskiperusteisen lähestymistavan kanssa.

Tietosuojaneuvoston suositukset sisältävät riskiperusteista lähestymistapaa huomattavasti ehdottomamman linjan: Yhdysvaltoihin siirretyille tiedoille tulee taata unionin tasoinen suoja Yhdysvalloissa tai siirto tulee keskeyttää. Koska suositukset ovat asettaneet entistä korkeammat EU-mukaiset vaateet tietojen viejille ja tuojille, tulisi tässä suhteessa tarkastella myös viranomaisten valvontamenetelmien riittävyyttä. Mikäli suositukset tulevat voimaan nykyisessä muodossaan, tulisi asetuksessa määriteltyjä tietosuojaviranomaisen valvontamenetelmiä tarkastella myös tässä suhteessa. Nykyiset asetuksessa määritellyt valvontamenetelmät eivät voi vastata nyt laadittuihin tiedonsiirroille asetettuihin tavoitteisiin, minkä takia valvontaviranomaisten toissijainen rooli on toisaalta perusteltua.

Suosituksissa edellytetään, että tietoja ei saa siirtää maihin, joissa ei voida taata unionissa määriteltyä suojan tasoa[160]. Koska Yhdysvaltain lainsäädäntö sallii tiedusteluviranomaisten valvontatoimet ilman rajoituksia, kuten edellä käsitellyt Yhdysvaltain tiedusteluviranomaisten tarkkailuohjelmia sääntelevät oikeussäännöt osoittavat, tulisi EU-alueelta Yhdysvaltoihin tehtävät tietosiirrot suojata aina joko salaamalla tai pseudonymisoimalla, ja salausavain tulisi säilyttää EU-alueella tai muulla alueella, joka ei poikkea EU:n asettamista tietosuojavaateista. Tämä on kuitenkin merkittävä käytännön, sillä esimerkiksi sähköpostien lähettäminen, asiakasmaksujen käsittely tai yritysten transaktiot edellyttävät, että tieto ei ole salattu.[161] Vaikka tietosuojaneuvoston peruste siirrettyjen tietojen korkeatasoiselle suojaamiselle on Yhdysvaltojen tiedustelulainsäädännön vuoksi perusteltua,

[158] Atallah 2020.
[159] Euroopan tietosuojaneuvoston suositukset 01/2020, 2.
[160] Yhdysvaltain kauppakamari 2020, 1–2 ja BusinessEurope, European Roundtable for Industry, et al, Schrems II Impact Survey Report.
[161] Yhdysvaltain kauppakamari 2020.

ei yksikään yritys voi toimia näin kapea-alaisella tulkinnalla riskiperusteisen arvioinnin mukaisesti. Tältä osin suositusten sisällön voi tulkita olevan ristiriidassa EUT:n ja tietosuoja-asetuksen riskiperusteisen toimintavan suhteen.

On kuitenkin huomioitava, että EUT:n lausui Schrems II -tuomiossaan, että tietojen viejän ja tuojan on ennen siirtoa varmistettava, että siirron kohteena olevassa maassa noudatetaan unionin tasoista tietojen suojaa. Mikäli siirrossa ei voida noudattaa vakiolausekkeita, eivätkä lisätoimenpiteet auta suojaamaan rekisteröidyn oikeuksia, tulee siirto keskeyttää tai sitä tulee lykätä.[162] Kuten edellä on osoitettu, Yhdysvaltain tiedusteluviranomaisten toimia löyhästi sääntelevät oikeusnormit ovat esteenä EU:n tietosuojan tason toteutumiselle kyseissä maassa. Vakiolausekkeiden suoja niiden sopimuksellisen luonteen vuoksi on täten riittämätön. Tällöin tietojen viejän tulee ottaa käyttöön joko lisäsuojatoimenpiteet tai olla aloittamatta siirtoa. Oletetusti rekisterinpitäjä haluaa jatkaa siirtoa. Kun asiaa vielä tarkastellaan tietosuoja-asetuksen riskiperusteisen lähestymistavan kannalta, on huomattava, että sen mukaan tietojen siirroissa tulee huomioida käsittelyn todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisteröidyn oikeuksille ja vapauksille. EU:n kannalta katsoen todennäköinen ja vakavuudeltaan merkittävä riski on rekisteröidyn perustuslaillisen yksityisyyttä koskevan oikeuden vaarantuminen. Tämän estämiseksi tietojen viejän on tietosuoja-asetuksen mukaan toteutettava tehokkaat tekniset ja organisatoriset toimenpiteet, kuten esimerkiksi tietojen pseudonymisointi (art. 25). Koska sopimukselliset ja organisatoriset lisäsuojakeinot eivät ole riittäviä suojaamaan Yhdysvaltoihin siirrettyjä tietoja viranomaisurkinnalta, jää tietojen viejien ainoaksi tehokkaaksi vaihtoehdoksi tekniset lisäsuojamenetelmät. Näin ollen tietosuojaneuvoston suositusten sisällön voi tulkita olevan edellä kuvatuilta osin EUT:n ja tietosuoja-asetuksen kanssa yhteneväinen.

Edellä kuvatun perusteella, kyse on lopulta siitä, minkä tyyppisiä henkilötietoja vakiolausekkeilla ja teknisillä lisäsuojatoimenpiteillä olisi tarpeellista suojata, jotta EU-kansalaisen oikeus yksityisyyteen ja henkilötietojen suojaan eivät vaarannu. Nyt määritellyt suositukset, tietosuojaneuvoston puheenjohtajan näkemyksistä[163] ja tietojen viejien vastuulla olevista arvioista huolimatta, noudattavat kaikesta huolimatta yhden mallin -periaatetta Yhdysvaltoihin tehdyissä tietosiirroissa. Se, että organisaatioiden tulisi aina salata tiedot, riippumatta siitä onko esimerkiksi viranomainen antanut Yhdysvalloissa sijaitsevalle tietojen tuojalle lakiperusteisen velvoitteen luovuttaa tietoja tai ovatko tiedot tiedusteluviranomaisen kiinnostuksen kohteena ylipäätään, ei ole EU-oikeuden kanssa

[162] EUT C-311/18, kohdat 133, 134, 142 ja 203.

[163] ”Ei ole olemassa yhtä kaikille sopivaa ratkaisua kaikkiin siirtoihin, koska tällöin jätettäisiin huomiotta tietojen viejien tilanteiden moninaisuus. Tietojen viejien on arvioitava tietojenkäsittelytoimensa ja -siirtonsa ja toteutettava tehokkaita toimenpiteitä ottaen huomioon oikeusjärjestyksen niissä kolmansissa maissa, joihin ne siirtävät tai aikovat siirtää tietoja.” Euroopan tietosuojaneuvoston 41. täysistunto.

yhteneväinen.[164]Lisäksi suosituksissa todetaan, että tekniset menetelmät ovat riittäviä silloin, kun viranomaiset eivät pääse tietoihin eli tekniset suojausmenetelmät estävät tietoihin tunkeutumisen. Se, miten yritysten tulisi kyetä varmistamaan, etteivät Yhdysvaltain viranomaiset pääse siirrettyihin tietoihin käytettävissään olevien resurssien avulla, on epäselvää. Tekniset menetelmät, kuten salaus, ovat erinomainen keino suojata salassa pidettäviä tietoja niitä väärinkäyttäviltä toimijoilta yksityisyyden takaamiseksi, mutta tämän teknisen vaateen ulottaminen koskemaan kaikkia eurooppalaisia henkilötietoja on kestämätön, minkä lisäksi se ei vastaa globaalin kaupankäynnin sisältämiä realiteetteja. Yhdysvaltain kauppakamarin mukaan useimmat Yhdysvalloissa sijaitsevista yrityksistä eivät edes käsittele tietoja, jotka olisivat Yhdysvaltojen tiedusteluviranomaisten mielenkiinnon kohteena. Jokainen tiedonsiirtotilanne on siis erilainen, jolloin niihin sisältyviä riskejä tulisi arvioida eri tavoin.[165]

Tietosuojaneuvoston laatimien suositusten tarve on kuitenkin tunnistettu ja niihin sisältyy potentiaali. Tietojen suojaus alkaa organisaatioiden käytänteistä ja henkilöstöstä, joista se siirtyy sopimuksiin, jotka ulottavat hyvät tietojen käsittelyn tavat myös Yhdysvalloissa sijaitsevaan tietojen tuojaan. Kun nämä kaksi on kattavasti toteutettu, tulisi jäljelle jääneet aukot suojata tapauskohtaisesti suoritetun arvioinnin perusteella teknisin menetelmin. EU-kansalaisen oikeus henkilötietojen suojaan ja yksityisyyteen on perustuslaillinen oikeus, jota tietosuojaneuvosto on halunnut suojella korkein tietosuojavaatein. Tietosuojaneuvosto tunnistaa myös erilaisten siirtojen luonteen ja vaihtelevat riskitasot, mutta se ei ole onnistunut sisällyttämään tätä lisäsuojatoimenpidesuosituksiin. Korkean tietosuojan tason toteumista koskeva vaade on nyt vastakkain kansainvälisten yritysten liiketoimintojen realiteettien kanssa, jossa yritykset on asetettu kohtuuttomaan asemaan. Suositusten tulisi huomioida tietosiirtojen monitahoisuus suosituksissaan paremmin, jotta lisäsuojamenetelmien käyttö olisi tavoitteeseen nähden oikeasuhteinen.

[164] Yhdysvaltain kauppakamari 2020.
[165] Yhdysvaltain kauppakamari 2020.

5 Lopuksi

Teknologia kehittyy huimaa vauhtia ja se luo internetin käyttäjille uusia mahdollisuuksia, mutta myös haasteita, erityisesti yksityisyyteen liittyen. Kun globaalit yritykset siirtävät liiketoimintojensa yhteydessä eurooppalaisia henkilötietoja Yhdysvaltoihin, ne voivat altistua kyseisen maan tiedusteluviranomaisten laittomalle sähköiselle valvonnalle, jota viranomaiset harjoittavat kansallisen turvallisuuden nimissä. Tämä korostaa siirrettävien henkilötietojen ekstraterritoriaalista suojan tarvetta. Perustavanlaatuisen ongelman unionin tasoisen suojan toteutumisessa Yhdysvalloissa muodostaa Yhdysvaltojen ja EU:n erilainen oikeuskäsitys ja sääntely yksityisyydestä. Kun EU pyrkii vahvistamaan asemaansa yksityisyyden suojelijana, toimitaan Yhdysvalloissa yksityisyyden suojaamisen suhteen rikkonaisesti ilman selkeää yhtenäistä linjaa.

EU:lle yksilön oikeudet ovat keskeisiä ja tärkeitä, kun taas Yhdysvallat keskittyy enemmän yksilöiden suojeluun kansana. Yhdysvaltojen lainsäädäntö mahdollistaa tiedusteluviranomaisten pääsyn EU-kansalaisia koskeviin siirrettyihin henkilötietoihin, heikentäen yksilön oikeutta päättää itseään koskevien tietojen käsittelytavoista silloin, kun tämä on vapaaehtoisesti luovuttanut henkilötietojaan. Lähtökohtaisesti oikeus yksityisyyteen tulisi kuitenkin olla yksilön, ei viranomaisen valinta. Laittoman sähköisen valvonnan kohteena olevat EU-kansalaiset omaavat myös heikot oikeussuojakeinot Yhdysvalloissa, mikä omalta osaltaan osoittaa tarpeen entistäkin tehokkaammille siirrettäviä henkilötietoja koskeville suojausmenetelmille, jotta yksilön oikeus yksityisyyteen voidaan taata[166]. Samalla tavoin kuin perusoikeuksien rajoittamisten tulisi olla suhteellisuudentajuisia, tulisi myös lisäsuojausmenetelmien rakentua arvioidulle riskille ja tästä muodostetulle oikeasuhteiselle lisäsuojausmenetelmien tarpeelle.

Sääntelyllä, kuten esimerkiksi tietosuoja-asetuksella, voidaan vaikuttaa suoraan yksityisyyden määräytymiseen. Lainsäädännöltä ei kuitenkaan voida odottaa täsmällisyyttä silloin, kun sen kohde ei ole riittävän selkeästi määritelty. Näin on esimerkiksi yksityisyydenkäsitteen suhteen. Vaikka yksityisyyden määrittelemättömyys onkin lainsäädännöllisesti katsoen sen heikkous, on se samalla myös sen vahvuus; tällöin lainsäädäntö voi sopeutua yhteiskunnan muutoksiin dynaamisesti. Näin ajateltuna se, että Yhdysvalloissa ei ole liittovaltion tasolla yhtenäistä yksityisyyttä koskevaa lainsäädäntöä, voitaisiin teoreettisesti perustella sillä, että yksityisyyskäsitettä ei ole määritelty Yhdysvaltojen lainsäädännössä, ei edes sen perustuslaissa. Toisaalta, koska sitä ei ole määritelty, on tämä jättänyt lainsäädännölle sopeutumistilaa, josta puolestaan osoituksena Yhdysvaltojen

[166] Sharma, Sanjay 2019, 8.

yksityisyyttä koskevan lainsäädännön monitahoisuus. Kokonaisuutena arvioiden, yksityisyyden tarkkarajainen määrittely on lopulta tarpeetonta[167]. Tätä todentaa se, että EU:ssa on laadittu kattavasti yksityisyyttä ja henkilötietojen suojaa koskevia lakeja, vaikka yksityisyyttä ei olekaan pystytty määrittelemään tarkasti.

Lainsäädännön voisi kenties jokseenkin sanoa heijastelevan kunkin maan tai alueen kulttuuria. Esimerkiksi Yhdysvalloissa terrori-iskut ovat vaatineet hallitukselta suojatoimia, joita on tehostettu muun muassa laajoilla sähköisillä tiedustelutoimilla. Yhdysvaltain hallitus tulee tuskin hellittämään otettaan näistä, sillä pelko väljempien valvontatoimien seurauksista on liian korkea. Toisen perusoikeuksista, joko yksityisyyden tai kansallisen turvallisuuden, on tullut maksaa hinta tästä, sillä kahden perusoikeuden kollisiossa, toinen joutuu taipumaan. Perusoikeuksien rajoittamisten tulisi kuitenkin niiden merkittävyyden vuoksi olla suhteellisuuteen nojaavia, vankkoja ja yhteiskunnallisen tarpeen kautta perusteltuja[168]. Mikään perusoikeus ei siis ole absoluuttinen, jolloin yksityisyyden ja henkilötietojen suojien täydellistä toteutumista voi hyvinkin rajoittaa kansallinen turvallisuus. Tämä asetelma tuntuukin juurtuneen syvälle yhdysvaltalaiseen hallinnolliseen ajattelutapaan. Yksilön suojelun sijaan, on päätetty suojella ihmisiä kansana, huomioimatta kuitenkaan suhteellisuutta yksilöiden yksityisyyden rajoittamisessa, mikä on olennaisesti ristiriidassa niin kansainvälisen kuin myös EU-sääntelyn kanssa. Kun henkilötietoja siirretään EU-alueen ulkopuolelle Yhdysvaltojen kaltaiseen maahan, joka ei kuulu komission hyväksymiin riittävän tietosuojan tason takaaviin maihin, henkilötietojen suojan taso heikkenee olennaisesti. Tämä luo yksityisyyteen kohdistuvia riskejä niille henkilöille, joiden tietoja siirretään. Näin ollen, on erityisen tärkeää määritellä selkeät perusteet ja vaatimukset niille menetelmille, joilla henkilötietoja voidaan siirtää Yhdysvaltoihin, jossa kansallinen turvallisuus on asetettu yksityisyyden edelle.

EUT mitätöi niin Safe Harbor kuin Privacy Shield -sopimuksen siksi, että niiden tarjoama suoja Yhdysvaltoihin siirretyille eurooppalaisille henkilötiedoille ei ollut riittävä. Tämän jälkeen EUT painotti, että vakiolausekkeet eivät takaa automaattisesti suojaa Yhdysvaltoihin siirretyille tiedoille, jolloin niiden ohella tulee *tapauskohtaisesti* hyödyntää lisäsuojatoimenpiteitä. EUT:n linjaus noudattaa tietosuoja-asetuksen riskiperusteista lähestymistapaa; rekisterinpitäjän vastuulla on huomioida jokaista tiedonsiirtotilannetta koskevat riskit ja valita riskin vaikuttavuuden perusteella sopivat tekniset ja organisatoriset toimenpiteet. EUT:n Schrems II -tuomion jälkeen, yritykset jäivät

[167] Saarenpää 2016a, 1–2.
[168] HE 309/1993 vp s. 29–30, PeVM 25/1994 vp, 5 ja EUT:n tuomio C-112/00, kohta 80.

odottamaan EU:lta jatkotoimenpiteitä, jotka auttaisivat niitä siirtämään tietoja Yhdysvaltoihin EU-tietosuojalainsäädännön mukaisesti.

Pian Schrems II -tuomion jälkeen Euroopan tietosuojaneuvosto laati suositukset lisäsuojatoimenpiteistä, jotka sisältävät konkreettisia ja täsmällisiä ohjeistuksia koskien ekstraterritoriaalisia tiedonsiirtoja. Lähtökohtaisesti lisäsuojatoimenpidesuositusten sopimukselliset, organisatoriset ja tekniset vaateet ovat yritysten täytettävissä, sillä ne ovat yritysten vaikutuspiirissä, minkä lisäksi nämä edellytykset on määritelty rekisterinpitäjiä velvoittaviksi jo uuden tietosuoja-asetuksen tultua voimaan. Koska suositukset eivät rakennu riskiperusteiselle arvioinnille, vaan pelkästään kohdemaan kykyyn taata suoja, on oletuksena, että Yhdysvaltojen kaltaisen heikon tietosuojan tason maahan tehdyt siirrot tulisi aina suojata teknisin menetelmin. Tämä vaade tietosiirroille EU:sta Yhdysvaltoihin on kuitenkin epärealistinen ja mahdoton sovittaa yritysten nykyisiin toimintoihin[169]. Käytännössä tämä tarkoittaisi, että yritysten tulisi suojata jokainen tietosiirto riippumatta sen rekisteröidylle aiheuttamien riskien tasosta. Tältä osin lisäsuojatoimenpidesuosituksissa määritelty ei vastaa tietosuoja-asetusta eikä EUT:n linjausta tapauskohtaisesta riskiperusteisesta lähestymistavasta. Toisaalta on korostettava, että niin julkiasiamies, EUT kuin tietosuojaneuvosto ovat yhteneväisiä sen suhteen, että siirto tulee keskeyttää tai siirtoa ei saa aloittaa, mikäli siirretyille tiedoille ei voida varmistaa EU:n tasoista suojaa. Tältä kannalta katsoen teknisten suojausmenetelmien kyvykkyys unionin tasoisen suojan varmistajana asettuu muita täydentäviä menetelmiä keskeisemmäksi. Sillä on todellinen, vaikkei aukoton, mahdollisuus suojan varmistajana. Tästä syystä, tietosuojaneuvoston suositukset, myös takeita koskevat, päätyvät tarjoamaan Yhdysvaltoihin tehtyjen siirtojen riittäväksi suojausmekanismiksi teknisiä menetelmiä, mikä on ristiriidassa siirtokohtaisen vaikutusten arvioinnin kanssa.

Haasteita liittyy myös tietosuojaneuvoston laatimiin suosituksiin valvontatoimien olennaisista eurooppalaisista takeista. Neljän takeen tulisi tarjota rekisterinpitäjille lisätukea, kun ne arvioivat vakiolausekkeiden lainmukaisuutta ja tehokkuutta suhteessa Yhdysvaltojen tiedustelulakeihin, joilla EU-kansalaisten yksityisyyteen puututaan. Takeiden kannalta katsoen, Yhdysvallat ei yllä EU-standardeihin, jolloin vakiolausekkeiden käyttäminen EU:n ja Yhdysvaltojen välisissä tietojen siirroissa voidaan tulkita olevan riittämättömiä. Tällöin vaihtoehdoiksi jäävät joko pyrkimys taata EU:n tasoinen suoja lisäsuojatoimenpitein tai olla siirtämättä tietoja lainkaan. Niin takeet kuin lisäsuojatoimenpiteet osoittavat Yhdysvaltojen ja EU:n toisistaan poikkeavaa käsitystä yksityisyyden suojasta, johtuen myös osin näiden suositusten varsin korkeasta EU-lähtöisyydestä. Kokonaisuutena

[169] Atallah 2020 ja Yhdysvaltain kauppakamari 2020, 1.

arvioiden, rekisterinpitäjien mahdollisuudet Yhdysvaltoihin tehtyjä siirtoja koskevien riskien arviointiin sekä siirron toteuttamiseen ylipäätään EU-sääntöjen mukaisesti, jäävät lähes olemattomiksi suositusten sisältämien kapea-alaisten määritysten vuoksi.

Niin julkiasiamies kuin EUT katsoivat, että komission päätös vakiolausekkeista on pätevä nimenomaan siihen sisältyvien rekisterinpitäjiä ja henkilötietojen käsittelijöitä koskevien velvoitteiden vuoksi. Jos siirtoa ei rekisterinpitäjän suorittaman kattavan selvityksen perusteella voida toteuttaa EU-sääntöjenmukaisesti, tulee siirto keskeyttää tai sitä tulee lykätä. Selvityksessä rekisterinpitäjien tulee huomioida kaikki siirtoon vaikuttavat olosuhteet ja osoitusvelvollisuutensa puitteissa kaikki vaiheet selvityksessä tulee dokumentoida. Asianmukaisten siirtomekanismien käyttäminen ja siirrettävien tietojen suojasta huolehtiminen on *ensisijaisesti* rekisterinpitäjän vastuulla ja vasta toissijaisesti valvontaviranomaisten vastuulla. Tietojen siirrosta vastaavien rooli unionin tasoisen suojan varmistajana on ilmeisen haastava, vaativa ja kenties mahdoton tehtävä. Se vaatii ammattitaitoa, joka voi asettaa pienet ja keskisuuret yritykset eriarvoiseen asemaan, sillä niiden tavoitellessa EU-sääntöjenmukaisuutta ne eivät välttämättä oma samanlaisia mahdollisuuksia kuin isommat toimijat. Yleisesti ja laaja-alaisesti arvioiden, nykyisessä muodossaan EU:n suositukset ja ohjeistukset voivat vaikuttaa merkittävästi rajat ylittävään kaupankäyntiin. Siinä missä EU velvoittaa yrityksiä toimimaan tietosuojansa globaaleina lähettiläinä, tulisi sen haastaa myös valvontaviranomaisten menetelmiä ja mukauttaa ne nykyisiin tavoitteisiin globaalista tietosuojan tasosta, olettaen, että suositukset tulevat säilymään nykyisessä muodossaan.

Psykoterapiakeskus Vastaamo Oy:n tapauksen yhteydessä tuolloin tietosuojavaltuutettuna toiminut Reijo Aarnio otti kolumnissaan kantaa viranomaisvalvonnan tehokkuudesta ja kirjoitti, että oletus siitä, että viranomaisten tulisi valvoa etukäteen, tehdä tarkastuksia tietojärjestelmiin ja näin ollen torjua hakkerointia, on haastavaa johtuen resurssien vähäisyydestä. Resurssien lisääminen puolestaan vaatisi todellista ponnistusta, sillä tietojärjestelmiä ja rekistereitä on pelkästään jo Suomessa yli miljoona.[170] Tätä samaa resurssihaastetta voidaan ulottaa tietosuojaneuvoston suositusten yrityksille asettamiin tavoitteisiin ja vaateisiin. Huomioiden yritysten tekemien siirtojen määrä, jokaiseen siirtoon kohdistuva selvitystyö sekä niihin tarvittavat jatkuvaluonteiset resurssit, ovat yritykset yhtä mahdottoman tehtävän edessä, kuin tietosuojaviranomaiset. Tämän perusteella yritykset on asetettu hyvin epäreiluun asemaan. Toistaiseksi on epäselvää missä määrin valvontaviranomaiset tulevat auttamaan tietojen viejiä ja tuojia täyttämään EU-sääntöjenmukaisuuden tietosiirroille, mutta mikäli EU:n tietosuojan taso kuitenkin halutaan ulottaa Yhdysvaltoihin ja se halutaan toteuttaa suositusten

[170] Aarnio 2020.

mukaisesti ilman mahdollisuutta tapauskohtaiseen riskiarviointiin, tulee myös valvontaviranomaisten menetelmiä ja resursseja tarkastella suhteessa uusiin vaatimuksiin. Yksilön yksityisyyttä tulisi suojella siinä määrin, kuin tapauskohtaisesti tehdyn arvioinnin kannalta on tarpeen. Vaikka vastuu tietosuojan tasosta ja tätä kautta yksityisyyden suojelusta tietosiirroissa on EUT:n mukaan ensisijaisesti tietojen viejillä ja tuojilla sekä toissijaisesti valvontaviranomaisilla, on myös rekisteröidyillä vastuu. Yksilö voi vaikuttaa siihen, mitä tietoja hän luovuttaa ja mihin. Tarkastemalla omaa toimintaansa, yksilö voi tietyissä tapauksissa vaikuttaa itseään koskevien henkilötietojen suojaamiseen.

Nyt laaditut lisäsuojatoimenpidesuositukset sekä osin myös vakiolausekkeet, ovat EU-keskeisiä, jossa yksityisyyden suojelu on viety lähes äärimmilleen. Tämä puolestaan heijastuu EU:n ja Yhdysvaltojen välillä toimivien yritysten arkisiin toimiin sekä kansainväliseen kaupankäyntiin. Liiallisella sääntelyllä EU on vaarassa pudota omaan ohjekeskeiseen kuiluun, jossa se jää digitaalisen talouden kehityksestä. Toisaalta EU ei voi olla suojelemattakaan sille merkittäviä arvoja, joiden puolesta se on taistellut jo pitkään. Toistaiseksi yksityisyyttä ei kuitenkaan voida taata Yhdysvalloissa samalla tavalla kuin EU-alueella. Tämä on tiedostettu EU:ssakin, mitä ilmentää lisäsuojatoimenpidesuosituksissakin esiin nostettu näkökohta siitä, etteivät EU:n laatimat menetelmät välttämättä takaa riittävää suojaa Yhdysvaltoihin siirretyille henkilötiedoille. Voidaan myös kysyä, tarvitseeko kaikkien siirrettyjen tietojen ollakaan suojattuja? Kuten Yhdysvaltain kauppakamari on todennut, kaikki Yhdysvaltoihin siirretyt tiedot eivät ole tiedusteluviranomaisten kohteena. Tähän näkemykseen istuu myös niin EUT:n kuin tietosuoja-asetuksen riskiperusteinen lähestymistapa.

Mikäli EU-standardien mukainen tietojen siirtäminen Yhdysvaltoihin olisi ratkaistavissa nopeasti, se olisi jo tehty. Kyseessä on kuitenkin ilmeisen monitahoinen haaste, joka vaatii aikaa ja oppimista. Yhdysvalloissa tietosuojaa ja yksityisyyttä koskeva sääntely on repaleinen, joka sallii niin osavaltioille, kuin niissä toimiville yrityksille omat säännöt. Tämän lisäksi Yhdysvaltain valvontalait sallivat tiedusteluviranomaisten harjoittaa laajaa sähköistä valvontaa ilman, että valvontaa olisi mitenkään rajattu vain tietyntyyppisiin tiedostoihin. On kuitenkin huomioitava, että EU on luonut hyvän ja vankan kansainvälisen perustan henkilötietojen suojaamista koskevan lainsäädännön tosiasiallisen täytäntöönpanon (art. 50) ja tietojen turvallisen siirtämisen suhteen. Tätä EU edistää toimimalla yhteistyössä muun muassa Yhdysvaltojen kanssa. Kansainvälisen yhteistyön ohella EU voi yrittää parantaa myös omaa kilpailukykyään ja luoda yhdysvaltalaisten teknologiajättien kanssa kilpailevia eurooppalaisia yrityksiä, jolloin tarve ekstraterritoriaalisille henkilötietojen siirroille voisi vähentyä. On myös mahdollista, että tekniset menetelmät kehittyvät siten, että rekisteröidyillä on tulevaisuudessa todellinen mahdollisuus päättää, kuka hänen tietojaan käsittelee ja mihin niitä

siirretään, jolloin samainen tekninen kehitys voisi sallia myös EU:n valvontaviranomaisten käytettävissä olevien valvontakeinojen ja resurssien tehostamisen.

Kuten Kaliforniassa hyväksytty uusi yksityisyyttä sääntelevä laki osoittaa, yksityisyyden yhteiskunnallinen merkitysarvo näkyy kasvavan pienin askelin myös Yhdysvalloissa, jolla toivotaan olevan laajempikin vaikutus. EU puolestaan on jo asemansa määrittänyt, ja se haluaa olla taistelemassa yksityisyyden puolesta. EU:n haaste onkin löytää kultainen keskitie sääntelyn ja yrityksille sallitun sopimuksellisen vapauden välillä. Yhdysvalloissa tilanne on monimutkaisempi. Hallitus kokee kansallisen turvallisuuden tärkeäksi, jossa yksilön yksityisyys jää sen varjoon. Yhdysvaltojen haaste on varmistaa, että valvontatoimet ovat oikeassa suhteessa tavoiteltuun päämäärään. Yhdessä EU:n ja Yhdysvaltojen tulisi pyrkiä löytämään ratkaisu, jonka puitteissa yritykset voivat siirtää tietoja näiden alueiden välillä niin EU:n kuin Yhdysvaltojenkin näkemyksiä kunnioittaen.