TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

Kansainväliset tiedonsiirrot asianmukaisia suojatoimia soveltaen

Yleisen tietosuoja-asetuksen mukaiset tiedonsiirrot EU:n ulkopuolella sijaitseviin kolmansiin valtioihin

Pro gradu -tutkielma
Turun yliopisto
Oikeustieteellinen tiedekunta
Taloudellinen toiminta, sopimus ja vastuu
Robert Porthan
27.8.2023

Tiivistelmä

Pro gradu -tutkielma

Oppiaine: Oikeustiede, Taloudellinen toiminta, sopimus ja vastuu
Tekijä: Robert Porthan

Otsikko: Kansainväliset tiedonsiirrot asianmukaisia suojatoimia soveltaen.
Yleisen tietosuoja-asetuksen mukaiset tiedonsiirrot EU:n ulkopuolella sijaitseviin kolmansiin valtioihin
Ohjaaja: Mika Viljanen
Sivumäärä: 76 s.
Päivämäärä: 27.8.2023

Tutkielman tarkoituksena on selvittää, miten yhteisöt voivat siirtää henkilötietoja EU:sta ja Euroopan talousalueelta EU:n ulkopuolelle, eli kolmansiin maihin. Henkilötietojen siirtämiseen kolmansiin maihin tulee noudattaa yleisen tietosuoja-asetuksen (GDPR) asettamia vaatimuksia tietojenkäsittelylle. Tutkielmassa selvitetään EU:n tietosuojalainsäädännön, oikeuskäytännön ja kirjallisuuden perusteella, mitkä vaatimukset ja lainsäädäntö on otettava huomioon, jotta tiedonsiirrot tehdään lainmukaisesti. Tutkielma pyrkii selvittämään myös, mikä on asianmukaisten suojatoimien määritelmä GDPR:n vaatimuksissa tiedonsiirroille.

Tutkielman pääasiallinen tutkimusmenetelmä on oikeusdogmatiikka. Tutkimusmenetelmän kautta tutkielma selvittää tiedonsiirtojen pääasialliset määritelmät, yleiset tietojenkäsittelyvaatimukset sekä tiedonsiirtovälineet, joiden avulla tiedonsiirtoja voidaan tehdä lainmukaisesti. Tutkielman johtopäätökset pyrkivät vastaamaan pääkysymyksiin ja antamaan tutkijan tulkinnan kansainvälisten tiedonsiirtojen asiayhteydessä.

Pääasialliset lainsäädännölliset tutkimusalueet ovat GDPR:n säännökset ja tietosuojaviranomaisten ratkaisukäytäntö tiedonsiirtoihin liittyvissä oikeustapauksissa. Tutkielmassa käytetään oikeuskirjallisuutta ja muita aiheeseen liittyviä julkaisuja johtopäätöksien tueksi. Kirjallisuuteen liittyy perinteistä oikeuskirjallisuutta, asiantuntijalausuntoja, tietokantoja, artikkeleita ja muuta aiheeseen liittyvää kirjallisuutta.

Kansainväliset tiedonsiirrot ovat olleet kiistelty osa-alue tietosuojalainsäädäntöä ja aiheelle tarvitaan sen vuoksi lisätutkimusta. Oikeustila on nykyisessä tietosuojan oikeusjärjestelmässä sirpaleinen ja tiedonsiirtojen vaatimukset ovat epäselviä. Eri viranomaiset, kuten kansalliset tietosuojaviranomaiset ja Euroopan tietosuojaneuvosto, pyrkivät yhdenmukaistamaan tietosuojalainsäädännön tulkintaa EU:ssa, mutta ristiriitaisuuksia tulkinnalle ja tiedonsiirtojen vaatimusten implementoinnille on olemassa. Myös näihin ristiriitaisuuksiin pyritään tutkielmassa vastaamaan oikeusdogmaattisen tutkimuksen ja johtopäätösten avulla. Tutkielman yleishyöty on täten pyrkimys hahmottaa, mitä tiedonsiirtovälineitä ja tietojenkäsittelyn vaatimuksia tulee noudattaa, jotta tiedonsiirrot tehdään lainmukaisina.

Asiasanat: tietosuoja, teknologia, henkilötieto, kansainväliset tiedonsiirrot, tiedonsiirtovälineet, GDPR, vertailu

Sisällysluettelo

Lähteet

Kirjallisuus

Bärlund, Johan – Nybergh, Frey: Finlands civil- och handelsrätt - En introduktion, Helsinki 2013, s. 9–14, s. 97

Carey, Peter: Data Protection – A practical guide to UK and EU law, Yhdistyneet Kuningaskunnat 2018, s.28-29, s.35-36, s.40, s.85, s. 105-107, s. 108-115, s. 109, s. 110-114, s.114-115, s. 115-116, s.117, s.121, s. 162-163

Daley, Bruce: Where data is wealth: profiting from data storage in a digital society, Oakamoor 2015, s. 3-5, s. 10-11, s.13-14.

Hemmo, Mika: Sopimusoikeus I, Helsinki 2005, s.114

Hemmo, Mika: Sopimusoikeus III, Helsinki 2005, s.11–15

Ilmarinen, Vesa – Koskela, Kai: Digitalisaatio, Yritysjohdon käsikirja, Helsinki 2015, s.136–137

Innanen, Antti – Saarimäki, Jarkko: Internetoikeus, Helsinki 2012, s.97–103

Korpisaari, Päivi – Pitkänen Olli – Warma-Lehtinen Eija: Tietosuoja, Helsinki 2022, s.3–4, s. 5–7, s.8–9 s.25–28, s.40–41, s.58–69, s.73–74, s.76–78, s.83–84, s. 87–88, s. 100, s.102–103, s.107, s. 299, s. 345–346, s.372, s.443, s.457–458, s.468, s. 486, s. 494, s.753–755

Määttä, Tapio – Paso, Mirjami: Johdatus oikeudellisen ratkaisun teoriaan, Helsinki 2022 s. 3 ja s.34–35

Nääv, Maria – Zamboni, Mauro – Andersson, Håkan – Bakardjieva Engelbrekt, Antonia – Bastidas, Vladimir – Grahn-Farley, Maria – Gräns, Minna – Hydén, Håkan – Kleineman, Jan – Reichel, Jane – Samuelsson, Joel – Schultz, Mårten – Spaak, Torben – Svensson, Eva-Maria – Valguarnera, Filippo – Wahlgren, Peter: Juridisk Metodlära, Ruotsi 2018, s. 21–26

Peczenik, Alexander: Juridikens allmänna läror, Ruotsi 2005 s. 249–251

Reka, Hazir: Companies struggle with GDPR and global privacy—a report, Thomson Reuters Legal Insights Europe 2019

Rosemary, Jay: Data Protection Law and Practice – Fifth edition, Lontoo 2020, s. 1

Staunton, Ciara – Slokenberga, Santa – Parziale, Andrea – Mascalzoni, Deborah: Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research, Bolzano, Lontoo, Uppsala, Rooma 2022, s. 2-3

Viljanen, Mika – Parviainen, Henni: AI Applications and Regulation: Mapping the Regulatory Strata, Turku 2022, s. 2–3

Vuotilainen, Tomi: Oikeus tietoon – informaatio-oikeuden perusteet, Helsinki 2019, s.88–89

Vuorenpää, Mikko – Helenius, Dan – Hietanen-Kunwald, Petra – Hupli, Tuomas – Koulu, Risto – Lappalainen, Juha – Lindfors, Heidi – Niemi, Johanna – Rautio, Jaakko – Saranpää, Timo – Turunen, Santtu – Virolainen, Jyrki: Prosessioikeus, Helsinki 2021, s. 292–296

W. Kuan Hon: Data localization laws and policy, Lontoo 2016, s. 69–70

Yakovleva, Svetlana: Personal data transfers in international trade and EU law: A tale of two “necessities”, Amsterdam, 2020, s. 888-889

Öman, Sören: Dataskyddsförordningen (GDPR) m.m. – En kommentar, Tukholma 2019 s.65–67, s.69–71, s. 100–101, s.108–109, s.111–112, s. 113–114, s. 411, s. 425–426, s. 480–481, s. 486–487, s. 488–489

Oikeuskäytäntö

Suomi

KÄO R 22/6666

TSV 1509/452/18

TSV 8040/163/2019

TSV 7684/171/22

Ruotsi

HFD 2016 ref. 40

Ranska

SAN 2023-003

Tanska

Datatilsynet 10-09-2021

Eurooppa

ETN 2021:313

ETN 2022:325

ETN 2023:1

EUT C-311/18

EUT C-184/20

EUT C-131/12

EUT T-557/20

Viranomaislähteet

ETN (Euroopan tietosuojaneuvosto) ohjeistus 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa.

ETN evästebanneri työryhmän raportti 18. Tammikuuta 2023, s. 4

ETN yleiset suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi 18. kesäkuuta 2021, s. 10 ja s. 45

ETN yleiset suositukset 01/2020, kohdat 74–76

ETN Ohjeet 4/2021 käytännesäännöistä siirtovälineinä

Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework 2023, s.22-26

Statens offentliga utredningar (SOU) 2003:40 s.190–197

Internetlähteet

Cox, Arthur 2021 – What are BCRs? (https://www.arthurcox.com/knowledge/what-are-bcrs/ vierailtu 30.5.2023)

EU Cloud Code of Conduct https://eucoc.cloud/en/home (vierailtu 19.8.2023)

European data protection board final one stop shop decisions tietokanta https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en (vierailtu 25.2.2023)

Euroopan Komission kotisivut riittävyyspäätöksistä https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (vierailtu 25.2.2023)

Euroopan tietosuojaneuvoston kotisivut: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_fi (vierailtu 16.3.2023)

Tietosuojavaltuutetun toimiston kotisivut: https://tietosuoja.fi/etusivu (vierailtu 16.3.2023)

Tietosuojavaltuutetun ratkaisukäytäntö https://www.finlex.fi/fi/viranomaiset/tsv/ (vierailtu 26.6.2023)

Standard Contractual Clauses for international transfers https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (vierailtu 26.6.2023)

Yle 10.3.2023 https://yle.fi/a/74-20021717 (vierailtu 9.5.2023)

Lyhenteet

BCR – Binding Corporate Rules

ETA – Euroopan talousalue

EU – Euroopan unioni

CoC – EU Cloud Code of Conduct

EUT – Euroopan Unionin tuomioistuin

EDPS – Euroopan tietosuojavaltuutettu

ETN – Euroopan Tietosuojaneuvosto

GDPR – Yleinen tietosuoja-asetus 2016/679

HFD – Högsta förvaltningsdomstolen, Ruotsi

ICT – Tieto ja viestintäteknologia

IP-osoite – Internetin protokollaosoite

ISO – International Organization for Standardization

SAN – Ranskan tietosuojaviranomaisen päätökset

SCC – Komission hyväksymät tietosuojaa koskevat vakiolausekkeet

SEUT – Euroopan unionin toiminnasta tehty sopimus 2012/C 326/01

SOU – Svenska offentliga utredningar

TCF – Transparency & Consent Framework IAB Europe

TSV – Tietosuojavaltuutetun toimisto, tietosuojavaltuutettu

1. Johdanto

1.1 Yleisesti tietosuojasta ja sen kehityksestä

Teknologinen kehitys on mullistanut yhteiskuntamme. Tietokoneiden kehittyminen 1970- ja 1980-luvuilla aiheutti yleisen huolen siitä, että jatkuva teknologinen kehitys saattaa heikentää ihmisoikeuksia. Tämä lisäsi painetta Euroopassa ja kansainvälisessä oikeusyhteisössä oikeusjärjestelmän uudelleentarkastelulle. Ensimmäiset kansainväliset lainsäädäntötyökalut, joilla teknologisestä kehityksestä aiheutuviin ihmisoikeusongelmiin pyrittiin puuttumaan, kehitettiin 1980-luvun alussa ja tästä lähtien lainsäädäntöprosessissa pyritään pysymään teknologisen kehityksen vauhdissa mukana.[1]

Tiedonsiirto on tapahtuma, jossa tietoja siirtyy tai jaetaan yhdeltä taholta toiselle. Tietoja siirretään nykyään erilaisten teknologisten ratkaisujen avulla, mutta myös fyysisesti ympäri maailmaa ja lähiympäristössä eri tavoin. Henkilötieto on GDPR:n määritelmän mukaan rekisteröidyn henkilön antama henkilötieto organisaatiolle, jota organisaatio pystyy käsittelemään eri tavoin. Henkilötietojen käsittelyn avulla organisaatio pystyy käyttämään henkilötietoja erilaisissa toimenpiteissä. Kun henkilötietoja siirretään, kyseessä on henkilötietojen käsittelytoimenpide, jossa henkilötietoa siirretään yhdeltä taholta toiselle. Kyseessä on usein ICT-järjestelmän kautta tehty toimenpide, jossa henkilötieto lähetetään toiselle taholle siten, että se kirjataan myös vastaanottavan tahon järjestelmään. Myös kirjeillä lähetetty henkilötieto on henkilötietojen siirtämistä.

Digitalisaation ja teknologisen kehityksen myötä tiedosta ja datasta on tullut hyödyke. 2000-luvulla organisaatiot ja yritykset huomasivat, että dataa ja tietoa, jota ennen käytettiin lähinnä hallinnollisiin ja arkipäiväisiin organisaation tehtäviin, pystyttiin käyttämään myös liiketoiminnassa hyödykkeenä. Monet yritykset tekevät nykyään suuren osan liikevaihdostaan hyödyntämällä tätä dataa ja tietoa eri tavoin. Kyseessä on erityisesti henkilötietojen käyttämistä hyödykkeenä näissä tapahtumissa. Näistä yrityksistä huomattavia ovat muun muassa Google, Twitter (nykyään X) ja eBay.[2] Datan kerääminen muun liiketoiminnan ohessa voi antaa osittaista lisäarvoa päätuotteen myymisen lisäksi. Esimerkiksi, terveyspalveluja myyvä yritys voi pitää yhteyttä vakioasiakkaihinsa helposti tulevaisuudessa tallentamalla heitä koskevat terveystiedot omiin yrityksen tietokantoihinsa.[3] Datan ja tiedon hallinta yleisesti on myös

[1] Rosemary 2020 s.1
[2] Daley 2015 s.13–14
[3] Ilmarinen – Koskela 2015, s. 136–137

merkittävä osa organisaatioiden arkipäiväisistä toimintaa. Tyypillisesti suuren organisaation sisällä siirretään dataa ja tietoa usein kansainvälisesti valtioiden välillä. Myös uudet teknologiset ratkaisut, kuten algoritmit ja tekoälyt käyttävät suuria määriä dataa ja tietoa. Näiden teknologioiden tietojenkäyttömahdollisuudet, voivat tuoda entistä enemmän eettisiä kysymyksiä liittyen henkilötietojen käyttöön.[4]

Yksi ongelma toisin sanoen on datan ja tiedon olemus hyödykkeen ja yleistiedon välillä. Data on arvokasta ja sitä voidaan hyödyntää liiketoiminnassa ja muissa organisaation tehtävissä, mutta datan tai tiedon käyttäminen voi olla ihmisoikeudellisesta näkökulmasta kyseenalaista. Varsinkin rekisteröityjen luonnollisten henkilöiden tietojen käsittely liiketoiminnassa on tietosuojalainsäädännön mukaista henkilötietojen käsittelyä, jolloin yhteisön on otettava huomioon tietosuojalainsäädännön vaatimukset henkilötietojen laillista käsittelyä varten. Yksityishenkilö, joka antaa henkilötietojaan tai dataa yhteisön käytettäväksi, ei välttämättä tiedä miten niitä käytetään, eikä siksi halua antaa henkilötietojansa käytettäviksi kaikkiin yhteisön tai yrityksen tarkoituksiin. Tietoa ja dataa ei kuitenkaan voida yksiselitteisesti määritellä arvoesineeksi. Toisin kuin muut immateriaaliset esineet, kuten patentit, ei esimerkiksi tietoa tai dataa voi omistaa samalla tavalla. Käytännössä on mahdotonta valvoa ja tietää tarkasti, kenellä tai millä taholla on halussaan tiettyä tietoa tai dataa.[5] Yhteisöllä voi olla rekisteri henkilötiedoille, mutta se ei kuitenkaan tee niistä immateriaalisia esineitä. Tämän vuoksi datan ja tiedon vaihdanta ei vastaa täysin perinteistä juridisten esineiden vaihdantaa.

Yhdistyneitten kansakuntien ihmisoikeuksien yleismaailmallisen julistuksen (10.12.1948) 12 artiklan mukaan kenenkään yksityiselämään ei saa mielivaltaisesti puuttua. Euroopan ihmisoikeussopimuksen (63/1999) 8 artiklan 1 osan mukaan kaikilla on oikeus nauttia yksityiselämästä. Yksityiselämän suojelu on ollut kansainvälisissä sopimuksissa tärkeää jo kauan. Teknologian kehittymisen myötä yksityiselämän suojan merkitys on laajentunut. Yksityiselämästä hankittu tieto tai data voi heikentää yksityisen henkilön yksityiselämän suojaa varsinkin, jos tätä tietoa siirretään ja jaetaan. EU:n lainsäädännössä määritellään tältä osin yksityiselämän suoja ja henkilötietojen suoja kahtena erillisenä osana. Yksityiselämän suoja on kokonaisuus oikeusperiaatteista, joissa turvataan fyysisten henkilöiden yksityisyys, sisäinen ja ulkoinen koskemattomuus ja esimerkiksi uskonnon- tai seksuaalisen suuntautumisen vapaus. Tietosuoja taas koskee fyysisten henkilöiden henkilötietojen suojaa ja tämän tiedon

[4] Viljanen – Parviainen 2022, s. 2–3
[5] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.25–28

suojaamiseen sen vaihdannassa, varsinkin, kun yhteisöt käsittelevät näitä henkilötietoja eri tarkoituksiin.[6]

Euroopan unionissa henkilötietojen suojan määritelmää on tarkennettu Euroopan unionin perusoikeuskirjan 8 artiklan 1 kohdassa sekä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklassa.[7] Euroopan unionin perusoikeuskirjan ja SEUT:n mukaan jokaisella on oikeus henkilötietojensa suojaan. Lisäksi EU:n perusoikeuskirjan 8 artiklan kohtien 2 ja 3 mukaan tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten asianomaisen henkilön suostumuksella. Riippumaton viranomainen valvoo sääntöjen noudattamista.

Yksi merkittävimmistä muutoksista henkilötietojen suojaamisessa oli EU:n päätös säätää kattava säännös henkilötietojen suojaamiselle ja asianmukaiselle käsittelylle. Vuonna 27.4.2016 EU:n yleinen tietosuoja-asetus (EU) 2016/679 (GDPR) astui voimaan. GDPR:n vaikutusta tietosuojaan Euroopan unionissa sekä kansainvälisesti voi arvioida olevan varsin merkittävää. Suomessa ja Euroopan unionissa GDPR:n vaikutukset ovat olleet tämän tutkielman kirjoittamisen aikana voimassa noin kuusi vuotta.

GDPR:llä on useita vaikutuksia. Organisaatioiden ja yritysten vastuullisuuteen liittyviä vaikutuksia ovat esimerkiksi tietoisuus ja huolellisuus tietosuojassa. Yhteisöihin, yrityksiin ja organisaatioihin liittyvät vaikutukset ovat esimerkiksi hallinnolliset seuraamusmaksut, joita voidaan määrätä, kun yhteisö jättää noudattamasta GDPR:n vaatimuksia. Suomen vastuuviranomainen, eli tietosuojavaltuutetun toimisto, alkoi määräämään seuraamusmaksuja ja seuraamuksia ensimmäistä kertaa vuonna 2020. Kansalliset viranomaiset EU:ssa määräävät seuraamusmaksuja jäsenvaltioittain. Kansainvälisissä tapauksissa, joissa mukana on enemmän kuin yksi EU:n valtio, määrää Euroopan tietosuojaneuvosto seuraamuksia ja seuraamusmaksuja. Yhteisöjen hallinnolliset muutokset ovat myös olleet merkittäviä, ja datan sekä tiedon säilyttämisen ja vaihdannan vaatimuksia on tarkennettu ja kiristetty. GDPR on ollut esikuva muille valtioille ja toiminut eurooppalaisena innovaationa muualle maailmaan. Esimerkiksi Intia ja Brasilia ovat implementoineet GDPR:n kaltaisia lakeja.[8]

[6] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.8–9. Kirjailijat toteavat muun muassa, että henkilötietojen suoja on käytännössä yksi yksityiselämän suojan osa-alue. Henkilötietojen suojaaminen ei kuitenkaan kata kaikkea yksityiselämän suojaan koskevaa, sillä myös yksityiselämän suojan ulkopuolella olevat tiedot voivat olla henkilötietoja ja ainoastaan kuulua tietosuojan osa-alueeseen.

[7] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.40–41

[8] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.753–755

Tietosuojalainsäädännön oikeustilasta käy ilmi mielipiteitä muun muassa oikeustieteellisessä kirjallisuudessa, joiden mukaan GDPR:n vaatimukset sekä lainsäädäntö on sirpaleista ja vaikeasti ymmärrettävää.[9] Tietosuoja on varsin uusi oikeustieteen alue, josta on viime vuosikymmenen aikana ilmestynyt enemmän kirjallisuutta ja tieteellistä tutkimusta. Kun tiedosta, datasta ja varsinkin henkilötiedoista on tullut hyödyke kaupallisesti ja hallinnollisesti, on kirjallisuudessa tutkittu, miten tietoja voidaan siirtää tai luovuttaa.

Henkilötietojen siirtämistä vaikeutettiin GDPR:n säännöillä. Varsinkin kansainväliset tiedonsiirrot ovat olleet keskustelun ja tutkimusten keskiössä liittyen yhteisöjen kansainväliseen kauppaan ja liikevaihtoon sekä yleiseen arkipäiväseen toimintaan. Nykyään tiedonsiirto on helppoa, ja dataa tai tietoa voi siirtää välittömästi vastaanottavalle osapuolelle. Data tai tieto on käytännössä immateriaalinen esine, jota eri juridiset henkilöt pystyvät hallinnoimaan. Tämä eroavaisuus fyysisiin esineisiin, tekee datan ja tiedon siirrettävyydestä erityisen kiinnostavaa. Dataa ja tietoa siirtyy maailman ympäri osapuolilta toisille niin paljon, että realistisesti kaiken tietoliikenteen määrän laskeminen on vaikeaa.[10] Tämän lisäksi datan ja tiedon vaihdantaa ei pystytä täysin vertaamaan perinteiseen yksityisoikeudelliseen sopimus- ja velvoiteoikeuteen, sillä kyseessä on käytännössä ajatuksia, ideoita ja muita immateriaalisia esineitä, joiden hallintaa on vaikea täysin valvoa.

Eri valtioiden omien tietosuojavaatimusten takia GDPR:n tavoitteena oli ensiksi varmistaa EU:n sisäisten henkilötietojen turvallisuus. GDPR sääntelee myös henkilötietojen siirtämistä EU:n sisältä EU:n ulkopuolelle. GDPR:n 1 luvun 4 artikla määrittelee henkilötiedon näin:

> ”henkilötiedolla tarkoitetaan kaikkia tunnistetun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja.”

EU:n ulkopuolelle siirtyvistä henkilötiedoista on säännelty GDPR:n 5 luvun 45 artiklan mukaisesti: EU:n komission antamilla riittävyyspäätöksillä. Käytännössä päätökset tarkoittavat, että EU:n komissio voi antaa päätöksen siitä, että EU:n ulkopuoleisella valtiolla, eli kolmansilla mailla, on samat vaatimukset tietosuojalle ja tietoturvalle kuin EU:lla ja sen jäsenmailla. Silloin kansainväliset tiedonsiirrot EU:sta kolmannelle maalle ovat helpompia toteuttaa ja ne tarvitsevat vähemmän suojatoimenpiteitä kuin ilman päätöstä.

[9] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.3–4

[10] Daley 2015, s.3–5 – Datan ja tiedon määrään ympäri maailman pystyy laskemaan tai ainakin arvioimaan. Daley toteaa, että muun muassa Sloan Digital Sky Survey teleskooppi keräsi sen ensimmäiset operatiiviset kuukaudet enemmän dataa kuin koko sen ajan, kun astronomiaa on kansainvälisesti harjoitettu tieteenä. Yhdistyneen kuningaskunnan viestinnän pääkonttori käyttää tiedon seurantajärjestelmää nimeltä Tempora. Tämä seurantajärjestelmä tallentaa kaikki puhelinsoitot, sähköpostiviestit, Facebook-päivitykset ja kaiken internetin käyttöön liittyvän tietoliikenteen UK:ssa. Datan seuraamista käytetään tiedonsiirtojen tilastoimiseen ja seuraamiseen, se on hyödyllistä teknologisen kehityksen näkökulmasta.

Mikäli EU:n komissio ei ole antanut riittävyyspäätöstä EU:n ulkopuoliselle valtiolle, pitää tiedonsiirrot näihin valtioihin tehdä noudattaen GDPR:n lukua 5 artikla 46 käyttäen GDPR:n määrittelemiä tiedonsiirtovälineitä. Riittävät suojatoimet ovat monipuolisia ja sekä GDPR:ssä että kirjallisuudessa on luetteloitu erilaisia vaihtoehtoja tiedonsiirtovälineille, joita osapuolet voivat käyttää. Riittävien suojatoimien käyttämistä ja niiden todistamista on kuitenkin kritisoitu hankalaksi sekä epäselväksi prosessiksi. Seuraavaksi kirjoittaja käy läpi tämän tutkielman tutkimuskysymyksiä ja aiheen rajausta.

1.2 Tutkimuskysymys ja aiheen rajaus

Tämän tutkielman tarkoitus on vastata kysymyksiin siitä, miten kansainvälisiä tiedonsiirtoja tehdään EU:n ulkopuolelle GDPR:ssä määritetyille kolmansille maille GDPR:n 5 luvun 46 artiklassa mainittujen suojatoimien avulla. Tutkielma keskittyy yleisiin tiedonsiirtovaatimuksiin ja siihen, mitä menetelmiä osapuolet voivat käyttää kansainvälisten tiedonsiirtojen suojatoimien todistamiselle. Monet GDPR:n 5 luvun 46 artiklassa käsiteltävät suojatoimet liittyvät tiedonsiirtosopimuksiin, joissa osapuolet määrittelevät ja todistavat, miten riittävä tietosuoja on otettu huomioon tiedonsiirroissa. Käytännössä tämä tarkoittaa sitä, että sopimuskokonaisuudessa on oltava GDPR:n 5 luvun 46 artiklasta sopimusehto, joka määrittelee tiedonsiirron tietosuojan. Näiden sopimusten vaatimusten ymmärtäminen voi olla ratkaisevaa yhteisölle, joka haluaa hyödyntää henkilötietojen tuomaa lisäarvoa liikevaihdossa ja toiminnassaan yleisesti. Liiketoiminta ei tietenkään aina ole tiedonsiirron syy, vaan yhteisöt siirtävät henkilötietoja myös muista syistä. Syy voi olla esimerkiksi yhteisön asiakaskunnan tavoittaminen myös jatkossa. Tiedonsiirto oikealla ja laillisella tavalla on osa organisaatioiden compliance-vaatimuksia siinä mielessä, että yksityishenkilöt voivat luottaa henkilötietojensa asianmukaiseen ja tietoturvalliseen rekisteröintiin ja käsittelyyn. Näin ollen tietosuoja organisaatiossa on osa isompaa compliance-kokonaisuutta, jolla rakennetaan yhteisön päivittäistä toimintaa, yritysten liiketoimintaa tai muun organisaation päätavoitteisiin liittyvää toimintaa.[11] Kun yhteisö noudattaa lainsäädännön vaatimuksia, se välttyy myös hallinnollisilta ja mahdollisesti rikosoikeudellisilta seuraamuksilta. Tutkielman lisäarvo auttaa organisaatioita ja myös yksityishenkilöitä ymmärtämään, miten yhteisöt voivat tehdä kansainvälisiä tiedonsiirtoja kolmansiin maihin GDPR:n vaatimusten mukaisesti.

Tutkimuksen toinen tutkimuskysymys liittyy eri tiedonsiirtovälineiden vaatimuksiin ja vaikutuksiin. Tutkielma käsittelee eri tiedonsiirtovälineiden vaikutuksia, hyötyjä ja

[11] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.372 – Sanaa ”compliance” käytetään myös synonyyminä vaatimustenmukaisuudelle ja vastuullisuudelle.

haittapuolia. Tarkoitus on oikeuskäytännön ja kirjallisuuden kautta selvittää, miten tiedonsiirtovälineitä käytetään kansainvälisissä tiedonsiirroissa tehokkaasti asianmukaisten suojatoimien todistamiseksi. Käytettävinä olevat tiedonsiirtovälineet ovat erilaisia ja ne ovat pääasiallisesti tarkoitettu käytettäviksi eri tilanteissa, vaikkakin niiden lainsäädännölliset vaikutukset ovat pitkälti samoja.

Aiheen rajauksen takia tutkielma käsittelee tietojenkäsittelyä käsitteleviä oikeustapauksia. Käsiteltävillä oikeustapaukset tulkitsevat tietojenkäsittelyä yleisesti ja kansainvälisten tiedonsiirtojen kannalta. Käytännössä oikeustapaukset ovat viranomaisten päätöksiä, kuten tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston päätöksiä. Näiden tapausten tulkitsemisen syy on se, että ne ottavat useimmiten kantaa johonkin kansainvälisen tiedonsiirtoon liittyvään kysymykseen. Tarkoituksena on antaa yleiskuva siitä, miten jäsenmaista siirretään henkilötietoja EU:n ulkopuolelle, mikäli näille maille ei ole annettu EU:n komission riittävyyspäätöstä. Aiheen laajuuden takia on vaikeaa antaa kokonaisvaltainen näkökulma siitä, miten kaikissa EU:n jäsenmaissa erityislainsäädäntöä tulkitaan. GDPR:n tulkinnalla ja oikeuskäytännöllä voidaan kuitenkin kuvata ainakin yleiset säännöt sille, miten ja kuinka oikeaoppisesti asetuksen sääntöjä ja vaatimuksia implementoidaan oikein kansainvälisissä tiedonsiirroissa. Tutkielman on hyödyllinen varsinkin yrityksille, organisaatioille, yhteisöille sekä aiheesta kiinnostuneille, koska aihetta ei ole tutkittu vielä paljon ja lisätutkimukselle on kirjoittajan mielestä tarvetta.

Tutkielman lopputuloksien tavoite on vastata seuraaviin tutkielman pääkysymyksiin eli:

1. mitkä ovat yleiset vaatimukset tiedonsiiroille, 2. mitkä ovat vaatimukset kansainvälisille tiedonsiirroille ja 3. mitä eri tiedonsiirtovälineet ovat ja mitkä ovat niiden eroavaisuudet. Pääkysymysten lopputulokset käsitellään viimeisessä luvussa 5.

1.3 Tutkielman metodiikka

Tutkielman pääasiallinen metodi on oikeusdogmatiikka tai lainoppi. Tutkielmassa käytetään tuloksia varten oikeuskirjallisuutta, muuta kirjallisuutta, lainsäädäntöä ja oikeustapauksia. Moni lainoppinut on tutkinut oikeusdogmatiikkaa oikeustieteellisen tutkimusprosessin metodina. Esimerkiksi Jan Kleineman toteaa, että oikeusdogmatiikka tutkii oikeusjärjestelmää ja oikeustilaa *de lege lata*-argumentaation kautta. *De lege lata*-tulkinta tutkii tämänhetkistä oikeusjärjestelmää.[12] Varsinkin pohjoismaisessa oikeusjärjestelmässä oikeusdogmatiikan luonne kiteytyy siitä näkökulmasta, että usein myös abstrakteista oikeussäännöistä voidaan

[12] Nääv – Zamboni – Andersson – Bakardjieva Engelbrekt – Bastidas – Grahn-Farley – Gräns – Hydén – Kleineman – Reichel – Samuelsson – Schultz – Spaak – Svensson – Valguarnera – Wahlgren 2018, s. 21–26

tehdä selviä ja argumentoivia johtopäätöksiä. Tapio Määttä ja Mirjami Paso taas kuvaavat oikeusdogmatiikkaa oikeustieteellisen tutkimuksen keskeisenä suuntauksena. Oikeusdogmaattinen metodi käyttää varsinkin kielellistä, systemaattista ja tavoitteellista tulkintaa erilaisten johtopäätösten tekemiseen.[13] Näistä näkökulmista oikeusdogmatiikan pääidea on siis laintulkinta ja siitä vedettävät johtopäätökset. Tulkinta oikeusdogmatiikan kautta antaa vastauksia pääasiallisesti sille, miten tietty oikeussääntö tai oikeustapaus antaa vastauksen tietylle oikeustieteelliselle kysymykselle. Yksinkertaisesti oikeusdogmatiikka systematisoi ja tulkitsee voimassa olevaa lakia.[14]

Tässä tutkielmassa yksi pääkysymyksistä on selvittää miten henkilötietoja siirrettään laillisesti EU:sta kolmansiin maihin. Oikeusdogmaattisen metodin kautta tutkielma selvittää, systematisoi ja tulkitsee voimassa olevaa lakia varsinkin *de lege lata*-näkökulmasta. Pääasiallisesti lähteet tutkielmalle on lainsäädäntö, oikeuskirjallisuus, muu kirjallisuus ja oikeustapaukset. Tutkielma sisältää myös joitain *de lege ferenda*-tyyppisiä johtopäätöksiä, sillä tietosuoja on tällä hetkellä erittäin nopeasti kehittyvä oikeustieteen osa-alue. Nämä johtopäätökset liittyvät mahdolliseen uuteen ratkaisukäytäntöön ja niiden avulla voidaan tehdä uusia johtopäätöksiä oikeusjärjestelmän nykytilasta. Näitä tapauksia on tutkijan mielestä paljon ja täysin yhtenäistä konsensusta tietosuojalainsäädännön tulkinnasta vaikuttaa olevan vaikeaa määritellä. Varsinkin tietosuojaan liittyvät määritelmät ovat laajalti kritisoituja ja teknologian kehityksen myötä niiden tulkinta saattaa nopeastikin muuttua. Toinen ongelmallisuus liittyy näyttöön henkilötietojen siirroissa. Kyseessä voi olla teknisesti vaikeista järjestelmistä, joiden yksiselitteisyys oikeustapauksissa ei ole mahdollista.

Pääkysymyksen vastaamiseksi pitää tutkielmassa yksiselitteisesti selittää mitä vaatimuksia tiedonkäsittelylle eli tiedonsiirroille yleisesti on ja tämän jälkeen kuvata niitä tiedonsiirtovälineitä, jotka määritellään GDPR:ssä.

Aihe rajautuu kuitenkin vain käsittelemään GDPR:n mukaisia tietosuojan vaatimuksia, sillä kuten edellä mainittiin, erikoislainsäädännön tulkinta kaikissa EU:n maissa ja kolmansissa maissa olisi kirjoittajan mielestä ainakin tässä tutkielmassa liian kattava ottaen huomioon tutkielman pituuden. Tämä on kuitenkin yksi aihe, josta voisi kirjoittaa enemmän myös tulevaisuudessa.

Seuraavaksi käsittelen tutkielmaan liittyviä muita yleisiä kysymyksiä aiheesta. Tutkielma on jaettu eri osiin. 2 luku käsittelee yleisesti aihetta ja GDPR:n määritelmiä, 3 luku käsittelee

[13] Määttä – Paso 2022, s. 3 ja s. 34–35
[14] Peczenik 2005, s. 249–251

GDPR:n yleisiä tiedonsiirtovaatimuksia ja yleisiä periaatteita, 4 luku käsittelee erityisesti tiedonsiirtoja ja niihin liittyviä tiedonsiirtovälineitä ja 5 luku käsittelee tutkielman lopputuloksia ja johtopäätöksiä.

2. Yleisesti aiheesta ja tietosuojan yleiset periaatteet ja määritelmät

2.1 Kansainvälisen tiedonsiirron hallinto ja yleisesti tiedonsiirroista

Seuraavassa luvussa, käsitellään lyhyesti tietosuojalainsäädännön hallintoa EU:ssa sekä kansainvälisten tietosiirtojen vaatimuksia ja määritelmiä, jotka ovat relevantteja tutkielman aiheelle.

2.1.1 Tietosuojalainsäädännön hallinto

Aiheen rajausta varten, tutkielma käsittelee aluksi tietosuojalainsäädäntöä yleisesti. GDPR astui voimaan vuonna 2016 ja sitä alettiin soveltaa 25.5.2018. Tietosuoja on muodostunut EU:ssa omaksi oikeusjärjestelmäkseen. Perinteisen oikeusjärjestelmien osa-alueiden mukaan tietosuoja on muun muassa laskettu osaksi henkilöoikeutta.[15]

EU:ssa valvovana viranomaisena toimii Euroopan tietosuojaneuvosto (ETN). Kyseessä on riippumaton EU:n viranomainen, joka valvoo tietosuojanlainsäädännön yhdenmukaista käytäntöä koko unionissa. Sen toimintapaikka on Bryssel. ETN koostuu sekä kansallisten tietosuojaviranomaisten edustajista että Euroopan tietosuojavaltuutetun (EDPS) edustajista. Sen tehtäviin kuuluu: Yleisen tietosuoja-asetuksen ja poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin sekä toimielinten, elinten ja laitosten koskevan tietosuojadirektiivin yhdenmukaisen soveltamisen varmistaminen ja valvonta. Lisäksi ETN laatii yleisiä ohjeita, joiden tarkoitus on selventää GDPR:n käsitteitä ja määritelmiä.

Yleisten ohjeiden (myös yleiset ohjeistukset) tehtävä on varmistaa yhdenmukainen tulkinta GDPR:stä EU:ssa. ETN:lla on valtuus antaa sitovia päätöksiä kansallisille valvontaviranomaisille varmistaakseen yhdenmukaisen soveltamisen. Tässä tutkielmassa näitä päätöksiä kutsutaan nimellä ETN päätös (Final One Stop Shop decisions). Päätösten tekeminen kuuluu ETN:n vastuulle GDPR:n 60 artiklan mukaan yhteistyöstä kansallisten viranomaisten kanssa. Näillä ETN:n päätöksillä on aina tietty kansainvälinen rajoja ylittävä ulottuvuus, minkä vuoksi ne ovat kiinnostavaa oikeuskäytäntöä tässä tutkielmassa. Toisin sanoen tapauksissa on aina mukana ainakin kaksi eri EU:n jäsenmaata. Osapuolet tapauksissa eivät sijaitse vain

[15] Bärlund – Nybergh 2013 s. 97, Bärlund ja Nybergh kommentoivat tietosuojalainsäädäntöä osana henkilöoikeutta yksityisyyden näkökulmasta. Yksityisyys on tärkeä osa itsemääräämisoikeuden kannalta yhteiskunnallisissa suhteissa. Itsemääräämisoikeudella, fyysiset henkilöt pystyvä vaikuttamaan omaan yksityisyytensä suojaan organisaatioilta, henkilöiltä ja tietyiltä olosuhteilta. Tietosuojalainsäädäntö on tästä näkökulmasta erikoistuneempi uudempi haara henkilöoikeudesta, joka kehittyi yksilön oikeuksien yleistymisen myötä.

yhdessä EU:n maassa. Mukana voi olla moneen eri valtioon kuuluvia osapuolia myös EU:n ulkopuolella.

Kansallisesti Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto, joka valvoo kokonaisvaltaisesti tietosuojalainsäädännön noudattamista Suomessa. Tietosuojavaltuutetun toimisto koostuu tietosuojavaltuutetusta ja apulaistietosuojavaltuutetuista, jotka muodostavat yhdessä seuraamuskollegion. Seuraamuskollegio määrää GDPR:n mukaisista hallinnollisista seuraamusmaksuista. Lisäksi tietosuojavaltuutetun toimistoon kuuluu asiantuntijalautakunta, jolle on määrätty aikamääräinen toimikausi. Asiantuntijalautakunta antaa lausuntoja tietosuojalainsäädäntöön liittyvistä merkittävistä kysymyksistä tietosuojavaltuutetun pyynnöstä.[16] Hallinnollisesti ETN vastaa tietosuojalainsäädännön kokonaisvaltaisesta yhdenmukaisesta tulkinnasta koko EU:ssa ja kansalliset viranomaiset, kuten Suomessa toimiva tietosuojavaltuutetun toimisto, vastaavat jäsenmaiden omasta hallinnosta. Kansallisten tietosuojaviranomaisten ja Euroopan tietosuojaneuvoston kannanotot ovat tärkeitä varsinkin GDPR:n tulkinnassa. Tutkielmassa tulkitaan siksi oikeuskäytännössä pääasiallisesti näiden viranomaisten päätöksiä, jotka liittyvät kansainvälisiin tiedonsiirtoihin.

2.1.2 Tiedonsiirtovälineet

Tutkielmassa tärkeässä osassa ovat tietosuojalainsäädännössä ja kirjallisuudessa mainitut tiedonsiirtovälineet. Kyseessä on GDPR:n 5 luvun 46 artiklassa määritetyt vaatimukset, joilla henkilötietoja voi siirtää EU:sta EU:n ulkopuolelle, eli kolmanteen maahan. Tiedonsiirtovälineitä käsitellään tarkemmin tutkielman luvussa 4.

2.1.3 Yleiset tietojenkäsittelyperiaatteet

Toinen merkittävä osa kansainvälisiä tiedonsiirtoja, ovat yleiset tietojenkäsittelyperiaatteet. Yleiset tietojenkäsittelyperiaatteet määritellään GDPR:n 2 luvussa 5–11 artikloissa. Yleiset tietojenkäsittelyperiaatteet määrittävät ne yleiset vaatimukset, joita rekisterinpitäjän tai henkilötietojen käsittelijän on noudatettava henkilötietojen käsittelyssä.

Kansainvälisiissä tiedonsiirroissa, yleisiä tietojenkäsittelyperiaatteita on noudatettava samalla tavalla kuin henkilötietojen käsittelyn tilanteissa, joissa henkilötietoja käsiteltäisiin EU:n sisällä. Yleiset tietojenkäsittelyperiaatteet perustavat käytännössä pohjan henkilötietojen käsittelylle. Yleisiä tietojenkäsittelyperiaatteita käsitellään luvussa 3.

2.2 Yleisen tietosuoja-asetuksen määritelmät

Tutkielman tarkoitusta varten katsaus tietosuojan eri periaatteisiin ja määritelmiin on paikallaan. Tietosuojaan liittyvässä oikeuskäytännössä arvioidaan tyypillisesti, täyttävätkö tietyt tekniset ratkaisut lainsäädännölliset vaatimukset. Esimerkiksi tietosuojavaltuutetun päätöksessä 1509/452/18 osapuolen kantelun kysymyksenasetteluna on ollut tietojen käsittelyn lainmukaisuus. Jotta tietosuojavaltuutettu pystyisi ratkaisemaan asian, on sen saatava kattavaa selvitystä siitä, miten tapauksessa on loukattu lainsäädännön vaatimuksia ja miten GDPR:n vaatimuksia on rikottu. Tässä tapauksessa oli spesifisti kysymys henkilötietojen käsittelyn lainmukaisuudesta GDPR:n 6 artiklan mukaisesti. Tapauksissa pitää usein myös selvittää, miten tapauksen osapuolten eri tekniset ratkaisut toimivat.[17]

Näyttö tapauksissa on muuten samanlaista kuin toisissa oikeudenaloissa, mutta teknisten termien ja määritelmien läsnäolo on tyypillistä tietosuojaan liittyvissä tapauksissa. Siksi periaatteiden ja määritelmien merkitys ja ymmärrys on tietosuojassa erittäin tärkeää. GDPR:n luonne asetuksena merkitsee myös sitä, että kansallinen lainsäädäntö ei voi poiketa GDPR:n säännöistä. Tietenkin GDPR:stä voi poiketa esimerkiksi erikoislainsäädännön kautta. Kansallisella lainsäädännöllä myös täytetään GDPR:n epäkohtia ja epäselvyyksiä.[18] Suomessa esimerkiksi tietosuojalaki poikkeaa tietyin määrin GDPR:stä.

GDPR:n määritelmät koskevat siis kaikkia EU:n jäsenmaita ja jäsenvaltiot eivät voi määritellä GDPR:ssä tarkoitettuja määritelmiä ja aiheita itse. Tiedonsiirroissa kaikki jäsenmaiden yhteisöt ovat siis samalla tavalla velvollisia noudattamaan asetusta. Tämä koskee myös EU:n ulkopuolella sijaitsevia yhteisöjä, kun ne haluavat siirtää tietoja EU:n sisälle ja sen ulkopuolelle. Tutkielmasta on huomioitava vielä, että kun tutkielmassa käytetään määritelmää tiedonsiirto, niin kyseessä on aina myös GDPR:n mukaista henkilötietojen käsittelyä, sillä tietojen siirtäminen on GDPR:n 4 artiklan 2 kohdan mukaan tietojenkäsittelyä. Kaikki periaatteet ja määritelmät koskevat suoraan tai epäsuorasti tiedonsiirtoja, mutta tutkielman aiheen rajauksen takia tämä tutkielma käy tarkemmin läpi relevantit tiedonsiirtoihin liittyvät tietosuojan periaatteet ja määritelmät. Muita tutkielmassa esiintyviä periaatteita ja määritelmiä käydään läpi lyhyesti, mikäli niitä esiintyy.[19]

[17] Tietosuojavaltuutetun päätös 21.3.2023 1509/452/18
[18] Viljanen – Parviainen 2022, s.3
[19] Korpisaari – Pitkänen – Warma-Lehtinen 2022 ja Öman 2019 käyvät läpi kattavasti kaikki Yleisen tietosuoja-asetuksen periaatteet ja määritelmät. Euroopan tietosuojaneuvoston ohjeissa annetaan myös lisätietoa GDPR:n määritelmistä ja asetuksen tulkinnasta samalla tavalla kuin hallituksen esityksissä. Ohjeita lisätään Euroopan tietosuojaneuvoston verkkosivuille tarpeiden mukaan, ohjeiden valmisteluissa konsultoidaan myös Euroopan tietosuojaneuvoston ulkopuolisia tahoja.

2.2.1 Henkilötietojen käsittelyyn ja henkilötietojen hallinnointiin liittyvät määritelmät

GDPR:n 1 luku 4 artikla listaa asetuksen eri käsitteiden määritelmät. Henkilötieto on GDPR:n 4 artiklan 1 kohdassa määritelty kaikkena tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvinä tietoina. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Tietty spesifioitu tieto, jonka avulla pystytään tunnistamaan fyysinen luonnollinen henkilö on aina GDPR:n määritelmän mukaisesti henkilötieto. Tärkeää on myös huomioida, että GDPR soveltuu ainoastaan henkilötietojen käsittelyyn. Sitä ei sovelleta oikeushenkilöiden tai oikeushenkilön muodossa perustettujen yritysten tietojen käsittelyyn. GDPR ei myöskään sovellu kuolleiden henkilöiden tietojenkäsittelyyn.[20] Eli mikäli spesifioitu tieto, jota käsitellään, ei ole määritelmältään henkilötieto, GDPR:ää ei sovelleta. Luonnollinen henkilö määritellään GDPR:ssä lisäksi ”rekisteröitynä”. Asetuksessa rekisteröidyllä tarkoitetaan luonnollista henkilöä, jonka henkilötietojen käsittelyä säännellään. Myös tutkielmassa rekisteröity viittaa aina luonnolliseen henkilöön.

Henkilötiedon käsitettä on kuvailtu laajaksi. Kaikki tieto, jolla luonnollinen henkilö pystytään tunnistamaan, on henkilötietoa. Tärkeää on huomata, että määritelmässä on kyseessä luonnollinen henkilö. Eli kuten edellä mainittiin, tieto, joka liittyy yritykseen tai organisaatioon, eli juridiseen henkilöön ei liity GDPR:n määritelmässä tarkoitettuun henkilötietoon. Tieto, joka liittyy luonnolliseen henkilöön, on henkilötieto riippumatta siitä, onko luonnollinen henkilö tunnistettu tai tunnistettavissa. Eli myös tieto, jolla pystytään tunnistamaan, kuka luonnollinen henkilö on, luokitellaan henkilötiedoksi. Erilaiset henkilötiedot, jotka liittyvät tunnistettuun henkilöön tai jolla henkilö voidaan tunnistaa, ovat monenlaisia. Kyseessä voi olla esimerkiksi henkilötunnus, sormenjälki tai tietokoneen IP-osoite. [21]

Henkilötietojen käsittelyllä tarkoitetaan GDPR:n 4 artiklan 2 kohdassa:

> ”toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti kuten tietojen keräämistä, tallentamista, järjestämistä, säilyttämistä,

[20] Vuotilainen 2019, s.88–89
[21] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.58–69 – Uusi ratkaisukäytäntö on tosin haastanut tätä tulkintaa. Katso esimerkiksi EUT T-557/20.

> muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.”

Henkilötietojen käsittelyn määritelmä on laaja. Kaikki toimenpiteet, jotka liittyvät henkilötietojen käsittelyyn, ovat henkilötietojen käsittelyä. Kun henkilötietoja käsitellään manuaalisesti tai automaattisesti tekniikasta riippumatta, on kyseessä toimenpide, joka lasketaan henkilötietojen käsittelyksi. Käytännössä GDPR:n tarkoituksena on ollut poissulkea mahdollisuus siitä, että jotakin tiettyä toimenpidettä ei laskettaisi henkilötietojen käsittelyksi. Kuten edellä mainittiin, kaikki henkilötietoihin liittyvät toimenpiteet, riippumatta siitä, tehdäänkö ne automaattisesti tai manuaalisesti, ovat henkilötietojen käsittelyä.[22] Tätä väitettä tukee esimerkiksi Ruotsin valtion tutkimus vuonna 2003 tehty tutkimus ehdotuksesta laille ulkomaalaisten tiedoista, jonka mukaan tietokannasta löytyvän henkilötiedon välittäminen kirjallisesti, suullisesti tai sähköisesti on henkilötiedon käsittelyä.[23]

Rekisteri on GDPR:n 4 artiklan 6 kohdan mukaan jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminallisin tai maantieteellisin perustein jaettu. Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisteri on jäsentävä kokoelma henkilötietoja, joka on käytettävissä tietyillä kriteereillä. Rekisterin merkitystä on pohdittu ja sen suora aineellinen soveltamisala vaikutta olevan suppea.[24]

Rekisteröidyn suostumuksella tarkoitetaan GDPR:n 4 artiklan 11 kohdan mukaan:

> ”vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.”

Henkilötietojen tietoturvaloukkauksena tarkoitetaan GDPR:n 4 artiklan 12 kohdan mukaan:

> ”tietoturvaloukkausta, jonka seurauksena siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin tapahtuu.”

[22] Öman 2019, s. 65–67 – Öman toteaa lisäksi, että on vaikeaa keksiä olemassa oleva tilanne, jossa henkilötietoja ei määritelmän mukaan käsitellä. Näin ollen asetuksen tarkoitus määritelmälle on säilynyt vahvana.
[23] SOU 2003:40 s.190–191
[24] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 73–74 ja Öman 2019 s.69

Rekisterinpitäjä voi kerätä henkilötietoja monessa eri paikassa samaan aikaan mutta rekisterinpitäjällä on kuitenkin vain yksi GDPR:n mukainen päätoimipaikka. Päätoimipaikka määritellään GDPR:n 4 artiklan 16 kohdassa näin:

> ”a) päätoimipaikalla on merkitystä, kun kyseessä on rekisterinpitäjä, jolla on toimipaikkoja useammassa kuin yhdessä jäsenvaltiossa ja sen keskushallinnon sijaintipaikka unionisissa ”

Pääsäännön mukaan rekisterinpitäjä voi itse päättää missä sen päätoimipaikka sijaitsee. Päätoimipaikka määrittelee rekisterinpitäjän toiminnan valvontaviranomaisen. Viranomainen voi kuitenkin riitauttaa rekisterinpitäjän linjavedon.[25] Siksi toimipaikan määritelmä aiheuttaa paljon erimielisyyksiä samalla tavalla kuin esimerkiksi forumin riitauttaminen siviiliprosesseissa.[26]

2.2.2 Tiedonsiirron määritelmä

Tiedonsiirto on yllä käsitellyn määritelmän mukaan henkilötietojen käsittelyä. Tiedonsiirron määritelmästä on kuitenkin jouduttu antamaan lisätietoa ja ohjeistuksia, sillä tietojenkäsittelyn määritelmän laajuus kuitenkin jättää paljon tietosuojaan liittyviä kysymyksiä tulkinnanvaraiseksi.

GDPR ei tarkalleen selitä, mikä tiedonsiirron määritelmä on. Euroopan tietosuojaneuvoston yleisissä ohjeistuksissa 05/2021 määritellään kuitenkin ne tietojenkäsittelyn tilanteet, joissa tiedonsiirto on aina kyseessä. Nämä tilanteet ovat seuraavat:

> ”1. Rekisterinpitäjän tai käsittelijän rooli: GDPR soveltuu rekisterinpitäjän tai käsittelijän käsittelytoimiin.

[25] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s.83–84 – Toimipaikan valinta ja sen oikein määritteleminen on rekisterinpitäjän vastuulla. Yleisesti tietosuoja-asetus asettaa vastuun ja näyttövelvollisuuden rekisterinpitäjälle. Euroopan tietosuojaneuvoston ohjeistuksessa 07/2020 puhutaan osoitusvelvollisuudesta, joka on suoraan osoitettu rekisterinpitäjälle. Osoitusvelvollisuus määritellään tarkemmin GDPR:n 24 artiklassa, jonka mukaan rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi ja osoittamiseksi, että käsittely suoritetaan yleisen tietosuoja-asetuksen mukaisesti. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarpeen mukaan. Ideana on pitää rekisteripitäjä velvollisena tietojenkäsittelyssä ja näin ollen varmistaa kattava tietosuoja sen toiminnalle. Esimerkiksi päätoimipaikan valitseminen on siten rekisterinpitäjän riski. Kun rekisterinpitäjän linjaveto riitautetaan, joutuu se osoittamaan, että GDPR:n asetukset on otettu huomioon. Osoitusvelvollisuus vastaa käytännössä todistustaakkaa tai väittämistaakkaa prosessioikeudessa, siltä osin, että rekisterinpitäjän pitää pystyä osoittamaan oikean lainmukaisen tiedonkäsittelyn.

[26] Muun muassa Vuorenpää – Helenius – Hietanen-Kunwald – Hupli – Koulu – Lappalainen – Lindfors – Niemi – Rautio – Saranpää – Turunen – Virolainen 2021, s. 292–295

2. Rekisterinpitäjä tai käsittelijä (tietojen lähettäjä) lähettää henkilötietoja edelleen toiselle rekisterinpitäjälle, yhteisrekisterinpitäjälle tai käsittelijälle (tietojen vastaanottaja).

3. Tietojenkäsittelijä (tietojen lähettäjä) sijaitsee kolmannessa maassa tai tietojenkäsittelijä on kansainvälinen organisaatio riippumatta siitä, onko tietojenkäsittelijä velvoitettu GDPR:n 3 artiklan mukaan."

Tämän perusteella voidaan todeta, että 1. tiedonsiirrot koskevat vain GDPR:ssä määriteltyä rekisterinpitäjiä ja käsittelijöitä, 2. tiedonsiirto tapahtuu, kun rekisterinpitäjä tai käsittelijä lähettää henkilötietoja edelleen toiselle rekisterinpitäjälle, yhteisrekisterinpitäjälle tai käsittelijälle ja 3. kyseessä on myös tiedonsiirto, kun tiedot siirretään Euroopasta kolmanteen maahan.[27] Euroopan tietosuojaneuvoston yleiset ohjeet ovat, kuten edellä todettiin, ohjeita, joilla GDPR:n ja tietosuojalainsäädännön tulkintaa on tarkoitus yhdenmukaistaa EU:ssa. Ohjeet ovat täten ainoastaan suuntaa antavia ja ohjeiden suora oikeusvoima on ollut oikeuskäytännössä rajallista.[28] Siksi myös ohjeiden johtopäätöksiin on suhtauduttava kriittisesti GDPR:n tulkinnan ja oikeuskäytännön arvioinnin kannalta.

W. Kuan Hon on esittänyt tarkemman määritelmän kansainvälisille tiedonsiirroille. Hänen mukaansa tietosuojaviranomaiset määrittelevät tiedonsiirron niin, että tiedonsiirron edellytyksenä on henkilötietojen fyysinen siirtyminen maantieteelliseltä alueelta toiselle. Väittämä on seuraava: 1. Kolmannen maan henkilötietojen sijainnin edellytyksenä on välttämättä tietojen luovuttaminen tai siirtäminen vastaanottajalle, joka sijaitsee kyseisessä maassa, ja 2. että vastaanottajan on myös sijaittava kyseisessä maassa ja saattaa olla ainoastaan kyseisen maan toimivaltaisen tuomiovaltaan alainen.[29] Aihe on erittäin kiistelty, ja siihen liittyy myös kritiikkiä monien kirjailijoiden ja tutkijoiden taholta henkilötietojen määritelmän suhteen. Kuan Honin esittämä näkemys nostaa esiin tämänhetkisen tietosuojalainsäädännön pääongelman, nimittäin määritelmien epäselvyyden. Euroopan tietosuojaneuvosto haluaa lähestyä tietosuojalainsäädäntöä suppeamman tulkinnan kautta, kun taas kirjailijat ja tutkijat kuten Kuan Hon haluavat avata ja tarkentaa määritelmiä. Vaikka tuomioistuin ratkaisee asian lopullisesti, selkeitä linjanvetoja esimerkiksi tiedonsiirron määritelmän suhteen eivät vielä ole tehty. Kuan Honin määritelmä tiedonsiirroille on kuitenkin tarkempi kuin Euroopan

[27] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 468 ja Euroopan tietosuojaneuvoston yleiset ohjeistukset 05/2021 s. 4
[28] Esimerkiksi tapauksessa EUT C-184/20, Liettuan valtio oli viitannut EDPB:n ohjeisiin 3/2019 tallentavan videokameran tietojenkäsittelystä. Tässä tapauksessa EUT oli huomioinut ohjeet tapauksen analyysissa. Ennakkoratkaisu ei kuitenkaan perustunut ohjeisiin.
[29] Kuan Hon 2016, s.69–70

tietosuojaneuvoston määritelmä, sillä se 1. toteaa, että tiedonsiirto on välttämätön toimenpide eikä tilanteessa voida edetä toisella tavalla, ja 2. vastaanottajan on sijaittava kolmannessa maassa, kun se vastaanottaa henkilötietoja.

Henkilötietojen siirtäminen määritellään siis GDPR:n mukaan henkilötietojen käsittelyksi. Henkilötietojen siirtäminen määritelmänä on tässä tutkielmassa henkilötietojen käsittelyä, jossa tietoa siirtyy yhdeltä tai monelta taholta toiselle tai monelle taholle. Useimmiten tutkielmassa ja kirjallisuudessa käytetään käsitettä tiedonsiirto. Tärkeintä on huomioida, että tiedonsiirron määritelmä on osa tietojenkäsittelyä, joka on laaja määritelmä ja kattaa monta erilaista tietojenkäsittelyn kaltaista toimenpidettä. Henkilötietojen siirtämistä ja henkilötietojen käsittelyyn liittyviä periaatteita käsitellään laajemmin seuraavassa luvussa 3.

2.2.3 Eri tietosuojaan liittyvien tahojen määritelmät

Rekisterinpitäjä on GDPR:n 4 artiklan 7 kohdan mukaan henkilötiedoista vastaava taho, joka yksin tai yhdessä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Euroopan unionin tuomioistuin on viitannut rekisterinpitäjän määritelmään sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY ja todennut, että rekisterinpitäjälle käsitteenä on annettu väljä määritelmä vastaavasta, jonka tehtävä on varmistaa tehokas ja täydellinen suoja tapauksessa tarkoitetuille osapuolille.[30]

Henkilötietojen käsittelijä on GDPR:n 4 artiklan 8 kohdan mukaan:

> ”luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.”

Käytännössä henkilötietojen käsittelijä on taho, joka käsittelee rekisterinpitäjän ylläpitämän tietokannan tietoja. Kyseessä voi olla esimerkiksi erilaisten palveluiden ulkoistaminen. Henkilötietojen käsittelijä ei siis vastaa siitä, mitä tietoja kerätään ja mitä tietoja rekisterissä on, mutta tämä taho käsittelee tietoja rekisteripitäjän määräämän toimeksiannon mukaan. Tällä taholla ei siis ole päätösvaltaa henkilötietojen keräämisestä, säilytyksestä, käyttämisestä tai muusta käsittelystä. Päätösvalta on yksin rekisterinpitäjällä. Tämä eroavaisuus on kiinnostavin ja tärkein ero käsittelijän ja rekisterinpitäjän välillä. Heti, kun käsittelijällä on jonkinlaista

[30] Öman 2019, s.69–71, Öman mainitsee muun muassa tapauksen EUT 13.5.2014, Google Spain ja Google C-131/12

päätösvaltaa siitä, mihin käytöstarkoitukseen tietoja käsitellään ja mitä keinoja käsittelyä varten käytetään, käsittelijä muuttuu rekisterinpitäjäksi.[31]

Käsittelijän on myös oltava erillinen yksikkö rekisterinpitäjästä ja sen pitää käsitellä henkilötietoja rekisterinpitäjän puolesta. Henkilötietojen käsittelyssä on olemassa toisin sanoen hierarkia, jossa rekisterinpitäjä päättää siitä, minkälaisia tietoja kerätään ja missä tarkoituksessa, kun käsittelijä ainoastaan käyttää tietoja rekisterinpitäjän päättämään tarkoitukseen.[32] Tässä tutkielmassa viitattaan usein tilanteisiin, joissa A. rekisterinpitäjä tai B. henkilötietojen käsittelijä käsittelee, siirtää tai tekee muita toimenpiteitä henkilötiedoille. Tutkielman selvyyden ja yhdenmukaisuuden takia näissä tilanteissa viitataan aina kumpaankin tahoon eli rekisterinpitäjään ja henkilötietojen käsittelijään, ellei erityisesti henkilötietojen käsittely ole ainoastaan jommankumman tahon vastuulla.

Vastaanottaja on GDPR:n 4 artiklan 9 kohdan mukaan:

> ”luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei. Viranomaiset, jotka mahdollisesti saavat henkilötietoja tietyn tutkimuksen puitteissa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti ei kuitenkaan pidetä vastaanottajina.”

Yritys on GDPR:n 4 artiklan 18 kohdan mukaan:

> ”taloudellista toimintaa harjoittava luonnollinen henkilö tai oikeushenkilö sen oikeudellisesta muodosta riippumatta, mukaan lukien kumppanuudet tai yhdistykset, jotka säännöllisesti harjoittavat taloudellista toimintaa. Konsernilla tarkoitetaan GDPR:n 4 artiklan 19 kohdan mukaan: määräysvaltaa käyttävää yritystä ja sen määräysvallassa olevia yrityksiä.”

Yritys on määritelty GDPR:ssä siten, että kyseessä voi olla yrityksen muotona luonnollinen henkilö, oikeushenkilö tai yhdistys, joka säännöllisesti harjoittaa taloudellista toimintaa.[33] Viranomainen ei kuuluu tähän määritelmään. Viranomaisilla on oma tietosuojalainsäädäntö GDPR:n mukaan EU:ssa (EUGDPR). Myös poliisiviranomaisilla on EU:ssa oma tietosuojalainsäädäntö (rikos-GDPR). Yrityksen merkitys määritelmänä liittyy esimerkiksi

[31] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 76–78
[32] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 76–78 – Tässä viitataan Euroopan tietosuojaneuvoston (EDPB European Data Protection Board) ohjeistukseen 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa.
[33] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 87–88

GDPR:n 47 artiklaan, joka käsittelee yritystä koskevia sääntöjä (Binding corporate rules, BCR). BCR on yksi niistä tiedonsiirtovälineistä, joilla henkilötietoja voidaan siirtää kansainvälisesti EU:n ulkopuolelle ilman EU:n komission myöntämää riittävyyspäätöstä. Muun muassa tätä tiedonsiirtovälinettä käsitellään pääkysymyksen kannalta luvussa 4. Tässä tutkielmassa käytetään kuitenkin yleisenä määritelmänä sanaa yhdistys. Yhdistys viittaa yrityksiin, organisaatioihin ja muihin yhteisöihin. Tutkielmassa käsiteltävät aiheet eivät eroa niin, että yrityksillä ja yhdistyksillä olisi eri vastuu tai velvollisuus henkilötietojen käsittelyn kannalta. Mikäli näitä tapauksia esiintyy, käytetään silloin sanaa yritys kuvaamaan erovaisuus toisten yhdistysmuotojen kanssa. Muuten sanaa yhdistys käytetään yleisesti.

Eniten vaikutusta määritelmällä on kuitenkin GDPR:n artiklaan 83 liittyen hallinnollisista seuraamusmaksuista. Seurantamaksulla voi olla suuri merkitys yritysten tilinpäätökseen, koska seurantamaksu on kahdesta neljään prosenttiyksikköön yrityksen kokonaisvaltaisesta tilinpäätöksestä. Yritysten kiinnostus dataa ja henkilötietoja kohtaan osana liiketoimintaa on GDPR:n määritelmien ja asetuksen säätämisen tarkoituksen perusteena. Yrityksen toiminnan tarkoitus ja yleinen taloudellinen toiminta voi erota, mutta mikäli yrityksen pääsääntöisenä tarkoituksena on henkilötietojen tai datan kauppaaminen tai hyödyntäminen muun liiketoiminnan kannalta, on tietosuoja otettava huomioon. Kyseessä on myös yleisesti hyvää yrityskäytäntöä vaatimustenmukaisuuden näkökulmasta. Hyvää medianäkyvyyttä ja luottamusta omaava yritys saa luontevasti enemmän myyntiä ja rahoitusta.

Konsernin määritelmän kannalta on tärkeintä se, että kun konsernin pääkonttori sijaitsee EU:n jäsenvaltiossa, pääkonttoria pidetään myös konsernin päätoimipaikkana.[34] Monien yritysten toimintamallit eroavat, mutta nykypäivänä yritysten toiminnassa yhdistää varsinkin se, että ne hallinnoivat ja käsittelevät suuria määriä dataa, joista merkittävä osa on henkilötietoja.[35] Datan ja henkilötiedon vastuullinen käsittely ja hallinnointi on yrityksen julkisuuden sekä laillisuuden kannalta tärkeää.

Valvontaviranomainen on GDPR:n 4 artiklan 21 kohdan mukaan jäsenvaltion 51 artiklan nojalla perustama riippumaton viranomainen. Suomessa viranomainen on tietosuojavaltuutetun toimisto.

Kansainväliset järjestöt tai organisaatiot ovat GDPR:n 4 artiklan 26 kohdan mukaan järjestöjä ja sen alaisia elimiä, joihin sovelletaan kansainvälistä julkisoikeutta tai muuta elintä, joka on perustettu kahden tai useamman välisellä sopimuksella tai tällaisen sopimuksen perusteella.

[34] Öman 2019 s. 100–101
[35] Daley 2015 s. 10–11

Näiden kohdalla ei käsitellä tutkielmassa erityistä kysymystä tai ongelmaa, mutta määritelmien hahmottaminen on kuitenkin tärkeää, jotta itse pääkysymykset voidaan tutkielmassa käsitellä. Seuraavaksi käsitellään kansainvälisissä tiedonsiirroissa GDPR:n yleisiä henkilötietojenkäsittelyn periaatteita.

3 Vaatimukset ja yleiset periaatteet tiedonsiirroille tai tiedonkäsittelylle

3.1. Kansainväliset tiedonsiirrot käytännössä

Kansainvälisissä tiedonsiirroissa GDPR jakaa valtiot kahteen ryhmään. Tarkemmin kyseessä on rajoitus, jossa GDPR:n mukaan tiedonsiirrot, jotka tehdään ETA:n (Euroopan talousalue) ulkopuolelle (mukaan lukien kaikki EU:n jäsenvaltiot sekä Islanti, Liechtenstein ja Norja, jotka myös kuuluvat Euroopan talousalueeseen) tehdään GDPR:n mukaan kolmessa eri tilanteessa:

> ”1. tiedonsiirto tehdään kolmanteen maahan, jolle on myönnetty Euroopan komission antama riittävyyspäätös, 2. riittävyyspäätöksen puuttuessa, tietojen käsittelijä tai rekisterinpitäjä varmistaa, että käytössä on riittävä määrä suojatoimia niin, että rekisteröidyn täytäntöönpano-oikeudet ja rekisteröidyn vahingonkorvausoikeudet täyttyvät, 3. riittävyyspäätöksen tai riittävien suojatoimien puuttuessa, tietojen käsittely kuuluu johonkin erityistilanteeseen, jonka asetus kattaa.”

Mikäli EU:n ulkopuoliselle valtiolle ei ole myönnetty EU:n komission riittävyyspäätöstä on EU:n ja ETA:n alueella toimivien yhteisöjen ja kolmansien maiden yhteisöt käytettävä GDPR:n 46 artiklan vaadittavia suojatoimia tiedonsiirroissa, eli tiedonsiirtovälineitä, siirtääkseen henkilötietoja kolmansiin maihin. Riittävyyspäätös todentaa, että EU:n ja ETA:n ulkopuolella olevalla maalla on saman tason tietosuoja vaatimukset kuin EU:lla ja näin ollen tiedonsiirrot voidaan tehdä ilman lisätoimenpiteitä. [36] Kun riittävyyspäätös toteaa, että EU:n ja ETA:n ulkopuolella olevalla maalla on samat tietosuojan vaatimukset kuin EU:lla, tämä tarkoittaa, että tiedonsiirtovälineet GDPR:n 46 artiklan pitäisi antaa saman tietosuojan tason kuin EU:n komission antama riittävyyspäätös. Tätä kysymystä käsitellään enemmän luvussa 4.

Tällä hetkellä voimassa olevat GDPR:n periaatteet, joiden mukaan komissio antaa riittävyyspäätöksiä, astuivat voimaan 2016, kun nykyinen GDPR astui voimaan. Careyn mukaan kansainväliset tiedonsiirrot ovat yksi vaikeimmista tietosuojan vaatimustenmukaisuuden haasteista Euroopan unionin sisällä toimiville yhteisöille. Oikeiden suojatoimien implementointi jokaisessa yksittäistapauksessa on aikaa vievää ja vaikeaa. Kysymykseen on täten haastavaa vastata ainoastaan tutkielman pohjalta. Mahdollista on

[36] Yakovleva 2020, s. 888–889

kuitenkin hahmottaa ne eroavaisuudet ja erikoisuudet, jotka löytyvät eri tiedonsiirtovaatimusten välillä. [37]

Esimerkiksi apulaistietosuojavaltuutetun päätöksessä 27.4.2023 7684/171/22 rekisterinpitäjä oli käyttänyt evästeohjelmaa Google Analyticsin ja reCAPTCHA ohjelman kautta. Nämä palvelut ovat Yhdysvalloissa kehitettyjä evästeohjelmia ja tapauksen selvityksen mukaan ohjelmien palvelimet sijaitsevat Yhdysvalloissa. Rekisterinpitäjä ei ollut tapauksessa määritellyt GDPR:n artikla 46 mukaisen asianmukaisen suojatoimen tiedonsiirroille ja tämän perusteella apulasitietosuojavaltuutettu määräsi rekisterinpitäjälle GDPR:n 58 artiklan 2 kohdan mukaisen huomautuksen. Apulaistietosuojavaltuutettu lisäsi, että rekisterinpitäjän olisi myös pitänyt tehdä GDPR:n 35 artiklan mukainen tietosuojaa koskevan vaikutuksenarvioinnin, sillä sen olisi pitänyt huomata, että tiedonsiirroissa on kyse korkean riskin kattavista tiedonsiirroista ja varteenotettavasta mahdollisuudesta, että tiedonsiirrot loukkaavat luonnollisen henkilön oikeuksia ja vapauksia.[38] Tapauksessa tosin herää kysymys siitä, riittääkö tiedonsiirtoväline riskiä poistavana toimenpiteenä, tai tuleeko rekisterinpitäjän aina laatia tietosuojaa koskevan vaikutuksenarviointi. Apulaistietosuojavaltuutettu vastasi itse kysymykseen myöhemmin 31.5.2023.

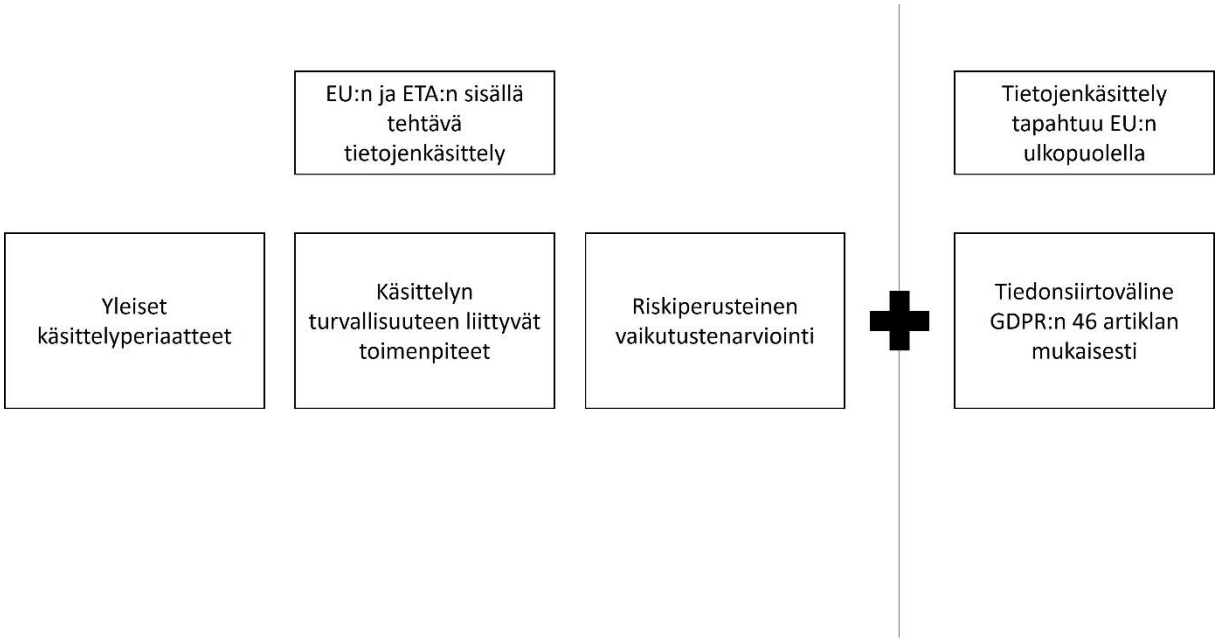
Apulaistietosuojavaltuutettu kumosi edellä olevan päätöksen uudella päätöksellään 31.5.2023 7684/171/22 ja varmisti, että tietosuojaa koskevan vaikutuksenarviointia ei tarvitse tehdä, mikäli pätevä tiedonsiirtoväline on jo käytössä. Päätös on julkaistu tutkielman kirjoittamisen aikana. Päätös on kuitenkin edelleen pätevä siinä mielessä, että tietosuojaa koskeva vaikutustenarviointi on aina pakollinen laatia, kun rekisteripitäjä arvioi, että kyseessä on korkean riskin tietojenkäsittely. Mutta kyseessä on vain tietojenkäsittelyyn liittyvät tapaukset, jotka suoraan viittaavat GDPR:n 35 artiklaan. Oikaistun TSV:n päätökseen mukaan voimme todeta, että tietosuojaan liittyvä vaikutustenarviointi on tehtävä silloin, kun rekisteripitäjä arvioi, että tietojenkäsittely käyttää etenkin uutta teknologiaa ja kun se todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Tästä näkökulmasta voidaan tehdä se johtopäätös, että apulaistietosuojavaltuutettu ei näe, että tietosuojaa koskevaa vaikutuksenarviointia tarvitsee tehdä, kun tietojenkäsittelyssä käytetään vakiintuneita teknologioita ja palveluita, kuten esimerkiksi Google Analyticsia. Päätökseen liittyvä arviointi tiedonsiirroista kolmanteen maahan pysyi kuitenkin voimassa. Päätöstä

[37] Carey 2018, s.121

[38] Tietosuojavaltuutetun päätös 27.4.2023 7684/171/22

arvioidaan tarkemmin alla luvussa 4.4.[39] Tietojenkäsittelyn vaikutuksenarviointia käsitellään alla luvussa 3.3.4.

Päätöksessä ei tosin oteta kantaa itse tiedonsiirtovälineiden tehokkuuteen tai puutteellisuuteen. Siinä yksinkertaisesti todetaan, että rekisterinpitäjä ei huomioinut asianmukaisia suojatoimia kansainvälisissä tiedonsiirroissa, sillä se ei ollut käyttänyt yhtäkään GDPR:n 46 artiklassa mainittua tiedonsiirtovälinettä. Tämä päätös puoltaa näkökulmaa siitä, että asianmukaiset suojatoimet kansainvälisissä tiedonsiirroissa ovat suoraan GDPR:n 46 artiklassa tarkoitetut tiedonsiirtovälineet ja että muut käsittelyyn liittyvät vaatimukset kuten käsittelyn turvallisuus, yleiset tietojenkäsittelyperiaatteet ja riskiperusteinen lähestymistapa ovat aina vaadittavia toimenpiteitä GDPR:n yleisten tietojenkäsittelyperiaatteiden mukaisesti. Oikeustilaa voi kuvata alla olevalla kaaviolla:



Kuten alla todetaan, GDPR:ssä on tiettyjä tietojenkäsittelyvaatimuksia, joita on huomioitava aina tietojenkäsittelyssä. Kaavion on tarkoitus kuvata sitä, että yleiset GDPR:ssä tarkoitetut tietojenkäsittelyvaatimukset on käytännössä tehtävä aina, kun tietoja käsitellään EU:n tai ETA-alueen sisällä ja että GDPR:n 46 artiklan mukaisia tiedonsiirtovälineitä tulee käyttää silloin, kun tietojenkäsittely tapahtuu EU:n tai ETA-alueen ulkopuolella kuten myös yllä olevan TSV:n päätöksessä todettiin. Tiedonsiirtovälineitä käsitellään lähemmin luvussa 4.

[39] Tietosuojavaltuutetun päätös 31.5.2023 7684/171/22

3.2 Yleiset tietojenkäsittelyperiaatteet

Tietojenkäsittelyssä on yleisesti otettava huomioon tietyt GDPR:n vaatimukset ja edellytykset. Näistä periaatteista ja vaatimuksista säännellään GDPR:n 2 luvussa. Tärkeimmät säännöt tietojenkäsittelyä varten ovat yleiset henkilötietojen käsittelyä koskevat periaatteet, käsittelyn lainmukaisuus ja suostumuksen edellytys. Myös tietosuojaa koskeva vaikutustenarviointi ja käsittelyn turvallisuus vaikuttaa tietojenkäsittelyn lainmukaisuuteen.

3.2.1 Henkilötietojen käsittelyä koskevat yleiset periaatteet

Yleisistä henkilötietojen käsittelyä koskevista periaatteista säännellään GDPR:n 2 luvun 5 artiklassa. Säännöksen mukaan:

> ”a) henkilötietoja on aina käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi, b) ne on kerättävä tiettyä nimenomaista ja laillista tarkoitusta varten, c) henkilötietojen on oltava asianmukaisia ja rajoitettuja siihen mikä on tarpeellista käsitellä, d) henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä, e) ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten, f) henkilötiedot tulee säilyttää tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus.”

Yleisesti nämä periaatteet jaetaan tietosuojalainsäädännön kymmeneksi keskeiseksi periaatteeksi. Nämä periaatteet ovat tietojenkäsittelyn lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus.

3.2.1.1 Lainmukaisuus

Tietojenkäsittelyn lainmukaisuus koskee itse käsittelytoimenpiteiden lainmukaisuutta. Sille on erikseen vaatimuksia GDPR:n artiklassa 6, jota käsitellään alla. Lisäksi lainmukaisuuteen voi myös vaikuttaa kansallinen lainsäädäntö. Tästä voidaan esimerkkinä mainita Suomen kansallisesta lainsäädännöstä tietosuojalain 2 luvun 5 § poikkeuksen GDPR:stä, jonka mukaan tietosuoja-asetuksen 6 artiklan 1 kohdasta saa poiketa, kun kyseessä on tietosuoja-asetuksen 4 artiklan 25 kohdassa tarkoitettujen tietoyhteiskunnan palvelujen tarjoamisesta. Ruotsista löytyy oikeuskäytäntöä korkeimmasta hallinto-oikeudesta HFD 2016 ref. 40, jossa todettiin, että lainmukaisuuden vaatimukset koskevat ainoastaan sen aikaisen tietosuojadirektiivin vaatimuksia sekä lakeja, joissa tietosuoja-asetukseen suoraan viitataan. Tapauksessa todettiin, että lainmukaisuuden vastaisuus muussa lainsäädännössä, kuten Ruotsin markkinointilaissa

2008:486 tai Ruotsin rikoslaissa 1962:700, ei vastannut lainmukaisuuden vaatimusta.[40] Ruotsin oikeuskäytännöstä voidaan todeta, että kansallisen lainsäädännön tulee suoraan viitata tietosuoja-asetukseen, mikäli poikkeuksia lainmukaisuusvaatimukseen GDPR:n 5 artiklan 1 kohdan mukaan halutaan tehdä. Muuten GDPR:n vaatimukset tulkitaan ensisijaisesti kansalliseen lainsäädännön verrattuna henkilötietoihin liittyvissä tapauksissa.

GDPR:n 6 artiklan vaatimukset käsittelyn lainmukaisuudesta ovat seuraavat. Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

> ”a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten; b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä; c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi; d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi; e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi; f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.”

Rekisterinpitäjän on arvioitava lainmukaisuuden kysymystä ennen kuin se rekisteröi tai käsittelee rekisteröidyn henkilötietoja. Tämä vaatimus pätee siis myös kansainvälisissä tiedonsiirroissa ja ottaen huomioon riskiperusteisen tietosuojan lähestymistavan, pitäisi rekisterinpitäjän huomioida, että kyseessä voi olla suurta riskiä rekisteröidylle aiheuttavaa tietojenkäsittelyä. Lainmukaisuus toisin sanoen antaa henkilötietojen käsittelylle lainmukaisen syyn ja rekisterinpitäjän tai henkilötietojenkäsittelijän on pystyttävä todistamaan tämä lainmukaisuus.

Tavallisin lainmukaisuuden peruste henkilötietojen käsittelylle on GDPR:n artikla 6.1 a) mukainen rekisteröidyn suostumus. Yksi esimerkki rekisteröidyn suostumuksen pyytämisestä, ovat evästeet internetsivustoilla. Evästeiden avulla internetsivusto voi tallentaa internetsivuoston käyttäjän aikaisemman yhteydenoton tietoja ja tällä tavalla erilaiset

[40] Öman 2019, s. 111–112

internetsivustoon liittyvät toimenpiteet ja prosessit suoriutuvat nopeammin seuraavalla kerralla.[41] Evästeissä kerättävät tiedot on todettu käytännössä ja ETN:n suosituksissa henkilötiedoiksi.[42] Rekisterinpitäjän on kuitenkin selvitettävä tietojenkäsittelyn lainmukaisuutta ennen kuin hän voi käsitellä rekisteröidyn henkilötietoja. Rekisterinpitäjä voi selvittää rekisteröidyn halukkuutta suostumukselle vapaamuotoisesti. Käytännössä tavallisin tapa evästeiden suostumuksen selvittämiselle on evästebanneri internetsivustolla, jolla käyttäjä pystyy joko 1. antamaan suostumuksensa henkilötietojensa käyttöön tai 2. olla suostumatta henkilötietojensa käyttöön.[43] Kansainvälisissä tiedonsiirroissa pääasia on se, että lainmukainen peruste henkilötietojenkäsittelylle on olemassa rekisterinpitäjän osoitusvelvollisuuden mukaisesti ennen kuin käsittelyyn tai rekisteröintiin liittyviä toimenpiteitä aloitetaan. Rekisterinpitäjä päättää itse millä tavalla hän varmistaa rekisteröidyn suostumuksen ja käsittelyn lainmukaisuuden. Tavallisin tapa tälle on tietojenkäsittelyn suostumuksen kysyminen rekisteröidyltä ja todiste tästä, joka sisällytetään tietojenkäsittelyn tietosuojaselosteeseen GDPR:n 30 artiklan mukaisesti.

GDPR:n lainmukaisuuden vaatimuksessa on tärkeää huomioida se, että rekisterinpitäjän ja henkilötietojen käsittelijän on ennen henkilötietojenkäsittelyä saatava a) rekisteröidyn suostumus henkilötietojen käsittelyyn, b) pystyttävä todistamaan, että henkilötietojen käsittely on tarpeellista tietyn sopimuksen täytäntöönpanemiseksi, c) käsittely on tarpeen rekisteröidyn tai rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi, d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Reksiterinpitäjän tai henkilötietojen käsittelijä päättää itse, miten lainmukaisuus todennetaan, mutta GDPR:n osoitusvelvollisuuden kautta yleisin tapa tälle

[41] Innanen – Saarimäki 2012, s.97–103

[42] Esim. tietosuojavaltuutetun päätös 14.5.2020 8040/163/2019. Evästeet ovat toisaalta usein myös määritelty pseudonymisoiduiksi tiedoiksi. Toisaalta EUT:n ratkaisussa EUT T-557/20 todettiin, että Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUGDPR) pseudonymisoitu henkilötieto voi tapauskohtaisesti olla niin hyvin suojattu, että sitä ei enää luokitella tietosuojalainsäädännön eli GDPR:n ja EUGDPR:n mukaiseksi henkilötiedoksi. Tapaus ei ole vielä saavuttanut lainvoimaa ja siitä voi valittaa. Henkilötietojen määritelmän tulkinnan muuttuminen voi vaikuttaa tulevaan oikeuskäytäntöön, mikäli kaikkia tietoja, joilla luonnollinen henkilö voidaan tunnistaa ei enää tulkita henkilötiedoiksi. Myös ETN final one stop shop decision D: 2022:330 s. 4–8 jossa todettiin, että tieto, joka löytyy IP-osoitteista tai evästeistä, voidaan yhdistää yksityiseen henkilöön ja tältä osin määritellä henkilötiedoksi.

[43] ETN evästebanneri työryhmän raportti 18. Tammikuuta 2023, s. 4

on lainmukaisuuden dokumentointi erillisesti esimerkiksi tietojenkäsittelysopimuksessa. Tietojenkäsittelysopimuksia käsitellään lisää alla.

3.2.1.2 Kohtuullisuus, läpinäkyvyys ja käyttötarkoitussidonnaisuus

Kohtuullisuus merkitsee sitä, että rekisterinpitäjällä pitää olla tietojenkäsittelylle alkuperäisen käyttötarkoituksen mukainen käyttötarkoitus. Rekisterinpitäjälle ei esimerkiksi saa antaa henkilötietoja käsiteltäväksi, jos tämä ei vastaa alkuperäistä henkilötietojen käyttötarkoitusta. Tätä vaatimusta voi verrata yleiseen siviilioikeuden *bona fide* käsitteeseen. Näin ollen henkilötietojen käsittelyssä on pystyttävä luottaa siihen, että rekisterinpitäjä on antanut henkilötiedot käsittelyyn hyvässä uskossa sitä käyttötarkoitusta varten, mihin henkilötietojen käsittely oli alun perin tarkoitettu.[44]

Läpinäkyvyys merkitsee sitä, että henkilötietojen rekisterinpitäjällä ja henkilötietojen käsittelijän pitää pystyä todistamaan rekisteröidylle, miten rekisteröityä koskevia henkilötietoja kerätään, käytetään sekä käsitellään. Esim. GDPR:n 12 artiklan mukaan rekisterinpitäjän on GDPR:n artikla 13 ja 14 perusteella ilmoitettava asianmukaiset toimenpiteet siitä, miten heidän henkilötietojansa käsitellään. Tämä velvollisuus korostuu myös rekisteröidyn GDPR:n 15 artiklan oikeudessa saada tietoja siitä, mitä henkilötietoja hänestä käsitellään.[45] Rekisteröidyllä on siis oikeus pyytää tietoja siitä, miten hänen henkilötietojansa käsitellään yhdistykseltä.

Käyttötarkoitussidonnaisuus vastaa laajalti kohtuullisuusperiaatetta. Verrattuna kohtuullisuusperiaatteeseen tarkoituksena on kuitenkin säätää velvollisuus rekisterinpitäjälle siitä, että tämän on ensinnäkin kohtuullisuusperiaatteen kautta käytettävä henkilötietoja vain alkuperäisen tarkoituksen mukaan, mutta myös otettava huomioon nimenomaisen käyttötarkoituksen sekä laillisen käyttötarkoituksen. Käyttötarkoitussidonnaisuudella on tarkoitus vahvistaa rekisterinpitäjän velvollisuus henkilötietojen rekisteröintiin ja käyttöön laillisella ja niiden käyttötarkoitusta vastaavalla tavalla.

3.2.1.3 Tietojen minimointi

Tietojen minimointi on tietosuojassa kiistelty ja keskustelua herättänyt periaate. Se on usein ollut tulkinnaltaan yhdistelmä muista tietosuojan yleisistä periaatteista. Carey kuvailee tietojen minimoinnin velvollisuuden noudattamisen vaativan 1. henkilötietojen käsittelyn käyttötarkoituksen määritteleminen ja 2. arviointi siitä, mikäli määritellyt käyttötarkoitukset ovat tarpeellisia.[46] Rekisterinpitäjä noudattaa tietojen minimoinnin periaatetta, kun se ensiksi

[44] Bärlund –Nybergh 2013, s. 9–14 ja Öman 2019, s. 113–114
[45] Korpisaari –Pitkänen – Warma-Lehtinen 2022, s.102–103
[46] Carey 2018, s. 35–36

määrittelee yleisten käsittelyperiaatteiden mukaan henkilötietojen käyttötarkoituksen ja tämän jälkeen arvioi, mikäli käyttötarkoitukset ovat tarpeellisia rekisterinpitäjän toimintaa varten. Kyseessä voi olla esimerkiksi sovelluksen käyttäjien sijaintietietojen käyttämisestä ICT-sovelluksen toimintaa varten. Henkilötietojen käsittely tietojen minimoinnin periaatteen mukaan edellyttää siis jatkuvaa arviointia rekisterinpitäjän ja henkilötietojen käsittelijän puolelta. Valvontaviranomaiset ovat kuitenkin suhtautuneet periaatteeseen vaihtelevasti. Tämä vaatimus vaikuttaa olevan myös oikeuskäytännössä omaksuttua. Esimerkiksi varsin tuoreessa Ranskan valvontaviranomaisen päätöksessä SAN-2023-003 valvontaviranomainen totesi, että sähköskootteriyritys, joka käsitteli henkilötietoja paikantaakseen asiakaskuntansa, rikkoi tietojen minimoinnin periaatetta, vaikka yritys oli GDPR:n artikla 5 yleisten tietojenkäsittelyperiaatteiden mukaan määritellyt tietojenkäsittelyn lainmukaisen ja tarkoituksenmukaisen tarkoituksen. Ranskan valvontaviranomainen totesi, että vaikka käyttötarkoitus oli määritelty, niin henkilötiedot, joita sijaintiteknologiaa käyttäen kerättiin, olisi voitu kerätä teknologisilla ratkaisuilla, jotka eivät seuranneet käyttäjien ja asiakaskunnan sijaintia niin tarkasti. Näin ollen sähköskootteriyritys ei ollut arvioinut tietojen minimisoinnin vaatimuksia ja se ei ollut tehnyt riittäviä toimenpiteitä tietojen minimointia varten.[47]

Kansainvälisisissä tiedonsiirroissa tietojen minimoinnin periaate on otettava huomioon varsinkin siinä mielessä, että henkilötiedot, jotka siirretään ovat 1. asianmukaisia (käyttötarkoitussidonnaisuus ja kohtuullisuus) 2. olennaisia ja 3. rajoitettuja siihen mikä on tarpeellista tietojenkäsittelyä varten. ETN suosittelee lisäksi, että kansainvälisissä tiedonsiirroissa tietojenminimoinnin periaate toteutuu parhaiten, jos rekisteripitäjä tekee säännöllisiä tarkastuksia omista siirtotoimenpiteistään.[48]

Tietojen minimoinnin periaate on rekisterinpitäjälle näkökulmasta kuitenkin vaikea velvollisuus toteuttaa, sillä se vaatii rekisterinpitäjää jatkuvasti arvioimaan henkilötietojen käyttötarkoitusta esimerkiksi tarkastuksen eli tietosuojan auditointien avulla. Kansainvälisissä tiedonsiirroissa periaatteen noudattamisen vaikeus korostuu siinä mielessä, että kerättävien henkilötietojen määrä on usein suuri ja suojatoimien implementointi on jatkuva prosessi. Lisäksi käyttötarkoituksen määritteleminen voi olla sopimusnäkökulmasta erittäin vaativaa, kun kyseessä on suuri määrä käsiteltäviä henkilötietoja ja tiedonsiirrot ovat usein automatisoituja.[49] Varsinkin automatisoitu henkilötietojen käsittelyprosessi on pystyttävä

[47] Ranskan valvontaviranomaisen ratkaisu SAN-2023-003
[48] ETN yleiset suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi 18. kesäkuuta 2021, s. 10 ja s. 45
[49] Carey 2018, s.108

uudelleenarvioimaan ja tarvittaessa muuttamaan nopeasti. Tästä näkökulmasta ennalta hyväksytyt tietojensiirtovälineet, kuten esimerkiksi yritystä koskevat sisäiset säännöt eli BCR-säännöt, ovat mahdollisesti tehokkain tapa noudattamaan tietojen minimoinnin periaatetta, sillä tiedonsiirrot tapahtuvat silloin yrityksen tai organisaation sisäisesti ja kyseessä on jatkuvia tiedonsiirtoja, jotka kaikki tulevat noudattaa samaa BCR-tiedonsiirtosopimuspohjaa. BCR-sääntöjä käsitellään enemmän seuraavassa luvussa 4.

3.2.1.4 Tietojen täsmällisyys, säilytyksen rajoittaminen ja tietojen eheys sekä luottamuksellisuus

Tietojen täsmällisyydellä tarkoitetaan sitä, että tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Tarkoituksena on pitää ne tiedot, joita käsitellään täsmällisinä ja poistaa tai oikaista niitä tietoja, jotka ovat virheellisiä tai epätarkkoja.

Säilytyksen rajoittaminen vastaa tietojen minimointiperiaatetta siitä näkökulmasta, että henkilötietojen säilytysajan on oltava mahdollisen lyhyt. Käyttötarkoituksella voidaan kuitenkin määritellä säilytysaika pidemmäksikin ajaksi, mutta kuten yllä olevassa Ranskan valvontaviranomaisen tapauksessa todetaan, on tämä rekisterinpitäjän vastuun kannalta tietynlaista tarkoituksenmukaisuuden tasapainottelua. Rekisterinpitäjällä voi myös olla lainmukainen velvollisuus säilyttää tietoja pidemmän ajan.[50]

Tietojen eheys ja luottamuksellisuus vastaa tietoturvallista tietojenkäsittelyä ja tietojen turvallisuuden vaatimusta, joita käsitellään alla. Henkilötietoja tulee käsitellä niin, että niiden asianmukainen turvallisuus varmistetaan ja niin että henkilötietojen häviäminen, tuhoutuminen tai vahingoittuminen estetään. Rekisteröidyn on pystyttävä luottamaan rekisterinpitäjään siinä mielessä, että hänestä luovutettavat henkilötiedot käsitellään luotettavalla tavalla. Mikäli rekisterinpitäjä epäonnistuu luottamuksellisuuden varmistamisessa, on hänen ryhdyttävä erilaisiin toimenpiteisiin. Esimerkiksi tietomurroissa on rekisterinpitäjän välittömästi ilmoitettava tapahtumasta valvontaviranomaiselle ja rekisteröidylle GDPR:n artikla 33 ja 34 mukaan.[51]

Kansainvälisissä tiedonsiirroissa tämä tarkoittaa yleensä sitä, että kansallinen valvontaviranomainen aloittaa yhteistyön tekemisen kaikkien niiden valtioiden valvontaviranomaisten kanssa, joissa tietojen käsittelyä on tehty. Tämä vaatimus on kuitenkin vain voimassa EU:n valvontaviranomaisilla, sillä kaikilla kolmansilla mailla ei ole

[50] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.107
[51] Carey 2018, s.40

tietosuojaviranomaisia. Kyseessä voi kuitenkin olla monen valtion välinen yhteistyö esimerkiksi laajan tietomurron seuraamusten torjunnassa.

3.2.1.5 Osoitusvelvollisuudesta liittyen yleisiin tietojenkäsittelyperiaatteisiin

GDPR:n 5 artiklan 2 kohdan mukaan rekisterinpitäjä vastaa siitä, että se pystyy osoittamaan että 5 artiklan 1 kohtaa on noudatettu. Rekisterinpitäjän osoitusvelvollisuus edellyttää siis rekisterinpitäjän tai henkilötietojen käsittelijän pystymään todistamaan, että tietosuojaperiaatteita on noudatettu. Todistusvelvollisuus on rekisterinpitäjällä ja henkilötietojen käsittelijällä.[52] Osoitusvelvollisuus ja tietojenkäsittelyn dokumentointi on tärkeää, sillä rekisterinpitäjällä on oltavat todisteina kaikki periaatteisiin liittyvä materiaali, mikäli se joutuu vastaajaksi kanteeseen GDPR:n 79, 82–84 artiklan mukaan. Esimerkiksi GDPR:n 82 artiklan 3 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä on vapautettava vastuusta ja korvausvelvollisuuksista, mikäli se pystyy osoittaa, ettei se ole vastuussa vahingon aiheuttaneesta tapahtumasta.[53] Tämä onnistuu esimerkiksi dokumentoimalla tietojenkäsittelyperiaatteiden noudattamisen tietosuojaselosteessa. Kansainvälisissä tiedonsiirroissa, käytetään usein niin sanottua datakartoitusta, missä kartoitetaan henkilötietojen siirtymistä eri tahojen välillä ja rakennetaan kokonaiskuva yhteisön tiedonsiirroista. Näin yhteisö pystyy arvioimaan, miten henkilötietoja siirretään tietojenkäsittelyn yhteydessä ja osoitusvelvollisuuden täyttäminen on yleisesti helpompaa.[54]

Sopimus tai muu unionin oikeuden tai jäsenvaltion lainsäädännön mukainen oikeudellinen asiakirja on vaadittava kokonaisuus GDPR:n 28 artiklan 3 kohdan mukaista henkilötietojen käsittelyä varten. Kaikki 28 artiklan 3 kohdan mukaiset henkilötietojen käsittelyä koskevien sopimusten on oltava kirjallisia tai sähköisessä muodossa saatavia sopimuskokonaisuuksia. Tämä varmistaa myös rekisterinpitäjän ja henkilötietojen käsittelijän osoitusvelvollisuuden täyttymistä, minkä perusteella rekisteröity voi oikeusturvatoimenpiteenä haastaa

[52] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.100 – Kuten edellä todettu alaviitteessä 25 niin yleiset tietosuojaperiaatteet vastaavat niitä lainsäädännöllisiä vaikutuksia, joilla halutaan vaatia rekisterinpitäjältä ja tietojenkäsittelijältä omaa osoitusvelvollisuutta. Eli kuten prosessioikeudessa rekisterinpitäjällä, tietojenkäsittelijällä tai toisella tiedoista vastaavalta taholta edellytetään, että kyseinen taho pystyy todistamaan sen, että se noudattaa tietosuojalainsäädäntöä. Velvollisuus todistamiselle on aina vastaavalla osapuolella. Varsinkin henkilötietojen käsittelyn yleiset periaatteet korostuvat tässä velvollisuudessa.

[53] Yle 10.3.2023 - Vastaamon tietomurto on todennäköisesti merkittävin tietoturvallisuursikoksiin ja tietosuojaan liittyvä rikostapaus Suomessa. Tutkielman kirjoittamisen aikana, tuomioistuinkäsittely on vielä kesken. Syyttäjä vaatii Vastaamon ex-toimitusjohtajalle Ville Tapiolle vankeutta tietosuojarikoksesta. Tietosuojarikos on rikoslain 1889/39 rekisterinpitäjän tai henkilötietojen käsittelijän törkeästä huolimattomuudesta liittyvä rikosnimike. Tutkielman kirjoituksen aikana Tapio on kiistänyt syytteet ja syyttänyt Vastaamon tietosuojavastaavia tietosuojan laiminlyönnistä. Tapion puolustus ajaa selvästi taktiikalla, jolla pyritään osoitusvelvollisuuden kautta osoittamaan, että Tapio ei toiminut huolimattomasti tapauksessa. Tämä pätee myös vahingonkorvauskanteisiin, joita käsitellään tietosuojarikoksen ohella.

[54] Carey 2018, s.85

tietojenkäsittelyn lainmukaisuuden. Näin ollen tietojenkäsittelysopimus on yleisin tietojenkäsittelyn osoitusvelvollisuuden väline oletettavasti myös siksi, että se kattaa valmiiksi GDPR:n 28 artiklan 3 kohdan vaatimukset ja sen pystyy helposti implementoimaan myös muihin tietojenkäsittelyn tilanteisiin.

3.2.1.6 Yleisten tietojenkäsittelyperiaatteiden vaikutus tietojenkäsittelyyn

Tietojenkäsittelyn yleiset periaatteet rakentavat tietosuojan pohjan ja ne tulee ottaa huomioon kansainvälisissä tiedonsiirroissa tarkasti ennen kuin tietojenkäsittelyn toimenpiteitä, kuten tiedonsiirtoja aletaan tehdä. Tietosuojaneuvoston ratkaisukäytännössä rajoja ylittävissä tapauksissa näkee varsin nopeasti, että tietojenkäsittelyn yleisten periaatteiden tulkinta on yleinen erimielisyyden kohde oikeuskäytännössä.[55] Tätä yksityiskohtaa puoltaa luultavasti se, että GDPR astui voimaan vuonna 2018 ja että varsinkin tietosuoja-asetuksen perusteet ovat olleet ensimmäisiä erimielisyyden kohteita. Saman trendin näkee, jos tutkii Suomen tietosuojavaltuutetun toimiston yleistä ratkaisukäytäntöä.[56] Varsin yksimielistä on kuitenkin se, että tietojenkäsittelyn toimenpiteet tulee lopettaa välittömästi, kun tietojenkäsittelyn yleisiä periaatteita ei enää noudateta tai pystytä noudattamaan.

Käytännössä tämä ei kuitenkaan ole yksinkertaista, sillä esimerkiksi tietojenkäsittely, joka perustuu yleissopimuksiin suurien konsernien ICT-järjestelmien kautta esimerkiksi Microsoftin pilvipalveluihin, sopimusehtoja on vaikea muuttaa lennosta. Tätä ongelmaa kuvastaa varsinkin Tanskan tietosuojaviranomaisen päätös Datatilsynet 10-09-2021, jossa Elsinoren kunnan koulujen pilvipalvelut eivät täyttäneet yleisiä tietojenkäsittelyperiaatteita. Elsinoren kunnalla oli voimassa oleva sopimus Googlen Chromebooks ja Workspace-palveluiden kanssa. Kun Googlen Chromebooks ja Workspace-palveluiden sopimusehtoja muutettiin, eivät enää yleiset henkilötietojenkäsittelyperiaatteet täyttyneet erityisesti lainmukaisuuden, tietojen minimoinnin ja henkilötietojen turvallisuuden puolesta. Lisäksi henkilötietoja siirtyi Yhdysvaltoihin ilman GDPR:n mukaisia yleisiä tietojenkäsittelyperiaatteita. Tanskan tietosuojaviranomainen määräsi Elsinoren kunnan lopettamaan tietojenkäsittelyn välittömästi. Ongelma ei kuitenkaan ratkaistu täysin, sillä Elsinoren kunnan kouluilla oli kaikilla jo Googlen-palvelut erittäin vakiintuneessa käytössä. Näin ollen Elsinoren kunta ei aluksi noudattanut Tanskan tietosuojaviranomaisen päätöstä. Elsinoren kunta ryhtyi toimenpiteisiin, kun Tanskan tietosuojaviranomainen määräsi sille myös seuraamusmaksun sekä erityisten varoituksen tietojenkäsittelyn laiminlyönnistä. Ongelmallisuus tapauksessa on se, että Elsinoren kunnalla ei ollut mahdollisuuksia neuvotella

[55] European data protection board final one stop shop decisions tietokanta
[56] Finlex, esim. tietosuojavaltuutetun ratkaisukäytäntö

Googlen kanssa yleissopimusten muuttamisesta ja ICT-palveluiden muuttaminen GDPR:n mukaiseksi nopeasti oli erittäin vaikeaa ja aikaa kestävä toimenpide. Näin ollen, GDPR:n vaatimusten noudattaminen voi olla erittäin vaikeaa heikommalle sopimusosapuolelle, eikä yleiset sopimusoikeudelliset käsitteet, kuten *bona fide* ja *pacta sunt servanda*, usein täyty. Tapaus kuvastaa mahdollisesti kuitenkin enimmäkseen yleistä ongelmallisuutta ICT-palveluiden tarjoajien sopimusehdoissa. Tutkielman kannalta merkittävä osa oli se, että yhteisön olisi pitänyt lopettaa tietojenkäsittelyn välittömästi, kun yleisiä tietojenkäsittelyperiaatteita ei enää pystytty noudattaa.[57]

3.3 Tiedonsiirtoja erityisesti koskevat periaatteet ja vaatimukset

Edellä käsiteltiin yleisiä GDPR:n tietojenkäsittelyperiaatteita. Nämä tietojenkäsittelyperiaatteet on aina otettava huomioon, kun henkilötietoja käsitellään eli myös kansainvälisissä tiedonsiirroissa.

3.3.1 Tiedonsiirron yleiset vaatimukset

Seuraavaksi käsitellään tiedonsiirtoihin liittyviä erityisiä vaatimuksia. Erovaisuus näiden yleisten periaatteiden välillä on se, että GDPR:n 2 luvun vaatimukset käsittelevät yleisesti rekisteröidyn suostumusta tietojenkäsittelyyn, kun taas GDPR:n 4 luvun vaatimukset käsittelevät itse *tietojenkäsittelyn* lainmukaisuutta ja turvallisuutta sekä tietoturvallisuutta.

Kansainvälisissä tiedonsiirroissa on noudatettava GDPR:n 44 artiklan yleistä periaatetta siirroista. GDPR:n 44 artiklan mukaan:

> ”Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.”

Mikäli henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle on rekisterinpitäjän tai henkilötietojen käsittelijän noudatettava GDPR:n 5 lukua. GDPR:n 5 luvun

[57] Datatilsynet 10-09-2021

lisäksi on rekisterinpitäjän tai henkilötietojen käsittelijän noudatettava yleisesti myös muita GDPR:n sääntöjä kuten GDPR:n 2 lukua.

Esimerkiksi GDPR:n II luvun 5 artiklan a) mukaan:

> ”Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia: a) niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (lainmukaisuus, kohtuullisuus ja läpinäkyvyys.)”

Henkilötietojen käsittelyn suhteen pitää aina huomioida käsittelyn lainmukaisuus, asianmukaisuus ja rekisteröidyn kannalta läpinäkyvyys. Lisäksi GDPR:n 2 luvun artikla 5 f) mukaan:

> ”henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.”

Henkilötietoja käsiteltäessä on rekisterinpitäjän tai henkilötietojen käsittelijän otettava huomioon asianmukainen turvallisuus henkilötietojen käsittelyssä. Asianmukainen turvallisuus korostuu vaatimuksena myös muualla GDPR:ssä, varsinkin GDPR:n 4 luvussa. Tietojenkäsittelyn turvallisuutta käsitellään alla luvussa 3.3.3.

3.3.2 Rekisterinpitäjän ja henkilötietojen käsittelijän vastuu

GDPR:n 4 luku käsittelee rekisterinpitäjän ja henkilötietojen käsittelijän vastuuta. GDPR:n 4 luku 1 jakso käsittelee yleisiä velvollisuuksia. GDPR:n 24 artiklan mukaan:

> ”Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.
>
> Kun se on oikeasuhteista käsittelytoimiin nähden, 1 kohdassa tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.”

Rekisterinpitäjällä on erityisesti vastuu huolehtia tietosuojan tason riittävyydestä tietojenkäsittelyssä ja tietojen rekisteröinnissä. Rekisterinpitäjän on huolehdittava myös siitä, että rekisterinpitäjä itse käsittelee henkilötietoja oikein ja että mahdolliset henkilötietojen käsittelijät, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun, käsittelevät niitä oikein.[58] Tässä voidaan vielä mainita, että rekisterinpitäjiä voi olla monta ja että he voivat myös toimia GDPR:n 28 artiklan mukaisina yhteisrekisterinpitäjinä. Näissä tilanteissa yhteisrekisterinpitäjät määrittelevät käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen yhdessä. Rekisterinpitäjällä on siis lopullinen vastuu tietojenkäsittelyn tarkoituksen ja tietosuojan tason riittävyyden määrittelemisessä.

Rekisterinpitäjä määrittelee henkilötietojen käsittelyn luonteen ja käsittelyn tarkoitukset. Henkilötietojen käsittelijä voi taas käsitellä tietoja rekisterinpitäjän puolesta. Henkilötietojen käsittelijä, joka käsittelee tietoja rekisterinpitäjän lukuun, on täytettävä vaatimukset GDPR:n 28 artiklan 1 kohdassa. GDPR:n 28 artiklan 1 kohdan mukaan:

> ”Jos käsittely on määrä suorittaa rekisterinpitäjän lukuun, rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.”

Henkilötietojen käsittelijän on täytettävä samat tietosuojan vaatimukset eli asianmukaiset tekniset ja organisatoriset toimet, joita rekisterinpitäjä käyttää tietojen suojaamisessa. Näin tietosuoja rekisterinpitäjän ja henkilötietojen käsittelijän välillä muodostaa hierarkian, jossa rekisterinpitäjä vastaa käsittelyn luonteesta ja mihin tarkoituksiin käsittelyjä tehdään. Henkilötietojen käsittelijä suorittaa siis henkilötietojen käsittelyä rekisterinpitäjän lukuun. Käytännössä tämä tarkoittaa esimerkiksi sitä, että rekisterinpitäjä on määritellyt tietyn tietosuojan riittävyyden tason. Tietojenkäsittelijän tulee noudattaa ja tehdä samat toimenpiteet kuin rekisteripitäjä, jotta rekisteripitäjän määrittelemä tietosuojan riittävyys toteutuu.

Henkilötietojen käsittelijä ei saa käyttää toisen käsittelijän palveluita ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Rekisterinpitäjä vastaa käsittelyn luonteesta. Mikäli käsittelijä käyttää toista henkilötietojen käsittelijää, syntyy henkilötietojen käsittelystä jatkumo. Hierarkiassa on silloin käytännössä lisää käsittelijöitä ja heitä voidaan lisätä enemmän, mikäli rekisterinpitäjä tämän sallii. Näitä käsittelijöitä kutsutaan alikäsittelijöiksi. Henkilötietojen

[58] Korpisaari – Pitkänen –Warma-Lehtinen 2022, s. 299

käsittely rekisterinpitäjän ja henkilötietojen käsittelyn alaisuudessa on lisäksi korostettu GDPR:n 29 artiklassa:

> ”Henkilötietojen käsittelijä tai kukaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, ei saa käsitellä niitä muuten kuin rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä niin vaadita.”

GDPR:n 29 artiklassa korostetaan rekisterinpitäjän käsittelyn luonteen ja tarkoituksen vaatimuksen noudattamista.

Rekisterinpitäjän on laadittava kirjallinen sopimus henkilötietojen käsittelijän kanssa, jossa käsittelijä sitoutuu noudattamaan rekisterinpitäjän käsittelyperiaatteita. Vaihtoehtoisesti sopimuksen sijaan voidaan käyttää muulla unionin oikeuden tai jäsenvaltion lainsäädännön oikeudellisella asiakirjalla.[59] GDPR:n 28 artiklan 3 kohdan mukaan sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä erityisesti kohdista a) – h). Vaatimukset liittyvät esimerkiksi käsittelyn rajaukseen rekisterinpitäjän mukaisesti ja henkilötietojen turvallisuuden toteuttamiseen GDPR:n 32 artiklan mukaisesti.

Samat säännöt pätevät GDPR:n 28 artiklan 4 kohdan mukaan myös alikäsittelijöitä. GDPR:n 28 artiklan 4 kohdan mukaan alikäsittelijöihin sovelletaan samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu 3 kohdassa tarkoitetussa rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa.

Onnistuneella tavalla rekisterinpitäjän alaisuudessa voi olla monta henkilötietojen käsittelijää, jotka kaikki käsittelevät tietoja rekisterinpitäjän käsittelyn luonteen ja tarkoituksen mukaan. Tämä ei kuitenkaan ole käytännössä helppoa, varsinkin, kun nämä niin sanotut ”tietojenkäsittelyketjut” voivat sisältää monta tahoa ja olla kansainvälisiä. Laajat kansainväliset tietojenkäsittelyketjut ovat entistä monimutkaisempia säilyttääkseen lainmukaisuuden, huomioiden EU:n tietosuojavaatimukset, erikoislainsäädännön sekä mahdolliset kolmansien maiden tietosuojavaatimukset ja erikoislainsäädäntö.

Ongelmallisuutta kuvaa ETN 2021:313 päätös, missä rekisterinpitäjä oli epäonnistunut tietosuojan toteuttamisessa niin, että rekisterinpitäjä ei ollut huomioinut niitä vaatimuksia, jotka GDPR:n 28 artiklan 3 ja 4 kohdat asettavat sopimukselle rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Tarkemmin, rekisteripitäjä oli käyttänyt tietojenkäsittelyn toimenpidettä

[59] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s. 345

varten tietojenkäsittelijää. Tämä tietojenkäsittelijä oli taas käyttänyt alikäsittelijöitä. Palvelin, jolla tietojenkäsittelyä tehtiin, oli myöhemmin joutunut tietomurron kohteeksi. ETN totesi, että vaikka rekisteripitäjä oli oikeaoppisesti ilmoittanut tietomurrosta valvontaviranomaiselle, niin tietojenkäsittelijät olivat epäonnistuneet riittävän tietosuojan toteuttamisessa, sillä rekisterinpitäjä ei ollut lisännyt tietojenkäsittelysopimukseen GDPR:n 28 artiklan 3 ja 4 kohdan vaatimuksia. Näin ollen henkilötietojen käsittelijät eivät pystyneet varmistamaan riittävän tietosuojan vaatimusten toteutumista rekisterinpitäjän käsittelyn luonteen ja tarkoituksen mukaisesti.[60] Kansainvälisissä tiedonsiirroissa varsinkin rekisterinpitäjän ja käsittelijän on oltava hyvin tietoisia tietojenkäsittelyn luonteesta ja tarkoituksesta, jotta tietojenkäsittely tehdään laillisesti.

3.3.3 Käsittelyn turvallisuus

Tietojenkäsittelyn turvallisuus on yksi tärkeimmistä vaatimuksista tietosuojassa.[61] Mikäli tietoja käsitellään kansainvälisesti, voidaan sanoa, että tietojenkäsittelyn turvallisuus korostuu entisestään. GDPR:n 32 artikla käsittelee tietojenkäsittelyn turvallisuutta. GDPR:n 32 artiklan mukaan tietojenkäsittelyssä on otettava huomioon:

> ”Uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet”

Tietosuojassa käytetään riskiperusteista lähestymistapaa.[62] Tarkoituksena on minimoida riskit ennen kuin vahinkoja tapahtuu. Sopimusoikeudessa tehdään myös riskienhallintaa. Perinteisesti sopimusoikeuden ideana on riskienhallinta sopimuksen laatimis- ja valmisteluprosessin aikana. Riskienhallinnan kautta osapuolet pystyvät tekemään intressi- ja tavoiteanalyysia sopimuksen olosuhteisiin ja ehtoihin liittyen. Mika Hemmo kuvailee intressi- ja tavoiteanalyysia sopimusoikeudessa sopimuksenkartoituksen strategiana, jossa otetaan huomioon sopimuksen liittyvät mahdolliset riskit, kuten korvausvastuuriski, sitovuusriski, tulkintariski,

[60] Euroopan tietosuojaneuvoston päätös ETN 2021:313
[61] Esim. tapauksessa ETN 2022:325 todettiin, että GDPR:n 32 artiklan laiminlyönti tietojenkäsittelyssä merkitsee usein sitä, että rekisterinpitäjä ei ole huomioinut käsittelyn turvallisuutta GDPR:n mukaan. Teknisten ja organisatoristen toimenpiteiden puuttuminen käsittelyn turvallisuuden arvioinnista arvioitiin tässä tapauksessa niin, että rekisteröityjen oikeuksia loukattiin. s.116–117
[62] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.443

sopimuskumppanin luotettavuus ja maksukyky sekä suorituskustannusriski. Tarkoituksena on sopimuksen luonnostelun yhteydessä kartoittaa, mitkä ovat osapuolten sopimukselle asettamat päämäärät ja niiden toteutumisen mahdollisuuden esteet.[63]

Käsittelyn turvallisuudessa riskienarvioinnin lähtökohdat ovat erilaiset kuin sopimusoikeudessa. Tarkoituksena on arvioida riskit ja minimoida ne käyttämällä asianmukaisia teknisiä ja organisatorisia toimenpiteitä. Riskien torjumiseen tietojenkäsittelyssä tulisi käyttää niitä toimenpiteitä, jotka parhaiten huomioivat uusimman tekniikan, toteuttamiskustannukset, käsittelyn luonteen, käsittelyn laajuuden, käsittelyn asiayhteyden, käsittelyn tarkoituksen ja luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.[64]

Käsittelyn turvallisuus on määritelmänä ja GDPR:n sääntöjen mukaan eri kuin GDPR:n 4 luvun 35 artiklan tietosuojaa koskeva vaikutustenarviointi. Tietosuojaa koskevaa vaikutustenarviointia käsitellään alla jaksossa 3.3.4, mutta tässä vaiheessa voidaan jo todeta, että kyseessä on eri toimenpide kuin käsittelyn turvallisuuteen liittyvät toimenpiteet. Vaikka kummassakin toimenpiteessä tehdään riskienarviointia, niin jälkimmäinen toimenpide, eli tietosuojaa koskeva vaikutustenarviointi, arvioi rekisteröidyn oikeuksien ja vapauksien toteutumista tietojenkäsittelyssä. Käsittelyn turvallisuudella halutaan arvioida tietojenkäsittely toimenpiteiden turvallisuutta.

Lisäksi käsittelyn turvallisuuden kannalta henkilötietojen tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ja rekisteröidylle, mikäli tietoturvaloukkauksia sattuu GDPR:n 4 luvun 33–34 artiklan mukaisesti. Kansainvälisissä tiedonsiirroissa, tulee loukkauksesta ilmoittaa jokaiselle valtion tietosuojaviranomaiselle, missä henkilötietojenkäsittelyä on tehty.

Lopuksi käsittelyn turvallisuus edellyttää, että rekisterinpitäjä tai henkilötietojenkäsittelijä noudattaa GDPR:n 32 artiklan vaatimuksia. Näin ollen tietojenkäsittelyssä on otettava huomioon uusin tekniikka ja toteuttamiskustannukset ja arvioitava, mikäli sen pitäisi a) salata tai pseudonymisoida henkilötietoja, b) taata käsittelyjärjestelmien jatkuva luottamuksellisuus, c) taata kyky nopeasti palauttaa tietojen saatavuus ja pääsy tietoihin fyysisen vian sattuessa sekä d) taata, että käsittelyn turvallisuutta testataan, tutkitaan ja arvioidaan säännöllisesti.

[63] Hemmo 2005, s. 11–15
[64] Öman 2019, s. 411

3.3.4 Tietosuojaa koskeva vaikutustenarviointi

Verrattuna tietojenkäsittelyn turvallisuuteen, GDPR:n 4 luvun 35 artikla suoraan toteaa, että tietosuojaa koskeva vaikutustenarviointi on tehtävä tilanteissa joissa:

> ”käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin.”

Kun tietojenkäsittelyn toimenpiteitä arvioidaan, on rekisterinpitäjän arvioitava ensiksi käsittelyn turvallisuuden vaatimuksia. Näitä vaatimuksia on yleisesti ottaen aina arvioitava tietojenkäsittelyssä. Tietosuojaa koskevan vaikutustenarvioinnin vaatimuksissa mainitaan, että käsittelyn on todennäköisesti aiheutettava henkilön oikeuksien ja vapauksien kannalta korkean riskin.[65] Toisin sanoen asetuksen mukaan, tietosuojaa koskeva vaikutustenarviointia ei säännöksen mukaan ole pakko tehdä, jos arvioidaan, että käsittely ei todennäköisesti aiheuta henkilön oikeuksien ja vapauksien kannalta korkeita riskejä.[66] Rekisterinpitäjä arvioi, mikäli tietosuojaa koskeva vaikutustenarviointi on tarpeellinen. Mikäli tietosuojavastaavaa on nimitetty, on rekisterinpitäjän myös pyydettävä tietosuojavastaavalta mielipidettä tietosuojan vaikutuksenarvioinnin tekemiseksi.

GDPR ei siis suoraan vaadi rekisterinpitäjää tekemään vaikutustenarviointia, mikäli asetuksen vaatimukset vaikutustenarvioinnille eivät täyty. Kansainvälisissä rajaa ylittävissä tiedonsiirroissa on kuitenkin usein kyse tietojenkäsittelystä niin suuressa mittakaavassa, että nämä vaatimukset useimmiten täyttyvät. Varsinkin tietojen määrä ja niiden sensitiivisyys puoltaa vaikutuksenarvioinnin laatimista ennen tietojenkäsittelyä. Esimerkiksi tapauksessa ETN 2022:325 riidanratkaisulautakunta totesi, että TCF-läpinäkyvyys- ja suostumuskehys (Transparency & Consent Framework IAB Europe) nettisivuilla ja ohjelmissa käsitteli niin suuren ryhmän henkilöiden henkilötietoja, että vastaajan olisi pitänyt laatia tietosuojaa koskevan vaikutustenarvioinnin ennen toimenpiteiden eli kansainvälisten tiedonsiirtojen aloittamista.[67]

Toinen yleinen tilanne vaikutuksenarvioinnin laatimiselle on uuden teknologian käyttöönotto, mikä todennäköisesti vaikuttaa luonnollisen henkilön oikeuksiin ja vapauksiin.[68]

[65] Staunton – Slokenberga – Parziale – Mascalzoni 2022, s. 2–3
[66] Apulaistietosuojavaltuutetun päätös 27.4.2023 7684/171/22
[67] ETN päätös 2022:325 s. 108–109, samat johtopäätökset voidaan vetää apulaistietosuojavaltuutetun päätöksestä 27.4.2023 7684/171/22 ja EUT C-311/18 (*Schrems II*)
[68] Öman 2019, s. 425–426

Rekisterinpitäjän on aina arvioitava tietojenkäsittelyssä, mikäli vaikutuksenarviointi on tarpeellinen. Kansainvälisissä tietojenkäsittelyissä artiklan vaatimusten toteutuminen on kuitenkin varsin todennäköistä. Lisäksi vaikutuksenarviointi on tehtävä, vaikka rekisteröity olisi antanut 6 ja 7 artiklan mukaisen suostumuksensa tietojenkäsittelyyn. Rekisterinpitäjän on oltava tarkka tietojenkäsittelyä edeltävissä toimenpiteissä, sillä hänellä on lopullinen vastuu laatia oikeat toimenpiteet lainsäädännönmukaiselle tietojenkäsittelylle.[69]

Kansainvälisissä tiedonsiirroissa voidaan todeta, että erityisesti tietojenkäsittelyiden kansainvälisyys, tietojenkäsittelyn suuruus ja mittakaava sekä teknologian valinta ovat sellaisia olosuhteita, joissa rekisterinpitäjän on varsinkin otettava huomioon arvioidessaan tietosuojan vaikutuksenarvioinnin tarpeellisuutta ja jos kyseessä on korkean riskin tietojenkäsittely. Korkean riskin aiheuttaa myös olosuhteet, missä riskejä on olemassa siitä, että kolmannen maan viranomaisilla on mahdollisuuksia päästä katsomaan tietojenkäsittelyn alaisia henkilötietoja.[70]

3.3.5 Tietosuojavastaavan vastuu

Kansallinen tietosuojaviranomainen ylläpitää ja antaa ratkaisuja liittyen tietosuojalainsäädännön seuraamiseen EU:n jäsenmaissa. Siksi organisaatioilla on usein nimitetty tietosuojavastaava, jos se käsittelee henkilötietoja tai ylläpitää tietokantoja henkilötiedoista. Tietosuojavastaava toimii organisaatiossa tietosuojaviranomaisen roolissa neuvoen, miten rekisterinpitäjä tai käsittelijän tulisi menetellä liittyen niihin toimenpiteisiin, joilla tietosuojaa toteutetaan.

GDPR:n 4 luvun 37 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava aina kun:

> ”tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin, rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, tai rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu 9 artiklan mukaisiin erityisiin henkilötietoryhmiin ja 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin.”

[69] Öman 2019, s. 426
[70] Esim. Apulaistietosuojavaltuutetun päätös 27.4.2023 7684/171/22 ja EUT C-311/18 (*Schrems II*)

Tietosuojavastaava vastaa GDPR:n 4 luvun 39 artiklan mukaan siitä, että rekisterinpitäjälle tai käsittelijälle sekä henkilötietoja käsitteleville työntekijöille annetaan riittävästi neuvoja ja tietoja GDPR:n ja muun jäsenvaltioiden tietosuojasäännösten tulkinnasta. Tietosuojavastaava myös seuraa, että GDPR:ä ja muita jäsenvaltioiden tietosuojasäännöstöjä noudatetaan. Lisäksi tietosuojavastaava neuvoo tarvittaessa tietosuojaa koskevasta vaikutustenarvioinnista ja sen toteutuksesta, tekee yhteistyötä kansallisen tietosuojaviranomaisen kanssa ja toimii tietosuojaviranomaisen yhteyshenkilönä käsittelyyn liittyvissä kysymyksissä.

3.4 Todetut vaatimukset

Yllä olevan perusteella voimme todeta, että liittyen käsittelyn turvallisuuteen on kansainvälisissä tiedonsiirroissa otettava huomioon: tietojenkäsittelyn yleiset periaatteet, rekisterinpitäjän ja käsittelijän oma vastuu, tietojenkäsittelyn turvallisuus, tietosuojaa koskeva vaikutustenarviointi ja tietosuojavastaavan vastuu sekä käsittelyn lainmukaisuus.

Onnistunut tiedonsiirto tietosuojalainsäädännön mukaisesti tehdään näitä GDPR:n vaatimuksia noudattaen. Kansainvälisisissä tiedonsiirroissa käytetään näiden vaatimusten lisäksi tiettyjä lainsäädännössä vaadittuja tiedonsiirtovälineitä siirtojen tekemiseen. Nämä käsitellään tarkemmin alla luvussa 4.

4. Eri tiedonsiirtovälineet kansainvälisille tiedonsiirroille

Yllä on käsitelty niitä yleisiä vaatimuksia, joita henkilötietoja siirtävän tahon on noudatettava yleisesti tietojenkäsittelyssä ja tietojenkäsittelyssä rajoja ylittävissä tilanteissa niin EU:n ja ETA:n sisällä kuin EU:n ulkopuolella, eli kansainvälisissä tiedonsiirroissa. Seuraavaksi käsitellään tarkemmin niitä menetelmiä, joita rekisterinpitäjä ja käsittelijä voivat käyttää, noudattaakseen GDPR:n vaatimuksia kansainvälisissä EU:n ja EU:n talousalueen ulkopuolisissa tiedonsiirroissa.

4.1 Kolmansille maille myönnetty EU:n komission riittävyyspäätös

Vuonna 2023 Euroopan komissio oli myöntänyt riittävyyspäätöksen Sveitsille, Kanadalle, Argentiinalle, Guernseylle, Mansaarille, Jerseylle, Färsaarille, Andorralle, Israelille, Uruguaylle ja Uudelle-Seelannille. Nykypäivänä myös Japanille ja Etelä-Korealle on myönnetty riittävyyspäätös. Lopuksi myös Yhdistyneelle kuningaskunnalle on myönnetty riittävyyspäätös Brexit-prosessin jälkeen GDPR:n mukaisesti. Hiljattain myös Yhdysvallat on saanut uuden riittävyyspäätöksen (EU-US Data Privacy Framework).[71]

GDPR:n 46 artiklan mukaan mikäli GDPR:n artikla 45 kohta 3 mukaista riittävyyspäätöstä ei ole tehty, voi rekisterinpitäjä tai henkilötietojen käsittelijä siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Ottaen huomioon GDPR:n luvun 5 vaatimukset tiedonsiirroille on rekisterinpitäjän tai henkilötietojen käsittelijän otettava huomioon myös muut yleiset vaatimukset tietojen siirtämiselle tietosuojalainsäädännössä.

Riittävyyspäätöksiä ei käsitellä tässä tutkielmassa enempää tutkielman rajauksen takia. Tarkoituksena on käsitellä muita tiedonsiirtovälineitä, jotka eivät ole riittävyyspäätöksiä.

4.2 Yleisesti tiedonsiirtovälineistä

Tiedonsiirtovälineet ovat GDPR:n 46 artiklan mukaisia toimenpiteitä, joiden avulla rekisterinpitäjä tai henkilötietojen käsittelijä pystyy osoittamaan asianmukaiset suojatoimet kansainvälisissä tiedonsiirroissa. Kuten edellä todettiin, tulee myös rekisterinpitäjän tai henkilötietojen käsittelijän noudattaa yleisiä tietojenkäsittelyperiaatteet, kun se käsittelee henkilötietoja kansainvälisesti. Eroavaisuus henkilötietojen käsittelyssä kansainvälisesti on kuitenkin se, että EU:n ja ETA:n sisällä tiedonsiirtovälineitä ei tarvitse käyttää, sillä kaikki

[71] Carey 2018, s. 108–115

EU:n jäsenmaat täyttävät jo EU:n yleiset tietosuojavaatimukset. Näissä tiedonsiirroissa tulee rekisterinpitäjän tai henkilötietojen ainoastaan huomioida yleiset tietojenkäsittelyperiaatteet. Kun tietoja siirretään EU:n ulkopuolelle, tarvitaan kuitenkin tietosuojavaatimusten todistamiseksi tiedonsiirtovälineitä. Yllä on käsitelty Euroopan komission kolmansille maille myöntämä riittävyyspäätös, joka on yksi tiedonsiirtoväline. Mikäli riittävyyspäätöstä ei ole voimassa kolmannessa maassa voimassa, tulee asianmukaiset suojatoimet todistaa alla käsiteltävillä tiedonsiirtovälineillä.

4.2.1 Tiedonsiirtovälineet

Mikäli rekisterinpitäjä tai tietojenkäsittelijä haluaa siirtää henkilötietoja EU:n tai EU:n talousalueen ulkopuolelle kolmanteen maahan ja tällä maalla ei ole EU:n komission myöntämää tietosuojan riittävyyspäätöstä, pitää tietoja siirtävän tahon huomioida muut GDPR:n kansainvälisiä tiedonsiirtoja edellyttämät vaatimukset.

Eri tiedonsiirtovälineet ovat GDPR:n 46 artiklan siirto asianmukaisia suojatoimia soveltaen, GDPR:n 47 artiklan yritystä koskevat sitovat säännöt ja GDPR:n 49 artiklan erityistilanteita koskevat poikkeukset. Lisäksi GDPR:n 48 artikla sääntelee tiedonsiirroista ja tiedonluovutuksista, joita ei sallita unionin lainsäädännössä. Erityistilanteita ja kiellettyjä tiedonluovutuksia ei käsitellä tutkielmassa, sillä ne eivät tarkalleen ottaen ole tiedonsiirtovälineitä.

4.2.2 Asianmukaisten suojatoimien määritelmä

GDPR:n 44 artiklan mukaan:

> ”Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.”

GDPR:n artikla 44 asettaa minimivaatimukset suojatoimille kansainvälisissä tiedonsiirroissa. Asianmukaisen suojatoimen määritelmälle ei ole kuitenkaan laadittu yhdenmukaista määritelmää oikeuskäytännön ja kirjallisuuden mukaan.

Tiedonsiirtovälineet ovat kuitenkin yksi osa, joita käytetään asianmukaisen tietosuojan varmistamiseksi kansainvälisissä tiedonsiirroissa. Tiedonsiirtovälineiden yleinen vaatimus on se, että siirretyille henkilötiedoille olisi olennaisilta osin tarkoitus tarjota EU:ssa taattua tasoa vastaavaa henkilötietojen suojaa.[72] Toinen osa on yleiset henkilötietojen käsittelyperiaatteet ja käsittelyn turvallisuutta koskevat määritelmät, joita on käsitelty alla luvussa neljä. Tutkielman johtopäätöksien mukaan nämä vaatimukset ovat tietojen siirtämisen yleiset vaatimukset, rekisterinpitäjän ja käsittelijän oma vastuu, tietojenkäsittelyn turvallisuus, tietosuojaa koskeva vaikutustenarviointi ja tietosuojavastaavan vastuu sekä käsittelyn lainmukaisuus sekä kansainvälisiä tiedonsiirtoja koskevat tiedonsiirtovälineet. Tiedonsiirtovälineet ja yleiset henkilötietojen käsittelyperiaatteet takaavat asianmukaiset suojatoimet kansainvälisissä tiedonsiirroissa. Tätä johtopäätöstä käsitellään lisää luvussa 4.4 ja 5.

EUT C-311/18 *Schrems II* ja GDPR:n johdanto-osan määritelmä ”unionissa taattua suojaa vastaavasta suojasta” tarkoittaa käytännössä sitä, että tietosuojan ja suojatoimien tason on vastattava sitä tasoa, mitä EU:ssa ja ETA:n alueella tietosuojan suojatoimista vaaditaan. Tämän määritelmän mukaan suojatoimien tulisi vastata kansainvälisisissä tiedonsiirroissa olennaisesti unionissa taattua suojaa. Käytännössä käsitteelle ei ole olemassa kirjallisuudessa yhtenäistä määritelmää, mutta kyseessä voi olla lainopillisen tulkinnan mukainen oikeuskäytännön ja kirjallisuuden määritelmä unionin tietosuojalle. Tietosuojan taso EU:ssa riippuu oikeushierarkian mukaisesti lainsäädännön, oikeuskäytännön ja kirjallisuuden määritelmästä. Analogisesti voi todeta, että vastaavasti tietosuojavaatimukset, jotka eivät päde EU:ssa, eivät myöskään velvoita kolmannen maan osapuolta, joka vastaanottaa henkilötietoja tiedonsiirrossa. Tietosuojan suojatoimien vaatimusten tason on minimivaatimuksena noudattava GDPR:n yleisiä tietojenkäsittelyperiaatteita ja käsittelyn turvallisuutta käsitteleviä periaatteita, joiden on todettu EU:ssa kattavan unionissa taattua suojaa henkilötiedoille. Toinen määritelmä voi olla yleinen tietosuojan taso tietoturvan näkökulmasta.

ETN on myös todennut, että mikäli kolmannen maan lainsäädäntö tai kolmannen maan käytäntö yleisesti heikentää tietosuojan tasoa siten, että EU:ssa taattua suojaa ei olennaisesti voida tiedonsiirroissa varmistaa, ei tiedonsiirtoa saa tehdä.[73] Tämä vastaa yllä olevaa ajatusta siitä, että EU:ssa taattu suoja on minimivaatimus ja että kansainvälisissä tiedonsiirroissa rekisterinpitäjän tai henkilötietojen käsittelijän on arvioitava tiedonsiirtoa suunnitellessaan miten kolmannen maan lainsäädäntö ja yleinen käytäntö saattaa vaikuttaa tietosuojan tasoon.

[72] EUT C-311/18 (*Schrems II*). Myös GDPR:n johdanto-osa kappaleet 108 ja 114
[73] ETN yleiset suositukset 01/2020, kohdat 74–76

Toisaalta asianmukaiset suojatoimet kansainvälisissä tiedonsiirroissa vastaavat ainoastaan GDPR:n 46 artiklassa käsiteltäviä kansainvälisiä tiedonsiirtovälineitä. Asianmukaiset suojatoimet tiedonsiirtovälineinä ovat tästä näkökulmasta vain lisätoimenpide kansainvälisiä tiedonsiirtoja varten. Näiden lisäksi tulee ottaa huomioon GDPR:n yleiset tiedonkäsittelyperiaatteet ja käsittelyn turvallisuutta koskevat periaatteet. GDPR: 46 artiklan 1 kohdan mukaan:

> ”Jollei 45 artiklan 3 kohdan mukaista päätöstä ole tehty, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.”

GDPR:n 46 artiklan 1 kohdan mukaan, rekisterinpitäjä tai henkilötietojenkäsittelijä voi siirtää henkilötietoja kolmanteen maahan vain, jos asianmukaiset suojatoimet ja luvussa 4 käsitellyt tietojenkäsittelyperiaatteet on toteutettu. Tämän perusteella voidaan todeta, että rekisterinpitäjä tai henkilötietojen käsittelijä, joka ei käytä tiedonsiirtovälineitä ei täytä asianmukaisia suojatoimia, ei saa siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle. Mikäli se siirtää tietoja, tulisi sen lopettaa tietojenkäsittelyntoimenpiteet välittömästi. Tämän määritelmän mukaan pääasia rekisteripitäjän tai henkilötietojen käsittelijän näkökulmasta on se, että rekisterinpitäjä tai henkilötietojen käsittelijä voi osoitusvelvollisuutensa mukaisesti todistaa, että GDPR:n 46 artiklan mukaisia tiedonsiirtovälineitä on tiedonsiirroissa käytetty.

Määritelmää voidaan tarkentaa oikeuskäytännön ja kirjallisuuden kautta, mihin tutkielma pyrkii tämän luvun lopussa. Ensiksi pitää kuitenkin käsitellä itse tiedonsiirtovälineet, sillä ne ovat niin kirjallisuudessa kuin myös lainsäädännössä määritelty vastaamaan asianmukaisia suojatoimia kansainvälisissä tiedonsiirroissa.

Tälle kysymykselle ei kuitenkaan voi saada tarkkaa vastausta lainopillisessa tutkielmassa. Tutkielma, joka keskittyisi ainoastaan määritelmään ja esimerkiksi keräisi dataa oikeuskäytännöstä liittyen tapauksiin, jotka käsittelevät asianmukaisia suojatoimia, voisi vastata entistä tarkemmin kysymykseen. Lainopillinen tutkielma pystyy tässä vaiheessa vain tekemään havaintoja oikeusjärjestelmän nykytilasta.

Asianmukaisen suojatoimen määritelmä kansainvälisissä tiedonsiiroissa on tästä näkökulmasta 1. EU:ssa taattu yleisen tietosuojan vaatimukset ja 2. GDPR:n yleisten henkilötietojenkäsittelyperiaatteiden ja kansainvälisten tiedonsiirtovälineiden käyttö

kansainvälisissä tiedonsiirroissa sekä 3. tiedonsiirtovälineiden käyttö kansainvälisissä tiedonsiiroissa.

4.3 Tiedonsiirto asianmukaisia suojatoimia soveltaen

Pääasiallinen tiedonsiirtoväline, jota rekisterinpitäjä tai tietojenkäsittelijä voi käyttää, on GDPR:n 46 artiklan tiedonsiirto asianmukaisia suojatoimia soveltaen. Artiklan mukaan:

> ”rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.”

Rekisterinpitäjän tai henkilötietojen käsittelijän on siis varmistettava, että tarvittavat asianmukaiset suojatoimet ovat toteutuneet ennen kuin tietoja siirretään. Lisäksi rekisteröityjen saatavilla on oltava täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.

Tarvittavat asianmukaiset suojatoimet viittaavat ensinäkin niihin yleisiin henkilötietojen turvallisuusperiaatteisiin, joita käsiteltiin yllä luvussa 3. Lisäksi käsittelyn on noudatettava GDPR:n 5 artiklaa henkilötietojen käsittelyä koskevista periaatteista ja 6 artiklaa käsittelyn lainmukaisuudesta. Lisäksi asianmukaiset suojatoimet on tulkittu oikeudenkäytännössä tapauskohtaisesti. Näitä tapauksia tulkitaan myös alla.

Menetelmät tietojen siirtämiselle ilman riittävyyspäätöstä ovat GDPR:n 46 artiklan kohta 1 mukaan seuraavat:

> ”a) viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline; b) 47 artiklan mukaiset yritystä koskevat sitovat säännöt; c) komission 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen antamat tietosuojaa koskevat vakiolausekkeet; d) tietosuojaa koskevat vakiolausekkeet, jotka tietosuojaviranomainen vahvistaa ja jotka komissio hyväksyy 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen; e) 40 artiklassa tarkoitetut hyväksytyt käytännesäännöt yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin; f) 42 artiklassa tarkoitettu hyväksytty sertifiointimekanismi yhdessä kolmannen maan rekisterinpitäjän tai

henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin.”

Lisäksi 46 artiklassa kohta 2 tarkoitetut suojatoimet, tarvitsevat erityisen valvontaviranomaisen antaman luvan tiedonsiirtojen tekemiseen.

> ”a) rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön rekisterinpitäjän, henkilötietojen käsittelijän tai vastaanottajan väliset sopimuslausekkeet; tai b) säännökset, jotka sisällytetään viranomaisten tai julkisten elinten välisiin hallinnollisiin järjestelyihin ja joihin sisältyy rekisteröityjen täytäntöönpanokelpoisia ja tehokkaita oikeuksia.”

Käytännössä asianmukaisten suojatoimien käyttö kansainvälisissä tiedonsiirroissa on tavallista. Koska EU:n tiedonsiirtojen riittävyyden päätöksen alaisia maita ei ole paljon, liittyvät luultavasti suurin määrä tiedonsiirtoja asianmukaisiin suojatoimiin liittyviin tiedonsiirtovälineisiin.[74] Toisaalta riittävyyspäätöksiä on vuonna 2023 enemmän ja merkittäviä valtioita, kuten Japani, Yhdysvallat ja Yhdistyneet kuningaskunnat, kuuluvat myös tähän ryhmään.

Rekisterinpitäjä on, kuten edellä on todettu, lopuksi vastuussa siitä, että oikeita suojatoimia käytetään tietosuojan toteuttamisessa. Tämä pätee myös kansainvälisiin tiedonsiirtoihin. Mikäli rekisterinpitäjä päättää käyttää 46 artiklan alaista tiedonsiirtovälinettä, on tämän pystyvä varmistaa, että kyseinen tiedonsiirtoväline on sopiva tiedonsiirtoa varten. Rekisterinpitäjän pitää siksi riskienhallintaperiaatteen mukaisesti arvioida, mikäli tietoja vastaanottava osapuoli voi varmistaa vastaavan tietosuojan tason, jonka EU:n ja ETA:n maiden sekä riittävyyspäätösten alaiset valtiot tietosuojasta takaavat. Arviointia suojatoimien vaativuudesta käsitellään alla.[75]

Lopuksi rekisterinpitäjän on tiedonsiirtovälineen arvioinnissa huomioitava GDPR:n 6.1 artikla, 5.1 ja mahdollisesti 9 artikla ennen kuin tiedonsiirtovälineitä käytetään. Rekisterinpitäjän on siis arvioitava, kuten edellä luvussa 3.2.1 mainittiin, GDPR:n artikla 6.1 mukaan mikäli käsittely on lainmukaista. Yleisten periaatteiden noudattaminen GDPR:n 5.1 artiklan mukaan tarkoittaa sitä, että rekisteripitäjän on huomioitava henkilötietojen käsittelyä koskevat yleiset periaatteet ennen kuin tiedonsiirtoja tehdään. Nämä olivat käsittelyn lainmukaisuus,

[74] Carey 2018, s. 114–115
[75] ETN yleiset suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi 2021, s.14

kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen/tietojen minimointi, eheys ja luottamuksellisuus sekä osoitusvelvollisuus, kuten edellä mainittiin luvussa 3.2.1. Lisäksi GDPR:n artikla 9 on otettava huomioon sitä varten, että käsittelyn tai rekisteröinnin kannalta tiedonsiirroissa käsitellään erityisiä henkilötietoryhmiä koskevia henkilötietoja, esimerkiksi terveyttä koskevia tietoja.[76]

4.3.1 Viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline

4.3.1.1 Siirtovälineen määritelmä

GDPR:n 46 artiklan 2 kohdan a) viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline voi käytännössä olla monimuotoinen tahdonilmaisu tai sopimus, jonka perusteella tietoja siirretään.[77]

Yleisesti viranomaisten tai julkisten elinten välineiden oikeudellisesti sitovia ja täytäntöönpanokelpoisia välineitä ovat olleet kansainväliset tai julkisoikeudelliset sopimukset. Englanninkielisessä GDPR:n käännöksessä puhutaan säädöksessä:

> ”A legally binding and enforceable instrument between public authorities or bodies.”

Kyseessä on suomeksi siis ”väline”. Kirjallisuudessa todetaan, että tämän välineen käytännöllisellä muodolla ei ole väliä. Tällä välineellä ei siis ole suoraan muodollisia vaatimuksia, mutta sen pitää pystyä osoittamaan, että oikeudellisesti sitova ja täytäntöönpanokelpoinen velvoite on olemassa.[78] Kansainväliset valtionkeskeiset sopimukset ovat tavallisimpia muotoja näistä velvoitteista. Esimerkkinä voidaan mainita EU:n ja Yhdysvaltojen välinen *privacy shield* ja sitä seuraamat päivitetyt versiot (nykyään riittävyyspäätös EU-US Data Privacy Framework).[79]

4.3.1.2 Esimerkkitapauksia oikeudellisesti sitovasta ja täytäntöönpanokelpoisesta välineestä

Viranomaisten tai julkisten elinten väliset oikeudellisesti sitovat ja täytäntöönpanokelpoiset välineet ovat, kuten edellä mainittiin, usein valtioiden kesken teettämiä sopimuskokonaisuuksia. Koska kyseessä on GDPR:n laatima suojatoimen vaatimus, jota

[76] Öman 2019, s.480–481
[77] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s.486
[78] Korpisaari – Pitkänen – Warma-Lehtinen, 2022 s. 486
[79] Carey 2018, s.110–114, Tätä käsitellään lisää alla.

voidaan käyttää kansainvälisessä tiedonsiirrossa, tulisi sopimuksen koskea ja olla juridisesti pätevä EU:n ja kolmannen osapuolen valtion välillä. GDPR:ssä ei tosin suoraan viitata siihen, että kyseessä ei voisi olla valtioiden keskeinen sopimus, joka ei sido koko EU:ta ja EU:n talousaluetta. Sopimuksen tekeminen koko EU:n ja EU:n talousalueen sekä kolmannen valtion välillä lienee kuitenkin tavallisempaa, sillä ETN:llä ja Euroopan komissiolla on halu ylläpitää tietosuojalainsäädännön yhdenmukaistamista koko Euroopan alueella. Jos valtiot alkavat laatimaan omia sopimuksiaan, heikkenee komission pääasiallinen tahto siitä, että tietosuojan on kolmannessa maassa vastattava vähintään samaa tietosuojan tasoa, joka on käytössä EU:ssa.[80]

Käytännössä viranomaisten ja julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline ei myöskään ole enää tavanomainen siirtomenetelmä. Kyseessä voi olla lainsäädännöllinen jäänne GDPR:ää edeltävästä ajasta, jolloin EU:lla oli käytössä kolmansien maiden kanssa olevia tiedonsiirtosopimuksia.[81] Säännös on enimmäkseen olemassa sen takia, että mahdolliset vanhat sopimukset olisivat vieläkin GDPR:n implementoinnin jälkeen voimassa.

Mikäli rekisterinpitäjä tai henkilötietojen käsittelijä haluaa käyttää viranomaisten tai julkisten elinten välistä oikeudellisesti sitovaa ja täytäntöönpanokelpoista välinettä siirtomenetelmänä ja asianmukaisten suojatoimien todistamiseksi, tulisi hänen viitata oikeaan välineeseen tietojenkäsittelysopimuksessa tai toisessa välineessä, millä tietojen siirtoa käytännössä todistetaan. Tietojenkäsittelysopimus ei käytännössä ole ainoa vaadittava väline tietojenkäsittelyä varten, mutta se on ainakin laajimmin käytetty väline tietosuojavaatimusten velvoitteiden osoittamiseksi ja myös vaatimus kuten edellä todettiin tietyissä tietojenkäsittelytoimenpiteissä kuten esimerkiksi GDPR:n 28 artiklan 3 kohdan täyttämiselle.[82]

4.3.2 Yritystä koskevat sisäiset säännöt

4.3.2.1 Siirtovälineen määritelmä

GDPR:n 46 artiklan 2 kohdan b) ja 47 artiklan mukaiset yritystä koskevat sisäiset säännöt (binding corporate rules, BCR-säännöt alla) ovat yritysten sisäistä toimintaa koskevia sääntöjä. Siirtovälineen tarkoitus on tehdä kansainvälisten konsernien ja organisaatioiden riittävän tietosuojan varmistaminen helpompaa. Kansainväliset organisaatiot ovat velvollisia

[80] Carey 2018, s.109
[81] Esim. Vanha EU:n ja Yhdysvaltojen välinen *privacy shield*-sopimus, joka oli voimassa jo ennen GDPR:n implementointia. Vanha *privacy shield* tuomittiin laittomaksi *Schrems I ja II* -ratkaisujen kautta.
[82] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 345–346

noudattamaan kansainvälisten tiedonsiirtojen vaatimuksia samalla tavalla kuin perinteisissä tiedonsiirroissa organisaation ulkopuolelle. Eroavaisuus näissä tilanteissa on se, että yhteisö tai organisaatio usein siirtää henkilötietoja yhteisön sisäisesti. Organisaation toimipaikat sijaitsevat kuitenkin usein eri valtioissa ja ne valtiot, jotka eivät kuulu riittävyyspäätösten ryhmään, tarvitsevat siirtovälineen asianmukaisten suojatoimen varmistamiseksi. BCR-säännöt vahvistavat, että koko tai ainakin osa organisaatiosta noudattaa samoja asianmukaisia suojatoimien edellytyksiä.[83]

Jotta BCR-sääntöjä voidaan käyttää tiedonsiirtoja varten, pitää valvontaviranomainen hyväksyä ne GDPR:n 47 artiklan 2 kohdan mukaan. Valvontaviranomainen on kansallinen valvontaviranomainen EU:ssa, joka on Suomessa tietosuojavaltuutetun toimisto. Kun valvontaviranomainen hyväksyy BCR-säännöt GDPR:n artikla 63 yhdenmukaisuusmekanismin mukaisesti, voidaan sääntöjä käyttää organisaation sisäisesti tiedonsiirtoja varten.[84] GDPR:n 63 artiklan mukainen yhdenmukaisuusmekanismi on järjestelmä, jonka mukaan valvontaviranomaisen on konsultoitava Euroopan tietosuojaneuvostoa ennen päätösten tekemistä. Konsultoinnin kautta Euroopan tietosuojaneuvosto pystyy varmistamaan yhdenmukaisen käytännön ja päätösten implementoinnin kokonaisvaltaisesti unionissa.[85] BCR-sääntöjen hyväksyminen vaatii siis kansallista valvontaviranomaista konsultoimaan Euroopan tietosuojaneuvostoa, ennen kuin se tekee päätöksen sääntöjen vahvistamisesta.

4.3.2.2 BCR-sääntöjen hyväksyminen

Kuten edellä mainittiin, tarvitsevat BCR-säännöt hyväksynnän kansalliselta viranomaiselta. Ennen kuin kansallinen viranomainen voi hyväksyä säännöt, tulee sen myös konsultoida GDPR:n yhdenmukaisuusmekanismin kautta Euroopan tietosuojaneuvoston mielipidettä säännöistä.

GDPR:n 47 artiklan 2 kohdan mukaan BCR-säännöissä tulee määritellä vähintään:

> ”a) konsernin tai yritysryhmän, joka harjoittaa yhteistä taloudellista toimintaa, ja sen kaikkien jäsenten rakenne ja yhteystiedot; b) tiedonsiirrot tai tiedonsiirtojen sarjat; c) sääntöjen oikeudellinen sitovuus sekä unionin sisällä että sen ulkopuolella; d) yleisten tietosuojaperiaatteiden soveltaminen; g) se, miten yritystä koskevista sitovista säännöistä ja erityisesti ilmoitetaan rekisteröidyille;

[83] Carey 2018, s.117
[84] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s. 494
[85] Carey 2018, s. 162–163

> h) yrityksen tai konsernin sisäiset nimitetyt tietosuojavastaavat i) valitusmenettelyt; j) mekanismit, joiden avulla konsernissa tai yritysryhmässä, joka harjoittaa yhteistä taloudellista toimintaa, pyritään varmistamaan, että yritystä koskevien sitovien sääntöjen noudattaminen varmistetaan; l) yhteistyömenettely valvontaviranomaisen kanssa sen varmistamiseksi, että kaikki konsernin tai yritysryhmän jäsenet noudattavat sääntöjä; m) mekanismit, joilla ilmoitetaan toimivaltaiselle valvontaviranomaiselle kolmannessa maassa konsernin tai yhteistä taloudellista toimintaa harjoittavan yritysryhmän jäseneen mahdollisesta sovellettavista oikeudellisista vaatimuksista, jotka todennäköisesti merkittävästi haittaavat yritystä koskeviin sitoviin sääntöihin sisältyviä takeita; ja n) asianmukainen tietosuojakoulutus henkilöstölle, jolla on pysyvä tai säännöllinen pääsy henkilötietoihin.[86]”

Kyseessä on usein suuria yhteisöjä, organisaatioita, yrityksiä ja konserneja koskeva siirtoväline ja näin ollen vaatimukset BCR-sääntöjen hyväksymiselle ovat varsin korkeat. BCR-sääntöjen hyväksyminen ja implementointi on varsin vaikea ja aikaa vievä prosessi, joka kestää usein 18–24 kuukautta. Prosessin hyödyt ovat kuitenkin selvät.[87] Valmiita BCR-sääntöjä voidaan käyttää yrityksen tai konsernin sisäisesti ilman erillisiä uusia tietojenkäsittelysopimuksia niin kauan kuin tiedonsiirrot tapahtuvat organisaation sisäisesti. BCR-säännöt ovat hankala tiedonsiirtoväline pienemmille yritykselle tai organisaatioille, jotka siirtävät tietoja toisille osapuolille, sillä hyväksymisprosessi säännöille voi kestää ja siirtoväline toimii ainoastaan yrityksen tai konsernin sisäisissä tiedonsiirroissa. BCR-sääntöjä voidaan siis käyttää vain yrityksen tai konsernin sisäisesti. Yrityksen ulkopuolella olevan osapuolen tulee käyttää toista tiedonsiirtovälinettä asianmukaisten suojatoimien todistamiseksi. BCR-sääntöjen hyödyt kansainvälisessä konsernissa ovat kuitenkin selvät. Hyväksytyt BCR-säännöt helpottavat päivittäistä yrityksen tai konsernin toimintaa, kun yksittäisiä tiedonsiirtoja ei tarvitse jatkuvasti auditoida, tarkastaa tai määritellä uudestaan.

4.3.3 Komission hyväksymät tietosuojaa koskevat vakiolausekkeet

4.3.3.1 Siirtovälineen määritelmä

Tietosuojaa koskevat vakiolausekkeet ovat komission hyväksymiä vakiosopimuslausekkeita kansainvälisiä tiedonsiirtoja varten. Komissio hyväksyi nykyiset versiot sopimuslausekkeista 4. kesäkuuta 2021. Vakiosopimuslausekkeiden mukaan niiden rooli rajoittuu asianmukaisten

[86] Öman 2019, s. 486–487
[87] Cox 2021

suojatoimien varmistamiseksi kansainvälisissä tiedonsiirroissa.[88] Niitä voidaan käyttää GDPR:n 46 artiklan 2 kohdan mukaisesti pohjana asianmukaisten suojatoimien todistamiseksi kansainvälisissä tiedonsiirroissa.

Vakiolausekkeet ovat käytännössä yleisin tietojensiirtoväline. Vakiolausekkeiden suosio voidaan selittää muun muassa sillä, että 1. niitä voidaan muuttaa varsin helposti tarpeen mukaan, 2. ne ovat yleisesti saatavilla Euroopan tietosuojaneuvoston ja kansallisten viranomaisten verkkosivuilla, 3. niitä voidaan implementoida eri tiedonsiirtotilanteissa ja 4. niiden implementointi ei vie suhteellisen paljon aikaa.[89]

4.3.3.2 Vakiolausekkeiden hyödyt ja puutteet

Vakiolausekkeiden merkittävin ja tärkein hyöty on se, että niitä pystyy muuttamaan tarpeen mukaan. Vakiolausekkeita käytetään useimmiten niin sanotuissa massasopimuksissa ja sopimuskokonaisuuksissa, joissa osapuolet haluavat käyttää samaa sopimuspohjaa useamman kerran.[90] Mikäli yhteisö haluaa laatia tiedonsiirtosopimuksen ja käyttää vakiolausekkeita tiedonsiirtovälineenä, voi tämä käyttää samoja vakiolausekkeita myös suurimmaksi osin tulevia tiedonsiirtoja varten. Tekniset kysymykset tiedonsiirroissa muuttuvat tosin aina, mutta vakiolausekkeiden vakioehdot ovat suunniteltu jatkuvaa käyttöä varten.

Vakiolausekkeet sisältävät neljä erilaista vakioehtoa, joita kutsutaan moduuleiksi. Nämä moduulit käsittelevät erilaisia tiedonsiirtotilanteita, joissa osapuolten juridiset määritelmät eroavat. Vakiolausekkeet koostuvat neljästä moduulista: Moduuli yksi käsittelee tiedonsiirtoja rekisterinpitäjältä rekisterinpitäjälle. Moduuli kaksi käsittelee tiedonsiirtoja rekisterinpitäjältä käsittelijälle. Moduuli kolme käsittelee tiedonsiirtoja käsittelijältä toiselle käsittelijälle. Moduuli neljä käsittelee tiedonsiirtoja käsittelijältä rekisterinpitäjälle. Osapuolten, jotka haluavat käyttää vakiolausekkeita tiedonsiirtosopimuksen tiedonsiirtovälineenä, tulee viitata vakiolausekkeiden yleisiin periaatteisiin sekä oikeaan moduuliin tiedonsiirtoa varten. Moduulien lisäksi osapuolten tulee kuvata, millä tavalla yleiset tietojenkäsittelyperiaatteet ovat huomioitu tiedonsiirtoa varten. Onnistunut tiedonsiirtosopimus, joka käyttää vakiolausekkeita, on juridisesti pätevä ja sitä voidaan käyttää muun muassa todisteena, jos tiedonsiirtosopimus riitautetaan.[91]

[88] Standard Contractual Clauses for international transfers, Direcotrarate-General for Justice and Consumers s. 1

[89] Öman 2019, s. 488–489
[90] Hemmo 2005, s.114
[91] Carey 2018, s.115–116

Vakiolausekkeiden toinen pääasiallinen hyöty verrattuna muihin tiedonsiirtovälineisiin on niiden muokattavuus. Komissio on hyväksynyt tällä hetkellä voimassa olevat vakiolausekkeet, ja ne sisältävät minimivaatimuksia lainmukaisen tiedonsiirtosopimuksen laatimiseen. Vakiolausekkeissa huomautetaan ja kannustetaan osapuolia muokkaamaan niitä.[92] Osapuolilla on täysi vapaus laatia tiukemmat ehdot vakiolausekkeisiin. Vakiolausekkeita voi tässä mielessä käyttää erilaisissa tiedonsiirroissa. Pienemmän riskin tiedonsiirto ei välttämättä tarvitse muokattuja vakiolausekkeita, mutta korkeamman riskin tiedonsiirto saattaa tarvita vakiolausekkeita tiukemmat ehdot tiedonsiirtoja varten.

Vakiolausekkeiden avulla osapuolet määrittelevät käytännössä itse asianmukaisten suojatoimien implementoinnin tiedonsiiroissa. Vakiolausekkeet ovat verrattuna esimerkiksi viranomaisten tai julkisten elinten väliseen oikeudellisesti sitovaan välineeseen itsenäisempiä ja niiden tehokkuus ei ole suoraan esimerkiksi valtioista riippuvaa.

4.3.4 Hyväksytyt käytännesäännöt

4.3.4.1 Siirtovälineen määritelmä

Käytännesäännöt ovat GDPR:n 46 artiklassa kohdassa 2 e) ja 40 artiklassa määritelty asianmukaisten suojatoimien tiedonsiirtoväline, joita organisaatiot voivat käyttää asianmukaisten suojatoimien implementoinniksi kansainvälisissä tiedonsiirroissa kolmansiin maihin. Käytännesääntöjen vaatimukset määritellään GDPR:n 40 artiklassa.

Yhteisö, joka haluaa käyttää käytännesääntöjä tiedonsiirtovälineenä, tulee laatia GDPR:n 40 artiklan mukaiset käytännesäännöt. Tämän jälkeen kansallisen valvontaviranomaisen on hyväksyttävä säännöt. Mikäli valvontaviranomainen ja komissio arvioi käytännesääntöjen vastaavan GDPR:n vaatimuksia, voi organisaatio käyttää niitä tiedonsiirtovälineenä tiedonsiirroissa. GDPR:n 40 artiklan vaatimukset ovat seuraavat GDPR:n 40 artiklan 2 kohdan e alakohdan mukaan:

> ”Yhdistykset ja muut elimet, jotka edustavat rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä, voivat tämän asetuksen säännösten soveltamisen täsmentämiseksi laatia käytännesääntöjä tai muuttaa tai laajentaa niitä muun muassa seuraavien osalta: a) käsittelyn asianmukaisuus ja läpinäkyvyys, b) rekisteripitäjän oikeutetut edut tietyissä yhteyksissä, c) henkilötietojen kerääminen, d) henkilötietojen pseydonymisointi, e) yleisölle ja rekisteröidyille tarkoitettu tiedotus, f) rekisteröidyn oikeuksien käyttäminen, g) lapsille tarkoitettu

[92] Standard contractual clauses 2021, s. 2

tiedotus ja lasten suojelu, h) asetuksen 24 ja 25 artiklassa tarkoitetut toimenpiteet, i) henkilötietojen turvaloukkauksista ilmoittaminen valvontaviranomaiselle ja rekisteröidylle, j) henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille tai K) tuomioistuimen ulkopuoliset ja muut riidanratkaisumenettelyt käsittelyä koskevien kiistojen ratkaisemiseksi”

Käytännesäännöt ovat BCR-sääntöjen kaltaisia siinä mielessä, että niitä voidaan käyttää tehokkaammin jatkuvissa tiedonsiirtotapahtumissa kuin vakiolausekkeita. Kun käytännesäännöt ovat hyväksytty valvontaviranomaisen ja komission puolesta, ovat ne päteviä todistamaan asianmukaisten suojatoimien implementoinnin kansainvälisissä tiedonsiirroissa.[93]

4.3.4.2 Käytännesääntöjen hyödyt ja puutteet

Merkittävin hyöty käytännesäännöissä tiedonsiirtovälineenä ovat 1. tiedonsiirtovälineen käyttö pitkäkestoisissa tiedonsiirtotapauksissa, 2. kolmannen maan osapuolen mahdollisuus käyttää käytännesääntöjä tiedonsiirtovälineenä ja 3. yhdistysten ja muiden elinten mahdollisuus käyttää käytännesääntöjä tiedonsiirtovälineenä.

Verrattuna erityisesti BCR-sääntöihin ovat käytännesäännöt erilaisia siinä mielessä, että organisaatiot, jotka voivat käyttää tiedonsiirtovälinettä ovat erityisesti toimiala- ja etujärjestöt, alakohtaiset organisaatiot, tiede- ja tutkimusalan järjestöt ja eturyhmät.[94] Euroopan tietosuojaneuvoston laatimat ohjeet eivät kuitenkaan poissulje sitä mahdollisuutta, että myös muut yhteisöt voisivat käyttää käytännesääntöjä tiedonsiirtovälineenä. Myös yritykset voivat siis käyttää käytännesääntöjä tiedonsiirtovälineenä. Kyseessä on ensisijaisesti Euroopan tietosuojaneuvoston suositus käytännesääntöjen käyttötarkoitukselle. Päätarkoitus on, että tietyllä alalla toimivat organisaatiot voivat tehostaa tiedonsiirtojen tekemistä tekemällä yhteistyötä vastaamalla tiettyyn alaan tai erityisosaamisalueeseen tarvittavia tietojenkäsittelytarpeita.[95]

Käytännesäännöt eivät ole vielä tässä vaiheessa yleinen tiedonsiirtoväline, mutta ETN:n määritelmän mukaan, käytännesääntöjä käytetään normaalisti varsinkin erilaisten alojen yhdistyksissä ja liitoissa. Myös erilaiset tutkimusryhmät saattavat käyttää käytännesääntöjä toiminnassaan. Yhteisöt pystyvät jakaman tietoa ja dataa liittyen niiden toiminta-alaansa myös kolmansien maiden osapuolille. Varsinkin kansainvälisissä tutkimusryhmissä, joissa tehdään esimerkiksi luonnontieteellistä tai lääketieteellistä tutkimusta, ovat käytännesääntöjen hyödyt

[93] ETN Ohjeet 4/2021 käytännesäännöistä siirtovälineinä, 2022 s. 3
[94] ETN Ohjeet 4/2021 käytännesäännöistä siirtovälineinä. 2022 s. 6
[95] ETN Ohjeet 4/2021 käytännesäännöistä siirtovälineinä. 2022 s. 6–7

selviä, sillä niiden avulla kansainvälinen tutkimusryhmä pystyy helposti ja jatkuvasti jakamaan tutkimusdataa ja henkilötietoa kansainvälisesti. Lisäksi BCR-sääntöihin verrattuna käytännesääntöjen käyttäminen ei edellytä sitä, että niitä käyttävien yhteisöjen tarvitsisi olla osa samaa yhteisöä tai konsernia. Toisin sanoen, yhdistyksiä voi olla monta ja niiden ei tarvitse olla kuten edellä mainitussa jaksossa 4.3.2.2 osana samaa konsernia niin kuin BCR-sääntöjen vaatimuksissa.

Esimerkkinä käytännesääntöjä käyttävälle taholle on EU:ssa toimiva EU Cloud Code of Conduct (CoC) joka on Euroopan tietosuojaneuvoston tukema laillinen käytännesääntömalli.[96] Pilvipalveluja käyttävät organisaatiot, jotka haluavat käyttää näitä käytännesääntöjä tiedonsiirtovälineenä, voivat hakea pätevyyttä EU Cloud CoC:in suorittamalla organisaation hyväksymisprosessin. Hyväksytyt hakijaorganisaatiot saavat EU Cloud CoC:n käytännesäännöt käytettäviksi tiedonsiirtovälineenä kansainvälisissä tiedonsiirroissa. EU Cloud CoC on Euroopan tietosuojaneuvoston ja valvontaviranomaisten hyväksymä tiedonsiirtoväline GDPR:n vaatimusten mukaan.

Käytännesääntöjen käyttö voi olla vaikeaa siinä mielessä, että niiden käyttöönotto ja implementointi on aikaa vievä prosessi. Käytännesäännöt on ensin laadittava ja tämän jälkeen valvontaviranomaisen on tarkistettava ja hyväksyttävä ne. Hyväksytyt käytännesäännöt tulevat olla:

> ”1. Laadittu ja suunniteltu yleisen tietosuoja-asetuksen mukaisiksi käytännesäännöiksi, ja käytännesääntöjä on tarkoitus käyttää kolmansien maiden rekisterinpitäjien tai henkilötietojen käsittelijöiden siirtovälineenä. 2. Käytännesääntöjen on oltava suunniteltuja yleisen tietosuoja-asetuksen mukaisiksi käytännesäännöiksi ja hyväksytty sellaisina.” [97]

Lisäksi myös komission tulee tarkistaa ja hyväksyä käytännesäännöt. Käytännesääntöjen käyttöönotto tiedonsiirtovälineenä voi kestää kauan ja ne soveltuvat ensisijaisesti erityiseen henkilötietojenkäsittelyyn. Käytännesäännöt eivät sovellu yhtä hyvin lyhyemmän aikavälin kestäviin tiedonsiirtoihin, toisin kuin esimerkiksi vakiosopimuslausekkeet.

[96] EU Cloud Code of Conduct verkkosivut
[97] ETN Ohjeet 4/2021 käytännesäännöistä siirtovälineinä 2022 s. 11

4.3.5. Sertifiointimekanismi

4.3.5.1 Tiedonsiirtovälineen määritelmä

Sertifiointimekanismista säännellään GDPR:n 46 artiklan kohdassa 2 f) sekä 42 artiklan kohdassa 2. Kyseessä on GDPR:ssä annettu oikeus sertifioida tiettyä henkilötietojen käsittelyyn liittyvää toimintaa. GDPR:n mukaisen sertifioinnin avulla, voidaan täyttää osoitusvelvollisuus henkilötietojen käsittelyyn liittyvässä toiminnassa ja näin ollen osoittaa GDPR:n sääntelyn noudattamista.[98]

Sertifiointia voidaan myös käyttää tiedonsiirtovälineenä tiedonsiirroissa. GDPR:n 42 artiklan kohdan 2 mukaan:

> ”Tietosuojaa koskevia sertifiointimekanismeja, sinettejä ja merkkejä, jotka on hyväksytty 5 kohdan mukaisesti ja joita sovelletaan tämän asetuksen soveltamisalaan kuuluviin rekisterinpitäjiin tai henkilötietojen käsittelijöihin, voidaan ottaa käyttöön myös tarkoituksena osoittaa, että rekisterinpitäjät tai henkilötietojen käsittelijät, joihin tätä asetusta ei sovelleta 3 artiklan nojalla, soveltavat asianmukaisia suojatoimia siirrettäessä henkilötietoja kolmansiin maihin tai kansainvälisille järjestöille 46 artiklan 2 kohdan f alakohdassa tarkoitettujen ehtojen mukaisesti.”

Sertifiointimekanismi voi siis toimia tiedonsiirtovälineenä, kun sen käyttötarkoituksena on osoittaa, että rekisteripitäjä tai henkilötietojen käsittelijä soveltaa asianmukaisia suojatoimia tiedonsiirroissa. Sertifiointimekanismeja on erilaisia ja eri elimet EU:ssa myöntävät niitä. Kansalliset valvontaviranomaiset sekä ETN voivat myöntää sertifiointimekanismeja. Lisäksi muut erityiset elimet voivat myöntää sertifiointimekanismeja. Näitä elimiä kutsutaan sertifiointielimiksi. Kansallisella valvontaviranomaisella on oikeus nimittää organisaatioita sertifiointielimiksi, mikäli niiden tietosuojaa koskeva asiantuntemus vastaa kansallisen valvontaviranomaisen vaatimuksia. Sertifiointielin, jolla on tietosuojaa koskeva riittävä asiantuntemus, voi myöntää sertifiointeja niitä hakeville yhteisöille.[99]

Koska sertifiointimekanismeja on monenlaisia ja ne voivat liittyä moneen eri alueeseen tietosuojalainsäädännöstä, tulisi tiedonsiirtovälineenä toimivan sertifiointimekanismin varmistaa asianmukaiset suojatoimet kansainvälisissä tiedonsiirroissa. Tarkalleen ottaen

[98] Korpisaari – Pitkänen – Warma-Lehtinen 2022 s. 457–458
[99] Carey 2018, s. 28–29 – Carey kertoo tarkemmin myös, miten sertifiointielin saa valtuudet sertifiointimekanismien myöntämiseen. Sertifiointielimen tulee muun muassa osoittaa itsenäisyyttä ja asiantuntemusta tietosuojalainsäädännön ymmärtämisessä. Sen tulee myös noudattaa ETN ja kansallisen valvontaviranomaisen laatimia kriteereitä.

sertifioinnin tulisi osoittaa, että EU:n ulkopuolella sijaitseva rekisterinpitäjä tai henkilötietojen käsittelijä tai EU:n ulkopuolella sijaitseva tietoja vastaanottava rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa kaikkia asianmukaisia suojatoimia ja toteuttaa tietosuojan tiedonsiirroissa asianmukaisia suojatoimia käyttäen.[100] Sertifiointimekanismi perustuu yleisesti siihen vaadittaviin kriteereihin. Hakuprosessia sertifioinnille kutsutaan akreditoinniksi. Näin ollen rekisteripitäjän tai henkilötietojen käsittelijän on pystyttävä todistamaan omien suojatoimiensa vastaavan vaadittuja sertifiointikriteereitä. Mikäli sertifiointielin, kansallinen valvontaviranomainen tai Euroopan tietosuojaneuvosto arvioi sertifiointia hakevan osapuolen suojatoimien vastaavan sertifiointimekanismin vaatimuksia, voi tämä osapuoli siten käyttää sertifiointimekanismia tiedonsiirtovälineenä GDPR:n 46 artiklan 2 kohdan f mukaan kansainvälisissä tiedonsiirroissa. Sertifiointimekanismi, joka voidaan käyttää tiedonsiirtovälineenä tulisi spesifisti noudattaa tiedonsiirtoja varten laadittua ISO 17065-standardia ja ETN suuntaviivoja 4/2018. Lisäksi sertifiointia hakevan tahon tulisi myös noudattaa yleisiä tietojenkäsittelyperiaatteita.[101]

Muihin tiedonsiirtovälineisiin verrattuna ISO 17065-standardilla on selvät vaatimukset asianmukaiselle tietosuojalle. Sertifiointia hakevan tahon tulisi noudattaa 1. resurssivaatimuksia, 2. prosessivaatimuksia ja 3. muutoksia koskevia vaatimuksia. Resurssivaatimukset edellyttävät, että sertifiointia hakevalla rekisterinpitäjällä tai henkilötietojen käsittelijällä on:

> ”tarvittavat resurssit varmentaa, että tietojen tuoja on sertifiointikriteerien edellyttämällä tavalla arvioinut asianmukaisesti sen kolmannen maan tai niiden kolmansien maiden oikeudellista tilannetta ja käytäntöjä, joihin se on sijoittautunut tai joissa se toimii.”

Prosessivaatimukset edellyttävät, että rekisterinpitäjä tai henkilötietojen käsittelijä on varmistanut siitä että:

> ”sertifiointimenettelyä voidaan tukea mahdollisilla paikan päällä tehtävillä tarkastuksilla, että käsittely tapahtuu kolmannessa maassa tai kolmansissa maissa ja että arviointi kattaa myös kolmansissa maissa voimassa olevan lainsäädännön ja politiikkojen käytännön täytäntöönpanon.”

[100] ETN Ohjeet 7/2022 sertifioinnin käytöstä tiedonsiirtovälineenä 2022, s.9

[101] ETN Ohjeet 7/2022 sertifioinnin käytöstä tiedonsiirtovälineenä 2022, s.10–12

Lopuksi muutoksia koskevat vaatimukset edellyttävät, että rekisterinpitäjä tai henkilötietojen käsittelijä:

> ”seuraa kolmannen maan lainsäädännön ja/tai oikeuskäytännön muutoksia, jotka voivat vaikuttaa arvioinnin kohteen soveltamisalaan kuuluvaan käsittelyyn.”

Tämän perustella voidaan arvioida, että asianmukaiset suojatoimet erityisesti sertifiointimekanismia käytettäessä vaativat, että niitä käyttävä taho on arvioinut kolmannen maan oikeudellista tilannetta ja käytäntöjä, tietojenkäsittely tapahtuu kolmannessa tai kolmansissa maissa, sertifiointimenettelyä voidaan tukea mahdollisilla paikan päällä tehtävillä tarkastuksilla ja että kolmannen maan lainsäädännön ja/tai oikeuskäytännön muutoksia seurataan jatkuvasti.[102]

4.3.5.2 Sertifiointimekanismien hyödyt ja puutteet

Kuten edellä todettiin, tulisi rekisterinpitäjän tai henkilötietojen käsittelijän hakea akreditointia sertifiointielimeltä, kansalliselta valvontaviranomaiselta tai Euroopan tietosuojaneuvostolta. Tiedonsiirtovälineenä sertifiointimekanismi vastaa käytännesääntöjä ja BCR-sääntöjä siinä mielessä, että niiden implementointi voi kestää pidemmän ajan kuin vakiolausekkeiden käyttö tiedonsiirtovälineenä. Akreditointiprosessi sertifiointimekanismia varten edellyttää sertifiointielimen hyväksynnän. Eli tiedonsiirtotoimenpiteitä ei voi aloittaa ennen kuin rekisterinpitäjä tai henkilötietojen käsittelijä on saanut hyväksytyn sertifioinnin kansainvälisille tiedonsiirroille.

Hyöty sertifiointimekanismissa on se, että hyväksytty sertifiointi voi kattaa tiedonsiirtoja pitkällä aikavälillä niin kauan kuin tiedonsiirrot vastaavat sertifiointimekanismin vaatimuksia. Kuten edellä todettiin, esimerkiksi kolmannen maan lainsäädännön muuttuminen siten, että tiedonsiirtoihin liittyvä lainsäädäntö muuttuu EU:n tietosuojan vaatimuksia huonommaksi, johtaisi siihen, että sertifiointimekanismia ei voi enää käyttää tiedonsiirtovälineenä. Tämän myötä tiedonsiirrot on lopetettava. Rekisterinpitäjän tai henkilötietojen käsittelijän on siis jatkuvasti seurattava tiedonsiirtoihin liittyviä olosuhteita, jotta GDPR:n vaatimukset ja spesifisti sertifiointimekanismin vaatimukset täyttyvät.

[102] ETN Ohjeet 7/2022 sertifioinnin käytöstä tiedonsiirtovälineenä 2022, s. 12

4.4 Arviointi tiedonsiirtovälineistä tiedonsiirroissa ja asianmukaisten suojatoimien määritelmä

Käytännössä tiedonsiirtoväline on useimmissa tapauksissa osa tietojenkäsittelyyn liittyvää kokonaisuutta ja sen tarkoitus on osoittaa osapuolten noudattavan samoja tietosuojan vaatimuksia kuin EU edellyttää sen jäsenmailta. GDPR:n 28 artiklan 3 kohdan mukaan:

> ”Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla”

Kuten edellä todettiin niin tietojenkäsittelyä varten ei ole pakollista käyttää tietojenkäsittelysopimusta, mutta se on yleisin tapa määritellä tietojenkäsittely osapuolien välillä. Vaihtoehtoisesti, osapuolet voivat käyttää EU:n tai jäsenvaltion lainsäädännön mukaista oikeudellista asiakirjaa.[103]

Mikäli osapuolet käyttävät tietojenkäsittelysopimusta ja he haluavat siirtää henkilötietoja EU:sta kolmanteen unionin ulkopuoliselle osapuolelle, on tiedonsiirtoväline lisättävä osaksi sopimuskokonaisuutta. Tiedonsiirtoväline on siis useimmiten sopimukseen lisättävä ehto tai liite. Tiedonsiirtoväline, joka on GDPR:n mukaisesti pätevä osoittamaan tiedonsiirron asianmukaiset suojatoimet antavat myös osapuolille pätevän osoitusvelvollisuuden, jos tietojenkäsittely riitautetaan osapuolen tai ulkoisen tahon puolesta. Kuten luvussa 3 todettiin, tulisi tietojenkäsittelysopimus sisältää GDPR:n yleisten tietojenkäsittelyperiaatteiden vaatimukset ja lisäksi tiedonsiirtovälineen osoittaa, millä tavalla tietosuoja toteutetaan tietojenkäsittelyssä asianmukaisia suojatoimia soveltaen. Kyseessä voi olla esimerkiksi osapuolten käyttämä pseudonymisoitu data tai salattu data, jolla tietojenkäsittelyn suoja huomioidaan. Euroopan tietosuojaneuvoston ja tietosuojaviranomaisten käytännön mukaan riittävän tietosuojan huomiointi on kuitenkin aina tapauskohtaista. GDPR:n vaatimukset ja tiedonsiirtoväline on aina huomioitava, mutta riippuen tietojenkäsittelyn luonteesta tulisivat osapuolten olla erittäin tarkkoja siitä, että oikeat toimenpiteet huomioidaan ja otetaan käyttöön tietojenkäsittelyä varten.

Tietosuojavaltuutetun päätöksessä TSV 30.12.2021 1509/452/18 oli kysymys Google Suite for Education -ohjelman käytöstä Suomessa sijaitsevassa koulussa. Tapauksessa osapuoli oli kannellut tietosuojavaltuutetulle siitä, mikäli koulu on ohjelman käytöllä menetellyt tietosuojalainsäädännön mukaisesti. Rekisterinpitäjän selvityksen mukaan Googlen palvelusta oli solmittu GDPR:n 28 artiklan mukaisen tietojenkäsittelysopimuksen.

[103] Korpisaari – Pitkänen – Warma-Lehtinen 2022, s. 345

Tietojenkäsittelysopimuksen tiedonsiirtovälineenä käytettiin komission tietosuojan riittävyyttä koskevalla päätöksellä sekä komission vakiolausekkeilla. Lisäksi palvelun yleisiä sopimusehtoja on päivitetty 24.9.2021 ja nämä päivitykset ovat odottaneet myös tietosuojavaltuutetun hyväksyntää. Tapauksessa kiinnostava oikeudellinen kysymys tietosuojavaltuutetulle oli, mikäli rekisteripitäjä on aisanmukaisesti huolehtinut siitä, että kansainväliset tiedonsiirrot tapahtuvat tietosuojasääntelyn mukaisesti.[104]

Tapauksessa tietosuojavaltuutettu totesi, että rekisterinpitäjän käyttämä henkilötietojen käsittelijä voi käsitellä henkilötietoja Yhdysvalloissa ja että tapauksessa käsittelyyn liittyy tiedonsiirtoja EU:sta Yhdysvaltoihin. Tietosuojavaltuutettu huomautti ensiksi, että tietosuojaa koskeva riittävyyspäätös ei ole ollut pätevä tiedonsiirtoväline, sillä edellinen komission riittävyyspäätös Yhdysvaltojen ja EU:n välillä eli *privacy shield*, oli kumottu C-311/18 *Schrems II*-ratkaisun perusteella. Tapauksessa rekisteripitäjä on myöhemmin käyttänyt komission hyväksymiä vakiolausekkeita. Tietosuojavaltuutettu totesi, että vakiolausekkeiden pätevyys tiedonsiirtovälineenä vaatii tapauskohtaista arviointia.

Kuten edellä todettiin, tiedonsiirtovälineen ja sen antaman asianmukaisen suojatoimen arviointi tapauksissa on tapauskohtaista. Tietosuojavaltuutetun päätöksessä 30.12.2021 olisi ollut kiinnostavaa nähdä miten tietosuojavaltuutettu olisi arvioinut tietojenkäsittelysopimuksen tiedonsiirtovälineen yksityiskohtia asianmukaisen tietosuojan takaamista varten. Tietosuojavaltuutettu kuitenkin jätti kysymyksen arvioimatta, sillä rekisterinpitäjä oli käyttänyt komission riittävyyspäätöstä tiedonsiirtovälineenä. Tiedonsiirtovälineen tehokkuuden arviointi on kuitenkin tapauksen perusteella aina tapauskohtaista. Tämä tarkoittaa sitä, että rekisterinpitäjän, joka lopullisesti vastaa tietojenkäsittelystä, on arvioitava tarkasti tiedonsiirtovälineessä mainittuja ehtoja ja itse tiedonsiirrossa käytettäviä toimenpiteitä, jotta tietojenkäsittely pysyisi laillisena. Riskiarvioinnin näkökulmasta, tämä tarkoittaisi, että tietojenkäsittelyn osapuolien on suositeltavaa välttää tarpeettomia riskejä ja oletetusti käyttää toimenpiteitä, jotka ovat parhaimpia tietosuojan takaamiselle.

Edellä käsiteltiin jo tietosuojavaltuutetun tapausta TSV 31.5.2023 7684/171/22 jossa oli kysymys verkkosivustolla käytettävistä seurantateknologioista ja siihen liittyvästä henkilötietojen käsittelystä. Tapauksessa ilmoituksen mukaan rekisteripitäjä oli käyttänyt Googlen verkkopalveluja tietojenkäsittelyyn. Verkkosivustolla käytettävät palvelut olivat Google Analytics- ja reCAPTCHA-palvelu.[105]

[104] Tietosuojavaltuutetun päätös 30.12.2021 1509/452/18
[105] Tietosuojavaltuutetun päätös 31.5.2023 7684/171/22

Apulaistietosuojavaltuutettu totesi, että GDPR:n 44 artiklan mukaan henkilötietoja, joita käsitellään tai joita on tarkoitus käsitellä kolmannessa maassa, saa käsitellä vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa GDPR:n 5 luvun sääntöjä liittyen suoraan tiedonsiirtovälineisiin. Rekisteripitäjä oli käsitellyt henkilötietoja tietosuojaa koskevalla riittävyyspäätöstä (*privacy shield*). Kuten edellä olevassa päätöksessä todettiin, niin *privacy shield* ei enää ollut pätevä tiedonsiirtoväline, sillä se oli kumottu C-311/18 *Schrems II*-ratkaisun perusteella. Rekisteripitäjä ei ollut myöskään käyttänyt GDPR:n artiklassa 46 mainittua toista tiedonsiirtovälinettä. Näin ollen rekisteripitäjä oli laiminlyönyt velvollisuutensa huolehtia asianmukaisista suojatoimista tiedonsiirroista kolmansiin maihin. Apulaistietosuojavaltuutettu huomautti lisäksi evästebannereista, että vaikka rekisterinpitäjällä olisi mahdollisuus kieltää evästeiden käytön evästebannerissa, niin tämä ei ole riittävä suojatoimenpide sillä rekisteröidyn henkilötietoja voi silloin kuitenkin siirtyä lainvastaisesti kolmanteen maahan. Rekisteripitäjän olisi pitänyt käyttää tiedonsiirtovälinettä GDPR:n 46 artiklan mukaisesti osoittaakseen tietojenkäsittelyssä asianmukaisten suojatoimien huomioinnin. Päätöksen perusteella voimme todeta, että rekisteripitäjä ei noudata GDPR:n 5 luvun vaatimuksia ryhtymällä ainoastaan toimenpiteisiin, joiden avulla se olettaa, että tiettyä palvelua käytettäessä tietojenkäsittelyä ei tehdä. Rekisteripitäjän on siis pakko käyttää tiedonsiirtovälinettä, kun tietojenkäsittelyä tehdään unionin ja kolmannen maan osapuolien välillä, jotta asianmukaiset suojatoimenpiteet tietojenkäsittelyssä täyttyvät.

Tietosuojaneuvoston kiistanratkaisupäätöksessä 13.4.2023 1/2023 oli kysymys Meta Platforms Ireland Ltd:n (alla Meta) Facebook palvelussa tehtävästä tietojenkäsittelystä heinäkuusta 2020 lähtien. Päätöksen tapauskuvauksen mukaan Meta oli jatkanut tiedonsiirtojen tekemistä, vaikka se oli C-311/18 *Schrems II*-ratkaisun perusteella määrätty lopettamaan tiedonsiirrot Yhdysvaltoihin. Meta oli *Schrems II*-ratkaisun jälkeen tehnyt tiedonsiirtoja käyttäen tiedonsiirtovälineenä vakiolausekkeita.[106]

Meta oli käyttänyt vakiolausekkeita tiedonsiirtovälineenä. Tietosuojaneuvosto kuitenkin katsoi, että:

> ”tiedonsiirrot vakiolausekkeiden perusteella ovat olleet tietosuoja-asetuksen vastaisia, sillä Yhdysvaltojen lainsäädännössä ei taata EU:n vaatimuksia vastaavaa tietosuojan tasoa. Myöskään vakiolausekkeita täydentävillä suojatoimilla ei ole ollut mahdollista puuttua riskeihin, joita yksilöiden oikeuksiin ja vapauksiin kohdistuu Yhdysvaltojen lainsäädännön vuoksi.”

[106] ETN 13.4.2023 1/2023

Pääongelma Yhdysvaltojen lainsäädännössä, on valtion mahdollisuus valvoa rekisteröityjen henkilötietoja valtiovälisen ja Yhdysvaltojen sisäisen vakoilun kautta.

Päätös on kiinnostava, koska se kuvastaa pääasiallista ongelmaa tiedonsiirtovälineiden käyttämisessä kansainvälisissä tiedonsiirroissa. Kuten edellä luvussa 3 ja 4 on todettu, rekisteripitäjän tulee käyttää kansainvälisissä tiedonsiirroissa GDPR:n 46 artiklan mukaista tiedonsiirtovälinettä. Tiedonsiirtovälineen huomiointi tietojenkäsittelyssä ja tiedonsiirroissa ei kuitenkaan välttämättä riitä sellaisenaan. Kuten edellä olevissa päätöksissä on todettu, arviointi suojatoimien toteutumisesta on aina tapauskohtaista. Pääasia tietosuojaneuvoston päätöksessä on kuitenkin se, että tiedonsiirtoväline ja tietojenkäsittely EU:n osapuolen ja kolmannen maan osapuolen välillä on laitonta, mikäli tietojenkäsittely ei täytä EU:n vaatimuksia vastaavaa tietosuojan tasoa. Näin ollen kaikki tietojenkäsittely, jossa osapuolena on EU:n ja kolmannen maan taho, tulisi lopettaa, jos tietojenkäsittely ei vastaa EU:n vaatimuksia vastaavaa tietosuojaa. Tiedonsiirtovälineet ovat tällöin tehottomia riippumatta niiden laillisesta ja oikeaoppisesta käytöstä, mikäli kolmannen maan valtio ei täytä EU:n vaatimuksia vastaavaa tietosuojan tasoa. Tiedonsiirrot ovat kuitenkin tiedonsiirtovälineiden avulla mahdollisia tehdä kolmansiin maihin, kuten Yhdysvaltoihin. Kuitenkin, kuten esimerkiksi yllä mainitussa TSV:n päätöksessä 31.5.2023 7684/171/22 on todettu, tiedonsiirtovälineen implementoinnin aikana tulisi rekisterinpitäjän tai henkilötietojen käsittelijän huomioida ylimääräiset vaihtoehdot puuttua tiedonsiirtoihin liittyviin riskeihin. Nämä toimenpiteet riippuvat tapauskohtaisesti tietojenkäsittelystä. Teknisesti tämä tarkoittaisi tapauksen tulkinnan mukaan, että mikäli esimerkiksi lainsäädännölliset riskit kolmannessa maassa voidaan jollakin tavalla eliminoida, asianmukaiset suojatoimet tiedonsiirroissa täyttyvät. Tutkija arvioi kuitenkin tämän olevan käytännössä erittäin vaativaa, ja riittävää oikeuskäytäntöä tällaisista toimenpiteistä ei ole. Ottaen huomioon myös esimerkiksi *Schrems*-ratkaisut, EU-tuomioistuin on todennut EU:n tietosuojan tason noudattamisen olevan kantava periaate kansainvälisissä tietojenkäsittelytapauksissa. Jos kansainvälisiä tiedonsiirtoja tehdään kolmanteen maahan eikä tietojenkäsittelyssä voida taata samaa unionissa taattua vastaavaa suojaa, on tietojenkäsittely laitonta riippumatta siitä, mikäli tiedonsiirroissa käytetään riittävyyspäätöstä tai tiedonsiirtovälinettä tietosuojan takaamiseksi.

Edellä käsiteltyjen tapausten perusteella voimme siis todeta, että tiedonsiirtoväline ei sellaisenaan aina riitä asianmukaisten suojatoimien todistamiseen kansainvälisessä tietojenkäsittelyssä. Kyseessä on oltava kokonaisuusarviointi ottaen huomioon tietojenkäsittelyn yleiset periaatteet, käytettävässä olevat tiedonsiirtovälineet ja valtioihin liittyvät lainsäädännölliset erot tai muut asianmukaisiin suojatoimiin vaikuttavat olosuhteet.

Mikäli arvioisimme tiedonsiirtovälineitä yleisesti tämän tutkielman pohjalta, niin tutkija on päättänyt jakaa tiedonsiirtovälineet kahteen eri ryhmään. Nämä ovat pitkäaikaiset tiedonsiirtovälineet ja lyhytaikaiset tiedonsiirtovälineet.

Pitkäaikaiset tiedonsiirtovälineet ovat viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline, yritystä koskevat sisäiset säännöt eli BCR-säännöt, käytännesäännöt, sertifiointimekanismit ja komission myöntämät tietosuojaa koskevat riittävyyspäätökset. Lyhytaikaiset tiedonsiirtovälineet ovat komission hyväksymät tietosuojaa koskevat vakiolausekkeet. Ero näiden välillä on se, että pitkäaikaiset tiedonsiirtovälineet vaativat yleisesti enemmän aikaa niiden implementoinnille sekä kattavampia toimenpiteitä asianmukaisten suojatoimien varmistamiseksi. Lyhytaikaiset tiedonsiirtovälineet ovat helpompia implementoida, mutta niitä on vaikeampaa käyttää pidemmän ajan kestävissä tiedonsiirtotapahtumissa.

5. Lopetus ja tutkielman johtopäätökset

Tutkielman viimeisessä luvussa käsitellään tutkielman tuloksia, johtopäätöksiä ja loppuajatuksia.

5.1 Tutkielman johtopäätökset

Tässä tutkielmassa on ollut yhteensä kolme varsinaista tutkimuskysymystä. Ne ovat 1. mitkä ovat yleiset vaatimukset tiedonsiiroille, 2. mitkä ovat vaatimukset kansainvälisille tiedonsiirroille ja 3. mitkä ovat eri tiedonsiirtovälineiden eroavaisuudet. Tässä luvussa tutkielman kirjoittaja arvioi omien tutkimuskysymyksiensä johtopäätöksiä.

Ensinäkin voimme todeta, että yleiset vaatimukset tiedonsiirroille ovat GDPR:n mukaan 2 luvun 5 artiklan yleiset tietojenkäsittelyperiaatteet. Tietojen siirtäminen on määritelmänä sama kuin tietojenkäsittely. Näin ollen tietojenkäsittelyssä, kuten myös tietojen siirtämisessä EU:sta kolmanteen maahan, tulisi aina noudattaa GDPR:n 2 luvun 5 artiklan yleisiä tietojenkäsittelyperiaatteita. Yleiset tietojenkäsittelyperiaatteet ovat GDPR:n 5 artiklan mukaan lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus ja osoitusvelvollisuus. Rekisterinpitäjän tai henkilötietojen käsittelijän on huomioitava yleiset tietojenkäsittelyperiaatteet, kun henkilötietoja käsitellään. Tämä pätee luonnollisesti myös kansainvälisiin tiedonsiirtoihin. Tutkielmassa on esitetty tiettyjä viranomaisten ja tuomioistuinten ratkaisuja, joissa erityisesti yleiset tietojenkäsittelyperiaatteet ovat olleet tiedonsiiroissa arvioinnissa. Arvioidun oikeuskäytännön mukaan yleisten tietojenkäsittelyperiaatteiden noudattaminen on aina pystyttävä osoittamaan, jotta tiedonsiirrot olisivat lainmukaisia. Varsinkin lainmukaisuuden ja tietojen minimoinnin periaatteiden toteutumista tietojenkäsittelyssä on vaikeaa arvioida.

Toiseksi voimme todeta, että kansainvälisillä tiedonsiirroilla on ankarammat vaatimukset kuin tietojenkäsittelyillä EU:n sisällä. Tiedonsiirtoja varten on noudatettava GDPR:n yleisiä tietojenkäsittelyperiaatteita. Kun kansainvälisiissä tiedonsiirroissa on mukana osapuoli, joka sijaitsee EU:n ulkopuolella, on tiedonsiirroissa noudatettava samoja GDPR:n vaatimuksia kuin EU:n sisäisessä tietojenkäsittelyssä ja lisäksi tulee tietojenkäsittelyissä noudattaa GDPR:n 5 luvun vaatimuksia. Näistä tärkeimmät ovat GDPR:n artiklat 44, 45 ja 46. GDPR:n artikla 44 välittää yleiset periaatteet kansainvälisille tiedonsiiroille. Artikla 45 määrittelee komission riittävyyspäätöksen käyttöä tiedonsiirtovälineenä ja artikla 46 määrittelee muut tiedonsiirtovälineet kansainvälisissä tiedonsiirroissa. GDPR:n artikla 44 mukaan rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä osoittamaan asianmukaiset

suojatoimet tiedonsiirroille, mikäli tiedonsiirtoja tehdään EU:ssa sijaitsevan tahon/tahojen ja kolmannessa maassa sijaitsevan tahon/tahojen välillä. Nämä tiedonsiirtovälineet ovat viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline, yritystä koskevat sisäiset säännöt eli BCR-säännöt, käytännesäännöt, sertifiointimekanismit, komission hyväksymät tietosuojaa koskevat vakiolausekkeet ja komission myöntämät tietosuojaa koskevat riittävyyspäätökset.

Kolmanneksi voimme todeta, että tiedonsiirtovälineissä on erovaisuuksia niiden implementointiprosesseissa ja niiden käyttötarkoituksissa. Suurimmat erovaisuudet liittyvät muun muassa siihen, miten ja minkä tahojen avulla tiettyjä tiedonsiirtovälineitä voi käyttää. Kaikki tiedonsiirtovälineet, paitsi vakiolausekkeet, tarvitsevat jonkin tietosuojaviranomaisen hyväksyntää, jotta niitä voisi käyttää tiedonsiirtovälineinä. Vakiolausekkeet tarvitsevat ainoastaan niitä käyttävien osapuolien hyväksynnän. Tutkielmassa tiedonsiirtovälineitä on vertailtu niiden antaman suojan ja implementoinnin vaativuuden perusteella. Lisäksi tutkielmassa on jaettu tiedonsiirtovälineet kahteen ryhmään perustuen siihen, kuinka tehokkaasti niitä pystyy käyttämään pitkäaikaisesti tai lyhytaikaisesti.

Merkittävin tutkielman löydös on tutkijan mielestä se, että voimme todeta asianmukaisten suojatoimien olevan yhdistelmä toimenpiteistä, joilla tietojenkäsittelyssä saavutetaan EU:n tietosuojan taso. Tietojenkäsittely saavuttaa EU:n tietosuojan tason, kun tiedonsiirroissa noudatetaan yleisiä tietojenkäsittelyperiaatteita ja tiedonsiirrossa käytetään jotain GDPR:n mukaista tiedonsiirtovälinettä. Tähän johtopäätökseen tutkija on tullut arvioimalla GDPR:n vaatimuksia tiedonsiirroille, oikeuskäytännön yleisiä vaatimuksia tiedonsiirroille sekä analysoimalla kirjallisuudessa esitettyjä tulkintoja.

Asianmukaiselle suojatoimelle ei ole olemassa tarkkaa määritelmää. Tutkijan tulkinnan mukaan asianmukaisilla suojatoimilla tarkoitetaan niitä tarvittavia toimenpiteitä, jotka rekisterinpitäjän tai henkilötietojen käsittelijän on suoritettava, jotta kansainvälinen tiedonsiirto olisi lainmukainen. Näihin kuuluu yleisten GDPR:n tietojenkäsittelyperiaatteiden noudattaminen, kuten esimerkiksi suostumuksen saaminen rekisteröidyltä henkilötietojen käsittelylle. Lisäksi lainmukaisuusvaatimukseen kuuluu tiedonsiirtovälineen käyttö kansainvälisessä tiedonsiirrossa todisteena siitä, että henkilötietojen käsittelyssä varmistetaan ja taataan samat tietosuojan vaatimukset, kuin EU:ssa. Lisäksi nämä toimenpiteet täyttävät rekisterinpitäjän tai henkilötietojen käsittelijän osoitusvelvollisuuden. Toisin sanoen voimme tutkielman lopputuloksilla todeta, että kansainväliseen tiedonsiirtoon tarvitaan pääasiallisesti kaksi toimenpidettä, eli yleisten GDPR:n 5 artiklan yleisten henkilötietojen käsittelyperiaatteiden noudattamista ja GDPR:n 46 artiklan tiedonsiirtovälineitä.

Tutkielman johtopäätökset ovat kuitenkin ainoastaan pintaraapaisua aiheesta. Esimerkiksi eri valtioiden erityislainsäädäntö saattaa vaikeuttaa asianmukaisten suojatoimien implementointia. Tiedonsiirtoihin saattaa myös liittyä muita huomioon otettavia asioita, kuten esimerkiksi erityisten henkilötietojen siirrot. Esimerkiksi GDPR:n 9 artiklaa koskevat erityisiä henkilötietoryhmiä koskeva sääntely vaikeuttaa tiedonsiirtoja entisestään. Myös erityistilanteet, kuten GDPR:n 49 artiklan poikkeukset, mahdollistavat tiedonsiirtoja myös poikkeustapauksissa. Varsinkin näitä aiheita tulisi tutkia enemmän. Tutkielman johtopäätösten perusteella voimme kuitenkin todeta, että asianmukaiset suojatoimet täyttyvät, mikäli yleisiä tietojenkäsittelyperiaatteita noudatetaan ja tiedonsiirtovälineitä käytetään tietojenkäsittelyssä.

Kyseessä on kuitenkin lopuksi aina tapauskohtainen arviointi toimenpiteistä. Olosuhteet, kuten kolmannen maan lainsäädäntö tai lainsäädännön muutokset sekä muut muutokset, voivat olennaisesti vaikuttaa tietojenkäsittelyn asianmukaisiin suojatoimiin. Näissä tapauksissa ei edes oikean tiedonsiirtovälineen ja tietojenkäsittelyn yleisten periaatteiden noudattaminen välttämättä riitä tiedonsiirtojen tekemiseen lainmukaisesti. Lisäksi tapauksissa, joissa todetaan äkillisesti puutteita tiedonsiirroissa, kansallinen valvontaviranomainen tai Euroopan tietosuojaneuvosto saattaa kieltää tiedonsiirrot välittömästi. Nämä tilanteet ovat niin rekisterinpitäjän kuin henkilötietojen käsittelijän ja muiden osapuolien kannalta erittäin vaikeita ratkaista. Äärimmäisimmät toimenpiteet saattavat johtaa siihen, että yhteisön henkilötietojen tietojenkäsittely on välittömästi lopetettava tai arvioitava uudelleen. Tämä on haastavaa ja vaikeaa yhteisön kannalta, mutta rekisteröidyn oikeussuojan kannalta hyvä. Tutkija haluaa näin ollen myös nostaa esiin realistisen kysymyksen siitä, kuinka hyvin ja tehokkaasti yleisesti yhteisöissä, organisaatioissa ja yrityksissä loppujen lopuksi pystytään noudattamaan GDPR:n henkilötietojenkäsittelyvaatimuksia. Joidenkin tutkimusten mukaan GDPR:n vaatimuksia on haastavaa implementoida ETN:n tietosuojalainsäädännön yhdenmukaistamispyrkimyksistä huolimatta.[107] Lisäksi tutkielmassa on noussut esille myös oikeuskäytäntöä, missä lisätoimenpiteitä, kuten tietosuojaa koskevaa vaikutustenarvioinnin implementointi on ollut suositeltavaa, mutta ei välttämätöntä.

5.2 Tiedonsiirrot tulevaisuudessa

Tulevaisuuden kannalta on kiinnostavaa nähdä, miten eri tiedonsiirtovälineitä käytetään kansainvälisissä tiedonsiirroissa. GDPR astui voimaan vuonna 2018, joten kaikkia tiedonsiirtovälineiden käyttömahdollisuuksia ei ole vielä kokeiltu.

[107] Reka 2019

EU:n komissio hyväksyi hiljattain uuden riittävyyssopimuksen EU:n ja Yhdysvaltojen välillä. Näin ollen tiedonsiirtoja tehdään Yhdysvaltoihin luultavasti entistä enemmän riittävyyspäätöksen perusteella. *Schrems*-ratkaisujen perusteella EU-Yhdysvallat riittävyyspäätökset eivät ole kuitenkaan historiallisesti pysyneet voimassa, joten tiedonsiirtovälineiden merkitys tulee pysymään myös tulevaisuudessa merkittävänä. Riittävyyspäätöksen alaisia maita ovat tällä hetkellä Andorra, Argentiina, Kanada, Färsaaret, Guernsey, Israel, Mansaaret, Japani, Jersey, Uusi Seelanti, Etelä-Korea, Sveitsi, Yhdistyneet kuningaskunnat, Norja, Liechtenstein, Islanti ja Yhdysvallat. Tiedonsiirroissa, joita tehdään EU:n ulkopuolelle kuin riittävyyspäätöksen omaaviin valtioihin tulee käyttää tiedonsiirtovälineitä.

Kiinnostava huomio on se, että EU vaatii samaa tietosuojan tasoa kolmansilta mailta. Riittävyyspäätöksen tulisi käytännössä taata se, että tietosuojan taso kolmannessa maassa on samalla tasolla kuin EU:ssa. Kuitenkin *Schrems*-ratkaisujen perusteella riittävyyspäätöksiä on todettu laittomiksi oikeuskäytännössä, koska kohdemaassa ei ole ollut samaa tietosuojan tasoa kuin EU:ssa. Uuden Yhdysvaltojen riittävyyspäätöksen kautta komissio ottaa käytännössä sen kannan, että Yhdysvalloissa on sama tietosuojan taso kuin EU:ssa. ETN on kuitenkin todennut, että uudesta riittävyyspäätöksestä huolimatta Yhdysvaltojen tiedusteluviranomaiset pystyvät tarkastamaan EU:sta siirrettäviä henkilötietoja, mikä on EU:n tietosuojan tason vastaista.[108] Tämä tekee kansainvälisiä tiedonsiirtoja koskevan tietosuojalainsäädännön tulkinnasta tutkijan mielestä ristiriitaista. Jää nähtäväksi, pysyykö nykyinen riittävyyspäätös voimassa sellaisenaan vai haastetaanko sen lainmukaisuus jälleen. Tutkijan mielestä on yhdenmukaisen tulkinnan kannalta ongelmallista, mikäli riittävyyspäätös pysyy voimassa. Lisäksi tilanne on haastava varsinkin kansainvälistä liiketoimintaa harjoittaville yrityksille, koska riittävyyspäätösten lainmukaisuuteen ja voimassaoloon ei voi aiemman oikeuskäytännön perusteella luottaa. Tiedonsiirtovälineet ovat tästä näkökulmasta varmempia lainsäädännöllisiä työkaluja asianmukaisten suojatoimien osoittamiselle, koska niissä säilyy suurimmilta osin osapuolten sopimusoikeudellinen vapaavalinnaisuus ja itsenäisyys. Tiedonsiirtovälineet ovat myös tietosuojan riskienarviointiperiaatteen mukaisesti parempi vaihtoehto, koska henkilötietoja käsittelevät osapuolet ovat itse vastuussa omasta tietosuojan tasostaan.

Lisäksi voimme todeta apulaistietosuojavaltuutetun päätöksistä, että täydellistä konsensusta tietosuojan vaikutuksenarvioinnin ja tiedonsiirtojen vaikutuksenarvioinnin implementoinnista ei ole. Pääsääntö on kuitenkin se, että mikäli rekisterinpitäjä tai henkilötietojen käsittelijä arvioi,

[108] Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework 2023, s.22-26

että esimerkiksi uusien teknologisten menetelmien käyttö tiedonsiirroissa saattaisi aiheuttaa erityisiä riskejä tiedonsiirtojen tekemisessä, niin yhteisö minimoi toimintaansa liittyvät riskit tekemällä tietosuojan vaikutuksenarvioinnin. Vaikka apualaistietovaltuutettu on päätöksessään 31.5.2023 7684/171/22 todennut, että vaikutuksenarvioinnin laatiminen ennen tiedonsiirtoja ei ole tarpeellista ja että vaikutuksenarvioinnin tekeminen suomalaisille organisaatioille olisi epäreilua muihin valtioihin verrattuna, kun tiedonsiirroissa käytetään vakiintuneita tiedonsiirtovälineitä kuten esimerkiksi SCC-vakiolausekkeita niin tiedonsiirtoja tekevällä osapuolella on kuitenkin GDPR:n velvoittama osoitusvelvollisuus. Kuten tutkielmassa on todettu, niin osoitusvelvollisuus velvoittaa rekisterinpitäjää tai henkilötietojen käsittelijää todistamaan, että se on implementoinut oikeat toimenpiteet tiedonsiirtoja varten. Rekisterinpitäjä tai henkilötietojen käsittelijä välttää ylimääräisiä riskejä tiedonsiirroissa, kun se laatii tietosuojan ja tiedonsiirtojen vaikutuksenarvioinnin. Mitään selvää konsensusta ei kuitenkaan tutkijan mielestä ole ja tämä on yleisesti tietosuojalainsäädännön noudattamisen kannalta ongelmallista.

Lopuksi todetaan, että tiedonsiirtovälineet ovat kansainvälisissä tiedonsiirroissa merkittävässä asemassa, koska niiden avulla osapuolet kansainvälisissä tiedonsiirroissa pystyvät osoittamaan GDPR:n osoitusvelvollisuuden mukaisen asianmukaisen tietosuojan noudattamisen tietojenkäsittelyissä. Tutkielman tulosten perusteella voidaan päätellä, että tiedonsiirtovälineiden rooli säilyy merkittävänä niin kauan kuin EU vaatii kolmansiin maihin tehtävissä tiedonsiirroissa samaa tietosuojan tasoa kuin EU:ssa.