Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi

Versio 2.0

Annettu [18. kesäkuuta] 2021

Aiemmat versiot

Versio 2.0	[18. kesäkuuta] 2021	Suositusten hyväksyminen julkisen kuulemisen jälkeen
Versio 1.0	10. marraskuuta 2020	Suositusten hyväksyminen julkista kuulemista varten

Tiivistelmä

EU:n yleisellä tietosuoja-asetuksella on kaksiosainen tavoite: sillä helpotetaan henkilötietojen vapaata liikkumista Euroopan unionissa ja suojellaan ihmisten perusoikeuksia ja -vapauksia, erityisesti heidän oikeuttaan henkilötietojen suojaan.

Asiassa C-311/18 (Schrems II) äskettäin antamassaan tuomiossa Euroopan unionin tuomioistuin (EUT) muistuttaa, että Euroopan talousalueella (ETA) henkilötiedoille myönnetyn suojan on siirryttävä kyseisten tietojen mukana kaikkialle. Henkilötietojen siirtämisellä kolmansiin maihin ei saa heikentää tai vesittää niille Euroopan talousalueella myönnettyä suojaa. Tuomioistuin vahvistaa tämän myös selventämällä, että kolmansissa maissa tarjottavan suojan tason ei tarvitse olla täysin sama kuin Euroopan talousalueella taattu suojan taso vaan pääosiltaan vastaava. Tuomioistuin puolustaa myös vakiosopimuslausekkeiden pätevyyttä tiedonsiirtovälineenä, jota voidaan käyttää varmistamaan sopimuksen nojalla, että kolmansiin maihin siirrettävien tietojen suojan taso vastaa pääosiltaan EU:ssa taattua suojan tasoa.

Vakiosopimuslausekkeita ja muita yleisen tietosuoja-asetuksen 46 artiklassa tarkoitettuja tiedonsiirtovälineitä ei käytetä tyhjiössä. Tuomioistuin toteaa, että tietojen viejinä toimivien rekisterinpitäjien tai henkilötietojen käsittelijöiden on tapauskohtaisesti ja tarvittaessa yhteistyössä kolmannessa maassa olevan tuojan kanssa tarkistettava, heikentääkö kolmannen maan laki tai käytäntö yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden sisältämiä asianmukaisia suojatoimia. Tällaisissa tapauksissa tuomioistuin antaa tietojen viejille vielä mahdollisuuden toteuttaa näitä suojan puutteita korjaavia lisätoimenpiteitä ja saattaa suoja EU:n lainsäädännössä edellytetylle tasolle. Tuomioistuin ei täsmennä, mitä nämä toimenpiteet voisivat olla. Tuomioistuin kuitenkin korostaa, että tietojen viejien on yksilöitävä ne tapauskohtaisesti. Tämä on yleisen tietosuoja-asetuksen 5 artiklan 2 kohdan osoitusvelvollisuuden periaatteen mukaista. Siinä edellytetään, että rekisterinpitäjä vastaa yleisen tietosuoja-asetuksen henkilötietojen käsittelyyn liittyvien periaatteiden noudattamisesta, ja sen on pystyttävä osoittamaan niiden noudattaminen.

Euroopan tietosuojaneuvosto on antanut suositukset, jotta tietojen viejiä (rekisterinpitäjiä tai henkilötietojen käsittelijöitä, yksityisiä yhteisöjä tai julkisia elimiä, jotka käsittelevät yleisen tietosuoja-asetuksen soveltamisalaan kuuluvia henkilötietoja) voidaan auttaa monimutkaisessa tehtävässä, jossa on arvioitava kolmansia maita ja tarvittaessa yksilöitävä asianmukaiset lisätoimenpiteet. Näissä suosituksissa esitetään tietojen viejille vaiheet, joita on noudatettava, mahdollisia tietolähteitä ja joitakin esimerkkejä lisätoimenpiteistä, joita on mahdollista ottaa käyttöön.

Ensimmäiseksi Euroopan tietosuojaneuvosto neuvoo tietojen viejiä **tuntemaan tiedonsiirtonsa**. Kaikkien kolmansiin maihin tehtyjen henkilötietojen siirtojen kartoittaminen voi olla työlästä. Henkilötietojen määränpää on kuitenkin tunnettava, jotta voidaan varmistaa, että niille tarjotaan unionissa taattua suojan tasoa pääosiltaan vastaava suojan taso aina, kun niitä käsitellään. Lisäksi on tarkistettava, että siirrettävät tiedot ovat asianmukaisia, olennaisia ja rajoittuvat siihen, mikä on tarpeen niiden käsittelyn kannalta.

Toiseksi on **tarkistettava, että tiedonsiirrossa käytettävä siirtoväline** luetellaan yleisen tietosuoja-asetuksen V luvussa. Jos Euroopan komissio on jo todennut, että maa, alue tai sektori, johon tietoja siirretään, tarjoaa riittävän tietosuojan tason jonkin sellaisen tietosuojan riittävyyttä koskevan päätöksensä perusteella, joka on tehty yleisen tietosuoja-asetuksen 45 artiklan mukaisesti tai sitä edeltäneen direktiivin 95/46/EY mukaisesti, mikäli päätös on edelleen voimassa, muita toimenpiteitä ei tarvita. Silloin on vain seurattava, että riittävyyttä koskeva päätös pysyy voimassa. Jos riittävyyttä koskevaa päätöstä ei ole, on käytettävä jotakin yleisen tietosuoja-asetuksen 46 artiklassa luetelluista tiedonsiirtovälineistä. Vain joissakin tapauksissa voi ehtojen täyttyessä turvautua johonkin yleisen tietosuoja-asetuksen 49 artiklassa säädettyyn poikkeukseen. Poikkeuksia ei voida alkaa käyttää säännönmukaisesti, vaan niiden käyttö on rajattava vain tiettyihin tilanteisiin.

Kolmanneksi on **arvioitava**, onko kolmannen maan voimassa olevissa laeissa ja/tai käytännöissä jotakin, mikä voi heikentää käytettävien tiedonsiirtovälineiden asianmukaisten suojatoimien tehokkuutta tietyn siirron yhteydessä. Arvioinnissa on keskityttävä ensisijaisesti kolmannen maan lainsäädäntöön, joka on merkityksellistä siirron ja yleisen tietosuoja-asetuksen 46 artiklassa tarkoitetun käytettävän tiedonsiirtovälineen kannalta. Myös kolmannen maan viranomaisten käytäntöjen tutkiminen auttaa varmentamaan, voidaanko siirtovälineen sisältämillä suojatoimilla käytännössä varmistaa siirrettävien henkilötietojen tehokas suojaaminen. Näiden käytäntöjen tutkiminen on tärkeää arvioinnissa etenkin, kun

(i.) kolmannen maan lainsäädäntöä, joka täyttää virallisesti EU:n vaatimukset, ei selvästi sovelleta/noudateta käytännössä

(ii.) käytännöt ovat siirtovälineeseen liittyvien sitoumusten vastaisia, jos kolmannen maan asianmukaista lainsäädäntöä ei ole

(iii.) siirrettävät tiedot ja/tai tuoja kuuluvat tai saattavat kuulua ongelmallisen lainsäädännön piiriin (kun se esimerkiksi heikentää siirtovälineen sopimukseen perustuvaa taetta pääosiltaan vastaavasta suojan tasosta eikä täytä EU:n vaatimuksia perusoikeuksien, välttämättömyyden ja oikeasuhteisuuden osalta).

Kahdessa ensimmäisessä tilanteessa siirto on keskeytettävä. Jos sitä halutaan jatkaa, on toteutettava asianmukaisia lisätoimenpiteitä.

Kolmannessa tilanteessa siihen, miten ongelmallista lainsäädäntöä mahdollisesti sovelletaan siirtoon, liittyy epäselvyyksiä, joten toimintavaihtoehdot ovat siirron keskeyttäminen tai lisätoimenpiteiden toteuttaminen siirron jatkamiseksi. Siirtoa voidaan myös jatkaa toteuttamatta lisätoimenpiteitä, jos voidaan katsoa, ettei ole syytä uskoa, että asianmukaista ja ongelmallista lainsäädäntöä tulkitaan ja/tai sovelletaan käytännössä siirrettäviin tietoihin ja tuojaan, kunhan tämä voidaan osoittaa ja dokumentoida.

Euroopan tietosuojaneuvoston eurooppalaisia olennaisia takeita koskevista suosituksista saa lisätietoja niiden tekijöiden arviointiin, jotka on otettava huomioon arvioitaessa kolmannen maan lainsäädäntöä, joka koskee viranomaisten pääsyä tietoihin tiedustelua varten.

Myös tämä arviointi on tehtävä asianmukaisen huolellisesti ja dokumentoitava. Toimivaltaiset valvonta- ja/tai oikeusviranomaiset voivat vaatia sitä ja pitää viejää vastuussa kaikista viejän tällä perusteella tekemistä päätöksistä.

Neljänneksi on **yksilöitävä ja hyväksyttävä lisätoimenpiteet**, jotka ovat tarpeen, jotta siirrettävien tietojen suojan taso vastaisi pääosiltaan EU:n vaatimuksia vastaavaa tasoa. Tämä vaihe on tarpeen vain, jos arvioinnista käy ilmi, että kolmannen maan lainsäädäntö ja/tai käytännöt heikentävät sen yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen tehokkuutta, jota käytetään tai aiotaan käyttää siirron yhteydessä. Näissä suosituksissa (liitteessä 2) luetellaan esimerkkejä lisätoimenpiteistä sekä joitakin edellytyksiä, joiden on täytyttävä, jotta toimenpiteet olisivat tehokkaita. Luettelo ei ole tyhjentävä. Yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden sisältämien asianmukaisten suojatoimien tavoin jotkin lisätoimenpiteet voivat olla tehokkaita joissakin maissa mutta eivät välttämättä kaikissa. Viejän on arvioitava niiden tehokkuus siirron yhteydessä sekä kolmannen maan lainsäädännön ja käytäntöjen sekä käytettävän tiedonsiirtovälineen valossa, sillä viejä on vastuussa kaikista tällä perusteella tekemistään päätöksistä. Tämä voi myös edellyttää useiden lisätoimenpiteiden yhdistämistä. Loppujen lopuksi voidaan kuitenkin huomata, että tietylle siirrolle ei voida millään lisätoimenpiteellä varmistaa suojan tasoa, joka pääosiltaan vastaa EU:ssa taattua suojan tasoa. Tällaisissa tapauksissa, joihin mikään lisätoimenpide ei sovellu, siirto on jätettävä tekemättä, keskeytettävä tai lopetettava, jotta henkilötietojen suojan tasoa ei vaaranneta. Myös tämä lisätoimenpiteiden arviointi on tehtävä asianmukaisen huolellisesti ja dokumentoitava.

Viidenneksi on **toteutettava** kaikki **muodolliset menettelyvaiheet**, joita lisätoimenpiteen hyväksyminen voi edellyttää sen mukaan, mitä yleisen tietosuoja-asetuksen 46 artiklan mukaista tiedonsiirtovälinettä käytetään. Jotkin näistä muodollisuuksista yksilöidään näissä suosituksissa. Joidenkin osalta on ehkä kuultava toimivaltaisia valvontaviranomaisia.

Kuudenneksi ja viimeiseksi on **arvioitava uudelleen** asianmukaisin väliajoin kolmanteen maahan siirretyille henkilötiedoille annetun suojan tasoa ja seurattava, onko jokin kehitys vaikuttanut siihen tai vaikuttaako se siihen jatkossa. Osoitusvelvollisuuden periaate edellyttää henkilötietojen suojan tason jatkuvaa tarkkailua.

Valvontaviranomaiset toteuttavat edelleen toimeksiantoaan yleisen tietosuoja-asetuksen soveltamisen seurannasta ja sen valvonnasta. Valvontaviranomaiset kiinnittävät asianmukaista huomiota toimiin, joita viejät toteuttavat varmistaakseen, että siirrettäville tiedoille annetaan EU:ssa taattua suojan tasoa pääosiltaan vastaava suojan taso. Tuomioistuin muistuttaa, että valvontaviranomainen keskeyttää tai kieltää tietojen siirrot niissä tapauksissa, joissa EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa ei voida varmistaa, tutkinnan tai valituksen yhteydessä.

Valvontaviranomaiset laativat edelleen ohjeita viejille ja koordinoivat toimiaan Euroopan tietosuojaneuvostossa, jotta EU:n tietosuojalainsäädännön yhdenmukainen soveltaminen voidaan varmistaa.

SISÄLLYSLUETTELO

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen 2016/679/EU, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon Euroopan talousalueesta (ETA) tehdyn sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6. heinäkuuta 2018 annetulla Euroopan talousalueen sekakomitean päätöksellä nro 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

sekä katsoo seuraavaa:

(1) Euroopan unionin tuomioistuin (EUT) toteaa 16. heinäkuuta 2020 asiassa *Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems,* C-311/18 antamassaan tuomiossa, että yleisen tietosuoja-asetuksen 46 artiklan 1 kohtaa ja 2 kohdan c alakohtaa on tulkittava siten, että näissä säännöksissä vaadituilla asianmukaisilla suojatoimenpiteillä, täytäntöönpanokelpoisilla oikeuksilla ja tehokkailla oikeussuojakeinoilla on varmistettava, että rekisteröidyt, joiden henkilötietoja siirretään kolmanteen maahan tietosuojaa koskevien vakiolausekkeiden perusteella, saavat sellaisen suojan tason, joka pääosiltaan vastaa tasoa, joka taataan Euroopan unionissa tämän asetuksen, luettuna Euroopan unionin perusoikeuskirjan valossa, nojalla[2].

(2) Kuten tuomioistuin korosti, luonnollisten henkilöiden suojan tasoa, joka Euroopan unionissa taataan yleisellä tietosuoja-asetuksella luettuna perusoikeuskirjan valossa, pääosiltaan vastaava suojan taso on näin ollen varmistettava riippumatta siitä, minkä V luvun säännöksen nojalla henkilötietojen siirto kolmanteen maahan on toteutettu. V luvun säännöksillä pyritään varmistamaan tämän suojan korkean tason jatkuvuus, kun henkilötietoja siirretään kolmanteen maahan[3].

(3) Yleisen tietosuoja-asetuksen johdanto-osan 108 kappaleessa ja 46 artiklan 1 kohdassa säädetään, että jos EU:n tietosuojan riittävyyttä koskevaa päätöstä ei ole tehty, rekisterinpitäjän tai henkilötietojen käsittelijän olisi toteutettava toimenpiteitä, joiden avulla rekisteröidylle voidaan tarjota asianmukaiset suojatoimet kolmannen maan puutteellisen tietosuojan kompensoimiseksi. Rekisterinpitäjä tai henkilötietojen käsittelijä voi tarjota asianmukaiset suojatoimet ilman valvontaviranomaisen nimenomaista lupaa käyttämällä jotakin yleisen tietosuoja-asetuksen 46 artiklan 2 kohdassa luetelluista tiedonsiirtovälineistä, kuten tietosuojaa koskevia vakiolausekkeita.

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan koko tässä asiakirjassa Euroopan talousalueen jäsenvaltioita.
[2] Euroopan unionin tuomioistuimen tuomio, 16.7.2020, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (jäljempänä C-311/18 (Schrems II)), toinen toteamus.
[3] C-311/18 (Schrems II), 92 ja 93 kohta.

(4) Tuomioistuin selventää, että komission antamilla tietosuojaa koskevilla vakiolausekkeilla pyritään ainoastaan tarjoamaan unioniin sijoittautuneille rekisterinpitäjille tai henkilötietojen käsittelijöille sopimukseen perustuvia suojatoimia, joita sovelletaan yhtenäisesti kaikissa kolmansissa maissa. Tietosuojaa koskevien vakiolausekkeiden sopimusluonteisuuteen kuuluu se, että ne eivät voi sitoa kolmannen maan viranomaisia, koska nämä eivät ole sopimuspuolia. Tietojen viejien on siksi ehkä täydennettävä kyseisten tietosuojaa koskevien vakiolausekkeiden sisältämiä suojatoimia lisätoimenpiteillä, jotta voidaan varmistaa, että unionin oikeudessa vaadittua tietosuojan tasoa noudatetaan tietyssä kolmannessa maassa. Tuomioistuin viittaa yleisen tietosuoja-asetuksen johdanto-osan 109 kappaleeseen, jossa tämä mahdollisuus mainitaan ja kannustetaan rekisterinpitäjiä ja henkilötietojen käsittelijöitä käyttämään sitä.[4]

(5) Tuomioistuin totesi, että tietojen viejän on ennen kaikkea tapauskohtaisesti ja tarvittaessa yhteistyössä tietojen tuojan kanssa tarkistettava, varmistetaanko kohdemaana olevan kolmannen maan oikeudessa tietosuojaa koskevien vakiolausekkeiden perusteella siirrettyjen henkilötietojen pääosiltaan vastaava suojan taso unionin oikeuden kannalta, ja järjestettävä tarvittaessa näillä lausekkeilla tarjottujen suojatoimien täydentämiseksi lisätoimenpiteitä[5].

(6) Jos unioniin sijoittautunut rekisterinpitäjä tai henkilötietojen käsittelijä ei voi toteuttaa riittäviä lisätoimenpiteitä unionin oikeudessa taattua suojan tasoa pääosiltaan vastaavan suojan tason varmistamiseksi, sen – tai toissijaisesti toimivaltaisen valvontaviranomaisen – on keskeytettävä tai lopetettava henkilötietojen siirto asianomaiseen kolmanteen maahan[6].

(7) Yleisessä tietosuoja-asetuksessa ei määritellä tai täsmennetä eikä tuomioistuin määrittele tai täsmennä yleisen tietosuoja-asetuksen 46 artiklan 2 kohdassa lueteltujen tiedonsiirtovälineiden suojatoimien ”muita suojatoimia”, ”lisätoimenpiteitä” tai ”lisäsuojatoimia”, joita rekisterinpitäjät ja henkilötietojen käsittelijät voivat tarjota, jotta voidaan varmistaa, että unionin oikeudessa vaadittua tietosuojan tasoa noudatetaan tietyssä kolmannessa maassa.

(8) Euroopan tietosuojaneuvosto on päättänyt omasta aloitteestaan tarkastella tätä kysymystä ja antaa tietojen viejinä toimiville rekisterinpitäjille ja henkilötietojen käsittelijöille suosituksia prosessista, jota ne voivat noudattaa lisätoimenpiteiden yksilöimisessä ja hyväksymisessä. Näiden suositusten tarkoituksena on tarjota tietojen viejille menetelmä, jonka avulla voidaan määrittää, onko niiden tekemiä siirtoja varten otettava käyttöön lisätoimenpiteitä ja mitä nämä toimenpiteet olisivat. Tietojen viejien ensisijaisena vastuuna on varmistaa, että siirrettäville tiedoille annetaan kolmannessa maassa sellainen suojan taso, joka pääosiltaan vastaa Euroopan talousalueella taattua suojaa. Näillä suosituksilla Euroopan tietosuojaneuvosto pyrkii tukemaan yleisen tietosuoja-asetuksen ja tuomioistuimen tuomioiden johdonmukaista soveltamista Euroopan tietosuojaneuvoston toimeksiannon mukaisesti[7].

ON ANTANUT SEURAAVAN SUOSITUKSEN:

---

[4] C-311/18 (Schrems II), 132 ja 133 kohta.
[5] C-311/18 (Schrems II), 134 kohta.
[6] C-311/18 (Schrems II), 135 kohta.
[7] Yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan e alakohta.

1 OSOITUSVELVOLLISUUS TIEDONSIIRROISSA

1. Oikeus tietosuojaan katsotaan EU:n primaarioikeudessa perusoikeudeksi[8]. Tietosuojaa koskevan oikeuden suojan taso on siten korkea, ja sitä voidaan rajoittaa ainoastaan lailla sekä oikeuden keskeistä sisältöä kunnioittaen. Suojan rajoitusten on oltava oikeasuhteisia ja välttämättömiä, ja niiden on vastattava tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.[9] Oikeus henkilötietojen suojaan ei ole absoluuttinen oikeus vaan sitä on tarkasteltava suhteessa sen tehtävään yhteiskunnassa, ja sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin[10].

2. Kun tietoja siirretään kolmansiin maihin Euroopan talousalueen ulkopuolelle, niiden mukana on siirrettävä myös sellainen suojan taso, joka pääosiltaan vastaa tasoa, joka taataan Euroopan unionissa. Näin varmistetaan, että yleisellä tietosuoja-asetuksella taattua suojan tasoa ei heikennetä siirron aikana eikä sen jälkeen.

3. Oikeus tietosuojaan on luonteeltaan aktiivinen. Se tarkoittaa, että tietojen viejille ja tuojille ei riitä (riippumatta siitä, ovatko ne rekisterinpitäjiä vai henkilötietojen käsittelijöitä) pelkästään tämän oikeuden hyväksyminen tai passiivinen noudattaminen[11]. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on pyrittävä noudattamaan oikeutta tietosuojaan aktiivisesti ja jatkuvasti panemalla täytäntöön oikeudellisia, teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan sen tehokkuus. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on myös pystyttävä osoittamaan nämä toimenpiteet rekisteröidyille ja tietosuojavalvontaviranomaisille. Tätä sanotaan osoitusvelvollisuuden periaatteeksi.[12]

4. Osoitusvelvollisuuden periaate on tarpeen sen varmistamiseksi, että yleisellä tietosuoja-asetuksella annettua suojan tasoa sovelletaan tehokkaasti myös kolmansiin maihin tehtäviin siirtoihin[13], koska myös ne ovat itsessään tietojen käsittelyä[14]. Kuten tuomioistuin tuomiossaan korosti, suojan tasoa, joka Euroopan unionissa taataan yleisellä tietosuoja-asetuksella luettuna perusoikeuskirjan valossa, pääosiltaan vastaava suojan taso on näin ollen varmistettava riippumatta siitä, minkä kyseisen luvun säännöksen nojalla henkilötietojen siirto kolmanteen maahan on toteutettu[15].

5. Asiassa Schrems II antamassaan tuomiossa tuomioistuin korostaa tietojen viejien ja tuojien vastuuta varmistaa, että henkilötietojen käsittely on suoritettu ja suoritetaan edelleen EU:n tietosuojalainsäädännössä asetetun suojan tason mukaisesti, ja keskeyttää tietojen siirto ja/tai

---

[8] Perusoikeuskirjan 8 artiklan 1 kohta, SEUT-sopimuksen 16 artiklan 1 kohta ja yleisen tietosuoja-asetuksen johdanto-osan 1 kappale ja 1 artiklan 2 kohta.
[9] EU:n perusoikeuskirjan 52 artiklan 1 kohta.
[10] Yleisen tietosuoja-asetuksen johdanto-osan 4 kappale ja asiassa C-507/17 Google LLC, jolle Google Inc:n oikeudet ovat siirtyneet, v. Commission nationale de l'informatique et des libertés (CNIL), annetun tuomion 60 kohta.
[11] C-92/09 ja C-93/02, Volker und Markus Schecke GbR v. Land Hessen, julkisasiamies Sharpstonin ratkaisuehdotus, 17. kesäkuuta 2010, 71 kohta.
[12] Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 28 artiklan 3 kohdan h alakohta.
[13] Yleisen tietosuoja-asetuksen 44 artikla ja johdanto-osan 101 kappale sekä 47 artiklan 2 kohdan d alakohta.
[14] Euroopan unionin tuomioistuimen asiassa *Maximillian Schrems v. Data Protection Commissioner (jäljempänä* C-362/14 (Schrems I)) 6. lokakuuta 2015 antaman tuomion 45 kohta.
[15] C-311/18 (Schrems II), 92 ja 93 kohta.

irtisanoa sopimus, kun tietojen tuoja ei voi tai ei enää voi noudattaa tietosuojaa koskevia vakiolausekkeita, jotka sisältyvät viejän ja tuojan väliseen asiaankuuluvaan sopimukseen[16]. Viejänä toimivan rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että tuojat tekevät tarvittaessa yhteistyötä viejän kanssa sen täyttäessä näitä vastuita, tiedottamalla esimerkiksi kaikesta kehityksestä, joka vaikuttaa tuojan maassa vastaan otettujen henkilötietojen suojan tasoon[17]. Näillä vastuilla sovelletaan yleisen tietosuoja-asetuksen osoitusvelvollisuuden periaatetta tiedonsiirtoihin[18].

2 ETENEMISSUUNNITELMA: OSOITUSVELVOLLISUUDEN PERIAATTEEN SOVELTAMINEN TIEDONSIIRTOIHIN KÄYTÄNNÖSSÄ

6. Seuraavaksi esitetään etenemissuunnitelma vaiheista, joiden avulla selvitetään, onko tietojen viejän otettava käyttöön lisätoimenpiteitä voidakseen siirtää laillisesti tietoja Euroopan talousalueen ulkopuolelle. ”Tietojen viejällä” tarkoitetaan tässä asiakirjassa tietojen viejänä[19] toimivaa rekisterinpitäjää tai henkilötietojen käsittelijää, joka käsittelee yleisen tietosuoja-asetuksen soveltamisalaan kuuluvia henkilötietoja – myös kyseisiä tietoja käsitteleviä yksityisoikeudellisia yhteisöjä ja julkisen sektorin elimiä, kun tietoja siirretään yksityisen sektorin elimille.[20] Julkisen sektorin elinten välisistä henkilötietojen siirroista annetaan erityisiä ohjeita asiakirjassa *Suuntaviivat 2/2020 asetuksen (EU) 2016/679 46 artiklan 2 kohdan a alakohdan ja 46 artiklan 3 kohdan b alakohdan soveltamisesta henkilötietojen siirtämisessä ETA-alueen ja sen ulkopuolisten viranomaisten ja julkisten elinten välillä*[21].

7. Tietojen viejän on dokumentoitava asianmukaisesti tämä arviointi sekä valitut ja toteutettavat lisätoimenpiteet ja annettava kyseinen dokumentaatio toimivaltaisen valvontaviranomaisen saataville pyynnöstä[22].

2.1 Vaihe 1: Siirtojen tunteminen

8. Jotta voidaan selvittää, mitä tietojen viejältä voidaan edellyttää, jotta henkilötietojen siirtämistä voidaan jatkaa tai uusia siirtoja tehdä[23], ensimmäiseksi on varmistettava, että tiedetään, mistä siirroissa on kyse (siirtojen tunteminen). Kaikkien siirtojen rekisteröinti ja kartoittaminen voi olla työlästä yhteisöille, jotka tekevät usein ja säännöllisesti erilaisia siirtoja kolmansien maiden kanssa

[16] C-311/18 (Schrems II), 134, 135, 139, 140, 141 ja 142 kohta.
[17] C-311/18 (Schrems II), 134 kohta.
[18] Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 28 artiklan 3 kohdan h alakohta.
[19] Henkilöä ei siis pidetä tietojen viejänä, jos hän on rekisteröity, joka antaa henkilötietonsa verkkokyselylomakkeen välityksellä kolmanteen maahan sijoittautuneelle rekisterinpitäjälle.
[20] Ks. Euroopan tietosuojaneuvoston ohjeet 3/2018 yleisen tietosuoja-asetuksen alueellisesta soveltamisalasta (3 artikla) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] Euroopan tietosuojaneuvoston suuntaviivat 2/2020 asetuksen (EU) 2016/679 46 artiklan 2 kohdan a alakohdan ja 46 artiklan 3 kohdan b alakohdan soveltamisesta henkilötietojen siirtämisessä ETA-alueen ja sen ulkopuolisten viranomaisten ja julkisten elinten välillä; ks. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[22] Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 24 artiklan 1 kohta.
[23] On huomattava, että siirroksi katsotaan myös se, että kolmannessa maassa sijaitseva yhteisö käyttää Euroopan talousalueella sijaitsevia tietoja etäyhteydellä.

ja käyttävät useita henkilötietojen käsittelijöitä ja alikäsittelijöitä. Siirtojen tunteminen on olennaisen tärkeä ensimmäinen vaihe osoitusvelvollisuuden periaatteen mukaisten velvollisuuksien täyttämisessä.

9. Siirtojen täydellisessä tuntemisessa voi olla apua käsittelytoimia koskevista selosteista, joita rekisterinpitäjänä tai henkilötietojen käsittelijänä on ehkä pidettävä yleisen tietosuoja-asetuksen 30 artiklan mukaisesti[24]. Myös aiemmat toimet, joilla täytetään yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan f alakohdan ja 14 artiklan 1 kohdan f alakohdan mukaiset velvollisuudet ilmoittaa rekisteröidyille näiden henkilötietojen siirroista kolmansiin maihin, voivat olla avuksi[25].

10. Siirtoja kartoitettaessa on muistettava ottaa huomioon tietojen siirtäminen edelleen, esimerkiksi se, siirtävätkö Euroopan talousalueen ulkopuolella olevat henkilötietojen käsittelijät, joille viejä on antanut käsittelyn tehtäväksi, henkilötietoja alikäsittelijälle toisessa kolmannessa maassa tai samassa kolmannessa maassa[26].

11. Yleisen tietosuoja-asetuksen tietojen minimoinnin periaatteen[27] mukaisesti on tarkistettava, että siirrettävät tiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista niiden käsittelyn kannalta.

12. Nämä toimet on tehtävä ennen minkään siirron tekemistä ja saatettava ajan tasalle ennen kuin siirrot aloitetaan uudelleen tiedonsiirtotoimien keskeyttämisen jälkeen. Viejän on tiedettävä, missä viedyt henkilötiedot voivat sijaita tai missä tuojat voivat niitä käsitellä (kohdekartta).

13. On pidettävä mielessä, että myös kolmannesta maasta käsin tehtävä henkilötietojen etäkäyttö (esimerkiksi tukitilanteissa) ja/tai niiden tallentaminen Euroopan talousalueen ulkopuolella sijaitsevaan, palveluntarjoajan tarjoamaan pilvipalveluun katsotaan tiedonsiirroksi[28]. Jos viejä tarkemmin sanottuna käyttää kansainvälistä pilvipalveluinfrastruktuuria, tämän on arvioitava, siirretäänkö tiedot kolmansiin maihin ja minne niissä, ellei pilvipalvelun tarjoaja ole sijoittautunut

---

[24] Ks. yleisen tietosuoja-asetuksen 30 artikla ja erityisesti sen 1 kohdan e alakohta ja 2 kohdan c alakohta. Lisäksi käsittelyselosteiden pitäisi sisältää kuvaus viejän käsittelytoimista (muun muassa rekisteröityjen ryhmät, henkilötietojen ryhmät ja käsittelytarkoitukset sekä erityistiedot tiedonsiirroista). Jotkin rekisterinpitäjät ja henkilötietojen käsittelijät vapautetaan velvoitteesta pitää selostetta käsittelystä (yleisen tietosuoja-asetuksen 30 artiklan 5 kohta). Tästä vapautuksesta on ohjeita 29 artiklan mukaisen tietosuojatyöryhmän kannanotossa poikkeuksista velvollisuuteen pitää yleisen tietosuoja-asetuksen 30 artiklan 5 kohdan mukaista selostetta käsittelytoimista (Euroopan tietosuojaneuvosto hyväksyi kannanoton 25. toukokuuta 2018).

[25] Yleisen tietosuoja-asetuksen läpinäkyvyyssääntöjen mukaan rekisteröidyille on ilmoitettava henkilötietojen siirroista kolmansiin maihin (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan f alakohta ja 14 artiklan 1 kohdan f alakohta). Rekisteröidyille on erityisesti ilmoitettava tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta tai, jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville. Rekisteröidylle annettavien tietojen on oltava täsmällisiä ja ajantasaisia, erityisesti siirtoja koskevan unionin tuomioistuimen oikeuskäytännön valossa.

[26] Jos rekisterinpitäjä on antanut erityisen tai yleisen kirjallisen ennakkoluvan yleisen tietosuoja-asetuksen 28 artiklan 2 kohdan mukaisesti.

[27] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohta.

[28] Ks. FAQ 11: olisi pidettävä mielessä, että siirroksi katsotaan myös se, että tiedot annetaan käyttöön kolmannesta maasta, esimerkiksi hallintotarkoituksiin, Euroopan tietosuojaneuvosto, usein esitettyjä kysymyksiä, jotka koskevat Euroopan unionin tuomioistuimen tuomiota asiassa C-311/18 – Data Protection Commissioner vastaan Facebook Ireland Ltd ja Maximillian Schrems, 23. heinäkuuta 2020.

Euroopan talousalueelle ja totea selkeästi sopimuksessaan, että tietoja ei käsitellä kolmansissa maissa lainkaan.

2.2 Vaihe 2: Käytettävien tiedonsiirtovälineiden yksilöiminen

14. Toisessa vaiheessa on yksilöitävä yleisen tietosuoja-asetuksen V luvussa luetelluista säädetyistä tiedonsiirtovälineistä ne, joita käytetään.

Riittävyyttä koskevat päätökset

15. Euroopan komissio voi tunnustaa **riittävyyttä koskevilla päätöksillään** joidenkin tai kaikkien niiden kolmansien maiden osalta, joihin viejä siirtää henkilötietoja, että ne tarjoavat riittävän henkilötietojen suojan tason[29].

16. Tällaisen riittävyyttä koskevan päätöksen perusteella henkilötiedot voidaan siirtää Euroopan talousalueelta kyseiseen kolmanteen maahan ilman, että tarvitaan mitään yleisen tietosuoja-asetuksen 46 artiklan mukaista tiedonsiirtovälinettä.

17. Riittävyyttä koskevat päätökset voivat koskea koko maata tai vain sen osaa. Riittävyyttä koskevat päätökset voivat koskea kaikkia tiedonsiirtoja maahan tai ne voidaan rajoittaa tietyntyyppisiin siirtoihin (esim. yhdellä sektorilla).[30]

18. Euroopan komissio julkaisee verkkosivustollaan luettelon riittävyyttä koskevista päätöksistä[31].

19. Jos henkilötietoja siirretään kolmansiin maihin, alueille tai sektoreille, joita komission riittävyyttä koskeva päätös koskee (soveltuvissa määrin), **muihin näissä suosituksissa kuvattuihin toimenpiteisiin ei tarvitse ryhtyä.**[32] Viejän on kuitenkin seurattava, kumotaanko tai mitätöidäänkö tämän siirtojen kannalta merkitykselliset riittävyyttä koskevat päätökset[33].

20. Riittävyyttä koskevat päätökset eivät kuitenkaan estä rekisteröityjä tekemästä valitusta. Ne eivät myöskään estä valvontaviranomaisia saattamasta asiaa kansallisen tuomioistuimen käsiteltäväksi, jos niillä on epäilyksiä päätöksen pätevyydestä, jotta kansallinen tuomioistuin voi pyytää Euroopan unionin tuomioistuimelta ennakkoratkaisua pätevyyden tutkimiseksi[34].

---

[29] Euroopan komissiolla on yleisen tietosuoja-asetuksen 45 artiklan nojalla valtuudet päättää, tarjoaako EU:n ulkopuolinen maa riittävän tietosuojan tason. Euroopan komissiolla on myös valtuudet päättää, että kansainvälinen järjestö tarjoaa riittävän suojan tason.

[30] Yleisen tietosuoja-asetuksen 45 artiklan 1 kohta.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Mikäli tietojen viejä ja tuoja ovat toteuttaneet toimenpiteitä yleisen tietosuoja-asetuksen muiden velvollisuuksien noudattamiseksi. Muussa tapauksessa kyseiset toimenpiteet on pantava täytäntöön.

[33] Euroopan komission on tarkasteltava säännöllisesti kaikkia riittävyyttä koskevia päätöksiä ja seurattava, varmistavatko kolmannet maat, joista on tehty riittävyyttä koskeva päätös, edelleen riittävän suojan tason (ks. yleisen tietosuoja-asetuksen 45 artiklan 3 ja 4 kohta). Myös Euroopan unionin tuomioistuin voi mitätöidä riittävyyttä koskevat päätökset (ks. sen tuomiot asioissa C-362/14 (Schrems I) ja C-311/18 (Schrems II)).

[34] C-311/18 (Schrems II), 118–120 kohta. Valvontaviranomaiset eivät saa jättää ottamatta huomioon riittävyyttä koskevaa päätöstä ja keskeyttää tai kieltää henkilötietojen siirtoa kyseisiin maihin viittaamalla vain suojan tason riittämättömyyteen. Ne voivat käyttää valtuuksiaan keskeyttää tai kieltää henkilötietojen siirrot kyseiseen kolmanteen maahan vain muilla perusteilla (esim. riittämättömät turvallisuustoimenpiteet yleisen tietosuoja-asetuksen 32 artiklan vastaisesti, tietojenkäsittelyn tukena ei ole pätevää oikeusperustetta, joten se on yleisen

Esimerkki:

EU:n kansalainen Maximillian Schrems teki kesäkuussa 2013 kantelun Irlannin tietosuojavaltuutetulle (Irish Data Protection Commission, DPC) ja pyysi valvontaviranomaista kieltämään tai keskeyttämään hänen henkilötietojensa siirtämisen Facebook Irelandista Yhdysvaltoihin, koska hän katsoi, että Yhdysvaltain lainsäädännöllä ja käytännöllä ei taattu sen alueella pidetyille henkilötiedoille riittävää suojaa tarkkailutoimilta, joita viranomaiset siellä harjoittivat. Tietosuojavaltuutettu hylkäsi kantelun erityisesti siksi, että Euroopan komissio oli katsonut päätöksessään 2000/520, että Yhdysvallat takasi safe harbour -järjestelmällä siirrettyjen henkilötietojen riittävän suojan (safe harbour -päätös). Maximillian Schrems kyseenalaisti tietosuojavaltuutetun päätöksen ja Irlannin High Court pyysi unionin tuomioistuimelta (EUT) ennakkoratkaisua päätöksen 2000/520 pätevyydestä. Unionin tuomioistuin päätti mitätöidä komission päätöksen 2000/520 safe harbour -periaatteiden antaman suojan riittävyydestä.[35]

Yleisen tietosuoja-asetuksen 46 artiklan mukaiset tiedonsiirtovälineet

21. Yleisen tietosuoja-asetuksen 46 artiklassa luetellaan joukko tiedonsiirtovälineitä, joissa on ”*asianmukaiset suojatoimet*” ja joita tietojen viejät voivat käyttää henkilötietojen siirtämiseen kolmansiin maihin, jos riittävyyttä koskevia päätöksiä ei ole. Yleisen tietosuoja-asetuksen 46 artiklan mukaisia tärkeimpiä tiedonsiirtovälineitä ovat

- tietosuojaa koskevat vakiolausekkeet
- yritystä koskevat sitovat säännöt
- käytännesäännöt
- sertifiointimekanismit
- tapauskohtaiset sopimuslausekkeet.

22. Riippumatta siitä, mikä yleisen tietosuoja-asetuksen 46 artiklan mukainen tiedonsiirtoväline valitaan, on varmistettava, että siirrettäviin henkilötietoihin sovelletaan asetuksen vaatimuksia pääosiltaan vastaavaa suojan tasoa.

23. Yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden asianmukaiset suojatoimet ovat pääosin sopimukseen perustuvia, ja niitä voidaan soveltaa kaikkiin kolmansiin maihin tehtäviin siirtoihin. Tietojen siirron kohteena olevassa kolmannessa maassa vallitsevan tilanteen perusteella voi olla näiden tiedonsiirtovälineiden ja niiden sisältämien suojatoimien täydentämiseksi tarpeen, että tietojen viejä toteuttaa lisätoimenpiteitä (”lisäsuojatoimia”) varmistaakseen yleistä tietosuoja-asetusta pääosiltaan vastaavan suojan tason.[36]

Poikkeukset

24. Riittävyyttä koskevien päätösten ja yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden lisäksi yleisessä tietosuoja-asetuksessa on kolmaskin keino siirtää

tietosuoja-asetuksen 6 artiklan vastainen). Valvontaviranomaiset voivat tarkastella täysin riippumattomasti, noudatetaanko kyseisten tietojen siirrossa yleisessä tietosuoja-asetuksessa esitettyjä vaatimuksia, ja tarvittaessa saattaa asian kansallisten tuomioistuinten käsiteltäväksi, jotta ne voivat pyytää Euroopan unionin tuomioistuimelta ennakkoratkaisua päätöksen pätevyyden tutkimiseksi, jos niillä on epäilyksiä komission riittävyyttä koskevan päätöksen pätevyydestä.

[35] Asia C-362/14 (Schrems I).

[36] C-311/18 (Schrems II), 130 ja 133 kohta. Ks. myös jäljempänä oleva 2.3 alakohta.

henkilötietoja tietyissä tilanteissa. Henkilötietoja voi siirtää tietyin edellytyksin yleisen tietosuoja-asetuksen 49 artiklassa lueteltujen poikkeusten perusteella.

25. Yleisen tietosuoja-asetuksen 49 artikla on poikkeuksellinen. Artiklassa tarkoitettuja poikkeuksia on tulkittava tavalla, joka ei ole vastoin poikkeusten luonnetta eli sitä, että ne ovat poikkeuksia sääntöön, jonka mukaan henkilötietoja ei saa siirtää kolmanteen maahan, ellei maa tarjoa riittävää tietosuojan tasoa tai ellei käytössä ole asianmukaisia suojatoimia. Poikkeuksia ei voida alkaa käyttää säännönmukaisesti, vaan niiden käyttö on rajattava vain tiettyihin tilanteisiin. Euroopan tietosuojaneuvosto on antanut asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevat ohjeet 2/2018. [37]

26. Ennen yleisen tietosuoja-asetuksen 49 artiklan poikkeukseen turvautumista on tarkistettava, täyttääkö siirto tiukat ehdot, joita säännöksessä kullekin niistä säädetään.

***

27. Jos siirto ei voi perustua laillisesti riittävyyttä koskevaan päätökseen eikä 49 artiklan mukaiseen poikkeukseen, on jatkettava vaiheeseen 3.

2.3 Vaihe 3: Arvioidaan, onko yleisen tietosuoja-asetuksen 46 artiklan mukainen käytettävä tiedonsiirtoväline tehokas kaikissa siirron olosuhteissa

28. Valitulla tiedonsiirtovälineellä, joka on yleisen tietosuoja-asetuksen 46 artiklan mukainen, on voitava varmistaa, että siirrolla ei vaaranneta yleisellä tietosuoja-asetuksella taattua suojan tasoa käytännössä[38].

29. Kolmanteen maahan siirrettäville henkilötiedoille on muun muassa annettava sellainen tietosuojan taso, joka pääosiltaan vastaa tasoa, joka taataan Euroopan talousalueella yleisellä tietosuoja-asetuksella, luettuna EU:n perusoikeuskirjan valossa.[39] Näin ei ole, jos tietojen tuojaa estetään noudattamasta yleisen tietosuoja-asetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen edellyttämiä velvollisuuksiaan siirtoon sovellettavien kolmannen maan lakien ja käytäntöjen vuoksi, myös tietojen siirron aikana viejältä tuojan maahan[40].

30. Tietojen viejän on ensin arvioitava, tarvittaessa yhteistyössä tuojan kanssa, onko kolmannen maan voimassa olevissa laeissa ja/tai käytännöissä[41] jotakin, mikä voi heikentää yleisen tietosuoja-asetuksen 46 artiklan mukaisten käytettävien tiedonsiirtovälineiden asianmukaisten suojatoimien tehokkuutta tietyn siirron yhteydessä. Tällöin on myös määritettävä, kuuluuko tämä siirto sellaisen lainsäädännön ja/tai sellaisten käytäntöjen soveltamisalaan, jotka voivat heikentää

---

[37] Ohjeista on lisätietoa osoitteessa https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.
[38] Yleisen tietosuoja-asetuksen 44 artikla ja asiassa C-311/18 (Schrems II) annetun tuomion 126, 137 ja 148 kohta.
[39] Asiassa C-311/18 (Schrems II) annetun tuomion 105 kohta ja toinen toteamus.
[40] Ks. asiassa C-311/18 (Schrems II) annetun tuomion 183 kohta luettuna yhdessä 184 kohdan kanssa.
[41] Ks. asiassa C-311/18 (Schrems II) annetun tuomion 126 kohta, jossa tuomioistuin nimenomaisesti viittaa ”asianomaisen kolmannen maan lainsäädännön tilaan ja siellä vallitseviin käytäntöihin” ja edellyttää, että on voitava ”[– –] käytännössä varmistaa asianomaiseen kolmanteen maahan siirrettyjen henkilötietojen tehokas suoja” (korostus lisätty), ja 158 kohta.

yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen tehokkuutta. Tämän arvioinnin on ennen kaikkea perustuttava julkisesti saatavilla olevaan lainsäädäntöön.

31. Tässä arvioinnissa on käsiteltävä tekijöitä, jotka koskevat tuojan kolmannen maan viranomaisten pääsyä on tietoihin, esimerkiksi seuraavien seikkojen osalta:

    - Voivatko tuojan kolmannen maan viranomaiset saada pääsyn tietoihin ilman, että tietojen tuoja tietää siitä, kun otetaan huomioon lainsäädäntö, käytäntö ja ilmoitetut ennakkotapaukset?
    - Voivatko tuojan kolmannen maan viranomaiset saada pääsyn tietoihin tietojen tuojan välityksellä taikka tietoliikenneyhteyksien tarjoajien tai viestintäkanavien välityksellä, kun otetaan huomioon lainsäädäntö, oikeudellinen toimivalta, viranomaisten käytettävissä olevat tekniset, taloudelliset ja henkilöstöresurssit sekä ilmoitetut ennakkotapaukset?

Siirron kaikkien olosuhteiden kannalta merkityksellisten lakien ja käytäntöjen yksilöiminen

32. On tarkasteltava kunkin siirron ominaisuuksia ja selvitettävä, vaikuttavatko siirtoihin sen maan kansallinen oikeusjärjestys ja/tai käytännöt, johon tietoja siirretään (tai siirretään edelleen), siirto. Arvioinnin laajuus rajataan siis niiden nimenomaisten tietojen, jotka siirretään, suojaamisen kannalta merkityksellisiin lakeihin ja käytäntöihin, toisin kuin niissä yleisissä ja laaja-alaisissa tietosuojan riittävyyttä koskevissa arvioinneissa, joita Euroopan komissio tekee yleisen tietosuoja-asetuksen 45 artiklan mukaisesti.

33. Sovellettava oikeudellinen kehys ja/tai käytännöt riippuvat siirron nimenomaisista olosuhteista, erityisesti

    - tarkoituksista, joita varten tietoja siirretään ja käsitellään (esim. markkinointi, henkilöstöhallinto, tallennus, IT, tuki, kliiniset kokeet)
    - käsittelyyn osallistuvien yhteisöjen tyypeistä (julkinen/yksityinen, rekisterinpitäjä / henkilötietojen käsittelijä)
    - sektorista, jolla siirto tapahtuu (esim. mainontateknologia, televiestintä, rahoitus)
    - siirrettävistä henkilötietoryhmistä (esim. lapsiin liittyvät henkilötiedot voivat kuulua kolmannessa maassa erityislainsäädännön piiriin)[42]
    - siitä, säilytetäänkö tietoja kolmannessa maassa vai käytetäänkö EU:ssa/Euroopan talousalueella säilytettäviä tietoja etäyhteydellä

[42] Henkilötietojen siirtäminen on käsittelytoiminto (yleisen tietosuoja-asetuksen 4 artiklan 2 kohta). Jos tarkoituksena on siirtää yleisen tietosuoja-asetuksen 9 ja 10 artiklassa tarkoitettuja arkaluonteisia tietoja, siirron voi tehdä vain, jos siihen voidaan soveltaa jotakin yleisen tietosuoja-asetuksen 9 ja 10 artiklassa esitetyistä poikkeuksista ja ehdoista sekä EU:n jäsenvaltioiden lainsäädäntöä. Yleisen tietosuoja-asetuksen 32 artiklan mukaisesti silloin, kun tuoja on myös rekisterinpitäjä tai henkilötietojen käsittelijä, on toteutettava tarvittavat asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan turvallisuustaso, joka vastaa siirrettyihin tietoihin kohdistuvan mahdollisen henkilötietojen tietoturvaloukkauksen (yleisen tietosuoja-asetuksen 4 artiklan 12 kohta) aiheuttamia rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä aiheuttaisi, vastaavan turvallisuustason varmistamiseksi. Siirrettävien tietojen ryhmät ja niiden arkaluonteisuus ovat merkityksellisiä, kun arvioidaan riskiä ja toimenpiteiden asianmukaisuutta.

- siirrettävien tietojen muodosta (eli pelkkänä tekstinä / pseudonymisoituna tai salattuna[43])
- mahdollisuudesta, että tietoja voidaan siirtää edelleen kolmannesta maasta toiseen kolmanteen maahan[44].

34. Arvioinnissa on otettava huomioon kaikki siirtoon osallistuvat toimijat (esim. rekisterinpitäjät, henkilötietojen käsittelijät ja alikäsittelijät, jotka käsittelevät tietoja kolmannessa maassa), jotka on yksilöity siirtojen kartoituksessa. Arviointi monimutkaistuu sitä mukaa, mitä enemmän rekisterinpitäjiä, henkilötietojen käsittelijöitä tai tietojen tuojia siihen osallistuu. Arvioinnissa on käsiteltävä myös kaikkia suunniteltuja siirtoja eteenpäin.

35. Viejän on joka tapauksessa kiinnitettävä erityistä huomiota kaikkiin asiaankuuluviin lakeihin, erityisesti lakeihin, joissa esitetään vaatimuksia henkilötietojen luovuttamisesta viranomaisille tai henkilötietoihin pääsyä koskevien oikeuksien myöntämisestä kyseisille viranomaisille (esimerkiksi rikosoikeudellista lainvalvontaa, sääntelyvalvontaa tai kansallista turvallisuutta varten). Jos nämä vaatimukset tai valtuudet rajoittavat rekisteröityjen perusoikeuksia niiden keskeistä sisältöä kunnioittaen ja vaikka ne olisivat demokraattisessa yhteiskunnassa välttämättömiä ja oikeasuhteisia toimenpiteitä, jotta voidaan turvata tärkeitä tavoitteita, kuten todetaan myös unionin oikeudessa tai EU:n jäsenvaltioiden lainsäädännössä,[45] ne eivät saa heikentää siirrossa käytettävään, yleisen tietosuoja-asetuksen 46 artiklan mukaiseen siirtovälineeseen sisältyviä sitoumuksia.

36. Asiaan liittyvät säännöt ja yleiset käytännöt on arvioitava siltä osin kuin ne vaikuttavat yleisen tietosuoja-asetuksen 46 artiklan mukaiseen siirtovälineeseen sisältyvien suojatoimien tehokkaaseen soveltamiseen.

37. Tämän arvioinnin tekemisessä merkityksellisiä ovat myös kyseisen kolmannen maan oikeusjärjestelmän eri näkökohdat, esimerkiksi yleisen tietosuoja-asetuksen 45 artiklan 2 kohdassa luetellut seikat. Esimerkiksi oikeusvaltioperiaatteen tilanne kolmannessa maassa voi olla merkityksellinen arvioitaessa niiden mekanismien tehokkuutta, joiden avulla yksilöt voivat hakea (oikeudessa) muutosta viranomaisten lainvastaiseen pääsyyn henkilötietoihin. Viranomaisten puuttumisen oikeasuhteisuuden varmistamisessa voi olla avuksi, että on olemassa kattava tietosuojalainsäädäntö tai riippumaton tietosuojaviranomainen sekä se, että noudatetaan tietosuojaa koskevia suojatoimia tarjoavia kansainvälisiä välineitä.

38. Näistä laeista ja käytännöistä johtuvien velvoitteiden ja valtuuksien katsotaan heikentävän yleisen tietosuoja-asetuksen 46 artiklan mukaisia sitoumuksia tai olevan niiden vastaisia, jos ne [46]

    - eivät kunnioita Euroopan unionin perusoikeuskirjan mukaisten perusoikeuksien ja vapauksien keskeistä sisältöä, tai

---

[43] Jotkin kolmannet maat eivät salli salattujen tietojen tuomista.

[44] Jos rekisterinpitäjä on antanut erityisen tai yleisen kirjallisen ennakkoluvan yleisen tietosuoja-asetuksen 28 artiklan 2 kohdan mukaisesti.

[45] Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[46] Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta, asiassa C-311/18 (Schrems II) annetun tuomion 174 ja 187 kohta sekä Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020.

- ylittävät sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, jotta voidaan turvata jokin niistä tärkeistä tavoitteista, jotka on tunnustettu myös unionin oikeudessa tai jäsenvaltion lainsäädännössä, kuten ne, jotka on lueteltu yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa.

39. On varmistettava, että tietojen tuojan sitoumuksia, joiden perusteella rekisteröidyt voivat käyttää oikeuksiaan yleisen tietosuoja-asetuksen 46 artiklan mukaisen siirtovälineen käytön yhteydessä (kuten siirrettyihin tietoihin tutustumista, niiden oikaisua ja poistamista koskevia pyyntöjä sekä muutoksen hakemista (oikeudessa)), voidaan soveltaa tehokkaasti käytännössä ja että niitä ei estetä kohteena olevan kolmannen maan lainsäädännöllä ja/tai käytännöillä.

40. EU:n vaatimuksia, kuten Euroopan unionin perusoikeuskirjan 47 ja 52 artiklaa, on käytettävä vertailukohtana etenkin arvioitaessa, onko kyseinen viranomaisille sallittu käyttö rajoitettu siihen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, ja onko rekisteröidyille tarjottu tehokas oikeussuojakeino.

41. Euroopan tietosuojaneuvoston suosituksissa eurooppalaisista olennaisista takeista[47] esitetään selvennyksiä tekijöistä, jotka on arvioitava sen selvittämiseksi, voidaanko kolmannen maan viranomaisten, sekä kansallisesta turvallisuudesta vastaavien virastojen että lainvalvontaviranomaisten, pääsyä henkilötietoihin koskeva oikeudellinen kehys katsoa perustelluksi puuttumiseksi[48] vai ei. Tähän on kiinnitettävä huomiota erityisesti, kun viranomaisten tietoihin pääsyä koskeva lainsäädäntö on moniselitteinen tai kun se ei ole yleisesti saatavilla. Eurooppalaisten olennaisten takeiden ensimmäinen vaatimus on se, että käytössä on oltava suunniteltua henkilötietoihin pääsyä koskeva oikeudellinen kehys, jonka on oltava julkisesti saatavilla ja riittävän selkeä.

42. Kun kyse on tiedonsiirtotilanteesta, joka perustuu 46 artiklan mukaisiin tiedonsiirtovälineisiin, tietojen viejä voi saada Euroopan tietosuojaneuvoston eurooppalaisia olennaisia takeita koskevista suosituksista ohjeita sen arvioimiseen, puututaanko kyseisillä valtuuksilla perusteettomasti tietojen viejän ja tuojan velvollisuuksiin varmistaa suojan taso, joka pääosiltaan vastaa yleisen tietosuoja-asetuksen mukaista tasoa tai siirtovälineeseen sisältyviä sitoumuksia. Pääosiltaan vastaavan suojan tason puuttuminen on erityisen selvää silloin, kun siirron kannalta merkittävät kolmannen maan lainsäädäntö ja/tai käytännöt eivät täytä eurooppalaisten olennaisten takeiden vaatimuksia. Tietosuojaneuvosto toistaa, että eurooppalaiset olennaiset takeet ovat viitestandardi arvioitaessa kolmannen maan tarkkailutoimenpiteisiin liittyvää puuttumista kansainvälisten tiedonsiirtojen yhteydessä. Nämä standardit on johdettu EU:n lainsäädännöstä sekä unionin tuomioistuimen ja ihmisoikeustuomioistuimen oikeuskäytännöstä, joka sitoo EU:n jäsenvaltioita.

43. Arvioinnin on ennen kaikkea perustuttava julkisesti saatavilla olevaan lainsäädäntöön. Myös kolmannen maan viranomaisten käytäntöjen tutkiminen auttaa varmentamaan, voivatko yleisen tietosuoja-asetuksen 46 artiklan mukaisen siirtovälineen sisältämät suojatoimet olla käytännössä riittävä keino varmistaa siirrettävien henkilötietojen tehokas suojaaminen.[49] Kolmannessa maassa

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[48] Tällöin kyse ei ole yleisen tietosuoja-asetuksen 46 artiklan mukaiseen siirtovälineeseen liittyvien sitoumusten heikentämisestä.

[49] C-311/18 (Schrems II), 126 kohta.

toteutettavien käytäntöjen tutkiminen on tärkeää etenkin silloin, kun arvioidaan jäljempänä kuvattuja tilanteita.

43.1 **Kolmannen maan lainsäädäntö voi muodollisesti täyttää perusoikeuksia ja vapauksia sekä niiden rajoittamisen välttämättömyyttä ja oikeasuhtaisuutta koskevat EU:n vaatimukset.** Kolmannen maan viranomaisten käytännöt (esimerkiksi pääsy yksityisen sektorin hallussa oleviin henkilötietoihin tai se, valvovatko valvonta- tai oikeusviranomaiset lainsäädännön noudattamista vai eivät) voivat kuitenkin osoittaa selvästi, etteivät ne yleensä sovella/noudata toimiinsa liittyvää lainsäädäntöä. Tässä tapauksessa nämä käytännöt on otettava huomioon arvioinnissa ja on muistettava, ettei yleisen tietosuoja-asetuksen 46 artiklan mukainen väline ole yksinään (ts. ilman lisätoimenpiteitä) riittävä varmistamaan pääosiltaan vastaavan suojan tasoa. Jos siirtoa on tarkoitus jatkaa, on siis toteutettava riittäviä lisätoimenpiteitä.

43.2 **Kolmannessa maassa ei välttämättä ole asiaan liittyvää lainsäädäntöä (joka koskisi esimerkiksi pääsyä yksityisen sektorin hallussa oleviin henkilötietoihin).** Siitä, ettei asiaan liittyvää lainsäädäntöä ole, ei kuitenkaan voida automaattisesti päätellä, että yleisen tietosuoja-asetuksen 46 artiklan mukaista siirtovälinettä voidaan käyttää tehokkaasti. Sen sijaan on selvitettävä, onko näyttöä siitä, että kyseisessä maassa sovelletaan sellaisia käytäntöjä, jotka ovat EU:n oikeuden ja yleisen tietosuoja-asetuksen 46 artiklan mukaiseen siirtovälineeseen liittyvien sitoumusten vastaisia. Jos tällaisia käytäntöjä on, pelkästään yleisen tietosuoja-asetuksen 46 artiklan mukaisella siirtovälineellä (ts. ilman riittäviä lisätoimenpiteitä) ei voida varmistaa pääosiltaan vastaavaa suojan tasoa. Jos siirtoa on tarkoitus jatkaa, on siis toteutettava riittäviä lisätoimenpiteitä.

43.3 **Arviointi voi osoittaa, että kolmannen maan asiaan liittyvä lainsäädäntö voi olla ongelmallista[50] ja että siirrettävät tiedot ja/tai kyseessä oleva tuoja kuuluvat tai saattavat kuulua tämän ongelmallisen lainsäädännön piiriin[51].**

Jos on epäselvää, voidaanko tiettyyn siirtoon mahdollisesti soveltaa ongelmallista lainsäädäntöä, toimintavaihtoehdot ovat seuraavat:

- Siirron keskeyttäminen.
- Lisätoimenpiteiden toteuttaminen[52], jotta vältetään riski siitä, että tietojen tuojaan ja/tai siirrettäviin tietoihin mahdollisesti sovellettaisiin tietojen tuojan kolmannen maan lakeja

[50] Ilmauksella ”ongelmallinen lainsäädäntö” tarkoitetaan sellaista lainsäädäntöä, joka 1) asettaa Euroopan unionista siirrettävien henkilötietojen vastaanottajalle velvollisuuksia ja/tai vaikuttaa siirrettäviin tietoihin tavalla, joka voi heikentää siirtovälineiden sopimukseen perustuvaa taetta pääosiltaan vastaavasta suojan tasosta ja 2) jossa ei kunnioiteta EU:n perusoikeuskirjassa tunnustettujen perusoikeuksien ja vapauksien keskeistä sisältöä tai joka ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, jotta voidaan turvata jokin tärkeistä tavoitteista, jotka on tunnustettu myös unionin oikeudessa tai EU:n jäsenvaltioiden lainsäädännössä, esimerkiksi ne, jotka on lueteltu yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa.

[51] Voi olla epäselvää, sisältyvätkö tuoja ja/tai siirrettävät tiedot sellaisiin kansallisessa turvallisuuslainsäädännössä usein käytettäviin yleisiin ilmauksiin, joilla lainsäädännön soveltamisalaa rajoitetaan, kuten ilmauksilla ”sähköisten viestintäpalvelujen tarjoaja” ja ”ulkomaantiedustelun tiedot”.

[52] Yleisen tietosuoja-asetuksen johdanto-osan 109 kappale ja asiassa C-311/18 (Schrems II) annetun tuomion 132 kohta.

ja/tai käytäntöjä, jotka ovat omiaan heikentämään siirtovälineen sopimukseen perustuvia takeita pääosiltaan Euroopan talousalueella taattua tasoa vastaavasta suojan tasosta.

- Vaihtoehtoisesti siirto voidaan tehdä ilman lisätoimenpiteiden toteuttamisen edellyttämistä, jos katsotaan, ettei ole syytä uskoa, että asiaan liittyvää ongelmallista lainsäädäntöä sovelletaan käytännössä siirrettäviin tietoihin ja/tai tietojen tuojaan. Arvioinnissa on osoitettava, tarvittaessa yhteistyössä tuojan kanssa, ettei lakia tulkita ja/tai sovelleta käytännössä siirrettäviin tietoihin ja tuojaan, ja tämä on myös dokumentoitava. Huomioon on otettava myös muiden samalla alalla ja/tai sellaisella alalla, jossa käsitellään henkilötietojen siirtämistä samalla tavalla, toimivien toimijoiden kokemukset sekä muut jäljempänä kuvatut tietolähteet[53].

  On siis osoitettava ja dokumentoitava yksityiskohtaisessa raportissa[54], ettei ongelmallista lainsäädäntöä sovelleta käytännössä siirrettäviin tietoihin ja/tai tuojaan ja ettei tämä lainsäädäntö estä tietojen tuojaa täyttämästä yleisen tietosuoja-asetuksen 46 artiklan mukaiseen siirtovälineeseen liittyviä velvollisuuksiaan[55].

Mahdolliset tietolähteet

44. Tietojen tuojan on annettava tietojen viejälle mahdolliset lähteet ja tiedot kolmannesta maasta, johon se on sijoittautunut, ja siirtoon sovellettavista laeista ja käytännöistä.

45. Velvollinen toimija ja tietojen tuoja voivat täydentää arviointia lähteistä saaduilla tiedoilla. Esimerkkejä tietolähteistä on lueteltu liitteessä 3.

46. Siirtoon sovellettavan kolmannen maan oikeudellisen kehyksen lisäksi tietolähteiden ja tietojen olisi oltava merkityksellisiä, objektiivisia, luotettavia, todennettavia ja julkisia tai muutoin helposti saatavilla, jotta voidaan määrittää, voidaanko 46 artiklan mukaista välinettä käyttää tehokkaasti[56]. On myös arvioitava, täyttyvätkö edellä esitetyt kriteerit, ja on dokumentoitava, että ne täyttyvät tai eivät täyty.

Merkityksellisyys: Tietojen on oltava tietyn siirron ja/tai tuojan kannalta merkityksellisiä, niiden on täytettävä unionin oikeudessa määritetyt ja yleisen tietosuoja-asetuksen 46 artiklan mukaista siirtovälinettä koskevat vaatimukset, eivätkä ne saa olla liian yleisluonteisia tai abstrakteja.

---

[53] Ks. 45–47 kohta.

[54] Laadittavien raporttien on sisällettävä kattavat tiedot lainsäädännön ja käytäntöjen oikeudellisesta arvioinnista ja siitä, miten niitä sovelletaan tiettyihin siirtoihin, sisäisestä menettelystä, jonka mukaan arviointi on laadittu (myös tiedot arviointiin osallistuneista toimijoista eli lakiasiaintoimistoista, konsulteista tai sisäisistä osastoista), sekä päivämäärät, joina tarkistukset on tehty. Viejän laillisen edustajan on hyväksyttävä nämä raportit.

[55] Sen osoittaminen, ettei ongelmallista lainsäädäntöä sovelleta käytännössä siirrettäviin tietoihin ja tuojaan, kun otetaan huomioon myös muiden samalla alalla ja/tai sellaisella alalla, jossa käsitellään henkilötietojen siirtämistä samalla tavalla, toimivien toimijoiden kokemukset, ei vapauta toimijaa toteuttamasta tarvittavia lisätoimenpiteitä, jotta henkilötietoja voidaan suojata, kun niitä siirretään kohteena olevaan kolmanteen maahan ja käsitellään siellä (ts. tietojen salaaminen päästä päähän – ks. liitteestä 2 esimerkkejä teknisistä täydentävistä toimista), jos kohteena olevan kolmannen maan sovellettavan lainsäädännön analyysi osoittaa, että tietoihin voi päästä käsiksi siirron aikana ilman tuojan toimiakin. Tällaisia toimia on jo voitu suunnitella, jos tuoja toimii myös rekisterinpitäjänä tai henkilötietojen käsittelijänä yleisen tietosuoja-asetuksen 32 artiklan mukaisesti.

[56] Ks. liitteestä 3 esimerkinomainen luettelo tietolähteistä, joita tietojen viejä ja tuoja voivat käyttää.

Objektiivisuus: Sellainen tieto, jota tukee aiemmin saatuun tietoon perustuva empiirinen näyttö ja joka ei perustu oletuksiin mahdollisista tapahtumista ja riskeistä.

Luotettavuus: Tietojen viejän ja tuojan on objektiivisesti arvioitava tietolähteen ja varsinaisten tietojen luotettavuus, ja kummankin osatekijän luotettavuus on arvioitava erikseen.

Todennettavuus: Tiedot ja päätelmät olisi voitava todentaa tai niitä olisi voitava verrata muuntyyppisiin tietolähteisiin osana kokonaisarviointia, jotta myös toimivaltainen valvonta- tai oikeusviranomainen voi tarkistaa tietojen objektiivisuuden ja luotettavuuden tarvittaessa.

Julkinen tai muutoin helposti saatavilla oleva tieto: Tiedon olisi oltava mieluiten julkista tai ainakin muutoin helposti saatavilla, jotta edellä esitetyt kriteerit voidaan todentaa ja jotta voidaan varmistaa, että tieto on mahdollista jakaa valvontaviranomaisille, oikeusviranomaisille ja myös rekisteröidyille.

47. Kannattaa myös ottaa huomioon tuojan dokumentoima käytännön kokemus kolmannen maan viranomaisilta aiemmin vastaanotetuista pyynnöistä saada pääsy tietoihin. Tuojan kokemusta voi käyttää vain lisätiedon lähteenä, jos kolmannen maan oikeudellinen kehys ei estä tuojaa antamasta tietoja viranomaisten tietojen luovuttamista koskevien pyyntöjen perusteella tai ilman niitä (ja tämä olisi myös dokumentoitava arvioinnissa). On kuitenkin muistettava, että pelkästään sitä, ettei tuoja ole saanut tietojen luovutuspyyntöjä aikaisemmin, ei voida koskaan pitää ratkaisevana tekijänä, kun arvioidaan yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen tehokkuutta siltä kannalta, voidaanko siirto toteuttaa ilman lisätoimenpiteitä. Nämä tiedot voidaan ottaa huomioon muista tietolähteistä saatujen toisentyyppisten tietojen rinnalla osana kolmannen maan lakeja ja käytäntöjä koskevaa kokonaisarviointia kyseisen siirron yhteydessä. Tuojan asiaan liittyvä ja dokumentoitu kokemus olisi vahvistettava, eikä se saa olla ristiriidassa sen asiaankuuluvan, objektiivisen, luotettavan, todennettavan ja julkisesti tai muutoin saatavilla olevan tiedon kanssa, joka koskee asianmukaisen lain soveltamista käytännössä (esim. tieto siitä, ovatko muut samalla alalla ja/tai sellaisella alalla, jossa käsitellään henkilötietojen siirtämistä samalla tavalla, toimivat toimijat saaneet tietoihin pääsyä koskevia pyyntöjä vai eivät[57], ja/tai lain soveltamista käytännössä koskeva tiedot, joita saadaan oikeuskäytännöstä ja riippumattomien valvontaelinten laatimista raporteista).

Arvioinnin tulokset

48. Tämä kokonaisarviointi, joka koskee tuojan kolmannen maan lakien ja käytäntöjen soveltamista tiettyyn siirtoon, on tehtävä asianmukaisen huolellisesti, ja se on dokumentoitava perusteellisesti. Toimivaltaiset valvonta- ja/tai oikeusviranomaiset voivat vaatia sitä ja pitää viejää vastuussa kaikista tällä perusteella tekemistään päätöksistä[58].

49. Arviointi voi loppujen lopuksi osoittaa, että yleisen tietosuoja-asetuksen 46 artiklan mukaisella käytettävällä tiedonsiirtovälineellä

[57] Tällaista kokemusta voidaan saada esimerkiksi muista yhteisöistä, jotka viejä tuntee ennestään aiemmin toteuttamiensa samantyyppisten siirtojen perusteella, tai oikeuskäytännöstä, kansalaisjärjestöjen raporteista jne. (ks. liite 3).

[58] Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta.

- varmistetaan tehokkaasti, että siirrettävät henkilötiedot saavat kolmannessa maassa suojan tason, joka vastaa pääosiltaan Euroopan talousalueella taattua suojan tasoa. Siirtoon sovellettavalla kolmannen maan lainsäädännön ja sovellettavien käytäntöjen perusteella tietojen tuoja voi noudattaa velvollisuuksiaan valitun tiedonsiirtovälineen mukaisesti. Arviointi olisi tehtävä uudelleen asianmukaisin väliajoin tai silloin, kun esiin tulee merkittäviä muutoksia (ks. vaihe 6).

- ei varmisteta tehokkaasti pääosiltaan vastaavaa suojan tasoa. Tietojen tuoja ei voi noudattaa velvollisuuksiaan, koska kolmannen maan lainsäädäntö ja/tai käytännöt, joita siirtoon sovelletaan, eivät täytä EU:n perusoikeuksia ja vapauksia sekä niiden rajoittamisen välttämättömyyttä ja oikeasuhteisuutta koskevia vaatimuksia, joiden tavoitteena on turvata oikeutettu yleinen etu. Unionin tuomioistuin korosti, että kun yleisen tietosuoja-asetuksen 46 artiklan mukaiset tiedonsiirtovälineet eivät riitä, tietojen viejän on joko otettava käyttöön riittäviä lisätoimenpiteitä tai oltava siirtämättä henkilötietoja[59].

Esimerkki:

Tausta:
Unionin tuomioistuin totesi esimerkiksi, että Yhdysvaltain ulkomaantiedustelun valvonnasta annetun lain (Foreign Intelligence Surveillance Act (FISA)) 702 § ei täytä niitä vähimmäisvaatimuksia, jotka unionin oikeudessa liittyvät suhteellisuusperiaatteeseen, eikä siten voida katsoa, että se olisi rajattu vain täysin välttämättömään. Tämä tarkoittaa, että FISA-lain 702 §:ään perustuvien ohjelmien suojan taso ei vastaa pääosiltaan EU:n lainsäädännössä edellytettyjä suojatoimia.

Arviointi:
Jos Yhdysvaltain kyseisen lainsäädännön arviointi antaa aihetta olettaa, että tietty siirto saattaa kuulua FISA-lain 702 §:n soveltamisalaan, mutta jos on epäselvää, sovelletaanko tätä lakia kuitenkaan käytännössä, toimintavaihtoehdot ovat seuraavat:

1. Siirron keskeyttäminen.
2. Sellaisten asianmukaisten lisätoimenpiteiden toteuttaminen, joilla siirrettäville tiedoille varmistetaan tehokkaasti pääosiltaan Euroopan talousalueella taattua suojaa vastaava suojan taso.
3. Muiden objektiivisten, luotettavien, merkityksellisten, todennettavien ja mieluiten julkisesti saatavilla olevien tietojen etsiminen (niihin voivat sisältyä myös tietojen tuojan toimittamat tiedot), jotta voidaan selventää, sovelletaanko FISA-lain 702 §:ää tiettyyn siirtoon käytännössä. Näiden tietojen avulla pitäisi saada vastaus esimerkiksi seuraaviin tärkeisiin kysymyksiin:

- Osoittavatko julkisesti saatavilla olevat tiedot, että tietojen antaminen tietystä pyynnöstä, joka koskee pääsyä vastaanotettuihin tietoihin, on kielletty laissa ja että yleisluonteisten tietojen antamista pyynnöistä, jotka koskevat pääsyä vastaanotettuihin tietoihin, tai siitä, ettei tällaisia pyyntöjä ole vastaanotettu, on rajoitettu laajasti?

- Onko tietojen tuoja vahvistanut, että se on saanut aikaisemmin Yhdysvaltojen viranomaisilta pääsyä tietoihin koskevia pyyntöjä? Tai onko tietojen tuoja vahvistanut, ettei se ole saanut aikaisemmin

[59] Euroopan unionin tuomioistuimen asiassa C-311/18 (Schrems II) antaman tuomion 134 ja 135 kohta.

Yhdysvaltojen viranomaisilta pyyntöjä, jotka koskevat pääsyä tietoihin, ja ettei tietojen antamista tällaisista pyynnöistä tai siitä, ettei niitä ole vastaanotettu, ole kielletty?

- Osoittavatko julkisesti saatavilla olevat tiedot, jotka ovat peräisin Yhdysvaltojen oikeuskäytännöstä ja valvontaelinten, kansalaisjärjestöjen ja tutkimuslaitosten laatimista raporteista[60], että tietojen tuojat, jotka toimivat samalla alalla kuin kyseinen tuoja, ovat vastaanottaneet pyyntöjä saada pääsy tietoihin samankaltaisten siirrettyjen tietojen yhteydessä aikaisemmin?

Kokonaisarvioinnin aikana näihin kysymyksiin saatujen vastausten perusteella voidaan päätellä seuraavaa:

- FISA-lain 702 §:ää sovelletaan kyseiseen siirtoon käytännössä, joten se heikentää yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen tehokkuutta. Jos siirto halutaan tehdä, on selvitettävä, tarvittaessa yhteistyössä tuojan kanssa, voidaanko toteuttaa lisätoimenpiteitä, joilla varmistetaan tehokkaasti, että siirrettävien tietojen suoja vastaa pääosiltaan Euroopan talousalueella taatun suojan tasoa. Jos tehokkaita lisätoimenpiteitä ei voida määrittää, henkilötietoja ei saa siirtää.
Tai
- FISA-lain 702 §:ää ei sovelleta kyseiseen siirtoon käytännössä, joten se ei heikennä yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen tehokkuutta. Siirto voidaan toteuttaa ilman lisätoimenpiteitä.

2.4 Vaihe 4: Lisätoimenpiteiden hyväksyntä

50. Jos vaiheessa 3 tarkoitetusta arvioinnista on käynyt ilmi, että yleisen tietosuoja-asetuksen 46 artiklan mukainen valittu tiedonsiirtoväline ei ole tehokas, tietojen viejän on pohdittava tarvittaessa yhteistyössä tuojan kanssa, onko olemassa lisätoimenpiteitä, jotka voidaan lisätä tiedonsiirtovälineisiin kuuluviin suojatoimiin ja varmistaa siten, että siirrettävät henkilötiedot saavat kolmannessa maassa hyväkseen suojan tason, joka pääosiltaan vastaa unionissa taattua suojan tasoa[61]. Määritelmänsä mukaan ”lisätoimenpiteet” täydentävät suojatoimia, jotka jo taataan yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen ja muiden yleisessä tietosuoja-asetuksessa säädettyjen, mahdollisesti sovellettavien tietoturvavaatimusten (esimerkiksi teknisten tietoturvatoimien) avulla.[62]

51. Tietojen viejän on yksilöitävä tapauskohtaisesti, mitkä lisätoimenpiteet voisivat olla tehokkaita tiettyyn kolmanteen maahan tehtävissä siirroissa, kun käytetään tiettyä yleisen tietosuoja-

[60] Esimerkiksi FISA-lain 702 §:n säännökset; ulkomaantiedustelun valvonnasta vastaavan tuomioistuimen (FISC) menettelytapasäännöt; FISCin muut kuin salassa pidettäväksi määrätyt lausunnot ja päätökset, Yhdysvaltojen tuomioistuinten oikeuskäytäntö; yksityisyyden ja kansalaisvapauksien valvontalautakunnan (PCLOB) raportit ja kuulemisista laaditut pöytäkirjat; tarkastusviranomaisen toimiston laatimat raportit – Yhdysvaltojen oikeusministeriö; NSA:n kansalaisvapauksia ja yksityisyyttä käsittelevän osaston johtajan laatimat raportit; kongressin tutkimuspalvelujen laatimat raportit; Yhdysvaltain kansalaisvapausliiton (ACLU) laatimat raportit.
[61] Asiassa C-311/18 (Schrems II) annetun tuomion 96 kohta.
[62] Yleisen tietosuoja-asetuksen johdanto-osan 109 kappale ja asiassa C-311/18 (Schrems II) annetun tuomion 133 kohta.

asetuksen 46 artiklan mukaista tiedonsiirtovälinettä. Arviointia ei tarvitse toistaa joka kerta, kun tehdään samanlainen siirto, jossa siirretään tietyntyyppisiä tietoja samaan kolmanteen maahan. Jotkin siirrettäväksi suunnitelluista tiedoista voivat edellyttää lisätoimenpiteitä, kun taas jotkin toiset eivät (kun otetaan huomioon kolmannen maan lain virallinen ja/tai käytännön soveltaminen). Myös aiempia vaiheissa 1, 2 ja 3 tehtyjä arviointeja voidaan hyödyntää, ja niissä tehtyjen havaintojen perusteella voidaan tarkistaa, ovatko lisätoimenpiteet mahdollisesti tehokkaita vaaditun suojan tason takaamisessa.

52. Lisätoimenpiteet voivat periaatteessa perustua sopimukseen tai ne voivat olla teknisiä tai organisatorisia. Erilaisten toimenpiteiden yhdistäminen toisiaan tukien ja hyödyntäen voi nostaa suojan tasoa ja edistää siten EU:n vaatimusten täyttämistä.

53. Sopimukseen perustuvilla ja organisatorisilla toimenpiteillä ei yleensä voida antaa kolmannen maan viranomaisille pääsyä henkilötietoihin, jos kolmannen maan lainsäädäntö ja/tai käytännöt ovat ongelmallisia[63]. Joissakin tilanteissa ainoastaan teknisillä toimenpiteillä voidaan estää kolmannen maan viranomaisten pääsy henkilötietoihin tai tehdä siitä tehotonta, etenkin tarkkailutarkoituksissa[64]. Tällaisissa tapauksissa teknisiä toimenpiteitä voidaan täydentää sopimukseen perustuvilla tai organisatorisilla toimenpiteillä ja vahvistaa siten yleistä tietosuojan tasoa (esimerkiksi ottamalla käyttöön tarkastuksia ja automaattisia mekanismeja, joilla estetään viranomaisten yritykset päästä tietoihin EU:n vaatimusten vastaisesti).

54. Tietojen viejä voi tarvittaessa yhteistyössä tietojen tuojan kanssa tarkastella seuraavaa esimerkinomaista tekijöiden luetteloa, jotta voidaan määrittää, millaisilla lisätoimenpiteillä siirrettäviä tietoja voidaan suojata tehokkaimmin viranomaisten pyrkimyksiltä saada pääsy tietoihin käytännössä sovellettavan ongelmallisen lainsäädännön perusteella:

    - siirrettävien tietojen muoto (eli pelkkänä tekstinä / pseudonymisoituna tai salattuna)
    - tietojen luonne (Euroopan talousalueella taataan korkeampi suojan taso yleisen tietosuoja-asetuksen 9 ja 10 artiklan mukaisille tietoryhmille)[65];
    - tietojenkäsittelyn työnkulun pituus ja monimutkaisuus, käsittelyssä mukana olevien toimijoiden määrä ja niiden välinen suhde (esim. se, onko siirroissa mukana useita rekisterinpitäjiä tai sekä rekisterinpitäjiä että henkilötietojen käsittelijöitä tai onko mukana henkilötietojen käsittelijöitä, jotka siirtävät tietoja tietojen viejältä tietojen tuojalle (ottaen

[63] Ilmauksella ”ongelmallinen lainsäädäntö” tarkoitetaan sellaista lainsäädäntöä, joka 1) asettaa Euroopan unionista siirrettävien henkilötietojen vastaanottajalle velvollisuuksia ja/tai vaikuttaa siirrettäviin tietoihin tavalla, joka voi heikentää siirtovälineiden sopimukseen perustuvaa taetta pääosiltaan vastaavasta suojan tasosta ja 2) jossa ei kunnioiteta EU:n perusoikeuskirjassa tunnustettujen perusoikeuksien ja vapauksien keskeistä sisältöä tai joka ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, jotta voidaan turvata jokin tärkeistä tavoitteista, jotka on tunnustettu myös unionin oikeudessa tai EU:n jäsenvaltioiden lainsäädännössä, esimerkiksi ne, jotka on lueteltu yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa.

[64] Jos tällainen pääsy ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[65] Katso alaviite 42.

huomioon niihin kohteena olevan kolmannen maan lainsäädännön mukaisesti sovellettavat asiaankuuluvat säännökset))[66]

- tekniikka tai parametrit, joiden avulla kolmannen maan lakia sovelletaan käytännössä vaiheessa 3 todetun mukaisesti;
- mahdollisuus siihen, että tietoja voidaan siirtää edelleen samassa kolmannessa maassa tai jopa muihin kolmansiin maihin (esim. siten, että siirrossa on mukana tietojen tuojan henkilötietojen alikäsittelijöitä[67]).

Esimerkkejä lisätoimenpiteistä

55. Liitteessä 2 olevissa luetteloissa, jotka eivät ole tyhjentäviä, annetaan esimerkkejä teknisistä, sopimukseen perustuvista ja organisatorisista toimenpiteistä, joiden käyttöä voitaisiin harkita, jos ne eivät jo sisälly yleisen tietosuoja-asetuksen 46 artiklan mukaiseen käytettävään tiedonsiirtovälineeseen.

***

56. Jos tietojen viejä on ottanut käyttöön tehokkaita lisätoimenpiteitä, joilla yhdessä yleisen tietosuoja-asetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen kanssa saavutetaan suojan taso, joka pääosiltaan vastaan Euroopan talousalueella taattua suojan tasoa: siirrot voidaan tehdä.

57. Jos tietojen viejä ei pysty löytämään tai ottamaan käyttöön tehokkaita lisätoimenpiteitä, joilla varmistetaan, että siirrettävät henkilötiedot saavat EU:ssa taattua suojan tasoa pääosiltaan vastaavan suojan tason[68], henkilötietojen siirtämistä kolmanteen maahan ei saa aloittaa yleisen tietosuoja-asetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen perusteella. Jos siirtoja jo tehdään, henkilötietojen siirto on keskeytettävä tai lopetettava[69] . Yleisen tietosuoja-asetuksen 46 artiklan mukaisen käytettävän tiedonsiirtovälineen sisältämien suojatoimien mukaisesti tiedot, jotka on jo siirretty kyseiseen kolmanteen maahan, ja niiden jäljennökset on palautettava tietojen viejälle tai tietojen tuojan on tuhottava ne kokonaisuudessaan[70].

[66] Yleisessä tietosuoja-asetuksessa osoitetaan rekisterinpitäjille ja henkilötietojen käsittelijöille erillisiä velvollisuuksia. Siirtoja voidaan tehdä rekisterinpitäjältä rekisterinpitäjälle, yhteisrekisterinpitäjien välillä, rekisterinpitäjältä henkilötietojen käsittelijälle ja, rekisterinpitäjän luvalla, henkilötietojen käsittelijältä rekisterinpitäjälle tai henkilötietojen käsittelijältä henkilötietojen käsittelijälle.

[67] Ks. alaviite 26.

[68] Jos tällainen pääsy ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[69] Asiassa C-311/18 (Schrems II) annetun tuomion 135 kohta.

[70] Ks. mallisopimuslausekkeita koskevan päätöksen 87/2010 liitteessä oleva lauseke 12, ks. mallisopimuslausekkeita koskevan päätöksen 2004/915/EY liitteessä B oleva (valinnainen) lausekkeiden irtisanomista koskeva lisälauseke.

Esimerkki:

Kolmannen maan lainsäädännössä kielletään tietojen viejän määrittämät lisätoimenpiteet (kielletään esimerkiksi salauksen käyttö) tai tehdään niistä muutoin tehottomia. Henkilötietojen siirtämistä kyseiseen maahan ei saa aloittaa tai kyseiseen maahan käynnissä olevat siirrot on lopetettava.

58. Toimivaltainen viranomainen voi määrätä muita korjaavia toimenpiteitä (esim. sakon), jos tietojen viejä aloittaa siirron huolimatta siitä, että kolmannessa maassa tarjottavan suojan tason ei voida osoittaa vastaavan pääosiltaan unionissa taattua suojan tasoa.

2.5 Vaihe 5: Tehokkaiden lisätoimenpiteiden määrittämistä seuraavat menettelyvaiheet

59. Kun täytäntöön pantavat tehokkaat lisätoimenpiteet on määritetty, sen jälkeen toteutettavat menettelyvaiheet voivat olla erilaisia sen mukaan, mitä yleisen tietosuoja-asetuksen 46 artiklan mukaista tiedonsiirtovälinettä käytetään tai aiotaan käyttää.

2.5.1 Tietosuojaa koskevat vakiolausekkeet (yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c ja d alakohta)

60. Kun tietosuojaa koskevien vakiolausekkeiden lisäksi aiotaan panna täytäntöön lisätoimenpiteitä, toimivaltaiselta valvontaviranomaiselta ei tarvitse pyytää lupaa tällaisten lausekkeiden tai lisäsuojatoimien lisäämiseksi, kunhan ne eivät ole suoraan tai epäsuorasti ristiriidassa tietosuojaa koskevien vakiolausekkeiden kanssa ja riittävät varmistamaan, että yleisellä tietosuoja-asetuksella taattua suojan tasoa ei heikennetä[71]. Tietojen viejän ja tuojan on varmistettava, että lisälausekkeiden ei voida tulkita millään tavalla rajoittavan tietosuojaa koskevissa vakiolausekkeissa olevia oikeuksia ja velvollisuuksia tai millään muulla tavalla alentavan tietosuojan tasoa. Tämä sekä kaikkien lausekkeiden yksiselitteisyys olisi voitava osoittaa osoitusvelvollisuuden periaatteen ja tietosuojan riittävän tason takaamista koskevan tietojen viejän velvollisuuden mukaisesti. Toimivaltaisilla valvontaviranomaisilla on valtuudet tarkastella näitä lisälausekkeita tarvittaessa (esim. valituksen vuoksi tai oma-aloitteisessa tutkinnassa).

61. Jos tietojen viejä aikoo muuttaa tietosuojaa koskevia vakiolausekkeita itse tai jo lisätyt lisätoimenpiteet ovat suoraan tai epäsuorasti ristiriidassa vakiolausekkeiden kanssa, tietojen viejän ei enää katsota noudattavan vakiosopimuslausekkeita[72], ja sen on haettava toimivaltaiselta

[71] Yleisen tietosuoja-asetuksen johdanto-osan 109 kappale: ”Se, että rekisterinpitäjä tai henkilötietojen käsittelijä voi käyttää joko komission tai valvontaviranomaisen hyväksymiä tietosuojaa koskevia vakiolausekkeita, ei saisi estää rekisterinpitäjää tai henkilötietojen käsittelijää sisällyttämästä tietosuojaa koskevia vakiolausekkeita laajempiin sopimuksiin, kuten henkilötietojen käsittelijän toisen henkilötietojen käsittelijän kanssa tekemään sopimukseen, eikä lisäämästä muita lausekkeita tai toteuttamasta muita suojatoimia, kunhan ne eivät ole suoraan tai epäsuorasti ristiriidassa komission tai valvontaviranomaisen hyväksymien vakiosopimuslausekkeiden kanssa eivätkä vaikuta rekisteröidyn perusoikeuksiin tai -vapauksiin.” Samanlaisia säännöksiä annetaan useissa Euroopan komission direktiivin 95/45/EY mukaisesti hyväksymissä tietosuojaa koskevissa vakiolausekkeissa.

[72] Ks. analogisesti Euroopan tietosuojaneuvoston lausunto 17/2020 Slovenian valvontaviranomaisen ehdotuksesta vakiosopimuslausekkeiksi (yleisen tietosuoja- asetuksen 28 artiklan 8 kohta). Sen 28 artiklan mukaisia vakiosopimuslausekkeita koskevassa kohdassa on samanlainen säännös (”Tietosuojaneuvosto

valvontaviranomaiselta lupaa yleisen tietosuoja-asetuksen 46 artiklan 3 kohdan a alakohdan mukaisesti.

2.5.2 Yritystä koskevat sitovat säännöt (yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan b alakohta)

62. Asiassa Schrems II annetussa tuomiossa esitettyä perustelua sovelletaan myös muihin yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan mukaisiin tiedonsiirtovälineisiin, koska kaikki nämä välineet ovat lähtökohtaisesti sopimusluonteisia, joten osapuolten niiden nojalla suunnittelemat takeet ja tekemät sitoumukset eivät voi sitoa kolmannen maan viranomaisia[73].

63. Asiassa Schrems II annettu tuomio pätee yritystä koskevien sitovien sääntöjen perusteella tehtyihin henkilötietoihin siirtoihin, koska kolmansien maiden lait voivat vaikuttaa kyseisillä välineillä tarjottuun suojaan.

64. Kaikki sitoumukset, jotka on sisällytettävä sääntöihin, mainitaan päivitetyn asiakirjan WP256/257 viitteissä[74]. Kaikkien ryhmien, jotka käyttävät yrityksiä koskevia sitovia sääntöjä tiedonsiirtovälineinä, on mukautettava nykyiset ja tulevat yrityksiä koskevat sitovat sääntönsä tämän asiakirjan mukaisesti.

65. Tuomioistuin korosti, että tietojen viejän ja tietojen tuojan velvollisuutena on arvioida, noudatetaanko asianomaisessa kolmannessa maassa unionin oikeudessa edellytettyä tietosuojan tasoa, jotta voidaan määrittää, voidaanko mallisopimuslausekkeilla tai yritystä koskevilla sitovilla säännöillä annettavat takeet täyttää käytännössä. Jos näin ei ole, tietojen viejän olisi arvioitava, voidaanko toteuttaa lisätoimenpiteitä, joilla varmistetaan Euroopan talousalueella taattavaa tietosuojan tasoa pääosiltaan vastaava tietosuojan taso, ja pystyykö kolmannen maan lainsäädäntö tai käytäntö heikentämään näitä lisätoimenpiteitä estämällä niiden tehokkuuden.

2.5.3 Tapauskohtaiset sopimuslausekkeet (yleisen tietosuoja-asetuksen 46 artiklan 3 kohdan a alakohta)

66. Asiassa Schrems II annetussa tuomiossa esitettyä perustelua sovelletaan myös muihin yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan mukaisiin tiedonsiirtovälineisiin, koska kaikki nämä välineet ovat lähtökohtaisesti sopimusluonteisia, joten osapuolten niiden nojalla suunnittelemat takeet ja tekemät sitoumukset eivät voi sitoa kolmannen maan viranomaisia[75]. Asiassa Schrems II annettu tuomio pätee näin ollen tapauskohtaisten sopimuslausekkeiden perusteella tehtyihin

---

muistuttaa lisäksi, että mahdollisuus käyttää valvontaviranomaisen hyväksymiä vakiosopimuslausekkeita ei estä osapuolia lisäämästä muita lausekkeita tai täydentäviä suojatoimia, mikäli ne eivät ole suoraan tai välillisesti ristiriidassa hyväksyttyjen vakiosopimuslausekkeiden kanssa tai vaikuta rekisteröityjen perusoikeuksiin ja -vapauksiin. Jos taas tietosuojaa koskevia vakiolausekkeita muokataan, osapuolten ei enää katsota panneen täytäntöön hyväksyttyjä vakiosopimuslausekkeita"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

[73] EUT, C-311/18 (Schrems II), 132 kohta.

[74] 29 artiklan mukaisen tietosuojatyöryhmän valmisteluasiakirja, jossa esitetään taulukko niistä seikoista ja periaatteista, joita yrityksiä koskevien sitovien sääntöjen on sisällettävä, sellaisena kuin se on viimeksi tarkistettuna ja hyväksyttynä 6. helmikuuta 2018, WP 256 rev.01; 29 artiklan mukaisen tietosuojatyöryhmän valmisteluasiakirja, jossa esitetään taulukko niistä seikoista ja periaatteista, joita yrityksiä koskevien sitovien sääntöjen on sisällettävä, sellaisena kuin on viimeksi tarkistettuna ja hyväksyttynä 6. helmikuuta 2018, WP 257 rev.01.

[75] EUT, C-311/18 (Schrems II), 132 kohta.

henkilötietojen siirtoihin, koska kolmansien maiden lait voivat vaikuttaa kyseisillä välineillä tarjottuun suojaan.

2.6 Vaihe 6: Uudelleenarviointi säännöllisin väliajoin

67. Tietojen viejän on seurattava jatkuvasti ja tarvittaessa tietojen tuojien kanssa henkilötietojen siirron kohteena olevassa kolmannessa maassa tapahtuvaa kehitystä, joka voi vaikuttaa alkuperäiseen arviointiin suojan tasosta ja sen perusteella tehtyihin päätöksiin siirroista. Osoitusvelvollisuus on jatkuva (yleisen tietosuoja-asetuksen 5 artiklan 2 kohta).

68. Käyttöön on otettava riittävän vankat mekanismit, joilla varmistetaan, että siirrot keskeytetään tai lopetetaan viipymättä, jos

    - tietojen tuoja on rikkonut yleisen tietosuoja-asetuksen 46 artiklan mukaisessa tiedonsiirtovälineessä tekemiään sitoumuksia tai ei pysty noudattamaan niitä tai
    - lisätoimenpiteet eivät ole enää tehokkaita kyseisessä kolmannessa maassa.

3 PÄÄTELMÄT

69. Yleisessä tietosuoja-asetuksessa esitetään säännöt henkilötietojen käsittelylle Euroopan talousalueella ja sallitaan niiden perusteella henkilötietojen vapaa liikkuminen Euroopan talousalueella. Yleisen tietosuoja-asetuksen V luku koskee henkilötietojen siirtoja kolmansiin maihin, ja siinä rima asetetaan korkealle: siirto ei saa heikentää yleisellä tietosuoja-asetuksella taattua luonnollisten henkilöiden suojan tasoa (yleisen tietosuoja-asetuksen 44 artikla). Unionin tuomioistuimen asiassa C-311/18 (Schrems II) antamassa tuomiossa korostetaan, että yleisellä tietosuoja-asetuksella annetun suojan tason jatkuvuus on varmistettava, kun henkilötietoja siirretään kolmanteen maahan[76].

70. Jotta tiedoille voidaan varmistaa unionissa taattua tasoa pääosiltaan vastaava suojan taso, siirrot on ensinnäkin tunnettava läpikotaisin. Lisäksi on tarkistettava, että siirrettävät tiedot ovat asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista niiden käsittelyn kannalta.

71. Myös tiedonsiirtoväline, jota siirroissa käytetään, on yksilöitävä. Jos tiedonsiirtoväline ei ole riittävyyttä koskeva päätös, on tarkistettava tapauskohtaisesti, heikentääkö kohteena olevan kolmannen maan laki tai käytäntö yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen sisältämiä suojatoimia omien siirtojen yhteydessä (vai ei). Jos pelkästään yleisen tietosuoja-asetuksen 46 artiklan mukaisella tiedonsiirtovälineellä ei pystytä saavuttamaan EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa siirrettäville henkilötiedoille, puutteet voidaan korjata lisätoimenpiteillä.

72. Jos tietojen viejä ei pysty löytämään tai ottamaan käyttöön tehokkaita lisätoimenpiteitä, joilla varmistetaan, että siirrettävät henkilötiedot saavat pääosiltaan vastaavan suojan tason, henkilötietojen siirtämistä kolmanteen maahan ei saa aloittaa valitun tiedonsiirtovälineen perusteella. Jos siirtoja jo tehdään, henkilötietojen siirto on keskeytettävä tai lopetettava viipymättä.

[76] C-311/18 (Schrems II), 93 kohta.

73. Toimivaltaisella valvontaviranomaisella on valtuudet keskeyttää tai lopettaa henkilötietojen siirrot kolmanteen maahan, jos EU:n lainsäädännössä, erityisesti yleisen tietosuoja-asetuksen 45 ja 46 artiklassa ja perusoikeuskirjassa, vaadittua siirrettävien tietojen suojaa ei voida varmistaa.

Euroopan tietosuojaneuvosto
Puheenjohtaja
(Andrea Jelinek)

LIITE 1: MÄÄRITELMÄT

- ’Kolmas maa’ tarkoittaa mitä tahansa maata, joka ei ole Euroopan talousalueen jäsenvaltio.
- ’ETA’ tarkoittaa Euroopan talousaluetta, ja siihen kuuluvat Euroopan unionin jäsenvaltiot sekä Islanti, Norja ja Liechtenstein. Viimeksi mainittuihin sovelletaan yleistä tietosuoja-asetusta ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37 nojalla.
- ’Yleinen tietosuoja-asetus’ tarkoittaa luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679.
- ’Perusoikeuskirja’ tarkoittaa Euroopan unionin perusoikeuskirjaa, EUVL C 326, 26.10.2012, s. 391–407.
- ’EUT’ tai ’unionin tuomioistuin’ tarkoittaa Euroopan unionin tuomioistuinta. Se on Euroopan unionin oikeusviranomainen, ja se varmistaa yhteistyössä jäsenvaltioiden tuomioistuinten kanssa EU:n lainsäädännön yhdenmukaisen soveltamisen ja tulkinnan.
- ’Tietojen viejä’ tarkoittaa Euroopan talousalueella sijaitsevaa rekisterinpitäjää tai henkilötietojen käsittelijää, joka siirtää henkilötietoja kolmannessa maassa olevalle rekisterinpitäjälle tai henkilötietojen käsittelijälle.
- ’Tietojen tuoja’ tarkoittaa kolmannessa maassa olevaa rekisterinpitäjää tai henkilötietojen käsittelijää, joka vastaanottaa Euroopan talousalueelta siirretyt henkilötiedot tai saa niihin pääsyn.
- ”Yleisen tietosuoja-asetuksen 46 artiklan mukainen tiedonsiirtoväline” tarkoittaa yleisen tietosuoja-asetuksen 46 artiklan mukaisia asianmukaisia suojatoimia, jotka tietojen viejien on otettava käyttöön siirtäessään henkilötietoja kolmanteen maahan, jos yleisen tietosuoja-asetuksen 45 artiklan 3 kohdan mukaista riittävyyttä koskevaa päätöstä ei ole. Yleisen tietosuoja-asetuksen 46 artiklan 2 ja 3 kohdassa on luettelo yleisen tietosuoja-asetuksen 46 artiklan mukaisista tiedonsiirtovälineistä, joita rekisterinpitäjät ja henkilötietojen käsittelijät voivat käyttää.
- ”Vakiosopimuslausekkeet” (tai ”mallisopimuslausekkeet”) ovat Euroopan komission hyväksymiä tietosuojaa koskevia vakiolausekkeita, joita käytetään henkilötietojen siirroissa Euroopan talousalueella sijaitsevien rekisterinpitäjien tai henkilötietojen käsittelijöiden välillä sekä Euroopan talousalueen ulkopuolella sijaitsevien rekisterinpitäjien tai henkilötietojen käsittelijöiden välillä. Euroopan komission hyväksymät tietosuojaa koskevat vakiolausekkeet ovat yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohdan ja 5 kohdan mukainen tiedonsiirtoväline.

LIITE 2: ESIMERKKEJÄ LISÄTOIMENPITEISTÄ

74. Seuraavat toimenpiteet ovat esimerkkejä lisätoimenpiteistä, joita voidaan harkita vaiheessa 4 ”Lisätoimenpiteiden hyväksyntä”. Tämä luettelo ei ole tyhjentävä. Myös muita lisätoimenpiteitä voidaan harkita. Tuleva teknologinen, lainopillinen tai organisatorinen kehitys voi johtaa siihen, että harkittavaksi tulee uusia lisätoimenpiteitä. Yhden tai useamman tällaisen toimenpiteen valitseminen ja täytäntöönpano ei välttämättä ja aina varmista, että täytetään EU:n lainsäädännön vaatimus siitä, että siirto vastaa pääosiltaan siinä taattua suojan tasoa. On valittava sellaiset lisätoimenpiteet, joilla siirroille voidaan taata tämäntasoinen suoja tehokkaasti.

75. Lisätoimenpide voidaan katsoa unionin tuomioistuimen asiassa Schrems II annetussa tuomiossa tarkoitetulla tavalla tehokkaaksi vain ja siinä määrin kuin sillä – joko yksinään tai muihin toimenpiteisiin yhdistettynä – puututaan erityisiin puutteisiin, joita on havaittu tietojen viejän kolmannen maan tilanteesta tekemässä arvioinnissa kolmannen maan lakien ja käytäntöjen osalta. Jos EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa ei viime kädessä voida varmistaa, henkilötietoja ei saa siirtää.

76. Rekisterinpitäjältä tai henkilötietojen käsittelijältä voidaan jo edellyttää joidenkin tässä liitteessä kuvattujen toimenpiteiden toteuttamista, jotta ne täyttäisivät yleisen tietosuoja-asetuksen vaatimukset. Tämä tarkoittaa sitä, että samanlaisia toimenpiteitä voidaan joutua ottamaan käyttöön, kun henkilötietoja käsitellään Euroopan talousalueella tai siirretään tietojen tuojalle riittävyyttä koskevan päätöksen nojalla taikka muihin kolmansiin maihin.[77]

2.1 Tekniset toimenpiteet

77. Tässä jaksossa annetaan esimerkkejä teknisistä toimenpiteistä, joilla voidaan täydentää yleisen tietosuoja-asetuksen 46 artiklan mukaisissa tiedonsiirtovälineissä olevia suojatoimia, jotta voidaan varmistaa EU:n lainsäädännössä edellytetyn suojan tason noudattaminen siirrettäessä henkilötietoja kolmanteen maahan. Luettelo ei ole tyhjentävä. Näitä toimenpiteitä tarvitaan erityisesti silloin, jos kyseisen kolmannen maan lainsäädännössä asetetaan tietojen tuojalle velvollisuuksia, jotka ovat yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden vastaisia ja siis omiaan heikentämään sopimukseen perustuvaa taetta pääosiltaan vastaavasta suojan tasosta mainitun kolmannen maan viranomaisten näihin tietoihin pääsyä vastaan[78].

78. Selkeyden vuoksi tässä osiossa annetaan ensin muutamia esimerkkejä skenaarioista, joissa jotkin tekniset toimenpiteet voivat olla tehokkaita pääosiltaan vastaavan suojan tason varmistamiseksi. Sen jälkeen tässä osiossa kuvataan skenaarioita, joita varten ei ole määritetty tämäntasoisen suojan varmistamiseen tarkoitettuja teknisiä toimenpiteitä.

[77] Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 32 artikla.
[78] C-311/18 (Schrems II), 135 kohta.

Esimerkkejä sellaisiin tapauksiin liittyvistä skenaarioista, joita varten on *tehokkaita* toimenpiteitä

79. Jäljempänä luetelluilla toimenpiteillä on tarkoitus varmistaa, että kolmannen maan viranomaisten pääsy siirrettyihin tietoihin ei heikennä yleisen tietosuoja-asetuksen 46 artiklan tiedonsiirtovälineiden sisältämien asianmukaisten suojatoimien tehokkuutta. Nämä toimenpiteet olisivat tarpeen, jotta voidaan taata Euroopan talousalueella taattua suojaa pääosiltaan vastaava suojan taso, vaikka viranomaisille annettu pääsy tietoihin olisi tuojan maan lainsäädännön mukaista ja vaikka käytännössä tämä pääsy ylittäisi sen, mikä on välttämätöntä ja oikeasuhteista demokraattisessa yhteiskunnassa[79]. Toimenpiteiden tavoitteena on sulkea pois mahdollinen oikeuksia loukkaava pääsy estämällä viranomaisia tunnistamasta rekisteröityjä, päättelemästä heitä koskevia tietoja, erottamasta tietoja toisessa yhteydessä tai yhdistämästä siirrettyjä tietoja toisiin tietokokonaisuuksiin, joita viranomaisilla voi olla hallussaan ja jotka voivat sisältää muiden tietojen muassa rekisteröityjen muissa yhteyksissä käyttämistä laitteista, sovelluksista, välineistä ja protokollista saatuja verkkotunnisteita.

80. Kolmansien maiden viranomaiset voivat yrittää päästä siirrettyihin tietoihin,

    a) kun tiedot ovat liikkeessä, pääsemällä käsiksi viestiyhteyksiin, joilla tietoja siirretään vastaanottajamaahan. Tämä pääsy voi olla passiivista, jolloin viestinnän sisältö vain jäljennetään, mahdollisesti valintaprosessin jälkeen. Pääsy voi kuitenkin myös olla aktiivista siinä mielessä, että viranomaiset tulevat mukaan viestintäprosessiin sekä lukemalla sisällön että peukaloimalla tai poistamalla sen osia

    b) kun tiedot ovat aiotun vastaanottajan hallussa, joko pääsemällä käsiksi itse tietojenkäsittelyjärjestelmään tai vaatimalla tietojen vastaanottajaa paikallistamaan niitä kiinnostavat tiedot, ottamaan ne talteen ja luovuttamaan viranomaisille.

81. Tässä jaksossa käsitellään tilanteita, joissa sovelletaan molemmissa tapauksissa tehokkaita toimenpiteitä. Tietyissä konkreettista siirtoa koskevissa olosuhteissa voidaan soveltaa erilaisia lisätoimenpiteitä, jotka voivat olla riittäviä, jos vastaanottajamaan lainsäädännössä säädetään vain yhdentyyppisestä pääsystä tietoihin. Siksi tietojen viejän on analysoitava huolellisesti – tietojen tuojan tuella – tuojalle koituvat velvollisuudet.

Esimerkiksi yhdysvaltalaisilla tietojen tuojilla, jotka kuuluvat FISA-lain 702 §:n (50 USC § 1881a) soveltamisalaan, on suora velvoite myöntää pääsy niiden hallussa, hoidossa tai valvonnassa oleviin tuotuihin henkilötietoihin tai luovuttaa ne. Tätä velvoitetta voidaan laajentaa kaikkiin salausavaimiin, joita tarvitaan, jotta tietoja voidaan lukea.

82. Näissä skenaarioissa kuvataan tiettyjä olosuhteita ja toteutettuja toimenpiteitä esimerkkeinä. Kaikki skenaarioissa tapahtuvat muutokset voivat johtaa erilaisiin päätelmiin. Skenaarioissa kuvataan tilanteita, joissa on todettu, että lisätoimenpiteet ovat ehdottomasti tarpeen,

[79] Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020.

esimerkiksi silloin, kun kolmannen maan ongelmallista lainsäädäntöä sovelletaan käytännössä kyseiseen siirtoon.

83. Rekisterinpitäjien on ehkä sovellettava joitakin tai kaikkia tässä kuvattuja toimenpiteitä riippumatta tietojen tuojaan sovellettavien lakien tarjoamasta suojan tasosta, koska niiden on noudatettava yleisen tietosuoja-asetuksen 25 ja 32 artiklaa siirron konkreettisissa olosuhteissa. Toisin sanoen tietojen viejien on ehkä pitänyt jo panna täytäntöön joitakin tässä asiakirjassa kuvattuja toimenpiteitä, vaikka tietojen tuojiin sovellettaisiin riittävyyttä koskevaa päätöstä, samalla tavoin kuin rekisterinpitäjien ja henkilötietojen käsittelijöiden on ehkä pitänyt panna niitä täytäntöön käsiteltäessä tietoja Euroopan talousalueella.

Esimerkkitapaus 1: Tietojen säilyttäminen varmuuskopiointia ja muita sellaisia tarkoituksia varten, joissa itse tietoihin ei tarvitse päästä

84. Tietojen viejä käyttää kolmannessa maassa säilytyspalvelujen tarjoajaa henkilötietojen säilyttämiseen esimerkiksi varmuuskopiointia varten.

Jos

1. henkilötietoja käsitellään käyttämällä vahvaa salausta ennen siirtämistä ja tuojan henkilöllisyys todennetaan,
2. salausalgoritmi ja sen parametrisointi (esim. avaimen pituus, toimintatapa soveltuvin osin) ovat uusimman tekniikan mukaisia ja ne voidaan katsoa kestäviksi vastaanottajamaan viranomaisten tekemää kryptoanalyysia vastaan viranomaisten käytössä olevat resurssit ja tekniset valmiudet (esim. tietojenkäsittelyteho väsytyshyökkäyksissä) huomioon ottaen[80],
3. salauksen vahvuudessa ja avaimen pituudessa otetaan huomioon tietty jakso, jonka ajan salattujen henkilötietojen luottamuksellisuus on säilytettävä[81],
4. salausalgoritmi otetaan asianmukaisesti käyttöön kunnolla ylläpidetyllä ohjelmistolla, jossa ei ole tunnettuja haavoittuvuuksia ja jonka on varmennettu olevan valitun algoritmin spesifikaation mukainen esimerkiksi sertifioinnilla,

---

[80] Arvioidessaan salausalgoritmien vahvuutta ja sitä, ovatko ne uusimman tekniikan mukaisia ja kestäviä kryptoanalyysia vastaan ajan kuluessa, tietojen viejät voivat hyödyntää teknisiä ohjeita, joita EU:n ja sen jäsenvaltioiden viralliset kyberturvallisuusviranomaiset ovat julkaisseet. Ks. esimerkiksi ENISAn raportti ”What is ’state of the art’ in IT security? ”, 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; Saksan tietoturvaviraston TR-02102-sarjan teknisissä ohjeissaan antama ohjeistus ja raportti ”Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018” osoitteessa https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Salausalgoritmien suojauskyky heikkenee ajan myötä. Se johtuu uusien kryptoanalyyttisten tekniikoiden ja uusien laskentaparadigmojen, kuten kvanttilaskennan, kehittämisestä sekä siitä, että käytettävissä oleva laskentateho kasvaa yleisesti, ellei voida osoittaa, että sovellettavat algoritmit ovat tietoteoreettisesti turvallisia. Tämä huolenaihe koskee etenkin julkisten avainten algoritmeja, jotka ovat tätä kirjoitettaessa yleisessä käytössä. Näin ollen tietojen viejän on otettava huomioon, että viranomaiset voivat yrittää päästä salattuihin tietoihin kohdassa 80 kuvatuissa olosuhteissa ja säilyttää tietoja siihen saakka, kunnes niillä on riittävät resurssit salauksen purkamiseen. Lisätoimenpidettä voidaan pitää tehokkaana vain, jos tällainen salauksen purkaminen ja sitä aikanaan seuraava tietojen käsittely ei enää loukkaisi rekisteröityjen oikeuksia vaikkapa siksi, ettei heitä voida enää yksilöidä suoraan tai epäsuorasti tietojen avulla.

5. avaimia hallinnoidaan (luodaan, jaetaan, säilytetään, tarvittaessa yhdistetään aiotun vastaanottajan henkilöllisyyteen ja kumotaan) luotettavasti [82], ja
6. avaimia säilytetään yksinomaan tietojen viejän valvonnassa tai sellaisen yhteisön valvonnassa, joille viejä on antanut tämän tehtäväksi ja jotka sijaitsevat Euroopan talousalueella tai sellaisella lainkäyttöalueella, jossa on Euroopan talousalueella taattua suojaa pääosiltaan vastaava suojan taso,

Euroopan tietosuojaneuvosto katsoo, että tehty salaus on tehokas lisätoimenpide.

Esimerkkitapaus 2: Pseudonymisoitujen tietojen siirto

85. Tietojen viejä pseudonymisoi ensin hallussaan olevat tiedot ja siirtää ne sitten kolmanteen maahan analysoitavaksi esimerkiksi tutkimusta varten.

Jos

1. tietojen viejä siirtää käsitellyt henkilötiedot siten, että henkilötietoja ei voi enää yhdistää tiettyyn rekisteröityyn eikä käyttää erottamaan rekisteröityä suuremmasta ryhmästä ilman lisätietoja[83],
2. lisätietoja säilytetään yksinomaan tietojen viejän valvonnassa ja niitä pidetään erillään jäsenvaltiossa tai kolmannessa maassa sellaisen yhteisön valvonnassa, jolle viejä on antanut tämän tehtäväksi, Euroopan talousalueella tai sellaisella lainkäyttöalueella, jossa on Euroopan talousalueella taattua suojaa pääosiltaan vastaava suojan taso,
3. kyseisten lisätietojen luovuttaminen tai luvaton käyttö estetään asianmukaisilla teknisillä ja organisatorisilla suojatoimilla ja varmistetaan, että algoritmi tai rekisteri, jonka avulla uudelleentunnistus voidaan tehdä lisätietojen avulla, on yksinomaan tietojen viejän valvonnassa, ja
4. rekisterinpitäjä on vahvistanut kyseessä olevien tietojen perusteellisen analyysin avulla ja ottaen huomioon kaikki tiedot, joita vastaanottajamaan viranomaisilla voidaan olettaa olevan hallussaan ja käyttävän, että pseudonymisoituja henkilötietoja ei voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, vaikka kyseisiä tietoja vertailtaisiin keskenään,

Euroopan tietosuojaneuvosto katsoo, että tehty pseudonymisointi on tehokas lisätoimenpide.

---

[82] NIST Special Publication 800-57, Recommendation for Key Management https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] Yleisen tietosuoja-asetuksen 4 artiklan 5 kohta: "'pseudonymisoimisella' [tarkoitetaan] henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu." Lisätiedot voivat olla taulukoita, joissa esitetään vierekkäin pseudonyymit ja yksilöivät attribuutit, jotka niillä korvataan, salausavaimet tai muita parametreja, joita attribuuttien muuntamisessa käytetään, taikka muita tietoja, joiden avulla pseudonymisoidut tiedot voidaan liittää tunnistettuihin tai tunnistettavissa oleviin luonnollisiin henkilöihin.

86. On pantava merkille, että useissa tilanteissa luonnollinen henkilö voidaan tunnistaa henkilön fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän, fyysisen sijainnin tai verkkopohjaisessa palvelussa tietyllä hetkellä toteutetun vuorovaikutuksen perusteella[84], vaikka hänen nimeään, osoitettaan tai muita selkeitä tunnisteita ei olisi.

87. Tämä pätee erityisesti silloin, kun tiedot koskevat tietopalvelujen käyttöä (käyttöaika, käytettyjen toimintojen järjestys, käytetyn laitteen ominaisuudet jne.). Näillä palveluilla voi henkilötietojen tuojan tapaan olla velvollisuus myöntää pääsy oman lainkäyttöalueensa samoille viranomaisille, joilla todennäköisesti on hallussaan tietoa siitä, miten kohteena oleva henkilö on käyttänyt kyseisiä tietopalveluja.

88. Koska joidenkin tietopalvelujen käyttö on luonnostaan julkista tai niitä hyödyntävät osapuolet, joilla on huomattavia resursseja, rekisterinpitäjien on lisäksi otettava erityisen huolellisesti huomioon se, että niiden lainkäyttöalueen viranomaisilla on todennäköisesti hallussaan tietoa kohteena olevan henkilön tietopalvelujen käytöstä.

89. Jos pseudonymisointia tehtäessä henkilötietoihin sisältyviä attribuutteja muunnetaan käyttämällä salausalgoritmia, on noudatettava alaviitteissä 80 ja 81 annettuja ohjeita. On siis suositeltavaa olla käyttämättä yksinomaan salausta ja käyttää taulukkohakumekanismeihin perustuvia muunnoksia.

Esimerkkitapaus 3: Tietojen salaus, jonka tarkoituksena on suojata ne tuojan kolmannen maan viranomaisten pääsyltä, kun tiedot kulkevat tietojen viejän ja tuojan välillä

90. Tietojen viejä haluaa siirtää tietoja kohdemaahan, jonka laki ja/tai käytännöt antavat viranomaisille pääsyn tietoihin, kun ne kulkevat viejän maan ja kohdemaan välillä.

    Jos

    1. tietojen viejä siirtää henkilötietoja tietojen tuojalle, joka on sellaisella lainkäyttöalueella, jonka laki ja/tai käytäntö sallii viranomaisten pääsyn tietoihin, kun niitä siirretään internetissä tähän kolmanteen maahan, johon ei sovelleta eurooppalaisia olennaisia takeita tällaisen pääsyn osalta, käytetään siirron salausta, jonka osalta on varmistettu, että käytetyt salausprotokollat ovat uusimman tekniikan mukaisia ja antavat tehokkaan suojan sellaisilta aktiivisilta ja passiivisilta hyökkäyksiltä, joissa käytetään resursseja, joiden tiedetään olevan kolmannen maan viranomaisten käytettävissä,
    2. viestinnässä mukana olevat osapuolet ovat sopineet luotettavasta julkisen avaimen varmenneviranomaisesta tai varmennusinfrastruktuurista,
    3. salatun liikenteen mahdollistaviin lähetys- ja vastaanottojärjestelmiin kohdistuvia aktiivisia ja passiivisia hyökkäyksiä vastaan käytetään erityisiä huipputeknisiä suojatoimenpiteitä, ja myös ohjelmistohaavoittuvuuksia ja mahdollisia takaportteja testataan,

---

[84] Yleisen tietosuoja-asetuksen 4 artiklan 1 kohta: "'henkilötiedoilla' [tarkoitetaan] kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella"

4. jos liikenteen salaus itsessään ei takaa asianmukaista turvallisuutta, koska käytettävässä infrastruktuurissa tai ohjelmistossa on haavoittuvuuksia, henkilötiedot salataan päästä päähän myös sovelluskerroksessa käyttämällä huipputeknisiä salausmenetelmiä,
5. salausalgoritmi ja sen parametrisointi (esim. avaimen pituus, toimintatapa soveltuvin osin) ovat uusimman tekniikan mukaisia ja ne voidaan katsoa kestäviksi viranomaisten tekemää kryptoanalyysia vastaan, kun näitä tietoja siirretään tähän kolmanteen maahan, viranomaisten käytössä olevat resurssit ja tekniset valmiudet (esim. laskentateho väsytyshyökkäyksissä) huomioon ottaen (ks. alaviite 80 edellä), [85]
6. salauksen vahvuudessa otetaan huomioon nimenomainen jakso, jonka ajan salattujen henkilötietojen luottamuksellisuus on säilytettävä,
7. salausalgoritmi otetaan asianmukaisesti käyttöön kunnolla ylläpidetyllä ohjelmistolla, jossa ei ole tunnettuja haavoittuvuuksia ja jonka on varmennettu olevan valitun algoritmin spesifikaation mukainen esimerkiksi sertifioinnilla,
8. viejä tai viejän luotettu yhteisö lainkäyttöalueella, joka tarjoaa unionissa taattua suojaa pääosiltaan vastaavan suojan tason, hallinnoi (luo, jakaa, tallentaa, tarvittaessa yhdistää aiotun vastaanottajan henkilöllisyyteen ja kumoaa) avaimia luotettavasti,

Euroopan tietosuojaneuvosto katsoo, että liikenteen salaus, tarvittaessa yhdessä sisällön päästä päähän -salauksen kanssa, on tehokas lisätoimenpide.

Esimerkkitapaus 4: Suojattu vastaanottaja

91. Tietojen viejä siirtää henkilötietoja kolmannessa maassa sijaitsevalle tietojen tuojalle, joka on nimenomaisesti suojattu kyseisen maan lailla, esimerkiksi sitä varten, että potilaalle annetaan yhdessä lääkehoitoa tai asiakkaalle tarjotaan lainopillisia palveluita.

Jos

1. kolmannen maan laissa myönnetään maassa sijaitsevalle tietojen tuojalle poikkeus mahdollisesti lainvastaisesta pääsystä kyseisen vastaanottajan hallussa oleviin tietoihin tiettyä tarkoitusta varten, esimerkiksi tietojen tuojaan sovellettavan salassapitovelvollisuuden nojalla,
2. kyseinen poikkeus koskee kaikkia tietojen tuojan hallussa olevia tietoja, joita voidaan käyttää kiertämään etuoikeustiedon suoja (salausavainten, salasanojen, muiden turvatekijöiden jne.),
3. tietojen tuoja ei käytä henkilötietojen käsittelijän palveluja niin, että viranomaiset voisivat päästä tietoihin, kun ne ovat henkilötietojen käsittelijän hallussa, eikä tietojen tuoja siirrä tietoja edelleen muulle suojaamattomalle yhteisölle yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden perusteella,
4. henkilötiedot salataan ennen siirtämistä huipputeknisellä menetelmällä, jolla taataan, että salausta ei voi purkaa ilman salausavaimen (päästä päähän -salaus) tuntemista koko sinä aikana, jona tiedot on suojattava,
5. salauksenpurkuavain on yksinomaan suojatun tietojen tuojan hallussa ja mahdollisesti viejän tai muun sellaisen yhteisön hallussa, jolle viejä on antanut tämän tehtävän ja joka sijaitsee Euroopan talousalueella taikka sellaisella lainkäyttöalueella, jossa suojan taso vastaa pääosiltaan Euroopan talousalueella taatun suojan tasoa, ja se on suojattu asianmukaisesti

[85] Ks. alaviitteestä 80 viittauksia teknisiin ohjeisiin, joita EU:n ja sen jäsenvaltioiden viralliset kyberturvallisuusviranomaiset ovat julkaisseet.

luvattomalta käytöltä tai luovuttamiselta huippuluokan teknisillä ja organisatorisilla toimenpiteillä, ja

6. tietojen viejä on vahvistanut luotettavasti, että salausavain, jota se aikoo käyttää, vastaa vastaanottajan hallussa olevaa salausavainta,

Euroopan tietosuojaneuvosto katsoo, että tehty liikenteen salaus on tehokas lisätoimenpide.

Esimerkkitapaus 5: Jaettu tai monen osapuolen toteuttama käsittely

92. Tietojen viejä haluaa, että henkilötietoja käsittelee yhdessä vähintään kaksi eri lainkäyttöalueilla sijaitsevaa riippumatonta henkilötietojen käsittelijää ilman, että niille luovutetaan tietojen sisältöä. Ennen siirtämistä viejä jakaa tiedot niin, että mikään yksittäisen henkilötietojen käsittelijän saama osa ei riitä henkilötietojen ennallistamiseen kokonaan tai osittain. Tietojen viejä saa käsittelyn tulokset kultakin henkilötietojen käsittelijältä erikseen ja yhdistää saadut tiedonosat siten, että lopputuloksena voi olla henkilötietoja tai yhdistelmätietoja.

Jos

1. tietojen viejä käsittelee henkilötiedot niin, että ne jaetaan vähintään kahteen osaan, joita ei voida enää tulkita tai yhdistää tiettyyn rekisteröityyn ilman lisätietojen käyttämistä,
2. kukin tiedonosa siirretään eri lainkäyttöalueella sijaitsevalle erilliselle henkilötietojen käsittelijälle,
3. vaihtoehtoisesti henkilötietojen käsittelijät käsittelevät tietoja yhdessä, esimerkiksi käyttämällä suojattua monen osapuolen laskentaa, siten, että niille ei paljasteta mitään tietoja, joita niiden hallussa ei ollut ennen laskentaa,
4. yhteisessä laskennassa käytettävä algoritmi on suojattu aktiivisilta kilpailijoilta,
5. rekisterinpitäjä on vahvistanut kyseessä olevien tietojen perusteellisen analyysin avulla ja ottaen huomioon kaikki puuttuvat tiedot, joiden voidaan olettaa olevan vastaanottajamaiden viranomaisten hallussa ja käytössä, että sen henkilötietojen käsittelijöille toimittamia henkilötietojen osia ei voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, vaikka kyseisiä tietoja vertailtaisiin keskenään,
6. ei ole näyttöä viranomaisten, jotka sijaitsevat niillä lainkäyttöalueilla, joilla kukin henkilötietojen käsittelijä sijaitsee, välisestä yhteistyöstä, jonka avulla ne voisivat päästä kaikkiin henkilötietojen käsittelijöiden hallussa oleviin henkilötietokokonaisuuksiin ja ennallistaa ne ja hyödyntää selkeässä muodossa olevaa henkilötietojen sisältöä olosuhteissa, joissa hyödyntäminen ei noudattaisi olennaisilta osiltaan rekisteröityjen perusoikeuksia ja -vapauksia. Minkään maan viranomaisilla ei myöskään pitäisi olla valtuuksia päästä henkilötietojen käsittelijöiden kaikilla kyseessä olevilla lainkäyttöalueilla hallussaan pitämiin henkilötietoihin.

Euroopan tietosuojaneuvosto katsoo, että tehty jaettu käsittely on tehokas lisätoimenpide.

Esimerkkejä sellaisiin tapauksiin liittyvistä skenaarioista, joita varten ei ole *tehokkaita* toimenpiteitä

93. Jäljempänä tiettyjen skenaarioiden yhteydessä kuvattavilla toimenpiteillä ei pystyttäisi tehokkaasti varmistamaan unionissa taattua suojaa pääosiltaan vastaavaa suojan tasoa kolmanteen maahan siirretyille tiedoille. Siksi niitä ei hyväksyttäisi riittäviksi lisätoimenpiteiksi.

Esimerkkitapaus 6: Siirto pilvipalvelujen tarjoajille tai muille henkilötietojen käsittelijöille, jotka edellyttävät pääsyä selkeässä muodossa oleviin tietoihin

94. Tietojen viejä siirtää henkilötietoja joko sähköisesti tai toimittamalla ne pilvipalvelujen tarjoajan tai muun henkilötietojen käsittelijän saataville, jotta ne käsittelevät henkilötietoja viejän ohjeiden mukaan kolmannessa maassa (esimerkiksi teknisen tuen saamista tai kaikenlaisen pilvipalvelussa tapahtuvaa käsittelyä varten), ja näitä tietoja ei – tai ei voida – pseudonymisoida esimerkkitapaus 2:ssa kuvatulla tavalla taikka salata esimerkkitapaus 1:ssä kuvatulla tavalla, koska käsittely edellyttää pääsyä selkeässä muodossa oleviin tietoihin.

Jos

1. rekisterinpitäjä siirtää tiedot pilvipalvelun tarjoajalle tai muulle henkilötietojen käsittelijälle,
2. pilvipalvelun tarjoaja tai muu henkilötietojen käsittelijä tarvitsee pääsyn selkeässä muodossa oleviin tietoihin voidakseen suorittaa sille osoitetun tehtävän ja
3. vastaanottajamaan viranomaisille myönnetyt valtuudet päästä siirrettyihin tietoihin ylittävät sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, kun kolmannen maan ongelmallista lainsäädäntöä sovelletaan käytännössä kyseisiin siirtoihin (ks. vaihe 3).[86]

Euroopan tietosuojaneuvosto ei pysty nykyisellä tekniikan tasolla määrittämään tehokasta teknistä toimenpidettä, jolla estettäisiin se, ettei kyseinen pääsy loukkaisi rekisteröityjen oikeuksia. Euroopan tietosuojaneuvosto ei sulje pois mahdollisuutta, että myöhemmän teknisen kehityksen myötä voidaan saada käyttöön toimenpiteitä, joilla saavutetaan aiotut liiketoimintatarkoitukset ilman, että tarvittaisiin pääsy selkeässä muodossa oleviin tietoihin.

95. Näissä skenaarioissa, joissa salaamattomat henkilötiedot ovat teknisesti tarpeen, jotta henkilötietojen käsittelijä voi tarjota palvelun, liikenteen salaus ja lepäävän datan salaus eivät yhdessäkään ole lisätoimenpide, jolla varmistetaan unionissa taattua suojaa pääosiltaan vastaava suojan taso, jos tietojen tuojalla on hallussaan salausavaimet.

Esimerkkitapaus 7: Henkilötietojen siirto liiketoimintaa varten myös etäkäytön avulla

96. Tietojen viejä siirtää henkilötietoja yhteisöille – kolmanteen maahan käytettäväksi yhteisessä liiketoiminnassa – joko sähköisesti tai asettamalla ne tietojen tuojan saataville etäkäyttöä varten, ja näitä tietoja ei – tai ei voida – pseudonymisoida esimerkkitapaus 2:ssa kuvatulla tavalla

[86] Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020.

taikka salata esimerkkitapaus 1:ssä kuvatulla tavalla, koska käsittely edellyttää pääsyä selkeässä muodossa oleviin tietoihin. Tyypillisessä kokoonpanossa voi olla jäsenvaltion alueelle sijoittautunut rekisterinpitäjä tai henkilötietojen käsittelijä, joka siirtää henkilötietoja kolmannessa maassa olevalle rekisterinpitäjälle tai henkilötietojen käsittelijälle, joka kuuluu samaan yrityskonserniin tai samaan taloudelliseen toimintaan osallistuvien yritysten ryhmittymään. Tietojen tuoja voi esimerkiksi käyttää saamiaan tietoja tietojen viejän henkilöstöpalvelujen tarjoamiseksi, mitä varten tarvitaan tietoja henkilöresursseista, tai ollakseen yhteydessä tietojen viejän Euroopan unionissa asuviin asiakkaisiin puhelimitse tai sähköpostitse.

Jos

1. tietojen viejä siirtää henkilötietoja tietojen tuojalle kolmannessa maassa asettamalla ne saataville tietojärjestelmässä siten, että tuoja pääsee suoraan valitsemiinsa tietoihin, tai siirtämällä ne suoraan, yksittäin tai erottelematta käyttämällä viestintäpalvelua,
2. tuoja[87] käsittelee selkeässä muodossa olevia tietoja kolmannessa maassa (myös omia tarkoituksiaan varten, jos tuoja on rekisterinpitäjä),
3. vastaanottajamaan viranomaisille myönnetyt valtuudet päästä siirrettyihin tietoihin ylittävät sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, kun kolmannen maan ongelmallista lainsäädäntöä sovelletaan käytännössä kyseisiin siirtoihin (ks. vaihe 3),

Euroopan tietosuojaneuvosto ei pysty määrittämään tehokasta teknistä toimenpidettä, jolla estettäisiin kyseistä pääsyä loukkaamasta rekisteröidyn perusoikeuksia.

97. Kyseessä olevissa tilanteissa, joissa salaamattomat henkilötiedot ovat teknisesti tarpeen, jotta henkilötietojen käsittelijä voi tarjota palvelun, liikenteen salaus ja lepäävän datan salaus eivät yhdessäkään ole lisätoimenpide, jolla varmistetaan unionissa taattua suojaa pääosiltaan vastaava suojan taso, jos tietojen tuojalla on hallussaan salausavaimet.

[87] Kolmannessa maassa oleva rekisterinpitäjä tai henkilötietojen käsittelijä, joka vastaanottaa Euroopan talousalueelta siirretyt henkilötiedot tai saa niihin pääsyn.

2.2 Sopimukseen perustuvat lisätoimenpiteet

98. Nämä toimenpiteet koostuvat tavallisesti yksipuolisista, kahdenvälisistä tai monenvälisistä[88] sopimukseen perustuvista sitoumuksista.[89] Jos käytetään yleisen tietosuoja-asetuksen 46 artiklan mukaista tiedonsiirtovälinettä, siihen sisältyy useimmissa tapauksissa jo useita (tavallisesti sopimukseen perustuvia) tietojen viejän ja tietojen tuojan sitoumuksia, joiden tarkoituksena on suojata henkilötiedot.[90]

99. Joissakin tilanteissa näillä toimenpiteillä voidaan täydentää ja vahvistaa suojatoimia, joita tiedonsiirtoväline ja kolmannen maan asiaankuuluva lainsäädäntö voivat tarjota, kun ne eivät siirron olosuhteet huomioon ottaen täytä kaikkia edellytyksiä, jotta suojan taso vastaisi pääosiltaan Euroopan talousalueella taattua suojan tasoa. Koska sopimukseen perustuvilla toimenpiteillä ei yleisesti pystytä sitomaan kyseisen kolmannen maan viranomaisia, kun ne eivät ole sopimuksen osapuolia[91], nämä toimenpiteet on usein yhdistettävä muihin teknisiin ja organisatorisiin toimenpiteisin, jotta vaadittu suojan taso saavutetaan. Yhden tai useamman tällaisen toimenpiteen valitseminen ja täytäntöönpano ei välttämättä ja aina varmista, että täytetään EU:n lainsäädännön vaatimus siitä, että siirto vastaa pääosiltaan siinä taattua suojan tasoa.

100. Sen mukaan, mitä sopimukseen perustuvia toimenpiteitä jo sisältyy yleisen tietosuoja-asetuksen 46 artiklan mukaiseen käytettävään tiedonsiirtovälineeseen, sopimukseen perustuvat lisätoimenpiteet voivat myös olla hyödyllisiä, jotta Euroopan talousalueella sijaitsevat tietojen viejät saavat tietoa uudesta kehityksestä, joka vaikuttaa kolmansiin maihin siirrettävien tietojen suojaan.

101. Sopimukseen perustuvilla toimenpiteillä ei pystytä estämään sellaisen kolmannen maan lainsäädännön soveltamista, joka ei täytä Euroopan tietosuojaneuvoston eurooppalaisia olennaisia takeita koskevaa vaatimusta, niissä tapauksissa, joissa lainsäädännöllä velvoitetaan tuojat noudattamaan viranomaisilta saamiaan määräyksiä tietojen luovuttamisesta.[92]

102. Jäljempänä annetaan muutamia esimerkkejä näistä mahdollisista sopimukseen perustuvista toimenpiteistä ja luokitellaan ne niiden luonteen mukaan:

Tiettyjen teknisten toimenpiteiden käyttöä koskeva sopimukseen perustuva velvoite

103. Siirtojen nimenomaisten olosuhteiden mukaan (ja myös sen mukaan, miten kolmannen maan lainsäädäntöä sovelletaan käytännössä) sopimuksessa on ehkä määrättävä, että siirtojen

---

[88] Esimerkiksi yritystä koskevissa sitovissa säännöissä, joilla pitäisi joka tapauksessa säännellä joitakin jäljempänä lueteltuja toimenpiteitä.

[89] Ne ovat luonteeltaan yksityisiä eikä niitä katsota kansainvälisiksi sopimuksiksi kansainvälisessä julkisoikeudessa. Siksi ne eivät tavallisesti sido kolmannen maan viranomaista, koska se ei ole sopimuksen osapuoli, kun sopimus tehdään kolmansien maiden yksityisten elinten kanssa, kuten unionin tuomioistuin korosti asiassa C-311/18 (Schrems II) antamansa tuomion 125 kohdassa.

[90] Ks. asiassa C-311/18 (Schrems II) annetun tuomion 137 kohta, jossa tuomioistuin totesi, että tietosuojaa koskevassa vakiolausekkeessa on ”tehokkaita mekanismeja, jotka käytännössä varmistavat, että unionin oikeudessa edellytettyä tietosuojan tasoa noudatetaan ja että tällaisiin lausekkeisiin perustuvat henkilötietojen siirrot keskeytetään tai kielletään, jos näitä lausekkeita rikotaan tai niiden noudattaminen on mahdotonta” (ks. myös 148 kohta).

[91] C-311/18 (Schrems II), 125 kohta.

[92] Euroopan unionin tuomioistuimen tuomio asiassa C-311/18 (Schrems II), 132 kohta.

tekeminen edellyttää tiettyjen teknisten toimenpiteiden toteuttamista (ks. jäljempänä ehdotetut tekniset toimenpiteet).

104. Tehokkuuden edellytykset:

- Tämä lauseke voisi olla tehokas tilanteissa, joissa viejä on havainnut, että teknisiä toimenpiteitä tarvitaan. Siitä olisi määrättävä oikeudellisesti, jotta varmistetaan, että myös tuoja sitoutuu ottamaan tarvittavat tekniset toimenpiteet käyttöön, jos se on tarpeen.

Avoimuusvelvoitteet:

105. Viejä voisi liittää sopimukseen liitteitä, joissa on tietoa siitä, että ennen sopimuksen tekemistä tuoja olisi parhaan kykynsä mukaan tarjonnut kohdemaan viranomaisille pääsyn tietoihin, myös tiedustelun alalla, jos lainsäädännössä noudatetaan Euroopan tietosuojaneuvoston suosituksia eurooppalaisista olennaisista takeista. Tämä voisi auttaa tietojen viejää täyttämään velvoitteensa dokumentoida oma arviointinsa suojan tasosta kolmannessa maassa. Sillä voidaan myös korostaa tuojan velvollisuutta auttaa viejää arvioinnissa ja kantaa vastuunsa antamalla viejälle objektiivista, luotettavaa, merkityksellistä, todennettavaa ja julkisesti tai muutoin saatavilla olevaa tietoa.

106. Tuojaa voitaisiin esimerkiksi vaatia

(1) luettelemaan tuojaan tai sen henkilötietojen (ali)käsittelijöihin kohdemaassa sovellettavat säädökset ja määräykset, joiden nojalla viranomaiset saisivat pääsyn siirron kohteen oleviin henkilötietoihin, erityisesti siirrettyjä tietoja koskevilla tiedustelun, lainvalvonnan, hallinnollisen valvonnan ja sääntelyvalvonnan aloilla

(2) antamaan, jos viranomaisten tietoihin pääsyä koskevia lakeja ei ole, tuojien kokemusten tai eri lähteistä (esim. kumppaneilta, avoimista lähteistä, kansallisesta oikeuskäytännöstä ja valvontaelinten päätöksistä) saatavien raporttien perusteella tietoja ja tilastoja viranomaisten pääsystä henkilötietoihin tilanteissa, jotka vastaavat kyseessä olevaa tiedonsiirtoa (eli tietyllä sääntelyn osa-alueella, niiden yhteisöjen tyypin mukaan, joihin tietojen tuoja kuuluu jne.)

(3) ilmoittamaan, mihin toimenpiteisiin on (mahdollisesti) ryhdytty pääsyn estämiseksi siirrettyihin tietoihin

(4) antamaan riittävän yksityiskohtaista tietoa kaikista viranomaisten tekemistä henkilötietoihin pääsyä koskevista pyynnöistä, jotka tuoja on ottanut vastaan tiettynä aikana[93], erityisesti edellä 1 kohdassa mainituilla osa-alueilla, siten, että niissä on tietoa vastaanotetuista pyynnöistä, pyydetyistä tiedoista, pyynnön esittäneestä elimestä ja luovuttamisen oikeusperusteesta sekä siitä, missä määrin tuoja on luovuttanut pyydettyjä tietoja[94]

[93] Jakson pituuden tulisi määräytyä sen mukaan, millainen riski niiden rekisteröityjen oikeuksille ja vapauksille kohdistuu, joiden tietoja kyseessä oleva siirto koskee – esim. tietojen viejän kanssa käytetyn tiedonvientivälineen sulkemista edeltävä vuosi.

[94] Tämän velvollisuuden noudattaminen ei itsessään tarkoita asianmukaisen suojan tason tarjoamista. Kaikki tosiasiallisesti tapahtuneet epäasianmukaiset luovutukset johtavat kuitenkin siihen, että lisätoimenpiteitä on pantava täytäntöön.

täsmentämään, onko tuojaa kielletty lainmukaisesti antamasta edellä 1–5 kohdassa tarkoitettuja tietoja ja missä määrin.

107. Näitä tietoja voitaisiin antaa jäsennellyissä kyselylomakkeissa, jotka tuoja täyttää ja allekirjoittaa ja joihin yhdistetään tuojan sopimukseen perustuva velvoite ilmoittaa tietyn ajan kuluessa kaikki mahdolliset muutokset näihin tietoihin, kuten tällä hetkellä toimitaan due diligence -prosessissa.

108. Tehokkuuden edellytykset:

- Tuojan on pystyttävä antamaan viejälle tällaiset tiedot parhaan tietonsa mukaan ja pyrittyään kaikin keinoin hankkimaan ne.
- Tällä tuojalle määrätyllä velvollisuudella voidaan varmistaa, että viejä saa tietoonsa tietojen siirtämiseen kolmanteen maahan liittyvät riskit ja pysyy niistä tietoisena. Siten viejä voi pidättäytyä tekemästä sopimusta tai, jos tiedot muuttuvat sopimuksen tekemisen jälkeen, täyttämään velvollisuutensa keskeyttää siirto ja/tai irtisanoa sopimus, jos kolmannen maan lainsäädännöllä, yleisen tietosuoja-asetuksen 46 artiklan mukaisen käytettävän tiedonsiirtovälineen sisältämillä suojatoimilla ja muilla sen mahdollisesti hyväksymillä lisäsuojatoimilla ei voida enää varmistaa Euroopan talousalueella taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa. Tällä velvollisuudella ei voida kuitenkaan perustella sitä, että tuoja luovuttaa henkilötietoja, eikä sen nojalla voida olettaa, että pääsypyyntöjä ei tule lisää.

***

109. Viejä voisi myös lisätä lausekkeita, joilla tuoja varmentaa, että 1) se ei ole tarkoituksella luonut takaportteja tai vastaavia ohjelmia, joita voitaisiin käyttää järjestelmään ja/tai henkilötietoihin pääsemiseen, 2) se ei ole tarkoituksella luonut tai muuttanut liiketoimintaprosessejaan siten, että niillä helpotetaan pääsyä henkilötietoihin tai järjestelmiin, ja 3) kansallisessa laissa tai hallituksen politiikassa ei vaadita tuojaa luomaan tai ylläpitämään takaportteja tai helpottamaan pääsyä henkilötietoihin tai järjestelmiin tai tuojaa pitämään hallussa salausavainta tai luovuttamaan sen[95].

110. Tehokkuuden edellytykset:

- Tästä lausekkeesta voi tulla tehoton, jos lainsäädännöllä tai hallituksen politiikalla estetään tuojia luovuttamasta tietoja. Silloin tuoja ei pysty tekemään sopimusta tai sen on ilmoitettava viejälle, että se ei pysty enää jatkossa noudattamaan sopimukseen perustuvia sitoumuksiaan.
- Sopimukseen täytyy sisältyä seuraamuksia ja/tai maininta siitä, että viejä voi irtisanoa sopimuksen lyhyellä varoitusajalla tapauksissa, joissa tuoja ei paljasta, että on olemassa takaportti tai vastaavia ohjelmia tai peukaloituja liiketoimintaprosesseja tai vaatimuksia näiden toteuttamisesta, tai tuoja ei ilmoita viejälle viipymättä, kun niiden olemassaolo tulee sen tietoon.
- Niitä tilanteita varten, joissa tietojen tuoja luovuttaa siirrettyjä henkilötietoja valittuun tiedonsiirtovälineeseen sisältyvien sitoumusten vastaisesti, sopimukseen voi sisällyttää myös

[95] Tämä lauseke on tärkeä, jotta voidaan taata riittävä suojan taso siirretyille henkilötiedoille, ja sen sisällyttämistä sopimukseen pitäisi yleensä vaatia.

korvauksen, jonka tietojen tuoja maksaa rekisteröidylle mahdollisesti koituneista aineellisista ja aineettomista vahingoista.

***

111. Viejä voisi vahvistaa valtuuksiaan tehdä tarkastuksia[96] tai tutkimuksia tuojan tietojenkäsittelyjärjestelmistä joko itse paikalla tai etäyhteydellä, tarkistaakseen, onko tietoja luovutettu viranomaisille ja millä edellytyksillä (pääsy ei ylitä sitä, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista), esimerkiksi määräämällä lyhyestä varoitusajasta ja mekanismeista, joilla varmistetaan tutkintaelinten nopea toiminta ja vahvistetaan viejän itsenäisyyttä tutkintaelinten valitsemisessa.

112. Tehokkuuden edellytykset:

- Tarkastuksen soveltamisalan pitäisi sisältää oikeudellisesti ja teknisesti kaikki käsittely, jonka tuojan henkilötietojen käsittelijät tai alikäsittelijät tekevät kolmanteen maahan siirretyille henkilötiedoille, jotta se olisi kokonaisuudessaan tehokasta.
- Pääsylokien ja muiden vastaavien jäljitysketjujen olisi oltava luotettavia (ts. ne on rakennettava käyttämällä uusimman tekniikan mukaisia salaustekniikoita, kuten tiivistämistä, ja ne on myös välitettävä viejälle säännöllisiin väliajoin), jotta tarkastajat voivat löytää todisteita luovuttamisesta. Pääsylokeissa ja muissa vastaavissa jäljitysketjuissa olisi myös tehtävä ero tavanomaisista liiketoimista johtuvien pääsyjen ja pääsyä koskevista määräyksistä tai pyynnöistä johtuvien pääsyjen välillä.

***

113. Jos tuojan kolmannen maan laki ja käytäntö on alustavasti arvioitu ja niiden on katsottu tarjoavan sellaisen suojan tason, joka pääosiltaan vastaa EU:ssa viejän siirtämille tiedoille tarjottua suojan tasoa, viejä voisi vielä tiukentaa tietojen tuojan velvollisuutta ilmoittaa viipymättä tietojen viejälle tilanteen muuttuessa siitä, että se ei pysty noudattamaan sopimukseen perustuvia sitoumuksia ja siten ”pääosiltaan vastaavaa tietosuojan tasoa” koskevaa vaatimusta.[97]

114. Se, ettei vaatimuksia voida noudattaa, voi johtua muutoksista kolmannen maan lainsäädännössä tai käytännössä[98]. Lausekkeissa voitaisiin asettaa erityiset tiukat aikarajat ja menettelyt tiedonsiirron ripeälle keskeyttämiselle ja/tai sopimuksen irtisanomiselle ja sille, että tuoja palauttaa tai poistaa saamansa tiedot. Viejän pitäisi saada saatujen pyyntöjen, niiden soveltamisalan ja niiden torjumiseksi hyväksyttyjen toimenpiteiden tehokkuuden seuraamisesta

[96] Ks. esim. päätöksen 2010/87/EU rekisterinpitäjien ja henkilötietojen käsittelijöiden mallisopimuslausekkeita koskevan lausekkeen 5 kohta f. Tarkastuksista voitaisiin määrätä myös käytännesäännöissä tai varmenteessa.

[97] Mallisopimuslausekkeita koskevan päätöksen 2010/87/EU 5 lausekkeen a kohta ja d kohdan i alakohta.

[98] Ks. asiassa C-311/18 (Schrems II) annetun tuomion 139 kohta, jossa tuomioistuin toteaa, että ”vaikka saman lausekkeen 5 kohdan d alakohdan i nojalla henkilötietojen siirron vastaanottaja voi silloin, kun kyse on lainsäädännössä esitetystä kiellosta – kuten rikoslainsäädännön mukainen kielto lainvalvontaan liittyvien tutkimusten luottamuksellisuuden säilyttämiseksi – olla antamatta unioniin sijoittautuneelle rekisterinpitäjälle tiedoksi täytäntöönpanosta vastaavan viranomaisen oikeudellisesti sitovaa pyyntöä luovuttaa henkilötietoja, sen on kuitenkin päätöksen 2010/87 lausekkeen 5 kohdan a nojalla ilmoitettava rekisterinpitäjälle, että se ei voi noudattaa mallisopimuslausekkeita”.

riittävästi tietoa, jotta se voi täyttää velvollisuutensa keskeyttää tai päättää siirto ja/tai irtisanoa sopimus.

115. Tehokkuuden edellytykset:

- Ilmoitus on tehtävä ennen kuin tietoihin myönnetään pääsy. Muussa tapauksessa yksilön oikeuksia on jo voitu loukata siihen mennessä, kun viejä saa ilmoituksen, jos pyyntö perustuu kyseisen maan lakeihin, jotka ylittävät sen, mitä EU:n lainsäädännössä tarjotussa suojan tasossa sallitaan. Ilmoitusta voidaan edelleen käyttää estämään tulevia loukkauksia ja antamaan viejän täyttää velvollisuutensa keskeyttää henkilötietojen siirto kolmanteen maahan ja/tai irtisanoa sopimus.
- Tietojen tuojan on seurattava kaikkea oikeudellista tai poliittista kehitystä, jonka vuoksi se ei voisi noudattaa velvoitteitaan, ja ilmoitettava viipymättä tietojen viejälle kaikista sellaisista muutoksista ja kehityksestä. Tämä on tehtävä mahdollisuuksien mukaan ennen niiden toteutumista, jotta tietojen viejä voi saada tiedot takaisin tietojen tuojalta.
- Lausekkeissa on määrättävä nopeasta mekanismista, jossa tietojen viejä antaa tietojen tuojalle luvan viipymättä suojata tai palauttaa tiedot tietojen viejälle tai, jos se ei ole mahdollista, poistaa tai salata turvallisesti tiedot ilman, että tuoja välttämättä odottaisi viejän ohjeita, jos tietojen viejän ja tietojen tuojan välillä sovittava erityinen kynnysarvo[99] täyttyy. Tuojan on pantava tämä mekanismi täytäntöön tiedonsiirron alusta alkaen ja testattava sitä säännöllisesti, jotta voidaan varmistaa, että sitä on mahdollista soveltaa lyhyellä varoitusajalla.
- Viejä voisi muiden lausekkeiden avulla seurata, noudattaako tuoja näitä velvoitteita, tekemällä tarkastuksia, tutkimuksia ja muita varmennustoimenpiteitä, ja valvomalla niiden noudattamista seuraamuksilla, jotka koskevat tuojan ja/tai viejän kykyä keskeyttää siirto ja/tai irtisanoa sopimus välittömästi.

***

116. Mikäli kolmannen maan kansallisessa lainsäädännössä sallitaan, sopimuksella voitaisiin tiukentaa tuojan avoimuusvelvoitteita ns. Warrant Canary -menetelmällä. Siinä tuoja sitoutuu julkaisemaan säännöllisesti (esim. vähintään kerran vuorokaudessa) salakirjoituksella allekirjoitetun viestin, jossa ilmoitetaan viejälle, että se ei ole tiettyyn päivään ja aikaan mennessä saanut määräystä henkilötietojen luovuttamisesta tai vastaavasta. Jos ilmoitusta ei saada, viejä tietää, että tuoja on voinut saada määräyksen.

117. Tehokkuuden edellytykset:

- Kolmannen maan määräyksissä on sallittava, että tietojen tuoja voi antaa tällaisen passiivisen ilmoituksen viejälle.
- Tietojen viejän on seurattava automaattisesti Warrant Canary -ilmoituksia.
- Tietojen tuojan on varmistettava, että sen Warrant Canary -ilmoitusten allekirjoittamista varten tarvittava yksityinen avain pidetään turvassa ja että sitä ei voida kolmannen maan lainsäädännöllä pakottaa antamaan vääriä Warrant Canary -ilmoituksia. Tätä varten voi olla hyödyllistä, jos ilmoituksen tekemiseen tarvitaan useita allekirjoituksia eri henkilöiltä ja/tai jos

[99] Tällä kynnysarvolla on tarkoitus varmistaa, että rekisteröidyille annetaan yhä Euroopan talousalueella taattua suojaa vastaavan tasoinen suoja.

Warrant Canary -ilmoituksen antaa kolmannen maan lainkäyttöalueen ulkopuolella oleva henkilö.

Erityistoimiin ryhtymistä koskevat velvollisuudet

118. Viejä voisi sitoutua tarkastelemaan kohdemaan lainsäädännön mukaisesti kaikkien tietojen julkaisemista koskevien määräysten laillisuutta ja erityisesti sitä, kuuluvatko ne määräyksen antavalle viranomaiselle myönnettyihin valtuuksiin, ja kyseenalaistamaan määräyksen, jos se katsoo huolellisen arvioinnin jälkeen, että kohdemaan lainsäädännössä ei ole perusteita sen tekemiselle. Määräyksen kyseenalaistaessaan tietojen tuojan olisi pyrittävä keskeyttämään väliaikaisilla toimenpiteillä määräyksen vaikutukset siihen asti, että tuomioistuin on tehnyt päätöksen sen pääasiasta. Tuoja ei saisi luovuttaa pyydettyjä henkilötietoja ennen kuin sitä vaaditaan tekemään niin sovellettavien menettelysääntöjen mukaisesti. Tietojen tuoja sitoutuisi määräykseen vastatessaan myös antamaan sallitun vähimmäismäärän tietoa määräyksen kohtuullisen tulkinnan perusteella.

119. Tehokkuuden edellytykset:

- Kolmannen maan oikeusjärjestyksessä on oltava tehokkaat oikeudelliset keinot tietojen luovuttamista koskevien määräysten kyseenalaistamiseen.
- Tämä lauseke tarjoaa aina vain vähän lisäsuojaa, koska tietojen luovuttamista koskeva määräys voi olla laillinen kolmannen maan oikeusjärjestyksen mukaisesti, mutta kyseinen oikeusjärjestys ei ehkä täytä EU:n vaatimuksia. Tällä sopimukseen perustuvalla toimenpiteellä väistämättä vain täydennetään muita lisätoimenpiteitä.
- Määräysten kyseenalaistamisella on oltava lykkäävä vaikutus kolmannen maan lainsäädännön mukaisesti. Muussa tapauksessa viranomaisilla olisi edelleen pääsy yksilöiden tietoihin, ja kaikki myöhemmin yksilön puolesta tehtävät toimet vaikuttaisivat vain rajallisesti siihen, että tämä voisi vaatia vahingonkorvauksia tietojen luovuttamisesta johtuvista kielteisistä seurauksista.
- Tuojan on pystyttävä dokumentoimaan toteuttamansa toimenpiteet ja osoittamaan ne viejälle sekä pyrittävä parhaan kykynsä mukaan täyttämään tämän sitoumuksen.

***

120. Edellä kuvattua vastaavassa tilanteessa tuoja voisi sitoutua ilmoittamaan määräyksen antaneelle viranomaiselle siitä, että määräys on yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen sisältämien suojatoimien vastainen[100], sekä siitä tuojalle johtuvasta velvoitteiden ristiriidasta. Tuoja ilmoittaisi tästä yhtä aikaa ja mahdollisimman pian viejälle ja/tai

[100] Mallisopimuslausekkeissa esimerkiksi määrätään, että tietojen käsittely, myös niiden siirtäminen, on pitänyt tehdä ja pitää tehdä jatkossakin *”sovellettavan tietosuojalainsäädännön”* mukaisesti. Tällaisella lainsäädännöllä tarkoitetaan *”lainsäädäntöä, jolla suojataan yksilöiden perusoikeudet ja -vapaudet ja erityisesti näiden yksilöiden oikeus yksityisyyteen henkilötietojen käsittelyssä ja jota sovelletaan rekisterinpitäjään siinä jäsenvaltioissa, johon tietojen viejä on sijoittautunut”.* Unionin tuomioistuin vahvistaa, että yleisen tietosuoja-asetuksen säännökset, perusoikeuskirjan valossa luettuna, ovat osa tätä lainsäädäntöä, ks. Euroopan unionin tuomioistuimen asiassa C-311/18 (Schrems II) antaman tuomion 138 kohta.

Euroopan talousalueella toimivaltaiselle valvontaviranomaiselle, mikäli se on mahdollista kolmannen maan oikeusjärjestyksen mukaan.

121. Tehokkuuden edellytykset:

- Tällaisilla tiedoilla EU:n lainsäädännön tarjoamasta suojasta ja velvoitteiden ristiriidasta pitäisi olla jonkin verran oikeusvaikutusta kolmannen maan oikeusjärjestyksessä, kuten pääsyä koskevan määräyksen tai pyynnön oikeudellinen tai hallinnollinen tarkastelu, tuomioistuimen määräyksen vaatiminen ja/tai määräyksen väliaikainen lykkääminen tietojen suojan lisäämiseksi.
- Maan oikeusjärjestelmässä ei saa estää tuojaa ilmoittamasta viejälle tai vähintään Euroopan talousalueella toimivaltaiselle valvontaviranomaiselle saadusta pääsyä koskevasta määräyksestä tai pyynnöstä.
- Tuojan on pystyttävä dokumentoimaan toteuttamansa toimenpiteet ja osoittamaan ne viejälle sekä pyrittävä parhaan kykynsä mukaan täyttämään tämän sitoumuksen.

Rekisteröityjen oikeuksien käyttöä koskevien mahdollisuuksien lisääminen

122. Sopimuksessa voitaisiin määrätä, että pelkkänä tekstinä tavanomaisessa liiketoiminnassa (myös tukipalvelujen yhteydessä) toimitettuihin henkilötietoihin voi päästä vain viejän ja/tai rekisteröidyn antaman, tiettyä pääsyä tietoihin koskevan nimenomaisen tai hiljaisen sopimuksen perusteella.

123. Tehokkuuden edellytykset:

- Tämä lauseke voisi olla tehokas tilanteissa, joissa tuojat saavat viranomaisilta pyyntöjä vapaaehtoisesta yhteistyöstä, verrattuna esimerkiksi viranomaisten tietoihin pääsyyn, joka tapahtuu ilman, että tuoja tietää siitä, tai sen tahdon vastaisesti.
- Joissakin tapauksissa rekisteröity ei ehkä pysty vastustamaan pääsyä tai antamaan suostumusta, joka täyttää kaikki EU:n lainsäädännössä asetetut ehdot (vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen) (esim. kun kyse on työntekijöistä)[101].
- Kansalliset määräykset tai toimintaperiaatteet, joilla pakotetaan tuoja olemaan julkistamatta pääsyä koskevaa määräystä, voivat tehdä tästä lausekkeesta tehottoman, ellei sitä voida tukea teknisillä menetelmillä, jotka edellyttävät viejän tai rekisteröidyn toimia, jotta pelkkänä tekstinä olevia tietoja voidaan käsitellä. Tällaisia pääsyä rajoittavia teknisiä toimenpiteitä voidaan määrätä erityisesti, jos pääsy myönnetään vain erityisissä tuki- tai palvelutapauksissa, mutta itse tietoja säilytetään Euroopan talousalueella.

***

124. Sopimuksella voitaisiin velvoittaa tuoja ja/tai viejä ilmoittamaan viipymättä rekisteröidylle kolmannen maan viranomaisilta saadusta pyynnöstä tai määräyksestä tai siitä, että tuoja ei pysty noudattamaan sopimukseen perustuvia sitoumuksia, jotta rekisteröity voi hakea tietoja ja tehokasta oikeussuojaa (esim. esittämällä vaatimuksen toimivaltaiselle valvontaviranomaiselle ja/tai oikeusviranomaiselle ja osoittamalla asiavaltuutensa kolmannen maan tuomioistuimissa)

[101] Yleisen tietosuoja-asetuksen 4 artiklan 11 kohta.

sekä korvauksia tietojen tuojalta mahdollisista aineellisista ja aineettomista vahingoista, joita rekisteröidylle on koitunut siitä, että hänen valitulla tiedonsiirtovälineellä siirrettyjä henkilötietojaan on luovutettu välineeseen sisältyvien sitoumusten vastaisesti.

125. Tehokkuuden edellytykset:

- Tällä ilmoituksella voitaisiin varoittaa rekisteröityä siitä, että kolmansien maiden viranomaiset ovat voineet päästä hänen tietoihinsa. Näin rekisteröity voisi hakea lisätietoja viejiltä ja esittää vaatimuksen toimivaltaiselle valvontaviranomaiselle. Tällä lausekkeella voitaisiin puuttua myös joihinkin hankaluuksiin, joita yksilöllä voi olla asiavaltuutensa (locus standi) osoittamisessa kolmannen maan tuomioistuimissa, jotta hän voi haastaa viranomaisten pääsyn tietoihinsa.
- Kansalliset määräykset ja toimintaperiaatteet voivat estää tämän ilmoituksen tekemisen rekisteröidylle. Viejä ja tuoja voisivat joka tapauksessa sitoutua ilmoittamaan rekisteröidyille heti, kun tietojen luovuttamista koskevat rajoitukset poistetaan, ja tekemään kaikkensa saadakseen poikkeusluvan luovuttamiskiellolle. Viejä tai toimivaltainen valvontaviranomainen voisi vähintään ilmoittaa rekisteröidylle tämän henkilötietojen siirron keskeyttämisestä tai lopettamisesta siksi, että tuoja ei pysty noudattamaan sopimukseen perustuvia sitoumuksiaan, koska se on saanut pääsyä koskevan pyynnön.

***

126. Sopimuksella voitaisiin velvoittaa viejä ja tuoja auttamaan rekisteröityä käyttämään oikeuksiaan kolmannen maan lainkäyttöalueella tapauskohtaisten oikeussuojamekanismien ja oikeudellisen neuvonnan avulla.

127. Tehokkuuden edellytykset

- Joidenkin kansallisten asetusten perusteella tietojen tuoja ei voi antaa tämäntyyppistä apua suoraan rekisteröidyille, vaikka tietojen tuoja voi näiden asetusten nojalla hankkia tällaista apua rekisteröidyille.
- Kansallisissa määräyksissä ja toimintaperiaatteissa voidaan määrätä ehtoja, jotka voivat heikentää käytettävissä olevien tapauskohtaisten oikeussuojamekanismien tehokkuutta.
- Oikeudellinen neuvonta voisi olla rekisteröidylle avuksi etenkin, kun otetaan huomioon, miten monimutkaista ja kallista rekisteröidyn voi olla ymmärtää kolmannen maan oikeusjärjestelmää ja nostaa kanteita ulkomailta, mahdollisesti vieraalla kielellä. Tämä lauseke tarjoaa kuitenkin aina vain rajallista suojaa, koska pelkästään avun ja oikeudellisen neuvonnan tarjoamisella rekisteröidyille ei voida muuttaa sitä, että kolmannen maan oikeusjärjestyksessä ei tarjota suojan tasoa, joka vastaa pääosiltaan Euroopan talousalueella taattua suojaa. Tällä sopimukseen perustuvalla toimenpiteellä väistämättä vain täydennetään muita lisätoimenpiteitä.
- Tämä lisätoimenpide olisi tehokas vain, jos kolmannen maan lainsäädännössä säädetään muutoksenhausta sen kansallisissa tuomioistuimissa tai jos on olemassa tapauskohtainen muutoksenhakumekanismi myös tarkkailutoimia varten.

2.3 Organisatoriset järjestelyt

128. Organisatoriset lisätoimenpiteet voivat koostua sisäisistä toimintaperiaatteista, organisatorisista menetelmistä ja vaatimuksista, joita rekisterinpitäjät ja henkilötietojen käsittelijät voisivat soveltaa itse ja määrätä tietojen tuojille kolmansissa maissa. Niillä voidaan auttaa varmistamaan henkilötietojen suojan johdonmukaisuus koko käsittelyjakson ajan. Organisatorisilla toimenpiteillä voidaan myös parantaa viejien riskitietoisuutta, lisätä niiden tietoa yrityksistä saada pääsy tietoihin kolmansissa maissa ja parantaa niiden valmiutta reagoida yrityksiin. Yhden tai useamman tällaisen toimenpiteen valitseminen ja täytäntöönpano ei välttämättä ja aina varmista, että täytetään EU:n lainsäädännön vaatimus siitä, että siirto vastaa pääosiltaan siinä taattua suojan tasoa. Siirron erityisten olosuhteiden ja kolmannen maan lainsäädännöstä tehdyn arvioinnin perusteella organisatorisia toimenpiteitä tarvitaan täydentämään sopimukseen perustuvia ja/tai teknisiä toimenpiteitä, jotta voidaan varmistaa, että henkilötietojen suojan taso vastaa pääosiltaan Euroopan talousalueella taattua suojaa.

129. Soveltuvimpien toimenpiteiden arviointi on tehtävä tapauskohtaisesti, ja siinä on pidettävä mielessä, että rekisterinpitäjien ja henkilötietojen käsittelijöiden on kunnioitettava osoitusvelvollisuuden periaatetta. Euroopan tietosuojaneuvosto antaa jäljempänä joitakin esimerkkejä organisatorisista toimenpiteistä, joita viejät voivat panna täytäntöön, vaikka luettelo ei olekaan tyhjentävä ja muutkin toimenpiteet voivat olla asianmukaisia:

Sisäiset toimintaperiaatteet, joilla hallinnoidaan siirtoja erityisesti yritysryhmittymien kanssa

130. Laaditaan asianmukaiset sisäiset toimintaperiaatteet, joissa osoitetaan selkeästi tiedonsiirtoa koskevat vastuut, raportointikanavat ja pysyväisohjeet tarkkailutapauksissa tai viranomaisten tietoihin pääsyä koskevissa virallisissa pyynnöissä. Etenkin silloin, kun kyse on siirroista yritysryhmittymien välillä, näihin toimintaperiaatteisiin voi sisältyä muun muassa sellaisen erityisen ryhmän nimittäminen, jonka tulisi koostua tietotekniikkaa, tietosuojaa ja yksityisyydensuojaa koskevan lainsäädännön asiantuntijoista ja käsitellä pyyntöjä, jotka liittyvät Euroopan talousalueelta siirrettyihin henkilötietoihin; ilmoittaminen lakiasiainosaston ylimmälle johdolle ja yrityksen johdolle sekä rekisteröidylle, kun kyseisiä pyyntöjä saadaan; vaiheet menettelyssä, jossa kyseenalaistetaan kohtuuttomat tai lainvastaiset pyynnöt; ja avoin tiedottaminen rekisteröidyille.

131. Suunnitellaan viranomaisten henkilötietoihin pääsyä koskevien pyyntöjen käsittelystä vastaavalle henkilöstölle erityisiä koulutusohjelmia, joita pitäisi päivittää säännöllisesti, jotta ne perustuvat uusimpaan kolmannessa maassa ja Euroopan talousalueella tapahtuneeseen lainsäädännölliseen ja lainopilliseen kehitykseen. Koulutusmenettelyjen pitäisi sisältää EU:n lainsäädännön vaatimukset viranomaisten pääsystä henkilötietoihin, erityisesti perusoikeuskirjan 52 artiklan 1 kohdasta johtuvat. Henkilöstön tietoisuutta olisi lisättävä erityisesti arvioimalla käytännön esimerkkejä viranomaisten tietoihin pääsyä koskevista pyynnöistä ja soveltamalla perusoikeuskirjan 52 artiklan 1 kohdasta johtuvaa vaatimusta kyseisiin käytännön esimerkkeihin. Tässä koulutuksessa olisi otettava huomioon tietojen tuojan erityistilanne, esimerkiksi kolmannen maan lainsäädäntö ja määräykset, joita sovelletaan tietojen tuojaan, ja sitä olisi kehitettävä mahdollisuuksien mukaan tietojen viejän kanssa.

132. Tehokkuuden edellytykset:

- Näitä toimintaperiaatteita voidaan suunnitella vain tapauksissa, joissa kolmannen maan viranomaisten pyyntö on EU:n lainsäädännön mukainen[102]. Kun pyyntö ei ole EU:n lainsäädännön mukainen, nämä toimintaperiaatteet eivät riitä varmistamaan henkilötiedoille suojan tasoa, joka vastaa pääosiltaan Euroopan talousalueella taattua suojaa, ja, kuten edellä on todettu, siirrot on lopetettava tai on otettava käyttöön asianmukaisia lisätoimenpiteitä pääsyn estämiseksi.

Läpinäkyvyyttä ja osoitusvelvollisuutta koskevat toimenpiteet

133. Dokumentoidaan ja rekisteröidään viranomaisilta saadut pääsyä koskevat pyynnöt ja annettu vastaus sekä lainopillinen perustelu ja mukana olevat toimijat (esim. se, onko viejälle ilmoitettu ja sen vastaus, kyseisten pyyntöjen käsittelystä vastaavan ryhmän arviointi). Nämä rekisterit olisi asetettava tietojen viejän saataville, ja se vuorostaan antaa ne tarvittaessa kyseessä oleville rekisteröidyille.

134. Tehokkuuden edellytykset:

- Kolmannen maan kansallisessa lainsäädännössä voidaan estää pyyntöjen tai niiden olennaisten tietojen luovuttaminen ja näin tehdä tästä käytännöstä tehotonta. Tietojen tuojan olisi ilmoitettava viejälle, että se ei pysty toimittamaan kyseisiä asiakirjoja ja rekistereitä, ja annettava siten viejälle mahdollisuus keskeyttää siirrot, jos tämä johtaisi siihen, ettei asianmukaista suojan tasoa voitaisi taata.

***

135. Julkaistaan säännöllisesti läpinäkyvyyttä koskevat raportit tai tiivistelmät tietoihin pääsyä koskevista viranomaisten pyynnöistä ja siitä, miten niihin on vastattu, mikäli se sallitaan paikallisen lainsäädännön nojalla.

136. Tehokkuuden edellytykset:

- Annettujen tietojen pitäisi olla merkityksellisiä, selviä ja mahdollisimman yksityiskohtaisia. Kolmannen maan kansallisella lainsäädännöllä voidaan estää yksityiskohtaisten tietojen julkistaminen. Näissä tapauksissa tietojen tuojan olisi pyrittävä parhaansa mukaan julkaisemaan tilastotietoja tai vastaavanlaisia yhdistelmätietoja.

Organisointimenetelmät ja tietojen minimointia koskevat toimenpiteet

137. Siirron yhteydessä hyödyllisiä toimenpiteitä voivat olla myös osoitusvelvollisuuden periaatteen nojalla jo voimassa olevat organisatoriset vaatimukset, kuten tiukkojen ja tarkkojen tietoihin pääsyä ja luottamuksellisuutta koskevien toimintaperiaatteiden ja parhaiden käytäntöjen hyväksyminen tiukasti tiedonsaantitarpeen perusteella sekä niiden seuranta säännöllisillä tarkastuksilla ja valvonta kurinpitomenettelyillä. Tietojen minimointi olisi otettava huomioon tässä yhteydessä, jotta voidaan rajoittaa henkilötietojen altistumista luvattomalle pääsylle. Joissakin tapauksissa ei välttämättä ole tarpeen siirtää tiettyjä tietoja (esim. jos kyse on

[102] Ks. asia C-362/14 (Schrems I), 94 kohta; asia C-311/18 (Schrems II), 168, 174, 175 ja 176 kohta.

etäpääsystä Euroopan talousalueella oleviin tietoihin, kuten tukitapauksissa, kun täyden pääsyn sijasta myönnetään rajoitettu pääsy, tai kun palvelun toimittaminen edellyttää vain rajallisen tietokokonaisuuden eikä koko tietokannan siirtämistä).

138. Tehokkuuden edellytykset:

- Käytössä olisi oltava säännölliset tarkastukset ja voimakkaat kurinpitotoimenpiteet, jotta tietojen minimointia koskevien toimenpiteiden noudattamista voidaan seurata ja valvoa myös siirron yhteydessä.
- Tietojen viejän on tehtävä hallussaan olevista henkilötiedoista arviointi ennen siirron tekemistä, jotta se voi tunnistaa tietokokonaisuudet, jotka eivät ole välttämättömiä siirrossa ja joita ei siksi jaeta tietojen tuojan kanssa.
- Tietojen minimointia koskevia toimenpiteitä olisi tuettava teknisillä toimenpiteillä, jotta voidaan varmistaa, että tietoihin ei pääse luvatta. Esimerkiksi suojattujen monen osapuolen laskentamekanismien käyttöönotolla ja salattujen tietokokonaisuuksien jakamisella eri luotetuille yhteisöille voidaan estää sisäänrakennetusti se, että yksipuolinen pääsy johtaisi tunnistettavissa olevien tietojen luovuttamiseen.

***

139. Kehitetään parhaita käytäntöjä, joiden avulla mahdollinen tietosuojavaltuutettu saadaan mukaan ja annetaan hänelle pääsy tietoihin asianmukaisesti ja oikea-aikaisesti sekä annetaan henkilötietojen kansainvälisiin siirtoihin liittyvissä asioissa pääsy tietoihin oikeudellisille ja sisäisille tarkastusyksiköille.

140. Tehokkuuden edellytykset:

- Mahdolliselle tietosuojavaltuutetulle sekä oikeudelliselle ja sisäiselle tarkastusryhmälle annetaan kaikki asiaankuuluvat tiedot ennen siirtoa, ja niitä kuullaan siitä, onko siirto tarpeen ja tarvitaanko mahdollisesti lisäsuojatoimia.
- Asiaankuuluviin tietoihin pitäisi sisältyä esimerkiksi tiettyjen henkilötietojen siirron tarpeellisuuden arviointi, katsaus sovellettavista kolmannen maan laeista ja suojatoimet, jotka tuoja on sitoutunut panemaan täytäntöön.

Vaatimusten ja parhaiden käytäntöjen laatiminen

141. Laaditaan tiukat tietosuojaa ja yksityisyyttä koskevat toimintaperiaatteet, jotka perustuvat EU:n sertifiointiin tai käytännesääntöihin tai kansainvälisiin standardeihin (esim. ISO-standardit) ja parhaisiin käytäntöihin (esim. ENISA), ja otetaan niissä asianmukaisesti huomioon uusin tekniikka käsiteltävien tietojen luokkia koskevan riskin mukaisesti.

Muut toimet

142. Laaditaan sisäiset toimintaperiaatteet, joilla arvioidaan täytäntöön pantujen lisätoimenpiteiden soveltuvuutta, ja arvioidaan niitä säännöllisesti, sekä yksilöidään ja toteutetaan tarvittaessa täydentäviä tai vaihtoehtoisia ratkaisuja, jotta voidaan varmistaa, että Euroopan talousalueella siirrettäville henkilötiedoille taattua suojan tasoa vastaavaa tasoa pidetään yllä.

***

143. Tietojen tuojan sitoumukset olla osallistumatta mihinkään henkilötietojen edelleen siirtämiseen samassa kolmannessa maassa tai muihin kolmansiin maihin tai keskeyttää käynnissä olevat siirrot, kun kolmannessa maassa ei voida taata henkilötiedoille suojan tasoa, joka vastaa pääosiltaan Euroopan talousalueella taattua suojaa.[103]

[103] C-311/18 (Schrems II), 135 ja 137 kohta.

LIITE 3: KOLMANNEN MAAN ARVIOINNISSA KÄYTETTÄVÄT MAHDOLLISET TIETOLÄHTEET

144. Tietojen tuojan pitäisi pystyä antamaan tietojen viejälle asiaankuuluvat lähteet ja tiedot kolmannesta maasta, johon tuoja on sijoittautunut, sekä tiedot laeista ja käytännöistä, joita tuojaan ja siirrettäviin tietoihin sovelletaan. Tietojen viejä ja tietojen tuoja voivat viitata useisiin tietolähteisiin, kuten jäljempänä lueteltuihin esimerkkeihin, jotka on esitetty tärkeysjärjestyksessä:

- Euroopan unionin tuomioistuimen (EUT) ja Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytäntö[104], johon viitataan eurooppalaisista olennaisista takeista annetuissa suosituksissa;[105]
- Riittävyyttä koskevat päätökset kohdemaassa, jos siirrossa käytetään eri oikeusperustetta;[106]
- Hallitustenvälisten järjestöjen, kuten Euroopan neuvoston[107], muiden alueellisten elinten[108] ja YK:n elinten ja virastojen (esim. YK:n ihmisoikeusneuvoston,[109] ihmisoikeuskomitean[110]) päätöslauselmat ja raportit;
- Toimivaltaisten sääntelyverkostojen, kuten Global Privacy Assemblyn (GPA:n), laatimat raportit ja analyysit;[111]
- Kansallinen oikeuskäytäntö tai kolmansien maiden yksityisyydensuojan ja tietosuojan alalla toimivaltaisten riippumattomien oikeus- tai hallintoviranomaisten tekemät päätökset;
- Riippumattomien valvontaelinten tai parlamentin elinten raportit;
- Raportit, jotka perustuvat käytännön kokemuksiin viranomaisten aiemmista tietojenluovutuspyynnöistä, tai jos niitä ei ole, tuojan kanssa samalla alalla toimivien yhteisöjen kokemuksiin;
- Warrant Canary -ilmoitukset muilta yhteisöiltä, jotka käsittelevät henkilötietoja samalla alalla kuin tuoja;
- Viejän maan tai muiden kolmansien maiden, jotka vievät tietoja siihen kolmanteen maahan, johon siirto tehdään, kauppakamarien, yrittäjäjärjestöjen, ammatti- ja toimialajärjestöjen,

---

[104] Ks. tietokooste joukkovalvontaa koskevasta EIT:n oikeuskäytännöstä: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Ks. tietosuojaneuvoston suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista, 10. marraskuuta 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] Asiassa C-311/18 (Schrems II) annetun tuomion 141 kohta; ks. riittävyyttä koskevat päätökset osoitteessa https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Ks. esimerkiksi Amerikan valtioiden ihmisoikeustoimikunnan maakohtaiset raportit (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[109] Ks. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Ks.: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Ks. esim. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

valtioiden diplomaattisten, kaupallisten ja investointeihin liittyvien edustustojen laatimat tai tilaamat raportit;

- Tutkimuslaitosten ja kansalaisyhteiskunnan järjestöjen (esim. kansalaisjärjestöjen) raportit;
- yksityisten liiketoimintatiedon tarjoajien laatimat raportit, jotka koskevat yritysten taloudellisia sekä sääntelyyn ja maineeseen liittyviä riskejä;
- Tuojan omat Warrant Canary -ilmoitukset; [112]
- Avoimuusraportit, jos niissä nimenomaisesti mainitaan, ettei pyyntöjä saada pääsy tietoihin ole vastaanotettu. Avoimuusraportit, joissa ei mainita tästä mitään, eivät kelpaa riittäväksi näytöksi, koska näissä raporteissa keskitytään useimmiten lainvalvontaviranomaisilta tulleisiin pyyntöihin saada pääsy tietoihin, ja niissä annetaan vain tätä koskevia lukuja mutta ei käsitellä niitä pyyntöjä, joissa pyydetään pääsyä tietoihin kansallisen turvallisuuden vuoksi. Tämä ei tarkoita sitä, ettei pyyntöjä saada pääsy tietoihin olisi vastaanotettu, vaan ennemminkin sitä, ettei tätä koskevia tietoja voida julkistaa; [113]
- Tuojan sisäiset lausunnot tai merkinnät, joissa nimenomaisesti todetaan, ettei pyyntöjä saada pääsy tietoihin ole vastaanotettu riittävän pitkän ajan kuluessa; ensisijaisia ovat sellaiset lausunnot ja merkinnät, jotka liittyvät tuojan vastuuseen ja/tai joiden laatijoilla on sellaiset sisäiset toimenkuvat, joihin liittyy tietty määrä itsenäisyyttä, kuten sisäisillä tarkastajilla, tietosuojavastaavilla jne. [114]

[112] Ks. kohdasta 47 edellytykset, joiden täyttyessä kannattaa ottaa huomioon tuojan dokumentoima käytännön kokemus kolmannen maan viranomaisilta aiemmin vastaanotetuista pyynnöistä saada pääsy tietoihin.
[113] Ks. edellinen alaviite.
[114] Ks. edellinen alaviite.