

Suosituksset



Translations proofread by EDPB Members.
This language version has not yet been proofread.

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

Annettu 10. marraskuuta 2020

Tiivistelmä

EU:n yleisellä tietosuojasetuksella 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 ETA:ssa myönnettyä suojaa. Tuomioistuin vahvistaa tämän myös selventämällä, että kolmansissa maissa tarjottavan suojan tason ei tarvitse olla täysin sama kuin ETA:ssa 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.

Vakiosopimuslausekkeitä ja muita yleisen tietosuojasetuksen 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, horjuttaako kolmannen maan laki tai käytäntö yleisen tietosuojasetuksen 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 edellytetyille tasolle. Tuomioistuin ei täsmennä, mitä nämä toimenpiteet voisivat olla. Tuomioistuin kuitenkin korostaa, että tietojen viejien on yksilöitävä ne tapauskohtaisesti. Tämä on yleisen tietosuojasetuksen 5 artiklan 2 kohdan osoitusvelvollisuuden periaatteen mukaista. Siinä edellytetään, että rekisterinpitäjä vastaa yleisen tietosuojasetuksen 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 tietosuojasetuksen 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 rajoitettuja siihen, mikä on tarpeellista niiden kolmanteen maahan siirtämisen ja siellä käsittelyn kannalta.

Toiseksi on tarkistettava, että tiedonsiirrossa käytettävä siirtoväline luetellaan yleisen tietosuojasetuksen V luvussa. Jos Euroopan komissio on jo todennut, että maa, alue tai sektori, johon tietoja siirretään, tarjoaa riittävän tietosuojan tason jonkin sellaisen tietosuojan riittävyttä koskevan päätöksensä perusteella, joka on tehty yleisen tietosuojasetuksen 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 riittävyttä koskeva päätös pysyy voimassa. Jos riittävyttä koskevaa päätöstä ei ole, on käytettävä jotakin yleisen tietosuojasetuksen 46 artiklassa luetelluista tiedonsiirtovälineistä säännöllisiä ja toistuvia siirtoja varten. Vain joissakin tapauksissa, kun siirrot ovat satunnaisia ja yksittäisiä, voi ehtojen täytyessä turvautua johonkin yleisen tietosuojasetuksen 49 artiklassa säädettyyn poikkeukseen.

Kolmanneksi on arvioitava, onko **kolmannen maan laeissa tai käytännöissä** jotakin, mikä voi horjuttaa käytettävien tiedonsiirtovälineiden asianmukaisten suojatoimien tehokkuutta nimenomaisen siirron yhteydessä. Arvioinnissa on keskityttävä ensisijaisesti kolmannen maan lainsäädäntöön, joka on merkityksellistä siirron ja yleisen tietosuoja-asetuksen 46 artiklassa tarkoitetun käytettävän tiedonsiirtovälineen kannalta ja joka voi heikentää sen suojan tasoa. Euroopan tietosuojaneuvoston EU:n keskeisiä suojatoimia koskevista suosituksista saa lisätietoja niiden tekijöiden arviointiin, jotka on otettava huomioon arvioitaessa kolmannen maan lainsäädäntöä, joka koskee viranomaisten pääsyä tietoihin tarkkailua varten. Tähän on kiinnitettävä huomiota erityisesti, kun viranomaisten tietoihin pääsyä koskeva lainsäädäntö on moniselitteinen tai se ei ole yleisesti saatavilla. Jos olosuhteista, joissa viranomaiset voivat päästä henkilötietoihin, ei ole lainsäädäntöä ja jos siirto halutaan edelleen tehdä, on tarkasteltava muita merkityksellisiä ja objektiivisia tekijöitä. Siinä ei pidä turvautua subjektiivisiin tekijöihin, kuten siihen, miten todennäköisesti viranomaiset pääsevät tietoihin EU:n vaatimusten vastaisesti. Tämä arviointi on tehtävä asianmukaisen huolellisesti, ja se on dokumentoitava perusteellisesti, koska viejä on vastuussa sen perusteella tehtävästä päätöksestä.

Neljänneksi on yksilöitävä ja hyväksyttävä lisätoimenpiteet, joita tarvitaan saamaan siirrettävien tietojen suojan taso pääosiltaan EU:n vaatimuksia vastaavalle tasolle. Tämä vaihe on tarpeen vain, jos arvioinnista käy ilmi, että kolmannen maan lainsäädäntö horjuttaa 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 olosuhteita, joita niiden tehokkuus edellyttää. 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 käytettävän tiedonsiirtovälineen valossa. Viejä on vastuussa tekemästään päätöksestä. Tämä voi myös edellyttää useiden lisätoimenpiteiden yhdistämistä. Loppujen lopuksi voidaan kuitenkin huomata, että tietyille 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. Kyseiset muodollisuudet yksilöidään näissä suosituksissa. Joidenkin osalta on ehkä kuultava toimivaltaisia valvontaviranomaisia.

Kuudenneksi ja viimeiseksi on arvioitava uudelleen asianmukaisin väliajoin kolmanteen maahan siirretyille tiedoille 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. Kuten tuomioistuimien muistuttaa, valvontaviranomaiset keskeyttävät tai kieltävät tietojen siirrot niissä tapauksissa, joissa tutkimuksen tai kantelun perusteella havaitaan, että pääosiltaan vastaavaa suojan tasoa ei voida varmistaa.

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

Sisällysluettelo

1	Osoitusvelvollisuus tiedonsiirroissa	7
2	Etenemissuunnitelma: osoitusvelvollisuuden periaatteen soveltaminen tiedonsiirtoihin käytännössä.....	8
2.1	Vaihe 1: Siirtojen tunteminen	8
2.2	Vaihe 2: Käytettävien tiedonsiirtovälineiden yksilöiminen.....	9
2.3	Vaihe 3: Arvioidaan, onko yleisen tietosuoja-asetuksen 46 artiklan mukainen käytettävä tiedonsiirtoväline tehokas kaikissa siirron olosuhteissa	12
2.4	Vaihe 4: Lisätoimenpiteiden hyväksyntä.....	15
2.5	Vaihe 5: Tehokkaiden lisätoimenpiteiden määrittämistä seuraavat menettelyvaiheet	17
2.6	Vaihe 6: Uudelleenarviointi säännöllisin väliajoin.....	19
3	Päätelmät	20
	LIITE 1: MÄÄRITELMÄT	21
	LIITE 2: ESIMERKKEJÄ LISÄTOIMENPITEISTÄ	22
	Tekniset toimenpiteet	22
	Sopimukseen perustuvat lisätoimenpiteet	29
	Organisatoriset toimenpiteet.....	36
	LIITE 3: KOLMANNEN MAAN ARVIOINNISSA KÄYTETTÄVÄT MAHDOLLISET TIETOLÄHTEET	40

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 ETA:n sekakomitean päätöksellä nro 154/2018¹,

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 tietosuoja koskevien vakiolausekkeiden perusteella, saavat sellaisen suojan tason, joka pääosiltaan vastaa tasoa, joka taataan Euroopan unionissa tämän asetuksen, luettuna Euroopan unionin perusoikeuskirjan valossa, nojalla².

(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 maahan³.

(3) Yleisen tietosuoja-asetuksen johdanto-osan 108 kappaleessa ja 46 artiklan 1 kohdassa säädetään, että jos EU:n tietosuojan riittävyttä 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 tietosujaa koskevia vakiolausekkeitä.

¹ Viittauksilla 'jäsenvaltioihin' tarkoitetaan koko tässä asiakirjassa ETA:n 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 selvittää, 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 siirron vastaanottajan 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 lisätoimenpiteitä⁵.

(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 maahan⁶.

(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 tasoa, joka taataan Euroopan unionissa. Näillä suosituksilla Euroopan tietosuojaneuvosto pyrkii tukemaan yleisen tietosuoja-asetuksen ja tuomioistuimen tuomioiden johdonmukaista soveltamista Euroopan tietosuojaneuvoston toimeksiannon mukaisesti⁷.

ON ANTANUT SEURAAVAN LAUSUNNON:

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 perusoikeudeksi⁸. Tietosuoja 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 perusoikeuksiin¹⁰.
2. Kun tietoja siirretään kolmansiin maihin ETA:n 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.
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 noudattaminen¹¹. 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, suurelle yleisölle 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 siirtoihin¹³, koska myös ne ovat itsessään tietojen käsittelyä¹⁴. 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 toteutettu¹⁵.
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 asetun suojan tason mukaisesti, ja keskeyttää tietojen siirto ja/tai irtisanoa sopimus, kun tietojen tuoja ei voi tai ei enää voi noudattaa tietosuoja koskevia vakiolausekkeita, jotka sisältyvät viejän ja tuojan väliseen asiaankuuluvaan sopimukseen¹⁶. Viejänä toimivan rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että tuojat tekevät tarvittaessa yhteistyötä viejän

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.

¹⁶ C-311/18 (Schrems II), 134, 135, 139, 140, 141 ja 142 kohta.

kanssa sen täyttäessä näitä vastuita, tiedottamalla esimerkiksi kaikesta kehityksestä, joka vaikuttaa tuojan maassa vastaan otettujen henkilötietojen suojan tasoon¹⁷. Näillä vastuilla sovelletaan yleisen tietosuoja-asetuksen osoitusvelvollisuuden periaatetta tiedonsiirtoihin¹⁸.

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 ETA:n ulkopuolelle. ”Tietojen viejällä” tarkoitetaan tässä asiakirjassa tietojen viejänä 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 elimille¹⁹. Julkisen sektorin elinten välisistä henkilötietojen siirroista annetaan erityisiä ohjeita *ohjeissa 2/2020 yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan a alakohdasta ja 46 artiklan 3 kohdan b alakohdasta, joita sovelletaan henkilötietojen siirtoihin ETA:n viranomaisten ja elinten sekä ETA:n ulkopuolisten viranomaisten ja elinten välillä*²⁰.
7. Tietojen viejän on dokumentoitava asianmukaisesti tämä arviointi sekä valitut ja toteutettavat lisätoimenpiteet ja annettava kyseinen dokumentaatio toimivaltaisen valvontaviranomaisen saataville pyynnöstä²¹.

2.1 Vaihe 1: Siirtojen tunteminen

8. Jotta voidaan selvittää, mitä tietojen viejältä voidaan edellyttää, jotta henkilötietojen siirtämistä voidaan jatkaa tai uusia siirtoja tehdä²², 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 ja käyttävät useita henkilötietojen käsittelijöitä ja alikäsittelijöitä. Siirtojen tunteminen on olennaisen tärkeä ensimmäinen vaihe osoitusvelvollisuuden periaatteen mukaisten velvollisuuksien täyttämässä.

¹⁷ C-311/18 (Schrems II), 134 kohta.

¹⁸ Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 28 artiklan 3 kohdan h alakohta.

¹⁹ 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_fi

²⁰ Euroopan tietosuojaneuvoston ohjeet 2/2020 yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan a alakohdasta ja 46 artiklan 3 kohdan b alakohdasta, joita sovelletaan henkilötietojen siirtoihin ETA:n viranomaisten ja elinten sekä ETA:n ulkopuolisten viranomaisten ja elinten välillä; ks. (englanniksi) https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en

²¹ Yleisen tietosuoja-asetuksen 5 artiklan 2 kohta ja 24 artiklan 1 kohta.

²² On huomattava, että siirroksi katsotaan myös se, että kolmannessa maassa sijaitseva yhteisö käyttää ETA:ssa sijaitsevia tietoja etäyhteydellä.

9. Siirtojen täydellisessä tuntemisessa voi olla apua käsittelytoimia koskevista selosteista, joita rekisterinpitäjänä tai henkilötietojen käsittelijänä on ehkä pidettävä yleisen tietosuoja-asetuksen 30 artiklan mukaisesti²³. 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 avuksi²⁴.
10. Siirtoja kartoitettaessa on muistettava ottaa huomioon tietojen siirtäminen edelleen, esimerkiksi se, siirtävätkö ETA:n ulkopuolella olevat henkilötietojen käsittelijät, joille viejä on antanut käsittelyn tehtäväksi, henkilötietoja alikäsittelijälle toisessa kolmannessa maassa tai samassa kolmannessa maassa²⁵.
11. Yleisen tietosuoja-asetuksen tietojen minimoinnin periaatteen²⁶ mukaisesti on tarkistettava, että siirrettävät tiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista niiden kolmanteen maahan siirtämisen ja siellä 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 ETA:n ulkopuolella sijaitsevaan pilvipalveluun katsotaan tiedonsiirroksi²⁷. Tarkemmin sanottuna, jos viejä käyttää kansainvälistä pilvipalveluinfrastruktuuria, tämän on arvioitava, siirretäänkö tiedot kolmansiin maihin ja minne niissä, ellei pilvipalvelun tarjoaja 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.

²³ 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 veloitteesta pitää selostetta käsittelystä (yleisen tietosuoja-asetuksen 30 artiklan 5 kohta). Tästä vapautuksesta on ohjeita 29 artiklan mukaisen tietosuojojatyöryhmän kannanotossa poikkeuksista velvollisuuteen pitää yleisen tietosuoja-asetuksen 30 artiklan 5 kohdan mukaista selostetta käsittelytoimista (Euroopan tietosuojaneuvosto hyväksyi kannanoton 25. toukokuuta 2018).

²⁴ 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.

²⁵ Jos rekisterinpitäjä on antanut erityisen tai yleisen kirjallisen ennakkoluvan yleisen tietosuoja-asetuksen 28 artiklan 2 kohdan mukaisesti.

²⁶ Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohta.

²⁷ 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.

Riittävyttä koskevat päätökset

15. Euroopan komissio voi tunnustaa **riittävyttä koskevilla päätöksillään** joidenkin tai kaikkien niiden kolmansien maiden osalta, joihin viejä siirtää henkilötietoja, että ne tarjoavat riittävän henkilötietojen suojan tason²⁸.
16. Tällaisen riittävyttä koskevan päätöksen perusteella henkilötiedot voidaan siirtää ETA:sta kyseiseen kolmanteen maahan ilman, että tarvitaan mitään yleisen tietosuojasetuksen 46 artiklan mukaista tiedonsiirtovälinettä.
17. Riittävyttä koskevat päätökset voivat koskea koko maata tai vain sen osaa. Riittävyttä koskevat päätökset voivat koskea kaikkia tiedonsiirtoja maahan tai ne voidaan rajoittaa tietyntyyppisiin siirtoihin (esim. yhdellä sektorilla).²⁹
18. Euroopan komissio julkaisee verkkosivustollaan luettelon riittävyttä koskevista päätöksistä³⁰.
19. Jos henkilötietoja siirretään kolmansiin maihin, alueille tai sektoreille, joita komission riittävyttä koskeva päätös koskee (soveltuissa määrin), **muihin näissä suosituksissa kuvattuihin toimenpiteisiin ei tarvitse ryhtyä**³¹. Viejän on kuitenkin seurattava, kumotaanko tai mitätöidäkö tämän siirtojen kannalta merkitykselliset riittävyttä koskevat päätökset³².
20. Riittävyttä koskevat päätökset eivät kuitenkaan estä rekisteröityjä tekemästä valitusta. Ne eivät myöskään estä valvontaviranomaisia saattamasta asiaa kansallisen tuomioistuimen käsiteltäväksi, jos niillä on epäilyksiä päätöksen pätevydestä, jotta kansallinen tuomioistuin voi pyytää Euroopan unionin tuomioistuimelta ennakkoratkaisua pätevyyden tutkimiseksi³³.

²⁸ Euroopan komissiolla on yleisen tietosuojasetuksen 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.

²⁹ Yleisen tietosuojasetuksen 45 artiklan 1 kohta.

³⁰ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

³¹ Mikäli tietojen viejä ja tuoja ovat toteuttaneet toimenpiteitä yleisen tietosuojasetuksen muiden velvollisuuksien noudattamiseksi. Muussa tapauksessa kyseiset toimenpiteet on pantava täytäntöön.

³² Euroopan komission on tarkasteltava säännöllisesti kaikkia riittävyttä koskevia päätöksiä ja seurattava, varmistavatko kolmannet maat, joista on tehty riittävyttä koskeva päätös, edelleen riittävän suojan tason (ks. yleisen tietosuojasetuksen 45 artiklan 3 ja 4 kohta). Myös Euroopan unionin tuomioistuin voi mitätöidä riittävyttä koskevat päätökset (ks. sen tuomiot asioissa C-362/14 (Schrems I) ja C-311/18 (Schrems II)).

³³ C-311/18 (Schrems II), 118–120 kohta. Valvontaviranomaiset eivät saa jättää ottamatta huomioon riittävyttä 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 tietosuojasetuksen 32 artiklan vastaisesti, tietojenkäsittelyn tukena ei ole pätevää oikeusperustetta, joten se on yleisen tietosuojasetuksen 6 artiklan vastainen). Valvontaviranomaiset voivat tarkastella täysin riippumattomasti, noudatetaanko kyseisten tietojen siirrossa yleisessä tietosuojasetuksessa 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 riittävyttä koskevan päätöksen pätevydestä.

Esimerkki: EU:n kansalainen Maximilian 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 tarkkailuilta, 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). Maximilian Schrems kyseenalaisti tietosuojavaltuutetun päätöksen ja Irlannin High Court pyysi unionin tuomioistuimelta (EUT) ennakkoratkaisua päätöksen 2000/520 pätevydestä. Unionin tuomioistuin päätti mitätöidä komission päätöksen 2000/520 safe harbour -periaatteiden antaman suojan riittävydestä.³⁴

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 riittävyttä koskevia päätöksiä ei ole. Yleisen tietosuoja-asetuksen 46 artiklan mukaisia tärkeimpiä tiedonsiirtovälineitä ovat
 - tietosuoja 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 siirrettävillä henkilötiedoilla on yleisesti ottaen asetuksen vaatimuksia pääosiltaan vastaava suojan taso.
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.³⁵

Poikkeukset

24. Riittävyttä koskevien päätösten ja yleisen tietosuoja-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden lisäksi yleisessä tietosuoja-asetuksessa on kolmaskin keino siirtää henkilötietoja tietyissä tilanteissa. Henkilötietoja voi siirtää tietyin edellytyksin yleisen tietosuoja-asetuksen 49 artiklassa lueteltujen poikkeusten perusteella.
25. Yleisen tietosuoja-asetuksen 49 artikla on poikkeuksellinen. Sen poikkeuksia on siis tulkittava suppeasti, ja ne koskevat pääasiassa satunnaisia ja toistumattomia käsittelytoimia. Euroopan

³⁴ Asia C-362/14 (Schrems I).

³⁵ C-311/18 (Schrems II), 130 ja 133 kohta. Ks. myös jäljempänä 2.3 kohta.

tietosuojaneuvosto on antanut asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevat ohjeet 2/2018.³⁶

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 riittävyttä koskevaan päätökseen eikä 49 artiklan poikkeukseen, on jatkettava vaiheeseen 3.

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

28. Yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen valitseminen ei vielä ehkä riitä. Tiedonsiirtovälineellä on varmistettava, että siirrolla ei vaaranneta yleisellä tietosuoja-asetuksella taattua suojan tasoa³⁷. Tiedonsiirtovälineen on siis oltava käytännössä tehokas.
29. Tehokkuudella tarkoitetaan, että siirrettävät henkilötiedot saavat kolmannessa maassa suojan tason, joka vastaa pääosiltaan ETA:ssa taattua suojan tasoa³⁸. Näin ei ole, jos tietojen tuojaa estetään noudattamasta yleisen tietosuoja-asetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen edellyttämiä velvollisuuksia siirtoon sovellettavien kolmannen maan lakien ja käytäntöjen vuoksi.
30. Siksi tietojen viejän on arvioitava, tarvittaessa yhteistyössä tuojan kanssa, onko kolmannen maan laeissa tai käytännöissä jotakin, mikä voi horjuttaa yleisen tietosuoja-asetuksen 46 artiklan mukaisten käytettävien tiedonsiirtovälineiden asianmukaisten suojatoimien tehokkuutta nimenomaisen siirron yhteydessä. Tarvittaessa tietojen tuojan on annettava tietojen viejälle asiaankuuluvat lähteet ja tiedot kolmannelle maasta, johon se on sijoittautunut, ja siirtoon sovellettavista laeista. Tietojen viejä voi myös käyttää muita tietolähteitä, muun muassa niitä, jotka ovat liitteessä 3 olevassa luettelossa, joka ei ole tyhjentävä³⁹.
31. 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 vastaanottajia siihen osallistuu. Arvioinnissa on esitettävä myös kaikki mahdolliset siirtämiset edelleen.
32. Sitä varten on tarkasteltava kunkin siirron ominaisuuksia ja selvítettävä, miten siirtoihin sovelletaan sen maan kansallista oikeusjärjestystä, johon tietoja siirretään (tai siirretään edelleen).
33. Sovellettava oikeudellinen kehys riippuu siirron 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)

³⁶ Ohjeista on lisätietoa osoitteessa https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_fi.

³⁷ Yleisen tietosuoja-asetuksen 44 artikla.

³⁸ C-311/18 (Schrems II), 105 kohta ja toinen toteamus.

³⁹ Ks. myös jäljempänä 43 kohta.

- sektorista, jolla siirto tapahtuu (esim. mainontateknologia, televiestintä, rahoitus)
 - siirrettävistä henkilötietoryhmistä (esim. lapsiin liittyvät henkilötiedot voivat kuulua kolmannessa maassa erityislainsäädännön piiriin)
 - siitä, säilytetäänkö tietoja kolmannessa maassa vai käytetäänkö EU:ssa/ETA:ssa säilytettäviä tietoja vain etäyhteydellä
 - siirrettävien tietojen muodosta (eli pelkkänä tekstinä / pseudonymisoituna tai salattuna⁴⁰)
 - mahdollisuudesta, että tietoja voidaan siirtää edelleen kolmannelle maalle toiseen kolmanteen maahan⁴¹.
34. Tietojen viejän on arvioitava, horjuttaako jokin sovellettavista laeista yleisen tietosuojasetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen sisältämiä sitoumuksia. Viejän on varmistettava, että sitoumuksia, joiden perusteella rekisteröidyt voivat käyttää oikeuksiaan kansainvälisten siirtojen yhteydessä (kuten siirrettyihin tietoihin tutustumista, niiden oikaisua ja poistamista koskevia pyyntöjä), voidaan soveltaa tehokkaasti käytännössä ja että niitä ei estetä kohteena olevan kolmannen maan lainsäädännöllä.
35. Viejän on arvioitava asiaankuuluvia yleisluonteisia sääntöjä, mikäli ne vaikuttavat yleisen tietosuojasetuksen 46 artiklan mukaisen tiedonsiirtovälineen sisältämien suojoimien tehokkaaseen soveltamiseen ja ihmisten perusoikeuksiin (erityisesti oikeussuojakeinoihin, joita rekisteröidyllä on, jos kolmannen maan viranomaiset pääsevät siirrettyihin tietoihin).
36. 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 ja kansallista turvallisuutta varten). Jos näitä vaatimuksia tai valtuuksia rajoitetaan siihen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista⁴², ne eivät saa horjuttaa yleisen tietosuojasetuksen 46 artiklan mukaisen käytettävän tiedonsiirtovälineen sisältämiä sitoumuksia.
37. EU:n vaatimuksia, kuten Euroopan unionin perusoikeuskirjan 47 ja 52 artiklaa, on käytettävä vertailukohtana arvioitaessa, onko kyseinen viranomaisille sallittu käyttö rajoitettu siihen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, ja onko rekisteröidyille tarjottu tehokas oikeussuojakeino.
38. Tämän arvioinnin tekemisessä merkityksellisiä ovat myös kyseisen kolmannen maan oikeusjärjestelmän eri näkökohdat, esimerkiksi yleisen tietosuojasetuksen 45 artiklan 2 kohdassa luetellut seikat⁴³. 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

⁴⁰ Jotkin kolmannet maat eivät salli salattujen tietojen tuomista.

⁴¹ Jos rekisterinpitäjä on antanut erityisen tai yleisen kirjallisen ennakkoluvan yleisen tietosuojasetuksen 28 artiklan 2 kohdan mukaisesti.

⁴² Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuojasetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 EU:n keskeisistä suojoimista, 10. marraskuuta 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_fi.

⁴³ C-311/18 (Schrems II), 104 kohta.

tietosuojalainsäädäntö tai riippumaton tietosuojaviranomainen sekä se, että noudatetaan tietosuojaa koskevia suojatoimia tarjoavia kansainvälisiä välineitä⁴⁴.

39. Euroopan tietosuojaneuvoston suosituksissa EU:n keskeisistä suojatoimista esitetään tekijöitä, jotka on arvioitava sen selvittämiseksi, voidaanko kolmannen maan viranomaisten (sekä kansallisesta turvallisuudesta vastaavien virastojen että lainvalvontaviranomaisten) pääsyä henkilötietoihin koskeva oikeudellinen kehys katsoa perustelluksi puuttumiseksi (joka ei siten horjuta yleisen tietosuojasetuksen 46 artiklan mukaisen tiedonsiirtovälineen perusteella tehtyjä sitoumuksia) vai ei. Tähän on kiinnitettävä huomiota erityisesti, kun viranomaisten tietoihin pääsyä koskeva lainsäädäntö on moniselitteinen tai se ei ole yleisesti saatavilla.
40. Kun kyse on tiedonsiirtotilanteesta, joka perustuu 46 artiklan mukaisiin tiedonsiirtovälineisiin, tietojen viejä ja tuoja voivat saada Euroopan tietosuojaneuvoston EU:n keskeisiä suojatoimia koskevista suosituksista ohjeita sen arvioimiseen, puututaanko kyseisillä valtuuksilla perusteettomasti tietojen tuojan velvollisuuksiin varmistaa suojan taso, joka pääosiltaan vastaa EU:ssa taattua tasoa.
41. Pääosiltaan vastaavan suojan tason puuttuminen on erityisen selvää silloin, kun siirron kannalta merkittävä kolmannen maan lainsäädäntö tai käytäntö ei täytä EU:n keskeisten suojatoimien vaatimuksia.
42. Arvioinnin on ennen kaikkea perustuttava julkisesti saatavilla olevaan lainsäädäntöön. Joissakin tilanteissa se ei kuitenkaan riitä, koska kolmansissa maissa ei ehkä ole kyseistä lainsäädäntöä. Jos siirto aiotaan tässä tapauksessa edelleen tehdä, on tarkasteltava muita merkityksellisiä ja objektiivisia tekijöitä⁴⁵. Siinä ei pidä turvautua subjektiivisiin tekijöihin kuten siihen, miten todennäköisesti viranomaiset käyttävät tietoja EU:n vaatimusten vastaisesti. Tämä arviointi on tehtävä asianmukaisen huolellisesti ja dokumentoitava perusteellisesti, koska viejä on vastuussa sen perusteella tehtävästä päätöksestä.⁴⁶
43. Arviointia voi täydentää muista lähteistä saaduilla tiedoilla⁴⁷, kuten
 - seikoilla, jotka osoittavat, että kolmannen maan viranomainen pyrkii pääsemään tietoihin tietojen tuojan tietäen tai tietämättä, ilmoitettujen ennakkotapausten, lainsäädännön ja käytännön perusteella
 - seikoilla, jotka osoittavat, että kolmannen maan viranomainen pystyy pääsemään tietoihin tietojen tuojan kautta tai sieppaamalla tietoja suoraan viestintäkanavasta, ilmoitettujen ennakkotapausten, oikeudellisten valtuuksien ja sen käytettävissä olevien teknisten ja taloudellisten resurssien ja henkilöresurssien perusteella.
44. Arviointi voi loppujen lopuksi paljastaa, että yleisen tietosuojasetuksen 46 artiklan mukaisella käytettävällä tiedonsiirtovälineellä ja sen sisältämällä asianmukaisilla suojatoimilla

⁴⁴ Esimerkiksi: yleissopimuksessa 108 (yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, Euroopan neuvoston sopimussarja, nro 108) tai yleissopimuksessa 108+ (nykyaikaistettu yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, ETS nro 223) säädetään täytäntöönpanokelpoisista kansainvälisistä oikeussuojakeinoista tietosuojarikkomuksissa ja edistetään henkilötietojen suojan ja yksityiselämän kunnioittamisen suojan vähimmäistason takaamista.

⁴⁵ Ks. jäljempänä 43 kohta sekä liite 3.

⁴⁶ Yleisen tietosuojasetuksen 5 artiklan 2 kohta.

⁴⁷ Ks. myös liite 3.

- varmistetaan tehokkaasti, että siirrettävät henkilötiedot saavat kolmannessa maassa suojan tason, joka vastaa pääosiltaan ETA:ssa taattua suojan tasoa. Siirtoon sovellettavalla kolmannen maan lainsäädännöllä ja sovellettavilla käytännöillä tietojen tuoja asetetaan tilanteeseen, jossa se noudattaa velvollisuuksiaan valitun tiedonsiirtovälineen mukaisesti. Arviointi on 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 siirtoon sovellettavan kolmannen maan lainsäädännön ja/tai sovellettavien käytäntöjen vuoksi. 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 henkilötietoja⁴⁸.

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 FISAn 702 §:ään perustuvien ohjelmien suojan taso ei vastaa pääosiltaan EU:n lainsäädännössä edellytettyjä suojatoimia. Jos siis tietojen tuoja tai muu myöhempi vastaanottaja, jolle tietojen tuoja voi luovuttaa tietoja, kuuluu FISAn 702 §:n soveltamisalaan⁴⁹, vakiosopimuslausekkeita tai muita yleisen tietosuoja-asetuksen 46 artiklan mukaisia tiedonsiirtovälineitä voidaan käyttää kyseisessä siirrossa vain, jos teknisillä lisätoimenpiteillä estetään pääsy siirrettyihin tietoihin tai tehdään siitä tehotonta.

2.4 Vaihe 4: Lisätoimenpiteiden hyväksyntä

45. Jos vaiheessa 3 tarkoitettu 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 tasoa⁵⁰. ”Lisätoimenpiteillä” täydennetään määritelmänsä mukaan suojatoimia, jotka jo mahdollistetaan yleisen tietosuoja-asetuksen 46 artiklan tiedonsiirtovälineissä⁵¹.
46. Tietojen viejän on yksilöitävä tapauskohtaisesti, mitkä lisätoimenpiteet voisivat olla tehokkaita tiettyyn kolmanteen maahan tehtävissä siirroissa, kun käytetään tiettyä yleisen tietosuoja-asetuksen 46 artiklan mukaista tiedonsiirtovälinettä. Siinä voi hyödyntää aiempia vaiheissa 1, 2 ja 3 tehtyjä

⁴⁸ EUT, C-311/18 (Schrems II), 134–135 kohta.

⁴⁹ FISAn 702 §:ää sovelletaan, jos tiedot saadaan sähköisen viestinnän palveluntarjoajalta tai sen avulla (FISAn 702 § = 50 USC § 1881a, h momentin 2 kohdan A alakohdan vi alakohdan mukaisesti). Se puolestaan määritetään 50 USC § 1881:n b momentin 4 kohdassa seuraavasti:

- a) televiestinnän toiminnanharjoittaja sellaisena kuin termi on määritelty 47 osaston 153 §:ssä
- b) sähköisen viestintäpalvelun tarjoaja sellaisena kuin termi on määritelty 18 osaston 2510 §:ssä
- c) etätietojenkäsittelyn palveluntarjoaja sellaisena kuin termi on määritelty 18 osaston 2711 §:ssä
- d) mikä tahansa muu viestintäpalvelun tarjoaja, jolla on pääsy langalliseen tai sähköiseen viestintään joko silloin, kun kyseistä viestintää siirretään, tai silloin, kun kyseistä viestintää tallennetaan, tai
- e) a, b, c tai d alakohdassa kuvatun yhteisön virkailija, työntekijä tai edustaja.

⁵⁰ C-311/18 (Schrems II), 96 kohta.

⁵¹ Yleisen tietosuoja-asetuksen johdanto-osan 109 kappale ja C-311/18 (Schrems II), 133 kohta.

arviointeja ja tarkistaa niiden havaintojen perusteella lisätoimenpiteiden mahdollisen tehokkuuden vaaditun suojan tason takaamisessa.

47. Lisätoimenpiteet voivat periaatteessa perustua sopimukseen tai ne voivat olla teknisiä tai organisatorisia. Erialaisten toimenpiteiden yhdistäminen toisiaan tukien ja hyödyntäen voi nostaa suojan tasoa ja edistää siten EU:n vaatimusten täyttämistä.
48. Pelkästään sopimukseen perustuvilla ja organisatorisilla toimenpiteillä ei tavallisesti estetä kolmannen maan viranomaisten pääsyä henkilötietoihin (jos tämä puuttuu perusteettomasti tietojen tuojan velvollisuuden varmistaa pääosiltaan vastaava suoja). Joissakin tilanteissa ainoastaan teknisillä toimenpiteillä voidaan estää kolmannen maan viranomaisten pääsy henkilötietoihin tai tehdä siitä tehotonta, etenkin tarkkailutarkoituksissa⁵². Tällaisissa tapauksissa teknisiä toimenpiteitä voidaan täydentää sopimukseen perustuvilla tai organisatorisilla toimenpiteillä ja vahvistaa siten yleistä tietosuojan tasoa, esimerkiksi luomalla esteitä viranomaisten yrityksille päästä tietoihin EU:n vaatimusten vastaisesti.
49. Tietojen viejä voi tarvittaessa yhteistyössä tietojen tuojan kanssa tarkastella seuraavaa tekijöiden luetteloa (joka ei ole tyhjentävä) siirrettäviä tietoja tehokkaimmin suojaavien lisätoimenpiteiden määrittämiseksi:
- siirrettävien tietojen muoto (eli pelkkänä tekstinä / pseudonymisoituna tai salattuna)
 - tietojen luonne
 - 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 huomioon niihin kohteena olevan kolmannen maan lainsäädännön mukaisesti sovellettavat asiaankuuluvat säännökset))⁵³
 - mahdollisuus siihen, että tietoja voidaan siirtää edelleen samassa kolmannessa maassa tai jopa muihin kolmansiin maihin (esim. siten, että siirrossa on mukana tietojen tuojan henkilötietojen alikäsittelijöitä⁵⁴).

Esimerkkejä lisätoimenpiteistä

50. Liitteessä 2 olevissa luetteloissa, jotka eivät ole tyhjentäviä, annetaan esimerkkejä teknisistä, sopimukseen perustuvista ja organisatorisista toimenpiteistä, joiden käyttöä voitaisiin harkita.

⁵² 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 EU:n keskeisistä suojatoimista, 10. marraskuuta 2020, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential.fi>.

⁵³ 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.

⁵⁴ Katso alaviite 25.

51. Jos tietojen viejä on ottanut käyttöön tehokkaita lisätoimenpiteitä, joilla yhdessä yleisen tietosuojasetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen kanssa saavutetaan suojan taso, joka pääosiltaan vastaa ETA:ssa taattua suojan tasoa, siirrot voidaan tehdä.
52. 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 tason⁵⁵, henkilötietojen siirtämistä kolmanteen maahan ei saa aloittaa yleisen tietosuojasetuksen 46 artiklan mukaisen valitun tiedonsiirtovälineen perusteella. Jos siirtoja jo tehdään, henkilötietojen siirto on keskeytettävä tai lopetettava⁵⁶. Yleisen tietosuojasetuksen 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 kokonaisuudessaan⁵⁷.

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

53. Jos tietojen viejä päättää jatkaa siirtoa riippumatta siitä, että tietojen tuoja ei pysty noudattamaan yleisen tietosuojasetuksen 46 artiklan mukaisessa tiedonsiirtovälineessä tehtyjä sitoumuksia, tietojen viejän on annettava se toimivaltaiselle valvontaviranomaiselle tiedoksi kyseessä olevaan yleisen tietosuojasetuksen 46 artiklan mukaiseen siirtovälineeseen sisältyvien erityissäännösten mukaisesti⁵⁸. Toimivaltainen valvontaviranomainen keskeyttää tai kieltää tietojen siirrot niissä tapauksissa, joissa EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa ei voida varmistaa⁵⁹.
54. 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

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

⁵⁵ Jos tällainen pääsy ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista, ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuojasetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset 2/2020 EU:n keskeisistä suojatoimista, 10. marraskuuta 2020, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential.fi>.

⁵⁶ C-311/18 (Schrems II), 135 kohta.

⁵⁷ 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.

⁵⁸ Ks. Euroopan tietosuojaneuvoston usein esitettyjä kysymyksiä, jotka koskevat unionin tuomioistuimen 23. heinäkuuta 2020 antamaa tuomiota asiassa C-311/18 – Data Protection Commissioner v. Facebook Ireland Ltd ja Maximilian Schrems ja erityisesti FAQ 5, 6 ja 9. Ks. myös komission päätöksen 2010/87/EU lausekkeen 4 kohta g sekä komission päätöksen 2001/497/EY lausekkeen 5 kohta a ja komission päätöksen 2004/915/EY liitteessä olevan kokonaisuuden II lausekkeen II kohta c.

⁵⁹ C-311/18 (Schrems II), 113 ja 121 kohta.

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

56. 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 tietosuojaa-asetuksella taattua suojan tasoa ei heikennetä⁶⁰. 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 on voitava osoittaa osoitusvelvollisuuden periaatteen ja tietosuojan riittävän tason takaamista koskevan tietojen viejän velvollisuuden mukaisesti. Toimivaltaisilla valvontaviranomaisilla on valtuudet tarkastella näitä lisälausekkeitä tarvittaessa (esim. valituksen vuoksi tai oma-aloitteisessa tutkinnassa).
57. Jos tietojen viejä aikoo muuttaa tietosuojaa koskevia vakiolausekkeitä itse tai jo lisätyt lisätoimenpiteet ovat suoraan tai epäsuorasti ristiriidassa vakiolausekkeiden kanssa, tietojen viejän ei enää katsota noudattavan vakiosopimuslausekkeitä⁶¹, ja sen on haettava toimivaltaiselta valvontaviranomaiselta lupaa yleisen tietosuojaa-asetuksen 46 artiklan 3 kohdan a alakohdan mukaisesti.

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

58. Asiassa Schrems II annetussa tuomiossa esitettyä perustelua sovelletaan myös muihin yleisen tietosuojaa-asetuksen 46 artiklan 2 kohdan mukaisiin tiedonsiirtovälineisiin, koska kaikki nämä välineet ovat lähtökohtaisesti sopimusluonteisia, joten osapuolten niiden nojalla suunnittelemaat takeet ja tekemät sitoumukset eivät voi sitoa kolmannen maan viranomaisia⁶².
59. Asiassa Schrems II annettu tuomio pätee yritystä koskevien sitovien sääntöjen perusteella tehtyihin henkilötietoihin siirtoihin, koska kolmansien maiden lait voivat vaikuttaa kyseisillä välineillä tarjottuun suojaan. Schrems II -tuomion täsmällisestä vaikutuksesta yritystä koskeviin sitoviin sääntöihin keskustellaan edelleen. Euroopan tietosuojaneuvosto antaa valmisteluasiakirjojen WP 256 ja WP 257

⁶⁰ Tietosuojaa-asetuksen johdanto-osan 109 kappale: ”Se, että rekisterinpitäjä tai henkilötietojen käsittelijä voi käyttää joko komission tai valvontaviranomaisen hyväksymiä tietosuojaa koskevia vakiolausekkeitä, ei saisi estää rekisterinpitäjää tai henkilötietojen käsittelijää sisällyttämästä tietosuojaa koskevia vakiolausekkeitä laajempiin sopimuksiin, kuten henkilötietojen käsittelijän toisen henkilötietojen käsittelijän kanssa tekemään sopimukseen, eikä lisäämästä muita lausekkeitä 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.

⁶¹ Ks. analogisesti Euroopan tietosuojaneuvoston lausunto 17/2020 Slovenian valvontaviranomaisen ehdotuksesta vakiosopimuslausekkeiksi (yleisen tietosuojaa-asetuksen 28 artiklan 8 kohta). Sen 28 artiklan mukaisia vakiosopimuslausekkeitä koskevassa kohdassa on samanlainen säännös (”Tietosuojaneuvosto muistuttaa lisäksi, että mahdollisuus käyttää valvontaviranomaisen hyväksymiä vakiosopimuslausekkeitä ei estä osapuolia lisäämästä muita lausekkeitä tai täydentäviä suojatoimia, mikäli ne eivät ole suoraan tai välillisesti ristiriidassa hyväksytyjen vakiosopimuslausekkeiden kanssa tai vaikuta rekisteröityjen perusoikeuksiin ja -vapauksiin. Jos taas tietosuojaa koskevia vakiolausekkeitä muokataan, osapuolten ei enää katsota panneen täytäntöön hyväksytyjä vakiosopimuslausekkeitä”), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_fi.pdf.

⁶² EUT, C-311/18 (Schrems II), 132 kohta.

viitteissä mahdollisimman pian lisätietoa siitä, onko yritystä koskeviin sitoviin sääntöihin sisällytettävä lisäsitoumuksia⁶³.

60. 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 koskevalla sitovilla säännöillä annettavat takeet täyttää käytännössä. Jos näin ei ole, tietojen viejän on arvioitava, voidaanko toteuttaa lisätoimenpiteitä, joilla varmistetaan Euroopan talousalueella taattavaa tietosuojan tasoa pääosiltaan vastaava tietosuojan taso, ja pystyykö kolmannen maan lainsäädäntö tai käytäntö horjuttamaan näitä lisätoimenpiteitä estämällä niiden tehokkuuden.

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

61. Asiassa Schrems II annetussa tuomiossa esitettyä perustelua sovelletaan myös muihin yleisen tietosuojaa-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 viranomaisia⁶⁴. Asiassa Schrems II annettu tuomio pätee näin ollen tapauskohtaisten sopimuslausekkeiden perusteella tehtyihin henkilötietojen siirtoihin, koska kolmansien maiden lait voivat vaikuttaa kyseisillä välineillä tarjottuun suojaan. Schrems II -tuomion täsmällisestä vaikutuksesta tapauskohtaisiin sopimuslausekkeisiin keskustellaan edelleen. Euroopan tietosuojaneuvosto antaa lisätietoa mahdollisimman pian.

2.6 Vaihe 6: Uudelleenarviointi säännöllisin väliajoin

62. 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 tietosuojaa-asetuksen 5 artiklan 2 kohta).
63. Käyttöön on otettava riittävän vankat mekanismit, joilla varmistetaan, että siirrot keskeytetään tai lopetetaan viipymättä, jos
- tietojen tuoja on rikkonut yleisen tietosuojaa-asetuksen 46 artiklan mukaisessa tiedonsiirtovälineessä tekemiään sitoumuksia tai ei pysty noudattamaan niitä tai
 - lisätoimenpiteet eivät ole enää tehokkaita kyseisessä kolmannessa maassa.

⁶³ Tietosuojatyöryhmä, 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; tietosuojatyöryhmä, 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.

⁶⁴ EUT, C-311/18 (Schrems II), 132 kohta.

3 PÄÄTELMÄT

64. Yleisessä tietosuojasetuksessa esitetään säännöt henkilötietojen käsittelylle ETA:ssa ja sallitaan niiden perusteella henkilötietojen vapaa liikkuminen ETA:ssa. Yleisen tietosuojasetuksen V luku koskee henkilötietojen siirtoja kolmansiin maihin, ja siinä rima asetetaan korkealle: siirto ei saa heikentää yleisellä tietosuojasetuksella taattua luonnollisten henkilöiden suojan tasoa (yleisen tietosuojasetuksen 44 artikla). Unionin tuomioistuimen asiassa C-311/18 (Schrems II) antamassa tuomiossa korostetaan, että yleisellä tietosuojasetuksella annetun suojan tason jatkuvuus on varmistettava, kun henkilötietoja siirretään kolmanteen maahan⁶⁵.
65. Jotta tiedoille voidaan varmistaa unionissa taattua tasoa pääosiltaan vastaava suojan taso, siirrot on ensinnäkin tunnettava läpikotaisin. Lisäksi on tarkistettava, että siirrettävät tiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista niiden kolmanteen maahan siirtämisen ja siellä käsittelyn kannalta.
66. Myös tiedonsiirtoväline, jota siirroissa käytetään, on yksilöitävä. Jos tiedonsiirtoväline ei ole riittävyttä koskeva päätös, on tarkistettava tapauskohtaisesti, heikentääkö kohteena olevan kolmannen maan laki tai käytäntö yleisen tietosuojasetuksen 46 artiklan mukaisen tiedonsiirtovälineen sisältämiä suojatoimia omien siirtojen yhteydessä (vai ei). Jos pelkästään yleisen tietosuojasetuksen 46 artiklan mukaisella tiedonsiirtovälineellä ei pystytä saavuttamaan EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa siirrettäville henkilötiedoille, puutteet voidaan korjata lisätoimenpiteillä.
67. 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.
68. Toimivaltaisella valvontaviranomaisella on valtuudet keskeyttää tai lopettaa henkilötietojen siirrot kolmanteen maahan, jos EU:n lainsäädännössä, erityisesti yleisen tietosuojasetuksen 45 ja 46 artiklassa ja perusoikeuskirjassa, vaadittua siirrettävien tietojen suojaa ei voida varmistaa.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)

⁶⁵ C-311/18 (Schrems II), 93 kohta.

LIITE 1: MÄÄRITELMÄT

- 'Kolmas maa' tarkoittaa mitä tahansa maata, joka ei ole ETA:n 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 ETA:ssa olevaa 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 ETA:sta 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 riittävyttä 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.
- Euroopan komissio hyväksyy 'vakiosopimuslausekkeita', 'tietosuoja koskevia vakiolausekkeita' ja 'mallisopimuslausekkeita' henkilötietojen siirtoja varten rekisterinpitäjien tai henkilötietojen käsittelijöiden välillä ETA:ssa ja rekisterinpitäjille tai henkilötietojen käsittelijöille ETA:n ulkopuolelle. Euroopan komission hyväksymät tietosuoja koskevat vakiolausekkeet ovat yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohdan ja 5 kohdan mukainen tiedonsiirtoväline.

LIITE 2: ESIMERKKEJÄ LISÄTOIMENPITEISTÄ

69. Seuraavat toimenpiteet ovat esimerkkejä lisätoimenpiteistä, joita voidaan harkita vaiheessa 4 ”Lisätoimenpiteiden hyväksyntä”. Tämä luettelo ei ole tyhjentävä. 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 ne lisätoimenpiteet, joilla voidaan tehokkaasti taata siirtojen kyseinen suojan taso.
70. Lisätoimenpide voidaan katsoa unionin tuomioistuimen asiassa Schrems II annetussa tuomiossa tarkoitetulla tavalla tehokkaaksi vain ja siinä määrin kuin sillä puututaan erityisiin puutteisiin, joita on havaittu tietojen viejän kolmannen maan oikeudellisesta tilanteesta tekemässä arvioinnissa. Jos EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa ei viime kädessä voida varmistaa, henkilötietoja ei saa siirtää.
71. Tietojen viejän on ehkä pitänyt jo rekisterinpitäjänä tai henkilötietojen käsittelijänä panna täytäntöön joitakin tässä liitteessä kuvattuja toimenpiteitä, vaikka tietojen tuojaan sovellettaisiin riittävyyttä koskevaa päätöstä, samalla tavoin kuin niitä on ehkä pitänyt panna täytäntöön käsiteltäessä tietoja ETA:ssa⁶⁶.

Tekniset toimenpiteet

72. Tässä jaksossa annetaan esimerkkejä teknisistä toimenpiteistä, joilla voidaan täydentää yleisen tietosuojasetuksen 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 tietosuojasetuksen 46 artiklan mukaisten tiedonsiirtovälineiden vastaisia ja siis omiaan horjuttamaan sopimukseen perustuvaa taetta pääosiltaan vastaavasta suojan tasosta mainitun kolmannen maan viranomaisten näihin tietoihin pääsyä vastaan⁶⁷.
73. Selkeyden vuoksi tässä jaksossa yksilöidään ensin tekniset toimenpiteet, jotka voisivat mahdollisesti olla tietyissä tilanteissa/esimerkkitapauksissa tehokkaita pääosiltaan vastaavan suojan tason varmistamisessa. Sen jälkeen jatketaan muutamalla tilanteella/esimerkkitapauksella, joissa kyseisen suojan tason varmistamiseksi ei ole pystytty löytämään teknisiä toimenpiteitä.

Tilanteet, joita varten voisi olla *tehokkaita* toimenpiteitä

74. Jäljempänä luetelluilla toimenpiteillä on tarkoitus varmistaa, että kolmannen maan viranomaisten pääsy siirrettyihin tietoihin ei horjuta yleisen tietosuojasetuksen 46 artiklan tiedonsiirtovälineiden sisältämien asianmukaisten suojatoimien tehokkuutta. Näitä toimenpiteitä sovelletaan, vaikka viranomaisten pääsyssä tietoihin noudatetaan tietojen tuojan maan lainsäädäntöä, jos kyseinen pääsy ylittää sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista⁶⁸. Toimenpiteiden tavoitteena on sulkea pois mahdollinen oikeuksia loukkaava pääsy estämällä

⁶⁶ Yleisen tietosuojasetuksen 5 artiklan 2 kohta ja 32 artikla.

⁶⁷ C-311/18 (Schrems II), 135 kohta.

⁶⁸ Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuojasetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset EU:n keskeisistä suojatoimista.

viranomaisia tunnistamasta rekisteröityjä, päättelemistä heitä koskevia tietoja, erottamasta tietoja toisessa yhteydessä tai yhdistämistä 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.

75. Kolmansien maiden viranomaiset voivat yrittää päästä siirrettyihin tietoihin,
- 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
 - 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.
76. Tässä jaksossa käsitellään tilanteita, joissa sovelletaan molemmissa tapauksissa tehokkaita toimenpiteitä. Konkreettisen siirron nimenomaisissa olosuhteissa voidaan soveltaa eri lisätoimenpiteitä, jotka voivat olla riittäviä, jos vastaanottajamaan lainsäädännössä säädetään vain yhdestä pääsyttyypistä. Siksi tietojen viejän on analysoitava huolellisesti tietojen tuojan tukemana tuojalle koituvat velvollisuudet.

Esimerkiksi yhdysvaltalaisilla tietojen tuojilla, jotka kuuluvat FISAn 702 §:n (50 USC § 1881a) soveltamisalaan, on suora velvollisuus myöntää pääsy niiden hallussa, hoidossa tai valvonnassa oleviin tuotuihin henkilötietoihin tai luovuttaa ne. Tätä velvollisuutta voidaan laajentaa kaikkiin salausavaimin, joita tarvitaan tietojen saamiseen luettavaksi.

77. Tilanteissa kuvaillaan nimenomaisia olosuhteita ja toteutettuja toimenpiteitä. Kaikki tilanteiden muutokset voivat johtaa erilaisiin päätelmiin.
78. Rekisterinpitäjien on ehkä sovellettava joitakin tai kaikkia tässä kuvattuja toimenpiteitä riippumatta tietojen tuojan 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 riittävyttä koskevaa päätöstä, samalla tavoin kuin rekisterinpitäjien ja henkilötietojen käsittelijöiden on ehkä pitänyt panna niitä täytäntöön käsiteltäessä tietoja ETA:ssa.

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

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

Jos

- henkilötietoja käsitellään käyttämällä vahvaa salausta ennen siirtämistä,
- salausalgoritmi ja sen parametrisointi (esim. avaimen pituus, toimintatapa soveltuvin osin) noudattavat uusinta tekniikkaa, ja ne voidaan katsoa kestäviksi vastaanottajamaan viranomaisten tekemää salauksen ratkontaa vastaan viranomaisten käytössä olevat resurssit ja tekniset valmiudet (esim. tietojenkäsittelyteho väsytyshyökkäyksissä) huomioon ottaen,

3. salauksen vahvuudessa otetaan huomioon nimenomainen jakso, jonka ajan salattujen henkilötietojen luottamuksellisuus on säilytettävä,
4. salausalgoritmi otetaan saumattomasti käyttöön asianmukaisesti ylläpidetyllä ohjelmistolla, jonka on varmennettu noudattavan valitun algoritmin eritelmiä, esimerkiksi sertifiointilla,
5. avaimia hallinnoidaan (luodaan, jaetaan, säilytetään, tarvittaessa yhdistetään aiotun vastaanottajan henkilöllisyyteen ja kumotaan) luotettavasti ja
6. avaimia säilytetään yksinomaan tietojen viejän valvonnassa tai sellaisten muiden yhteisöjen valvonnassa, joille tämä tehtävä on uskottu ja jotka sijaitsevat ETA:ssa tai kolmannessa maassa, kolmannen maan alueella tai yhdellä tai useammalla määritetyllä sektorilla tai kansainvälisessä järjestössä, jonka osalta komissio on vahvistanut yleisen tietosuojasetuksen 45 artiklan mukaisesti, että riittävä suojan taso varmistetaan,

Euroopan tietosuojaneuvosto katsoo, että tehty salaus on tehokas lisätoimenpide.

Esimerkkitapaus 2: Pseudonymisoidujen tietojen siirto

80. 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 lisätietoja⁶⁹,
2. kyseiset lisätiedot ovat yksinomaan tietojen viejän hallussa, ja niitä pidetään erillään jäsenvaltiossa tai kolmannessa maassa, kolmannen maan alueella tai yhdellä tai useammalla määritetyllä sektorilla tai kansainvälisessä järjestössä, jonka osalta komissio on vahvistanut yleisen tietosuojasetuksen 45 artiklan mukaisesti, että riittävä suojan taso varmistetaan,
3. kyseisten lisätietojen luovuttaminen tai luvaton käyttö estetään asianmukaisilla teknisillä ja organisatorisilla suojaustoimilla 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 voi olla hallussaan, että pseudonymisoiduja henkilötietoja ei voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, vaikka kyseisiä tietoja vertailtaisiin keskenään,

Euroopan tietosuojaneuvosto katsoo, että tehty pseudonymisointi on tehokas lisätoimenpide.

81. On pantava merkille, että useissa tilanteissa luonnollinen henkilö voidaan tunnistaa henkilön fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän, fyysisen

⁶⁹ Yleisen tietosuojasetuksen 4 artiklan 5 kohta: ”’pseudonymisoinnilla’ [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”.

sijainnin tai verkkopohjaisessa palvelussa tietyllä hetkellä toteutetun vuorovaikutuksen perusteella⁷⁰, vaikka hänen nimeään, osoitettaan tai muita selkeitä tunnisteita ei olisi.

82. 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 oikeudenkäyttöalueensa samoille viranomaisille, joilla on sitten todennäköisesti hallussaan tietoa siitä, miten kohteena oleva henkilö on käyttänyt kyseisiä tietopalveluja.
83. Lisäksi, koska joidenkin tietopalvelujen käyttö on luonnostaan julkista tai niitä hyödyntävät osapuolet, joilla on huomattavia resursseja, rekisterinpitäjien on otettava erityisen huolellisesti huomioon se, että niiden oikeudenkäyttöalueen viranomaisilla on todennäköisesti hallussaan tietoa kohteena olevan henkilön tietopalvelujen käytöstä.

Esimerkkitapaus 3: Salatut tiedot, jotka vain kulkevat kolmansien maiden kautta

84. Tietojen viejä haluaa siirtää tietoja kohteeseen, jonka katsotaan tarjoavan riittävän suojan yleisen tietosuojasetuksen 45 artiklan mukaisesti. Tiedot reititetään kolmannen maan kautta.

Jos

1. tietojen viejä siirtää henkilötietoja tietojen tuojalle, joka on riittävän suojan varmistavalla oikeudenkäyttöalueella, tiedot siirretään verkossa ja tiedot voidaan maantieteellisesti reitittää sellaisen kolmannen maan kautta, joka ei tarjoa suojan tasoa, joka pääosiltaan vastaa unionissa taattua,
2. käytetään siirron salausta, jonka osalta on varmistettu, että käytetyt salausprotokollat ovat huipputeknisiä ja tarjoavat tehokkaan suojan sellaisilta aktiivisilta ja passiivisilta hyökkäyksiltä, joissa käytetään resursseja, joiden tiedetään olevan kolmannen maan viranomaisten käytettävissä,
3. salauksen purku on mahdollinen vain kyseessä olevan kolmannen maan ulkopuolella,
4. viestinnässä mukana olevat osapuolet ovat sopineet luotettavasta julkisen avaimen varmenneviranomaisesta tai varmennusinfrastruktuurista,
5. salattuun liikenteeseen kohdistuvia aktiivisia ja passiivisia hyökkäyksiä vastaan käytetään erityisiä huipputeknisiä suojaustoimenpiteitä,
6. jos liikenteen salaus itsessään ei takaa asianmukaista turvallisuutta, koska käytettävässä infrastruktuurissa tai ohjelmistossa on haavoittuvuuksia, henkilötiedot salataan päästä päähän myös sovelluserroksessa käyttämällä huipputeknisiä salausmenetelmiä,
7. salausalgoritmi ja sen parametrisointi (esim. avaimen pituus, toimintatapa soveltuvin osin) noudattavat uusinta tekniikkaa ja ne voidaan katsoa kestäviksi kauttakulkumaan viranomaisten tekemää salauksen ratkontaa vastaan viranomaisten käytössä olevat resurssit ja tekniset valmiudet (esim. tietojenkäsittelyteho väsytyshyökkäyksissä) huomioon ottaen,
8. salauksen vahvuudessa otetaan huomioon nimenomainen jakso, jonka ajan salattujen henkilötietojen luottamuksellisuus on säilytettävä,

⁷⁰ Yleisen tietosuojasetuksen 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”

9. salausalgoritmi otetaan saumattomasti käyttöön asianmukaisesti ylläpidetyllä ohjelmistolla, jonka on varmennettu noudattavan valitun algoritmin eritelmiä, esimerkiksi sertifiointilla,
10. takaporttien olemassaolo (laitteistossa ja ohjelmistossa) on suljettu pois,
11. viejä tai viejän luotettu yhteisö oikeudenkäyttöalueella, joka tarjoaa unionissa taattua suojaa pääosiltaan vastaavan suojan tason, hallinnoi (luo, jakaa, tallentaa, tarvittaessa yhdistää aiotun vastaanottajan henkilöllisyyteen ja kumooa) avaimia luotettavasti,

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

Esimerkkitapaus 4: Suojattu vastaanottaja

85. Tietojen viejä siirtää henkilötietoja kolmannen maan tietojen tuojalle, joka on nimenomaisesti suojattu kyseisen maan lailla, esimerkiksi sitä varten, että potilaalle annetaan yhdessä lääkettä tai asiakkaalle tarjotaan lainopillisia palveluita.

Jos

1. kolmannen maan laissa myönnetään maassa sijaitsevalle tietojen tuojalle poikkeus mahdollisesti lainvastaisesta pääsystä kyseisen vastaanottajan hallussa oleviin tietoihin nimenomaista tarkoitusta varten, esimerkiksi tietojen tuojan sovellettavan salassapitovelvollisuuden nojalla,
2. kyseinen poikkeus koskee kaikkia tietojen tuojan hallussa olevia tietoja, joita voidaan käyttää kiertämään etuoikeustiedon suoja (salasavainten, 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 tietosuojaa-asetuksen 46 artiklan mukaisten tiedonsiirtovälineiden perusteella,
4. henkilötiedot salataan ennen siirtämistä huipputeknisellä menetelmällä, jolla taataan, että salausta ei voi purkaa ilman salasavaimen (päästä päähän -salauksen) tuntemista koko sinä aikana, jona tiedot on suojattava,
5. salauksenpurkuavain on yksinomaan suojatun tietojen tuojan hallussa, ja se on suojattu asianmukaisesti luvattomalta käytöltä tai luovuttamiselta huippuluokan teknisillä ja organisatorisilla toimenpiteillä, ja
6. tietojen viejä on vahvistanut luotettavasti, että salasavain, jota se aikoo käyttää, vastaa vastaanottajan hallussa olevaa salasavainta,

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

Esimerkkitapaus 5: Jaettu tai monen osapuolen toteuttama käsittely

86. Tietojen viejä haluaa, että henkilötietoja käsittelee yhdessä vähintään kaksi eri oikeudenkäyttöalueella 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 yhdistelmä tietoja.

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 oikeudenkäyttöalueella 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. ei ole näyttöä viranomaisten, jotka sijaitsevat niillä oikeudenkäyttöalueilla, 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 oikeudenkäyttöalueilla hallussaan pitämiin henkilötietoihin,
6. rekisterinpitäjä on vahvistanut kyseessä olevien tietojen perusteellisen analyysin avulla ja ottaen huomioon kaikki tiedot, joita vastaanottajamaiden viranomaisilla voi olla hallussaan, että sen henkilötietojen käsittelijöille toimittamia henkilötietojen osia ei voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, vaikka kyseisiä tietoja vertailtaisiin keskenään,

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

Tilanteet, joita varten *ei ole tehokkaita toimenpiteitä*

87. Seuraavaksi tiettyjen tilanteiden yhteydessä kuvattavilla toimenpiteillä ei pystyittäisi tehokkaasti varmistamaan unionissa taattua suojaa pääosiltaan vastaavaa suojan tasoa kolmanteen maahan siirretyille tiedoille. Siksi niitä ei hyväksyttäisi lisätoimenpiteiksi.

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

88. Tietojen viejä käyttää pilvipalvelujen tarjoajaa tai muuta henkilötietojen käsittelijää käsittelemään henkilötietoja ohjeidensa mukaan kolmannessa maassa.

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 myönnettyt valtuudet päästä siirrettyihin tietoihin ylittävät sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista⁷¹,

⁷¹ Ks. Euroopan unionin perusoikeuskirjan 47 ja 52 artikla, yleisen tietosuoja-asetuksen 23 artiklan 1 kohta ja Euroopan tietosuojaneuvoston suositukset EU:n keskeisistä suojatoimista.

Euroopan tietosuojaneuvosto ei pysty nykyisellä tekniikan tasolla määrittämään tehokasta teknistä toimenpidettä, jolla estettäisiin kyseistä pääsyä loukkaamasta rekisteröityjen oikeuksia. Euroopan tietosuojaneuvosto ei sulje pois mahdollisuutta, että myöhemmän teknisen kehityksen myötä voidaan saada käyttöön toimenpiteitä, joilla saavutetaan aiotut liiketoimintatarkoitukset edellyttämättä pääsyä selkeässä muodossa oleviin tietoihin.

89. 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.

Esimerkkitapaus 7: Etäpääsy tietoihin liiketoimintaa varten

90. Tietojen viejä antaa henkilötietoja kolmannessa maassa olevien yhteisöjen saataville yhteistä liiketoimintaa varten. 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 antamalla ne saataville yleisesti käytettävässä tietojärjestelmässä siten, että tuoja pääsee suoraan valitsemiinsa tietoihin, tai siirtämällä ne suoraan, yksittäin tai erottelematta käyttämällä viestintäpalvelua,
2. tuoja käyttää selkeässä muodossa olevia tietoja omia tarkoituksiaan varten,
3. vastaanottajamaan viranomaisille myönnettyt valtuudet päästä siirrettyihin tietoihin ylittävät sen, mikä on demokraattisessa yhteiskunnassa välttämätöntä ja oikeasuhteista,

Euroopan tietosuojaneuvosto ei pysty määrittämään tehokasta teknistä toimenpidettä, jolla estettäisiin kyseistä pääsyä loukkaamasta rekisteröityjen oikeuksia.

91. 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.

Sopimukseen perustuvat lisätoimenpiteet

92. Nämä toimenpiteet koostuvat tavallisesti yksipuolisista, kahdenvälisistä tai monenvälisistä⁷² sopimukseen perustuvista sitoumuksista⁷³. 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 henkilötiedot⁷⁴.
93. Joissakin tilanteissa näillä toimenpiteillä voidaan täydentää ja vahvistaa suoja-toimia, joita tiedonsiirtoväline ja kolmannen maan asiaankuuluva lainsäädäntö voivat tarjota, ja kun ne eivät siirron olosuhteet huomioon ottaen täytä kaikki edellytyksiä, jotta suojan taso vastaisi pääosiltaan EU:ssa taattua. Koska sopimukseen perustuvilla toimenpiteillä ei yleisesti pystytä sitomaan kyseisen kolmannen maan viranomaisia, kun ne eivät ole sopimuksen osapuolia⁷⁵, nämä toimenpiteet olisi yhdistettävä muihin teknisiin ja organisatorisiin toimenpiteisiin, 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.
94. Sen mukaan, mitä sopimukseen perustuvia toimenpiteitä jo sisältyy yleisen tietosuoja-asetuksen 46 artiklan mukaiseen käytettävään tiedonsiirtovälineeseen, sopimukseen perustuvat lisätoimenpiteet voivat myös olla hyödyllisiä, jotta ETA:ssa sijaitsevat tietojen viejät saavat tietoa uudesta kehityksestä, joka vaikuttaa kolmansiin maihin siirrettävien tietojen suojaan.
95. Sopimukseen perustuvilla toimenpiteillä ei pystytä estämään sellaisen kolmannen maan lainsäädännön soveltamista, joka ei täytä Euroopan tietosuojaneuvoston EU:n keskeisiä suoja-toimia koskevaa vaatimusta, niissä tapauksissa, joissa lainsäädännöllä veloitetaan tuojat noudattamaan viranomaisilta saamia määräyksiä tietojen luovuttamisesta⁷⁶.
96. Jäljempänä annetaan joitakin esimerkkejä näistä mahdollisista sopimukseen perustuvista toimenpiteistä ja luokitellaan ne niiden luonteen mukaan:

Erityisten teknisten toimenpiteiden käyttöä koskeva sopimukseen perustuva velvoite

97. ***Siirtojen nimenomaisten olosuhteiden mukaan sopimuksessa on ehkä määrättävä, että siirtojen tekeminen edellyttää tiettyjen teknisten toimenpiteiden käyttöönottoa (ks. jäljempänä ehdotetut tekniset toimenpiteet).***

⁷² Esimerkiksi yritystä koskevissa sitovissa säännöissä, joilla pitäisi joka tapauksessa säännellä joitakin jäljempänä lueteltuja toimenpiteitä.

⁷³ 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.

⁷⁴ Ks. asiassa C-311/18 (Schrems II) annetun tuomion 137 kohta, jossa tuomioistuin totesi, että tietosuoja 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 lausekkeitä rikotaan tai niiden noudattaminen on mahdotonta” (ks. myös 148 kohta).

⁷⁵ C-311/18 (Schrems II), 125 kohta.

⁷⁶ EUT:n tuomio asiassa C-311/18 (Schrems II), 132 kohta.

98. **Tehokkuuden edellytykset:**

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

Avoimuusveloitteet:

99. **Viejä voisi liittää sopimukseen liitteitä, joissa on tietoja siitä, että tuoja tarjoaisi parhaan kykynsä mukaan kohdemaan viranomaisille pääsyn tietoihin, myös tiedustelun alalla, jos lainsäädännössä noudatetaan Euroopan tietosuojaneuvoston EU:n keskeisiä suojatoimia. Tämä voisi auttaa tietojen viejää täyttämään veloitteensa dokumentoida oma arviointinsa suojan tasosta kolmannessa maassa.**

100. 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 tyyppin 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 tiettyinä aikoina⁷⁷, 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 tietoja⁷⁸

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

101. 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.

102. **Tehokkuuden edellytykset:**

⁷⁷ Jakson pituuden pitäisi riippua riskistä niiden rekisteröityjen oikeuksille ja vapauksille, joiden tietoja kyseessä oleva siirto koskee – esim. edellinen vuosi ennen tietojen viejän kanssa käytetyn tiedonvientiä välineen sulkemista.

⁷⁸ Tämän velvollisuuden noudattaminen ei itsessään tarkoita asianmukaisen suojan tason tarjoamista. Kaikki tosiasiallisesti tapahtuneet epäasianmukaiset luovutukset johtavat kuitenkin siihen, että lisätoimenpiteitä on pantava täytäntöön.

- Tuojan on pystyttävä antamaan viejälle tällaiset tiedot parhaan tietonsa mukaan ja pyrittäen kaikin keinoin hankkimaan ne⁷⁹.
- Tällä tuojalle määrättyllä 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 tietosuojasetuksen 46 artiklan mukaisen käytettävän tiedonsiirtovälineen sisältämällä suojoimilla ja muilla sen mahdollisesti hyväksymillä lisäsuojatoimilla ei voida enää varmistaa EU:ssa taattua suojan tasoa pääosiltaan vastaavaa suojan tasoa. Tällä velvollisuudella ei voida kuitenkaan perustella sitä, että tuoja luovuttaa henkilötietoja, eikä sen nojalla voida olettaa, että pääsyyntöjä ei tule lisää.

103. ***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***⁸⁰.

104. ***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 sitoumuksiaan⁸¹.
- Sopimukseen täytyy sisältyä seuraamuksia ja/tai viejän kyky irtisanoa sopimus lyhyellä varoitusajalla tapauksissa, joissa tuoja ei paljasta, että on olemassa takaportti tai vastaavia ohjelmia tai peukaloituja liiketoimintaprosesseja tai mikä tahansa vaatimus panna jokin näistä täytäntöön, tai tuoja ei ilmoita viejälle viipymättä, kun niiden olemassaolo tulee sen tietoon.

105. ***Viejä voisi vahvistaa valtuuksiaan tehdä tarkastuksia⁸² 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.***

⁷⁹ Ks. edellä 32.5 kohta.

⁸⁰ Tämä lauseke on tärkeä, jotta voidaan taata riittävä suojan taso siirretyille henkilötiedoille, ja yleisesti ottaen sitä pitäisi vaatia.

⁸¹ Ks. edellä 32.5 kohta.

⁸² Ks. esim. päätöksen 2010/87/EU rekisterinpitäjien ja henkilötietojen käsittelijöiden mallisopimuslausekkeita koskevan lausekkeen 5 kohta f. Tarkastuksista voitaisiin määrätä myös käytännössä tai varmenteessa.

106. **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 väärinkäytöltä suojattuja, jotta tarkastajat pystyvät löytämään todisteet luovuttamisesta. Pääsylokeissa ja muissa vastaavissa jäljitysketjuissa olisi myös tehtävä ero tavanomaisista liiketoimista johtuvien pääsyjen ja pääsyä koskevista määräyksistä tai pyynnöistä johtuvien pääsyjen välillä.

107. ***Jos tuojan kolmannen maan laki ja käytäntö on alustavasti arvioitu ja niiden on katsottu tarjoavan suojan tason, joka pääosiltaan vastaa EU:ssa viejän siirtämille tiedoille tarjottua suojan tasoa, viejä voisi edelleen vahvistaa tietojen tuojan velvollisuutta ilmoittaa viipymättä tietojen viejälle siitä, että se ei pysty noudattamaan sopimukseen perustuvia sitoumuksia ja siten "tietosuojan pääosiltaan vastaavaa tasoa" koskevaa vaatimusta.***^{83.}

108. Tämä kyvyttömyys noudattaa vaatimuksia voi johtua muutoksista kolmannen maan lainsäädännössä tai käytännössä⁸⁴. 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 hyväksytyjen toimenpiteiden tehokkuuden seuraamisesta riittävästi tietoa, jotta se voi täyttää velvollisuutensa keskeyttää tai päättää siirto ja/tai irtisanoa sopimus.

109. **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 odottamatta välttämättä viejän ohjeita, jos tietojen viejän ja tietojen tuojan välillä sovittava erityinen kynnyksiarvo täyttyy. Tuojan on

⁸³ Mallisopimuslausekkeitä koskevan päätöksen 2010/87/EU 5 lausekkeen a kohta ja d kohdan i alakohta.

⁸⁴ 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 kiellostä – 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 mallisopimuslausekkeitä".

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.

110. ***Mikäli kolmannen maan kansallisessa lainsäädännössä sallitaan, sopimuksella voitaisiin vahvistaa tuojan avoimuusvelvoitteita niin sanotulla 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.***

111. ***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 yksityinen avain Warrant Canary -ilmoitusten allekirjoittamista varten pidetään turvassa ja että sitä ei voida kolmannen maan lainsäädännöllä pakottaa antamaan väärä Warrant Canary -ilmoituksia. Sitä varten voisi olla hyödyllistä, jos ilmoituksen tekemiseen tarvitaan useita allekirjoituksia eri henkilöiltä ja/tai jos Warrant Canary -ilmoituksen antaa kolmannen maan oikeudenkäyttöalueen ulkopuolella oleva henkilö.

Erityistoimiin ryhtymistä koskevat velvollisuudet

112. ***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 on 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.***

113. ***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.

114. ***Edellä kuvattua vastaavassa tilanteessa tuoja voisi sitoutua ilmoittamaan määräyksen antaneelle viranomaiselle siitä, että määräys on yleisen tietosuoja-asetuksen 46 artiklan mukaisen tiedonsiirtovälineen sisältämien suojatoimien vastainen⁸⁵, sekä siitä tuojalle johtuvasta velvoitteiden ristiriidasta. Tuoja ilmoittaisi tästä yhtä aikaa ja mahdollisimman pian viejälle ja/tai ETA:n toimivaltaiselle valvontaviranomaiselle, mikäli se on mahdollista kolmannen maan oikeusjärjestyksen mukaan.***

115. ***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 ETA:n toimivaltaiselle valvontaviranomaiselle saadusta pääsystä 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](#)

116. ***Sopimuksessa voitaisiin määrätä, että pelkkänä tekstinä tavanomaisessa liiketoiminnassa (myös tukitapauksissa) toimitettuihin henkilötietoihin voi päästä vain viejän ja/tai rekisteröidyn nimenomaisen tai hiljaisen suostumuksen perusteella.***

⁸⁵ 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. EUT, C-311/18 (Schrems II), 138 kohta.

117. **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)⁸⁶.
- Kansalliset määräykset tai toimintalinjat, 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 ETA:ssa.

118. ***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).***

119. **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 toimintalinjat voivat estää tämän ilmoituksen tekemisen rekisteröidylle. Viejä ja tuoja voisivat joka tapauksessa sitoutua ilmoittamaan rekisteröidylle heti, kun tietojen luovuttamista koskevat rajoitukset poistetaan, ja tekemään kaikkensa saadakseen poikkeusluvan luovuttamiskielloseksi. 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.

120. ***Sopimuksella voitaisiin velvoittaa viejä ja tuoja auttamaan rekisteröityä käyttämään oikeuksiaan kolmannen maan oikeudenkäyttöalueella tapauskohtaisten oikeussuojamekanismien ja oikeudellisen neuvonnan avulla.***

⁸⁶ Yleisen tietosuojasetuksen 4 artiklan 11 kohta.

121. **Tehokkuuden edellytykset**

- Kansallisissa määräyksissä ja toimintalinjoissa 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 pelkäästään avun ja oikeudellisen neuvonnan tarjoamisella rekisteröidyille ei voida muuttaa sitä, että kolmannen maan oikeusjärjestyksessä ei tarjota suojan tasoa, joka vastaa pääosiltaan EU:ssa taattua. 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. Tämä ei kuitenkaan missään tapauksessa olisi tehokas lisätoimenpide tarkkailutoimenpiteitä vastaan, jos muutoksenhakumekanismia ei ole.

Organisatoriset toimenpiteet

122. Organisatoriset lisätoimenpiteet voivat koostua sisäisistä toimintalinjoista, 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 EU:ssa taattua.
123. 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 toimintalinjat, joilla hallinnoidaan siirtoja erityisesti yritysten ryhmittymien kanssa

124. ***Laaditaan asianmukaiset sisäiset toimintalinjat, joissa osoitetaan selkeästi tiedonsiirtoa koskevat vastuut, raportointikanavat ja pysyväisohjeet tarkkailutapauksissa tai viranomaisten tietoihin pääsyä koskevissa virallisissa pyynnöissä. Etenkin, kun kyse on siirroista yritysten ryhmittymien välillä, näihin toimintalinjoihin voi sisältyä muun muassa sellaisen erityisen ryhmän nimittäminen, jonka pitäisi sijaita ETA:ssa, koostua tietotekniikkaa, tietosuojaa ja yksityisyydensuojaa koskevan lainsäädännön asiantuntijoista ja käsitellä pyyntöjä, jotka liittyvät EU:sta siirrettyihin henkilötietoihin; ilmoittaminen ylimmälle oikeudelliselle ja yrityksen johdolle sekä rekisteröidylle, kun kyseisiä pyyntöjä saadaan; vaiheet menettelyssä, jossa kyseenalaistetaan kohtuuttomat tai lainvastaiset pyynnöt; ja avointen tietojen antaminen rekisteröidyille.***

125. Laaditaan viranomaisten henkilötietoihin pääsyä koskevien pyyntöjen käsittelystä vastaavalle henkilöstölle erityisiä koulutusmenettelyjä, joita pitäisi päivittää säännöllisesti, jotta ne perustuvat kolmannen maan ja ETA:n uusimpaan 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.

126. **Tehokkuuden edellytykset:**

- Näitä toimintalinjoja voidaan suunnitella vain tapauksissa, joissa kolmannen maan viranomaisten pyyntö on EU:n lainsäädännön mukainen⁸⁷. Kun pyyntö ei ole EU:n lainsäädännön mukainen, toimintalinjat eivät riitä varmistamaan henkilötiedoille suojan tasoa, joka vastaa pääosiltaan EU:ssa taattua, ja, kuten edellä on todettu, siirrot on lopetettava tai on otettava käyttöön asianmukaisia lisätoimenpiteitä pääsyn estämiseksi.

Läpinäkyvyyttä ja osoitusvelvollisuutta koskevat toimenpiteet

127. ***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 on annettava tietojen viejän saataville, ja se vuorostaan antaa ne tarvittaessa kyseessä oleville rekisteröidyille.***

128. **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 tällainen kykenemättömyys johtaisi suojan tason laskemiseen.

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

130. **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 yhdistelmä tietoja.

⁸⁷ Ks. asia C-362/14 (Schrems I), 94 kohta; C-311/18 (Schrems II), 168, 174, 175 ja 176 kohta.

Organisointimenetelmät ja tietojen minimointia koskevat toimenpiteet

131. ***Siirron yhteydessä hyödyllisiä toimenpiteitä voivat olla myös osoitusvelvollisuuden periaatteen nojalla jo voimassa olevat organisatoriset vaatimukset, kuten tiukkojen ja tarkkojen tietoihin pääsyä ja luottamuksellisuutta koskevien toimintalinjojen 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 pääsulle. Joissakin tapauksissa ei ehkä ole tarpeen siirtää tiettyjä tietoja (esim. jos kyse on etäpääsystä ETA-tietoihin, kuten tukitapauksissa, kun täyden pääsyn sijasta myönnetään rajoitettu pääsy, tai kun palvelun toimittaminen edellyttää vain rajallisen tietokokonaisuuden eikä koko tietokannan siirtämistä).***

132. ***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.

133. ***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.***

134. ***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

135. ***Laaditaan tiukat tietosuojaa ja yksityisyyttä koskevat toimintalinjat, jotka perustuvat EU:n sertifiointiin tai käytännesääntöihin tai kansainvälisiin standardeihin (esim. ISO-standardit) ja parhaisiin käytäntöihin (esim. ENISA), ja otetaan siinä asianmukaisesti huomioon uusin tekniikka***

käsiteltävien tietojen luokkia koskevan riskin mukaisesti sekä sen mukaan, miten todennäköisesti viranomaiset yrittävät päästä tietoihin.

Muut

136. ***Laaditaan ja arvioidaan säännöllisesti sisäiset toimintalinjat, joilla arvioidaan täytäntöön pantujen lisätoimenpiteiden soveltuvuutta sekä yksilöidään ja toteutetaan tarvittaessa täydentäviä tai vaihtoehtoisia ratkaisuja, jotta voidaan varmistaa, että EU:ssa siirrettäville henkilötiedoille taattua suojan tasoa vastaavaa tasoa pidetään yllä.***

* * *

137. ***Tietojen tuojan sitoumukset olla osallistumatta mihinkään henkilötietojen siirtämiseen edelleen samassa kolmannessa maassa tai muihin kolmansiin maihin tai keskeyttää käynnissä olevat siirrot, kun kolmannessa maassa ei voida taata henkilötiedoille suojan tasoa, joka vastaa pääosiltaan EU:ssa taattua⁸⁸.***

⁸⁸ C-311/18 (Schrems II), 135 ja 137 kohta.

LIITE 3: KOLMANNEN MAAN ARVIOINNISSA KÄYTETTÄVÄT MAHDOLLISET TIETOLÄHTEET

138. Tietojen tuojan pitäisi pystyä antamaan tietojen viejälle asiaankuuluvat lähteet ja tiedot kolmannesta maasta, johon tuoja on sijoittautunut ja jonka lakeja sovelletaan siihen. Tietojen viejä voi myös käyttää useita muita tietolähteitä. Niitä on muun muassa seuraavassa luettelossa, joka ei ole tyhjentävä.

- Euroopan unionin tuomioistuimen (EUT) ja Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytäntö⁸⁹, johon viitataan suosituksissa EU:n keskeisistä suojaustoimista⁹⁰
- Riittävyttä koskevat päätökset kohdemaassa, jos siirrossa käytetään eri oikeusperustetta⁹¹
- hallitustenvälisten järjestöjen, kuten Euroopan neuvoston⁹², muiden alueellisten elinten⁹³ ja YK:n elinten ja virastojen (esim. YK:n ihmisoikeusneuvoston,⁹⁴ ihmisoikeuskomitean⁹⁵) päätöslauselmat ja raportit
- kansallinen oikeuskäytäntö tai kolmansien maiden yksityisyydensuojan ja tietosuojan alalla toimivaltaisten riippumattomien oikeus- tai hallintoviranomaisten tekemät päätökset
- tutkimuslaitosten ja kansalaisyhteiskunnan järjestöjen (esim. kansalaisjärjestöjen ja toimialajärjestöjen) raportit.

⁸⁹ Ks. tietokooste joukkovalvontaa koskevasta EIT:n oikeuskäytännöstä: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

⁹⁰ <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

⁹¹ C-311/18 (Schrems II), 141 kohta; ks. riittävyttä koskevat päätökset osoitteessa https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

⁹² <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

⁹³ Ks. esim. Amerikan valtioiden ihmisoikeustoimikunnan maakohtaiset raportit osoitteessa <https://www.oas.org/en/iachr/reports/country.asp>.

⁹⁴ Ks. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

⁹⁵ Ks. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5