Ohjeet

Suuntaviivat 7/2022 sertifioinnin käytöstä tiedonsiirtovälineenä

Versio 2.0

Hyväksytty 14. helmikuuta 2023

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

VERSIOHISTORIA

Versio 1.0	14. kesäkuuta 2022	Suuntaviivojen hyväksyminen julkista kuulemista varten
Versio 2.0	14. helmikuuta 2023	Suuntaviivojen hyväksyminen julkisen kuulemisen jälkeen

TIIVISTELMÄ

Yleisen tietosuoja-asetuksen 46 artiklassa edellytetään, että tietojen viejät ottavat käyttöön asianmukaiset suojatoimet, kun henkilötietoja siirretään kolmansiin maihin tai kansainvälisille järjestöille. Tätä varten yleisessä tietosuoja-asetuksessa monipuolistetaan asianmukaisia suojatoimia, joita tietojen viejät voivat käyttää 46 artiklan nojalla kolmansiin maihin suuntautuvien siirtojen yhteydessä, muun muassa ottamalla käyttöön sertifiointi uutena siirtomekanismina (42 artiklan 2 kohta ja 46 artiklan 2 kohdan f alakohta).

Näissä suuntaviivoissa annetaan ohjeita yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan soveltamisesta henkilötietojen siirtämiseen kolmansiin maihin tai kansainvälisille järjestöille sertifioinnin perusteella. Asiakirja muodostuu neljästä osasta sekä liitteestä.

Asiakirjan ensimmäisessä osassa (”Yleistä”) selvennetään, että suuntaviivoilla täydennetään sertifioinnista aiemmin annettuja yleisiä suuntaviivoja 1/2018 ja että niissä käsitellään yleisen tietosuoja-asetuksen V luvun erityisvaatimuksia, joita sovelletaan, kun tiedonsiirtovälineenä käytetään sertifiointia. Yleisen tietosuoja-asetuksen 44 artiklan mukaan kaikissa henkilötietojen siirroissa kolmansiin maihin tai kansainvälisille järjestöille on noudatettava kyseisen asetuksen V luvun säännöksiä ja täytettävä myös asetuksen muissa säännöksissä vahvistetut edellytykset. Näin ollen ensiksi on varmistettava yleisen tietosuoja-asetuksen yleisten säännösten noudattaminen, ja toiseksi, että siirroissa noudatetaan myös asetuksen V luvun säännöksiä. Ensimmäisessä osassa kuvataan myös siirtoihin osallistuvat toimijat ja niiden keskeiset roolit. Kuvauksessa keskitytään erityisesti tietojen tuojaan, jolle sertifiointi myönnetään, ja tietojen viejään, joka käyttää sertifiointia tiedonsiirtovälineenä (vastuu käsittelyn vaatimustenmukaisuudesta säilyy kuitenkin tietojen viejällä). Sertifiointiin voi sisältyä myös tiedonsiirtovälinettä täydentäviä toimenpiteitä, joilla varmistetaan EU:ssa henkilötiedoille taatun suojan tason noudattaminen. Suuntaviivojen ensimmäisessä osassa on myös tietoa tiedonsiirtovälineenä käytettävän sertifioinnin hankkimismenettelystä.

Suuntaviivojen toisessa osassa (”Akkreditointivaatimusten soveltamisohjeet”) muistutetaan, että sertifiointielinten akkreditointia koskevat vaatimukset käyvät selville ISO 17065 -standardista ja tulkitsemalla sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen 43 artiklan mukaisesti annettuja suuntaviivoja 4/2018 yhdessä yleisen tietosuoja-asetuksen V luvun kanssa. Sen sijaan näissä suuntaviivoissa selitetään tarkemmin joitakin akkreditointivaatimuksia, joita sertifiointielimiin sovelletaan siirtojen yhteydessä.

Suuntaviivojen kolmannessa osassa (”Yksittäiset sertifiointikriteerit”) annetaan ohjeita suuntaviivoissa 1/2018 jo luetelluista sertifiointikriteereistä ja vahvistetaan lisäkriteerejä, jotka olisi sisällytettävä kolmansiin maihin suuntautuvissa siirroissa käytettäviin sertifiointimekanismeihin. Nämä kriteerit koskevat seuraavia näkökohtia: kolmannen maan lainsäädännön arviointi, viejien ja tuojien yleiset velvoitteet, tietojen edelleen siirtämistä koskevat säännöt, oikeussuojakeinot ja niiden täytäntöönpano, menettelyt ja toimet tilanteissa, joissa kansalliset lait tai käytännöt estävät sertifioinnin mukaisten sitoumusten noudattamisen, sekä kolmansien maiden viranomaisten esittämien tietopyyntöjen noudattaminen.

Suuntaviivojen neljännessä osassa (”Sitovat ja täytäntöönpanokelpoiset sitoumukset”) käsitellään seikkoja, jotka olisi otettava huomioon sitovissa ja täytäntöönpanokelpoisissa sitoumuksissa, jotka yleisen tietosuoja-asetuksen ulkopuolisten rekisterinpitäjien tai henkilötietojen käsittelijöiden olisi tehtävä osoittaakseen, että ne soveltavat asianmukaisia suojatoimia kolmansiin maihin siirrettäviin tietoihin. Näihin sitoumuksiin, jotka voidaan esittää muun muassa sopimuksissa, on erityisesti sisällyttävä

takeet siitä, että tuojalla ei ole syytä uskoa, että kyseiseen käsittelyyn sovellettavat kolmannen maan lait ja käytännöt, mukaan lukien henkilötietojen luovuttamista koskevat vaatimukset tai toimenpiteet, jotka mahdollistavat viranomaisten pääsyn tietoihin, estävät tuojaa täyttämästä sertifioinnin mukaisia sitoumuksiaan.

Näiden suuntaviivojen liitteessä esitetään joitakin esimerkkejä lisätoimenpiteistä, joita voidaan soveltaa, kun sertifiointia käytetään tiedonsiirtovälineenä. Nämä toimenpiteet noudattavat suositusten 1/2020 (suositukset toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi) liitteessä II esitettyjä toimenpiteitä. Esimerkkien avulla pyritään kiinnittämään huomiota kriittisiin tilanteisiin.

SISÄLLYSLUETTELO

Euroopan tietosuojaneuvosto, joka

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

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT:

1 YLEISTÄ

1.1 Tarkoitus ja soveltamisala

1. Tässä asiakirjassa annetaan ohjeita yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan soveltamisesta henkilötietojen siirtämiseen kolmansiin maihin tai kansainvälisille järjestöille sertifioinnin perusteella. Euroopan tietosuojaneuvosto on jo aiemmin julkaissut yleisiä ohjeita yleisen tietosuoja-asetuksen mukaisesta sertifioinnista[2] ja akkreditoinnista[3]. Näin ollen näissä uusissa suuntaviivoissa käsitellään ainoastaan erityisiä näkökohtia, jotka liittyvät sertifioinnin käyttöön tiedonsiirtovälineenä. Suuntaviivoissa täsmennetään yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan ja 42 artiklan 2 kohdan soveltamista antamalla tältä osin käytännön ohjeita ja sisällyttämällä uusia näkökohtia jo julkaistuihin suuntaviivoihin.

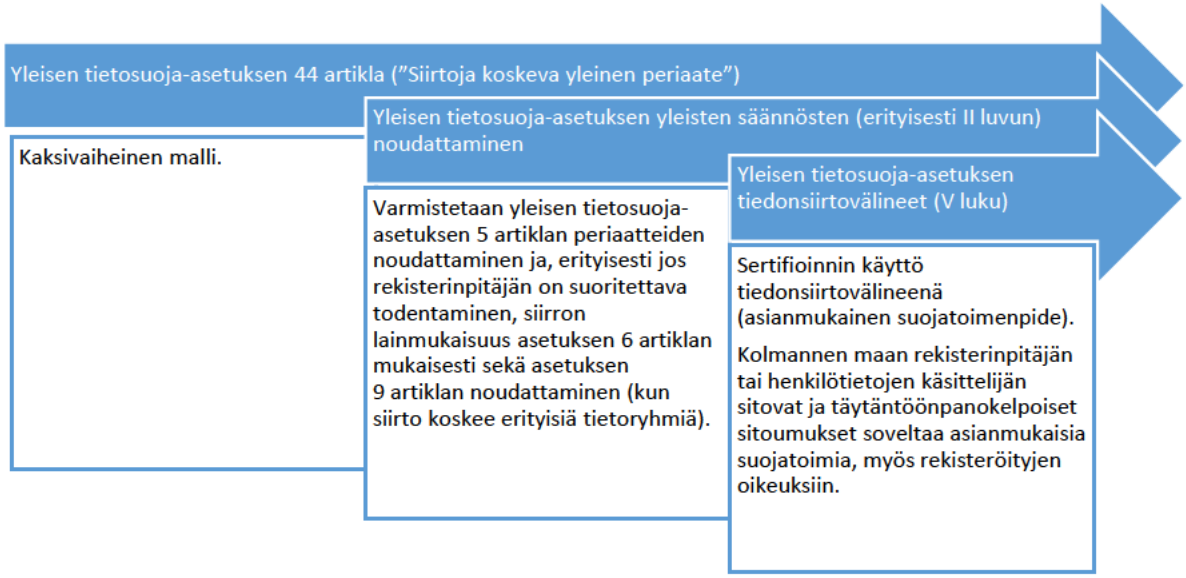
2. Tietosuojaneuvosto arvioi näiden suuntaviivojen toimivuutta niiden käytännön soveltamisesta saatujen kokemusten perusteella ja antaa lisäohjeita selventääkseen jäljempänä esitettyjä seikkoja, myös sertifiointisopimuksen roolista yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdassa tarkoitettujen sitovien ja täytäntöönpanokelpoisten sitoumusten yhteydessä.

1.2 Kansainvälisiin siirtoihin sovellettavat yleiset säännöt

3. Yleisen tietosuoja-asetuksen 44 artiklan mukaan kaikissa henkilötietojen siirroissa kolmansiin maihin[4] tai kansainvälisille järjestöille on noudatettava kyseisen asetuksen V luvun säännöksiä ja täytettävä myös asetuksen muissa säännöksissä vahvistetut edellytykset. Näin ollen kussakin siirrossa on noudatettava muun muassa yleisen tietosuoja-asetuksen 5 artiklassa säädettyjä tietosuojaperiaatteita, siirron on oltava asetuksen 6 artiklassa tarkoitetulla tavalla lainmukainen ja siirrossa on noudatettava asetuksen 9 artiklaa, jos siirto koskee erityisiä tietoryhmiä. Tässä yhteydessä on sovellettava kaksivaiheista

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETA:n jäsenvaltioita.
[2] Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen (EU) 2016/679 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018.
[3] Suuntaviivat 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen ((EU) 2016/679) 43 artiklan mukaisesti.
[4] Suuntaviivat 5/2021 3 artiklan soveltamisen ja yleisen tietosuoja-asetuksen V luvun mukaisten kansainvälisiä siirtoja koskevien säännösten vuorovaikutuksesta, s. 4.

testiä: ensiksi on varmistettava yleisen tietosuoja-asetuksen yleisten säännösten noudattaminen, ja toiseksi, että siirto noudattaa myös asetuksen V luvun säännöksiä.



4. Yleisen tietosuoja-asetuksen 46 artiklassa täsmennetään, että ”jollei 45 artiklan 3 kohdan mukaista päätöstä ole tehty, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja”. Yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan mukaan tällaisia asianmukaisia suojatoimia voivat olla hyväksytty sertifiointimekanismi yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin.

5. Näin ollen tietojen viejä voi halutessaan käyttää tietojen tuojan saamaa sertifiointia osoituksena siitä, että se on noudattanut esimerkiksi yleisen tietosuoja-asetuksen 24 artiklan 3 kohdan tai 28 artiklan 5 kohdan mukaisia velvoitteitaan. Tietojen tuoja puolestaan voi hakea sertifiointia osoittaakseen, että asianmukaiset suojatoimet on toteutettu.

6. Sekä tietojen viejällä että tietojen tuojalla voi olla erilaisia rooleja (kuten rekisterinpitäjä ja henkilötietojen käsittelijä)[5] V luvun mukaisesta käsittelystä riippuen, ja eri rooleihin voi liittyä erilaisia vastuita:

7. Sen lisäksi, että käytetään sertifiointia tai muita yleisen tietosuoja-asetuksen 45 ja 46 artiklassa tarkoitettuja siirtovälineitä tai -mekanismeja, asetuksen 49 artiklassa säädetään, että kansainväliset siirrot

[5] Ks. jäljempänä oleva kohta ”Sertifiointikriteerien soveltamisohjeet”.

ovat mahdollisia tietyissä erityistilanteissa, vaikka mitään V luvun mukaista mekanismia ei noudatettaisi.[6] Kuten tietosuojaneuvoston aiemmissa suuntaviivoissa selitetään, yleisen tietosuoja-asetuksen 49 artiklassa säädettyjä poikkeuksia on kuitenkin tulkittava suppeasti ja niiden on liityttävä pääasiassa satunnaisiin käsittelytoimiin, jotka eivät ole toistuvia.[7]

1.3 Toimijat ja roolit, kun sertifiointia käytetään tiedonsiirtovälineenä

8. **Euroopan tietosuojaneuvostolla** on valtuudet hyväksyä ETA:n laajuiset sertifiointikriteerit (eurooppalainen tietosuojasinetti) ja antaa johdonmukaisuuden varmistamiseksi lausuntoja valvontaviranomaisten päätösluonnoksista, jotka koskevat sertifiointikriteerejä ja sertifiointielimiin sovellettavia akkreditointivaatimuksia. Sen tehtävänä on myös koota kaikki sertifiointimekanismit sekä tietosuojasinetit ja -merkit rekisteriin ja asettaa ne julkisesti saataville.[8]

9. **Valvontaviranomaiset** hyväksyvät sertifiointikriteerit silloin, kun sertifiointimekanismi ei ole eurooppalainen tietosuojasinetti.[9] Ne voivat myös akkreditoida sertifiointielimen, laatia sertifiointikriteerit ja myöntää sertifioinnin, jos niiden jäsenvaltion kansallisessa lainsäädännössä niin säädetään.[10]

10. **Kansallinen akkreditointielin** voi akkreditoida kolmansien osapuolten sertifiointielimiä soveltamalla ISO 17065 -standardia ja valvontaviranomaisten vahvistamia akkreditointia koskevia lisävaatimuksia, joiden olisi oltava näiden suuntaviivojen osan 2 mukaisia. Joissakin jäsenvaltioissa akkreditoinnin voi myöntää myös toimivaltainen valvontaviranomainen ja sen voi suorittaa kansallinen akkreditointielin tai molemmat edellä mainituista.

11. **Järjestelmän omistaja** on organisaatio, joka on laatinut sertifiointikriteerit ja menetelmävaatimukset, joiden mukaisesti vaatimustenmukaisuutta on määrä arvioida. Arvioinnit tekevä organisaatio voisi olla sama organisaatio, joka on kehittänyt järjestelmän ja omistaa sen, mutta käytössä voi myös olla järjestelyjä, joissa yksi organisaatio omistaa järjestelmän ja toinen (tai useampi) toimii arvioinnit suorittavana sertifiointielimenä.

12. Kansallisesta lainsäädännöstä riippuen valvontaviranomaisen sijasta myös edellä kuvatulla tavalla akkreditoitu **sertifiointielin** voi myöntää sertifioinnin.[11] Lisäksi se voi laatia sertifiointikriteerit ja toimia siten myös järjestelmän omistajana (ks. edellä oleva 11 kohta). Sillä on kuitenkin oltava toimipaikka ETA:ssa, jotta se voi käyttää tehokkaasti yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan f alakohdassa säädettyjä korjaavia toimivaltuuksia. Sertifiointielin voi teettää tarkastustoimia alihankintana ETA:n ulkopuolisilla paikallisilla asiantuntijoilla tai laitoksilla.[12] Se ei kuitenkaan saa ulkoistaa sertifioinnin myöntämistä tai myöntämättä jättämistä koskevia päätöksiä.

---

[6] Lisätietoja 49 artiklasta ja sen yleisestä vuorovaikutuksesta 46 artiklan kanssa annetaan asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevissa suuntaviivoissa 2/2018.

[7] Ks. asetuksen (EU) 2016/679 49 artiklan mukaisia poikkeuksia koskevat tietosuojaneuvoston suuntaviivat 2/2018, s. 5.

[8] Yleisen tietosuoja-asetuksen 42 artiklan 8 kohta.

[9] Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen (EU) 2016/679 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018, 2.2 kohta.

[10] Yleisen tietosuoja-asetuksen 42 artiklan 5 kohta ja 43 artiklan 1 kohta.

[11] Yleisen tietosuoja-asetuksen 42 artiklan 5 kohta.

[12] Sertifiointielinten on arvioitava paikalliset asiantuntijansa noudattaen ISO 17065 -standardia ja valvontaviranomaisen vahvistamia akkreditointia koskevia lisävaatimuksia (yleisen tietosuoja-asetuksen 43 artiklan 1 kohdan b alakohta).

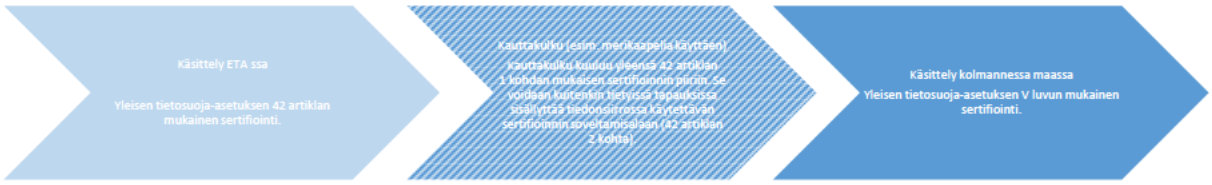
13. **Tietojen tuoja** on kolmannessa maassa sijaitseva yhteisö (rekisterinpitäjä tai henkilötietojen käsittelijä), joka vastaanottaa tietoja tietojen viejältä.

14. **Tietojen viejä** on yhteisö (rekisterinpitäjä tai henkilötietojen käsittelijä), joka siirtää tietoja ETA:sta tietojen tuojalle. Viejän on varmistettava, että yleisen tietosuoja-asetuksen V luvun säännöksiä noudatetaan.

1.4 Sertifioinnin soveltamisala ja kohde, kun sertifiointia käytetään tiedonsiirtovälineenä

15. Yleisen tietosuoja-asetuksen 42 artiklan 2 kohdan mukaisena tiedonsiirtovälineenä käytettävällä sertifiointimekanismilla on pyrittävä varmistamaan asianmukaiset suojatoimet 46 artiklan 2 kohdan f alakohdan mukaista henkilötietojen käsittelyä varten. Sertifioinnin on osoitettava, että ETA:n ulkopuolinen rekisterinpitäjä tai henkilötietojen käsittelijä tai ETA:n rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä tietoja vastaanottava kansainvälinen organisaatio on toteuttanut asianmukaiset suojatoimet henkilötietojen siirtämiseen liittyvien erityisten riskien torjumiseksi.

16. Yleensä toimessa, jolla henkilötietoja siirretään jäsenvaltiosta kolmanteen maahan, on kyse yleisen tietosuoja-asetuksen 4 artiklan 2 kohdassa tarkoitetusta henkilötietojen käsittelystä jäsenvaltion alueella[13], jolloin se voidaan sertifioida yleisen tietosuoja-asetuksen 42 artiklan 1 kohdan mukaisesti. Kuitenkin joissakin tilanteissa myös kauttakulku voidaan sisällyttää tiedonsiirrossa käytettävän sertifioinnin soveltamisalaan. Tällöin sertifioinnin kohteena (joka on sama kuin arvioinnin kohde sertifioinnin aikana[14]) olisi yleensä oltava tietojen tuojan suorittama ETA:sta vastaanotettujen tietojen käsittely kolmannessa maassa sekä näiden tietojen reitittäminen kolmannen maan kautta, jos se tapahtuu tuojan valvonnassa.



17. Sertifioinnin kohteena voi olla yksittäinen käsittelytoimi tai toimien sarja, joka voi muodostua organisatoristen toimenpiteiden kaltaisista hallintoprosesseista, jolloin ne ovat olennainen osa käsittelytoimea.[15]

18. Kolmannessa maassa sijaitseva tietojen tuoja olisi näin ollen sertifioinnin kohteen osalta sertifiointia hakeva yhteisö.

1.5 Viejän rooli, kun sertifiointia käytetään tiedonsiirtovälineenä

---

[13] Euroopan unionin tuomioistuimen tuomio 16.7.2020, *Facebook Ireland* ja *Schrems*, C-311/18, ECLI:EU:C:2020:559, 83 kohta.
[14] Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen (EU) 2016/679 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018, s. 18.
[15] Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen (EU) 2016/679 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018, s. 17 (esim. valitusten käsittelymekanismit).

19. Tietojen viejän suorittama siirto sellaisenaan kuuluu yleensä suoraan yleisen tietosuoja-asetuksen soveltamisalaan. Tämä tarkoittaa, että viejän on noudatettava yleisen tietosuoja-asetuksen mukaisia velvoitteitaan ja erityisesti varmistettava, että tiedot siirretään turvallisesti 32 artiklan ja V luvun mukaisesti, jotta varmistetaan, että kyseisellä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta (yleisen tietosuoja-asetuksen 44 artikla).[16] Tämä voidaan tehdä 42 artiklan 1 kohdan mukaisesti.

20. Lisäksi tietojen viejän, joka haluaa käyttää sertifiointia asianmukaisena suojatoimenpiteenä yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan f alakohdan mukaisesti, on erityisesti tarkistettava, onko kyseinen sertifiointi tehokas aiotun käsittelyn ominaispiirteet huomioon ottaen. Tätä varten viejän on tarkistettava, onko myönnetty sertifiointi voimassa eikä vanhentunut, kattaako se suoritettavan siirron ja kuuluuko henkilötietojen kauttakulku sertifioinnin soveltamisalaan, onko siirrossa kyse tietojen edelleen siirtämisestä ja onko siirrosta toimitettu asianmukaiset asiakirjat. Viejän on myös tarkistettava, että sertifioinnin myöntäneen sertifiointielimen on akkreditoinut kansallinen akkreditointielin tai toimivaltainen valvontaviranomainen. Lisäksi viejän olisi mainittava sertifioinnin käyttämisestä tiedonsiirtovälineenä yleisen tietosuoja-asetuksen 28 artiklan mukaisessa käsittelysopimuksessa, kun siirto tapahtuu rekisterinpitäjältä henkilötietojen käsittelijälle, tai tietojen tuojan kanssa tehtävässä yhteiskäyttösopimuksessa, kun siirto tapahtuu rekisterinpitäjältä toiselle rekisterinpitäjälle

21. Koska viejä on vastuussa V luvun säännösten soveltamisesta, sen on myös arvioitava, onko sertifiointi, jota se aikoo käyttää tiedonsiirtovälineenä, tehokas ottaen huomioon siirron kannalta merkitykselliset kyseisessä kolmannessa maassa voimassa olevat lait ja käytännöt. Tätä arviointia varten ja voidakseen osoittaa noudattavansa velvoitteitaan viejä voi pyytää sertifiointielintä todentamaan dokumentaation, jonka tuoja on laatinut kyseisen kolmannen maan lainsäädännöstä ja käytännöistä suorittamastaan arvioinnista.

22. Jos tuojan suorittaman arvioinnin perusteella tuojan ja/tai tietojen viejän on mahdollisesti toteutettava sertifioinnin edellyttämiä lisätoimenpiteitä, jotta voidaan varmistaa olennaisilta osin samantasoinen suoja kuin ETA:ssa, viejän on tarkistettava sertifioinnin saaneen tuojan määrittämät lisätoimenpiteet ja se, kykeneekö se toteuttamaan tuojan edellyttämät tekniset toimenpiteet ja (mahdolliset) lisätoimenpiteet.

23. Jos nämä vaatimukset eivät täyty, viejän on vaadittava tuojaa ottamaan käyttöön mukautettuja lisätoimenpiteitä tai toteutettava ne itse.

1.6 Sertifiointimenettely, kun sertifiointia käytetään tiedonsiirtovälineenä

24. Sertifiointi on vapaaehtoinen, mutta jos sitä haetaan, se on myönnettävä pakollisiin sääntöihin perustuvalla avoimella menettelyllä. Yleisessä tietosuoja-asetuksessa painotetaan yksityisiin sertifiointime-

[16] Tältä osin on tärkeää huomata, että yleisen tietosuoja-asetuksen 44 artiklassa säädetään selvästi, että siirron voi suorittaa rekisterinpitäjän lisäksi myös henkilötietojen käsittelijä. Tällöin on kyseessä siirto, jossa henkilötietojen käsittelijä lähettää tietoja toiselle henkilötietojen käsittelijälle tai jopa kolmannessa maassa sijaitsevalle rekisterinpitäjälle rekisterinpitäjänsä antamien ohjeiden mukaisesti (yleisen tietosuoja-asetuksen 28 artiklan 3 kohdan a alakohta). Näissä tapauksissa henkilötietojen käsittelijä toimii tietojen viejänä rekisterinpitäjän puolesta, ja sen on varmistettava, että rekisterinpitäjän ohjeiden mukaisesti suoritettavassa siirrossa noudatetaan V luvun säännöksiä (esim. varmistetaan asianmukaisen tiedonsiirtovälineen käyttö). Lisäksi koska siirto on rekisterinpitäjän puolesta suoritettava käsittelytoimi, myös rekisterinpitäjä on vastuussa toimesta V luvun nojalla. Siksi sen on varmistettava, että henkilötietojen käsittelijä antaa riittävät takeet 28 artiklan mukaisesti.

kanismeihin perustuvaa ”säänneltyä itsesääntelyä”. Näillä mekanismeilla on varmistettava, että sertifiointi täyttää olennaisilta osin yleisen tietosuoja-asetuksen 46 artiklassa määritellyt asianmukaisia suojatoimia koskevat vaatimukset.

25. Siksi sertifioinnin on perustuttava sertifiointikriteerien arviointiin, joka suoritetaan sitovaa tarkastusmenetelmää noudattaen. Kansalliset valvontaviranomaiset tai tietosuojaneuvosto hyväksyvät nämä kriteerit yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaisesti. Sertifiointikriteereihin on sisällytettävä vaatimuksia, joita sovelletaan tietojen tuojan suorittaman käsittelyn (mukaan lukien tietojen edelleen siirtäminen) ja kolmannen maan asiaa koskevan oikeudellisen kehyksen arviointiin. Tällä pyritään välttämään se, että kolmannen maan säännöt ja käytännöt estävät tuojaa noudattamasta sertifioinnin mukaisia velvoitteitaan.

26. Sertifiointimenettelyssä kansallisen akkreditointielimen tai toimivaltaisen valvontaviranomaisen akkreditoima sertifiointielin tarkastaa arvioinnin kohteen sertifiointikriteerien mukaisesti.[17]

27. Yleisen tietosuoja-asetuksen 43 artiklan 1 kohdan mukaan sertifioinnin myöntää ja uusii sertifiointielin, jolla on tietosuojaan liittyvä asianmukaisen tason asiantuntemus, sen jälkeen kun se on tiedottanut asiasta valvontaviranomaiselle, jotta tämä voi tarvittaessa käyttää 58 artiklan 2 kohdan h alakohdan mukaisia valtuuksiaan.

28. Yleisen tietosuoja-asetuksen 43 artiklan 5 kohdassa edellytetään, että sertifiointielimet ilmoittavat toimivaltaiselle valvontaviranomaiselle syyt pyydetyn sertifioinnin myöntämiseen tai peruuttamiseen. Tämä ei kuitenkaan tarkoita, että sertifiointielin tarvitsee sertifioinnin myöntämiseen valvontaviranomaisen luvan. Sertifiointielin valvoo, että sen asiakkaat noudattavat sertifiointikriteerejä.

29. Valvontaviranomaisella on korjaavat toimivaltuudet peruuttaa yleisen tietosuoja-asetuksen 42 ja 43 artiklan mukaisesti annettu sertifiointi tai määrätä sertifiointi peruutettavaksi taikka kieltää sertifiointielintä antamasta sertifiointia silloin kun sertifiointia koskevat vaatimukset eivät enää täyty.

30. Kansainvälisiä tiedonsiirtoja koskeva eurooppalainen tietosuojasinetti voi myös toimia kolmansiin maihin suuntautuvien siirtojen välineenä, kun sitä käytetään yhdessä sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa.[18]

31. Tiedonsiirrossa käytettäviä sertifiointeja voidaan myöntää myös ETA-maiden kansallisesti hyväksyttyjen sertifiointijärjestelmien mukaisesti. Tällaisia sertifiointeja voidaan kuitenkin soveltaa ainoastaan sellaisiin siirtoihin, joissa sertifiointijärjestelmän hyväksyneen ETA-maan viejä siirtää tietoja kolmansiin maihin. Näin on siksi, että eri ETA-maiden sertifiointeja ei tunnusteta vastavuoroisesti. Eri ETA-maiden valvontaviranomaiset voivat kuitenkin vapaasti hyväksyä saman sertifiointimekanismin tiedonsiirtoja varten.[19]

---

[17] Suuntaviivat 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen ((EU) 2016/679) 43 artiklan mukaisesti, s. 9.

[18] Ks. yleisen tietosuoja-asetuksen 42 artiklan 5 kohta ja sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskevat tietosuojaneuvoston suuntaviivat 1/2018, 35 kohta.

[19] Jos sertifiointikriteerit hyväksytään valvontaviranomaisen johdolla kansallisen aloitteen mukaisesti ja sen jälkeen muut maat haluavat ottaa käyttöön samat sertifiointikriteerit (otettuaan huomioon kyseisen järjestelmän kriteerit ja sovellettavat kansalliset erityissäännökset), ne voivat ottaa ne käyttöön ilman yleisen tietosuoja-asetuksen 64 artiklan mukaista tietosuojaneuvoston lausuntoa vedoten jo ensimmäiselle valvontaviranomaiselle asiasta annettuun lausuntoon yleisen tietosuoja-asetuksen 64 artiklan 3 kohdan mukaisesti (ks. tältä osin suuntaviivoja 1/2018 koskeva lisäys (liite sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskeviin suuntaviivoihin 1/2018), 66 kohta).

2 AKKREDITOINTIVAATIMUSTEN SOVELTAMISOHJEET

32. Vaatimukset, joita sovelletaan sertifiointielinten akkreditointiin tiedonsiirtovälineenä, käyvät selville ISO 17065 -standardista ja tulkitsemalla suuntaviivoja 4/2018[20] yhdessä yleisen tietosuoja-asetuksen V luvun kanssa, kuten jäljempänä selitetään.

33. Tietosuojaneuvosto katsoo, että suuntaviivojen 4/2018 ja ISO 17065 -standardin perusteella laaditut akkreditointia koskevat lisävaatimukset, jotka on jo aiemmin hyväksytty tietosuoja-asetuksen 64 artiklan 1 kohdan c alakohdan mukaisesti, kattavat jo erityisvaatimukset, joita sertifiointielinten akkreditointi tiedonsiirtovälineenä edellyttää. Joidenkin vaatimusten selittäviä huomautuksia ja tulkintaa on kuitenkin tarpeen tarkentaa tiedonsiirtojen yhteydessä.

34. Resurssivaatimusten osalta (ks. suuntaviivojen 4/2018 liitteessä 1 oleva vaatimus 6) sertifiointielimen on varmistettava, että sillä on tarvittavat resurssit varmentaa, että tietojen tuoja on sertifiointikriteerien edellyttämällä tavalla arvioinut asianmukaisesti sen kolmannen maan tai niiden kolmansien maiden oikeudellista tilannetta ja käytäntöjä, joihin se on sijoittautunut tai joissa se toimii.[21] Tämä arviointi olisi tehtävä niiden käsittelytoimien perusteella, jotka sertifioidaan osana arvioinnin kohdetta yleisen tietosuoja-asetuksen 46 artiklassa säädettyjen asianmukaisten suojatoimien osalta, ja sen olisi tarvittaessa katettava myös tuojan yksilöimät ja toteuttamat lisätoimenpiteet. Tähän sisältyy myös esimerkiksi asiaankuuluvien paikallisten lakien ja käytäntöjen laaja tuntemus sekä riittävä kielitaito kyseiset kolmannet maat huomioiden.

35. Prosessivaatimusten osalta (ks. suuntaviivojen 4/2018 liitteessä 1 oleva vaatimus 7) sertifiointielimen on varmistettava, että sertifiointimenettelyä voidaan tukea mahdollisilla paikan päällä tehtävillä tarkastuksilla, että käsittely tapahtuu kolmannessa maassa tai kolmansissa maissa ja että arviointi kattaa myös kolmansissa maissa voimassa olevan lainsäädännön ja politiikkojen käytännön täytäntöönpanon.

36. Sertifiointiin vaikuttavia muutoksia koskevien vaatimusten osalta (ks. suuntaviivojen 4/2018 liitteessä 1 oleva vaatimus 7.10) sertifiointielimen on seurattava kolmannen maan lainsäädännön ja/tai oikeuskäytännön muutoksia, jotka voivat vaikuttaa arvioinnin kohteen soveltamisalaan kuuluvaan käsittelyyn.

3 YKSITTÄISET SERTIFIOINTIKRITEERIT

37. Yksittäisten sertifiointikriteerien tarkastelun osalta nämä suuntaviivat perustuvat sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskevien suuntaviivojen 1/2018 (versio 3.0) vastaavaan liitteeseen 2, jossa käsitellään 42 artiklan 5 kohdan mukaisten sertifiointikriteerien tarkastelua ja arviointia, sekä kyseisten suuntaviivojen sertifiointikriteerien arviointia koskevaan lisäykseen (”*Certification criteria assessment*”).

38. Tietosuojaneuvosto katsoo, että suuntaviivojen 1/2018 liitteen 2 ja sertifiointikriteerien arviointia koskevan lisäyksen perusteella laaditut sertifiointikriteerit kattavat jo suurimman osan kriteereistä, jotka on otettava huomioon laadittaessa tiedonsiirtovälineenä käytettävää sertifiointijärjestelmää. Joitakin näistä olemassa olevista kriteereistä saattaa kuitenkin olla tarpeen tarkentaa, jotta niitä voidaan so-

[20] Suuntaviivat 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen ((EU) 2016/679) 43 artiklan mukaisesti sekä sen liite.
[21] Ks. edellä oleva 12 kohta.

veltaa tiettyihin tiedonsiirtoskenaarioihin (ks. kohta 3.1). Lisäksi saattaa olla tarpeen laatia lisäkriteerejä asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksien osalta (ks. kohta 3.2).

3.1 SERTIFIOINTIKRITEERIEN SOVELTAMISOHJEET

39. Sertifiointimekanismin soveltamisala ja arvioinnin kohde (ks. suuntaviivojen 1/2018 liite 2, kohta 2.a) olisi kuvattava selkeästi asiaa koskevissa asiakirjoissa, myös siltä osin, onko kyse henkilötietojen siirtämisestä kolmanteen maahan tai onko sertifioinnin tarkoitus kattaa myös tietojen kauttakulku.

40. Sertifiointimekanismin soveltamisalan ja arvioinnin kohteen osalta (ks. suuntaviivojen 1/2018 liite 2, kohta 2.b) asiaa koskevissa asiakirjoissa olisi kuvattava konkreettisesti, minkä tyyppisiin yhteisöihin (esim. rekisterinpitäjä ja/tai henkilötietojen käsittelijä) sertifiointimekanismia sovelletaan.

41. Sertifiointimekanismin soveltamisalan ja arvioinnin kohteen osalta (ks. suuntaviivojen 1/2018 liite 2, kohta 2.f) kriteereissä olisi edellytettävä, että arvioinnin kohde määritellään konkreettisesti väärinkäsitysten välttämiseksi. Määrittelyyn on sisällytettävä vähintään seuraavat tiedot:

42. käsittelytoimi (käsittelytoimet), myös siinä tapauksessa, että tiedot aiotaan siirtää edelleen

    a) käsittelyn tarkoitus

    b) yhteisön tyyppi (esim. rekisterinpitäjä ja/tai henkilötietojen käsittelijä)

    c) siirrettävien tietojen tyyppi ottaen huomioon, onko kyseessä yleisen tietosuoja-asetuksen 9 artiklassa määritellyt erityiset henkilötietoryhmät

    d) rekisteröityjen ryhmät

    e) maat, joissa käsittely tapahtuu.

43. Avoimuuden ja rekisteröityjen oikeuksien osalta (ks. suuntaviivojen 1/2018 liite 2, kohta 8) sertifiointikriteereissä olisi edellytettävä, että

    a) rekisteröidyille annetaan tietoja käsittelytoimista, tarvittaessa myös henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle (ks. yleisen tietosuoja-asetuksen 12, 13 ja 14 artikla);

    b) rekisteröidyille taataan oikeus tutustua tietoihin, oikaista ja poistaa tietoja, rajoittaa käsittelyä, saada ilmoitus henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista ja vastustaa käsittelyä sekä oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin. Tämä vastaa olennaisilta osin yleisen tietosuoja-asetuksen 15–19, 21 ja 22 artiklassa säädettyjä oikeuksia;

    c) sertifioinnin saanut tietojen tuoja ottaa käyttöön asianmukaisen valitusten käsittelymenettelyn rekisteröityjen oikeuksien tehokkaan täytäntöönpanon varmistamiseksi;

    d) toteutetaan arviointi, jossa selvitetään, ovatko nämä oikeudet rekisteröityjen kannalta täytäntöönpanokelpoisia asianomaisessa kolmannessa maassa ja missä määrin, sekä mahdolliset muut asianmukaiset toimenpiteet, jotka saattavat olla tarpeen näiden oikeuksien täytäntöönpanemiseksi. Näihin voi sisältyä muun muassa vaatimus siitä, että tuoja tunnustaa viejän (viejien) toimivaltaisen valvontaviranomaisen lainkäyttövallan ja suostuu tekemään yhteistyötä toimivaltaisten viranomaisten kanssa kaikissa menettelyissä, joiden tarkoituksena on varmistaa näiden oikeuksien noudattaminen, ja että tuoja suostuu vastaamaan tiedusteluihin, suostumaan tarkastuksiin ja noudattamaan edellä mainitun

valvontaviranomaisen vahvistamia toimenpiteitä, mukaan lukien korjaavat ja korvaavat toimenpiteet.

44. Suojelun takaavien teknisten ja organisatoristen toimenpiteiden osalta (suuntaviivojen 1/2018 liite 2, kohta 10.q) sertifiointikriteereissä olisi edellytettävä, että tuoja ilmoittaa henkilötietojen tietoturvaloukkauksista viejälle ja, jos tuoja toimii rekisterinpitäjänä, myös viejän (viejien) osalta toimivaltaiselle ETA:n valvontaviranomaiselle. Lisäksi sen on ilmoitettava rekisteröidyille, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille, kuten yleisen tietosuoja-asetuksen 34 artiklassa edellytetään.

3.2 MUUT YKSITTÄISET SERTIFIOINTIKRITEERIT

45. Ottaen huomioon yleisen tietosuoja-asetuksen 46 artiklan mukaiset muita tiedonsiirtovälineitä koskevat suojatoimet (kuten yritystä koskevat sitovat säännöt tai käytännesäännöt) ja yhdenmukaisen suojan tason varmistamiseksi ja ottaen huomioon unionin tuomioistuimen asiassa Schrems II antama tuomio, tietosuojaneuvosto katsoo, että kolmansiin maihin tehtävissä siirroissa käytettävään sertifiointimekanismiin olisi sisällytettävä myös jäljempänä luetellut kriteerit.

1. Kolmannen maan lainsäädännön arviointi

a) Edellytetäänkö kriteereissä, että tuoja on arvioinut sen kolmannen maan säännöt ja käytännöt, jossa se toimii, ja sen, estävätkö ne tuojaa noudattamasta sertifioinnin mukaisia sitoumuksiaan?
b) Edellytetäänkö kriteereissä, että tuoja dokumentoi sen kolmannen maan sääntöjen ja käytäntöjen arvioinnin, jossa se toimii, ja pitää asiakirjat sertifiointielimen saatavilla sekä pyynnöstä myös viejän osalta toimivaltaisen ETA:n valvontaviranomaisen ja viejän saatavilla?
c) Edellytetäänkö kriteereissä, että tuoja on yksilöinyt ja toteuttanut organisatoriset ja tekniset toimenpiteet, joilla varmistetaan yleisen tietosuoja-asetuksen 46 artiklan mukaiset asianmukaiset suojatoimet, ottaen huomioon suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi?
d) Edellytetäänkö kriteereissä, että tuoja dokumentoi organisatoriset ja tekniset toimenpiteet, jotka on tosiasiallisesti toteutettu asianmukaisten suojatoimien varmistamiseksi yleisen tietosuoja-asetuksen 46 artiklan mukaisesti, ja pitää asiakirjat sertifiointielimen saatavilla sekä pyynnöstä myös toimivaltaisten tietosuojaviranomaisten ja viejän saatavilla?
e) Edellytetäänkö kriteereissä, että tuoja on yksilöinyt ja toteuttanut organisatoriset ja tekniset toimenpiteet, joilla varmistetaan siirrettyjen henkilötietojen turvallisuus, ottaen huomioon suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, jos kauttakuljetus sisältyy tiedonsiirtovälineenä käytettävän sertifioinnin soveltamisalaan?
f) Edellytetäänkö kriteereissä, että tuoja antaa sertifiointielimelle ja viejälle takeet siitä, että tuojalla ei ole syytä uskoa, että siihen sovellettavat lait tai käytännöt voivat estää sitä täyttämästä sertifioinnin mukaisia velvoitteitaan?

2. Viejien ja tuojien yleiset velvoitteet

a) Edellytetäänkö kriteereissä, että viejien ja tuojien välisissä sopimuksissa (esim. voimassa olevassa palvelusopimuksessa) esitetään kuvaus siirrosta, johon sertifiointia sovelletaan, ja

siitä, että edunsaajana olevien kolmansien osapuolten oikeudet tunnustetaan asianomaisten rekisteröityjen osalta?

b) Jos kriteerit edellyttävät erityistä sisältöä näille sopimuksille tai välineille ja tästä on laadittu malli, edellytetäänkö kriteereissä, että myös ne on arvioitava?

3. Tietojen edelleen siirtämistä koskevat säännöt

a) Edellytetäänkö kriteereissä, että tietojen edelleen siirtämiseen sovelletaan yleisen tietosuoja-asetuksen V luvun vaatimusten mukaisia erityisiä suojatoimia sen varmistamiseksi, että ETA:ssa taattu suojan taso ei heikkene, ja edellytetäänkö kriteereissä, että asianmukaiset asiakirjat on pidettävä viejän (viejien) osalta toimivaltaisen sertifiointielimen ja ETA:n valvontaviranomaisen sekä pyynnöstä myös viejän saatavilla?

4. Oikeussuojakeinot ja niiden täytäntöönpano

a) Edellytetäänkö kriteereissä, että rekisteröidyt voivat vedota oikeuksiinsa edunsaajana olevana kolmantena osapuolena tietojen tuojaa vastaan rekisteröidyn asuinpaikan ETA-tuomioistuimessa tai kansainvälisessä järjestössä, mukaan lukien oikeuteen saada korvaus rekisteröidylle aiheutuneesta vahingosta, jos tuoja ei noudata asiaankuuluvaa sertifiointijärjestelmää?
b) Voidaanko kriteerien perusteella arvioida asianmukaisesti, että tuoja on vastuussa ETA:ssa rekisteröidylle aiheutuneesta vahingosta, jos se ei noudata asiaankuuluvaa sertifiointijärjestelmää?
c) Edellytetäänkö kriteereissä, että rekisteröidyt voivat tehdä kantelun tuojasta ETA:n valvontaviranomaiselle, erityisesti siinä ETA-maassa, jossa rekisteröidyn vakinainen asuinpaikkansa tai työpaikkansa sijaitsee tai joka on toimivaltainen tietojen viejän (viejien) osalta?
d) Edellytetäänkö kriteereissä, että tuoja tekee yhteistyötä tietojen viejän (viejien) osalta toimivaltaisen ETA:n valvontaviranomaisen kanssa ja hyväksyy sen suorittaman tarkastuksen, ottaa huomioon sen neuvot ja noudattaa sen päätöksiä?

5. Menettelyt ja toimet tilanteissa, joissa kansallinen lainsäädäntö estää sertifiointiin liittyvien sitoumusten noudattamisen

a) Edellytetäänkö kriteereissä sitoutumista siihen, että jos tietojen tuojalla kolmannessa maassa tai kansainvälisessä järjestössä on syytä uskoa, että muutokset siihen sovellettavissa lainsäädännössä tai käytännöissä saattavat estää sitä täyttämästä sertifioinnin mukaisia velvoitteitaan, se ilmoittaa tästä viipymättä sertifiointielimelle ja tietojen viejälle, jotta viimeksi mainittu voi arvioida, onko siirrot keskeytettävä välittömästi?
b) Edellytetäänkö kriteereissä kuvausta toimenpiteistä, joihin on ryhdyttävä (mukaan lukien ilmoittaminen ETA:n viejälle ja asianmukaisten lisätoimenpiteiden toteuttaminen), jos tietojen tuoja saa tiedon kolmannen maan lainsäädännöstä tai käytännöistä, jotka estävät sertifioinnin mukaisten velvoitteiden noudattamisen, sekä toimenpiteistä, joihin on ryhdyttävä kolmannen maan viranomaisten esittämien tietopyyntöjen yhteydessä (mukaan lukien velvollisuus tarkistaa ja tarvittaessa riitauttaa pyynnön laillisuus ja minimoida luovutettavat tiedot)?

6. Kolmansien maiden viranomaisten esittämien tietopyyntöjen käsittely

a) Edellytetäänkö kriteereissä, että tietojen tuoja ilmoittaa viipymättä tietojen viejälle kolmansien maiden viranomaisten esittämistä tietopyynnöistä ja ryhtyy niiden osalta asianmukaisiin lisätoimenpiteisiin?
b) Edellytetäänkö kriteereissä, että siirtoja, jotka johtuvat kolmansien maiden viranomaisten suhteettomista tietopyynnöistä, erityisesti pyynnöistä, jotka edellyttävät henkilötietojen laajamittaista ja rajoittamatonta siirtoa, ei saa toteuttaa?

7. Viejää koskevat lisätoimenpiteet

46. Edellytetäänkö kriteereissä, että tietojen tuoja varmistaa, myös tietojen viejää koskevilla sitovilla vaatimuksilla, että viejä lisätoimenpiteet vastaavat tuojan yksilöimiä lisätoimenpiteitä ottaen huomioon myös tietosuojaneuvoston suositukset 1/2020 ja esitetyt esimerkkitapaukset, jotta voidaan varmistaa tuojan lisätoimenpiteiden tehokas täytäntöönpano?

4 SITOVAT JA TÄYTÄNTÖÖNPANOKELPOISET SITOUMUKSET

47. Yleisen tietosuoja-asetuksen 42 artiklan 2 kohdassa edellytetään, että tietosuoja-asetuksen ulkopuoliset rekisterinpitäjät ja henkilötietojen käsittelijät, jotka noudattavat tiedonsiirtoihin käytettäviä sertifiointimekanismeja, tekevät lisäksi joko sopimusperusteisesti tai muulla oikeudellisesti sitovalla välineellä[22] sitovat ja täytäntöönpanokelpoiset sitoumukset, joiden mukaan ne soveltavat sertifiointimekanismin mukaisia suojatoimia, myös rekisteröityjen oikeuksiin.

48. Kuten yleisessä tietosuoja-asetuksessa säädetään, tällaiset sitoumukset voidaan tehdä käyttämällä sopimusta, mikä vaikuttaa olevan yksinkertaisin ratkaisu. Myös muita välineitä voidaan käyttää edellyttäen, että sertifiointimekanismia noudattavat rekisterinpitäjät ja henkilötietojen käsittelijät pystyvät osoittamaan, että tällaiset muut keinot ovat sitovia ja täytäntöönpanokelpoisia.

49. Sitovuus ja täytäntöönpanokelpoisuus on joka tapauksessa varmistettava unionin oikeuden mukaisesti, minkä lisäksi sitoumusten olisi oltava sitovia ja täytäntöönpanokelpoisia myös rekisteröidyille, jotka ovat edunsaajana olevia kolmansia osapuolia.

50. Yksinkertainen vaihtoehto olisi sisällyttää sitovat ja täytäntöönpanokelpoiset sitoumukset tietojen viejän ja tietojen tuojan väliseen sopimukseen. Käytännössä osapuolet voisivat käyttää olemassa olevaa sopimusta (kuten viejän ja tuojan välistä palvelusopimusta, yleisen tietosuoja-asetuksen 28 artiklan mukaista rekisterinpitäjän ja henkilötietojen käsittelijän välistä käsittelysopimusta tai erillisten rekisterinpitäjien välistä yhteiskäyttösopimusta), johon sitovat ja täytäntöönpanokelpoiset sitoumukset voitaisiin sisällyttää. Nämä sitoumukset olisi kuitenkin erotettava selvästi muista lausekkeista. Toinen vaihtoehto voisi olla esimerkiksi erillisen sopimuksen tekeminen siten, että tiedonsiirtoihin käytettävään sertifiointimekanismiin sisällytetään mallisopimus, joka kolmannessa maassa sijaitsevien rekisterinpitäjien tai henkilötietojen käsittelijöiden ja kaikkien tietojen viejien olisi allekirjoitettava.

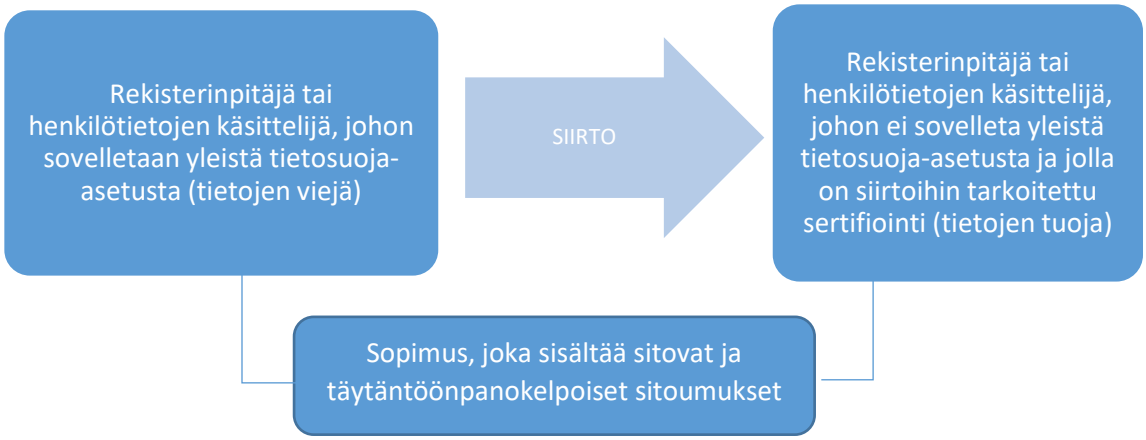
51. Sopivimman vaihtoehdon valinnassa olisi oltava joustovaraa kulloisenkin tilanteen mukaan.

52. Kun sertifiointimekanismia on tarkoitus käyttää tiedonsiirroissa ja tietojen siirroissa edelleen henkilötietojen käsittelijältä alikäsittelijöille, myös henkilötietojen käsittelijän ja sen rekisterinpitäjän välisessä

[22] Tämä oikeudellisesti sitova väline ei saa olla toinen V luvun tiedonsiirtoväline (kuten vakiosopimuslauseke), koska 46 artiklan 2 kohdan f alakohdassa tarkoitetut sitovat ja täytäntöönpanokelpoiset sitoumukset on laadittava siten, että niillä varmistetaan, että tietojen tuoja noudattaa sertifiointikriteerejä.

käsittelysopimuksessa olisi viitattava sertifiointimekanismiin ja välineeseen, johon sitovat ja täytäntöönpanokelpoiset sitoumukset perustuvat.

Esimerkki tietojen viejän ja tietojen tuojan väliseen sopimukseen sisällytetyistä sitovista ja täytäntöönpanokelpoisista sitoumuksista:



53. Yleensä sopimuksessa tai muussa oikeudellisesti sitovassa välineessä on määrättävä, että sertifioinnin saanut tuojana toimiva rekisterinpitäjä tai henkilötietojen käsittelijä sitoutuu noudattamaan siirtoihin käytetyssä sertifioinnissa määriteltyjä sääntöjä käsitellessään ETA:sta vastaanottamiaan tietoja ja takaa, että sillä ei ole mitään syytä uskoa, että kyseiseen käsittelyyn sovellettavat kolmannen maan lait ja käytännöt, mukaan lukien henkilötietojen luovuttamista koskevat vaatimukset tai toimenpiteet, jotka mahdollistavat viranomaisten pääsyn tietoihin, estävät sitä täyttämästä sertifioinnin mukaisia sitoumuksiaan. Lisäksi se sitoutuu ilmoittamaan viejälle kaikista asiaa koskeviin lakeihin tai käytäntöihin tehdyistä olennaisista muutoksista.

54. Sopimuksessa tai muussa välineessä on myös määrättävä mekanismeista, joiden avulla tällaiset sitoumukset voidaan panna täytäntöön, jos tuojana toimiva rekisterinpitäjä tai henkilötietojen käsittelijä ei noudata sertifioinnin sääntöjä ja erityisesti niiden rekisteröityjen oikeuksia, joiden tietoja siirretään sertifiointia käyttäen.

55. Sopimuksessa tai muussa välineessä olisi erityisesti käsiteltävä seuraavia näkökohtia:

- Rekisteröidyillä, joiden tietoja siirretään sertifiointia käyttäen, on oikeus edunsaajana olevana kolmantena osapuolena valvoa sertifioinnin saaneen tuojan sertifioinnin yhteydessä tekemien sitoumusten noudattamista.

- Kysymys vastuusta tapauksissa, joissa ETA:n ulkopuolella sertifioinnin saanut tuoja ei noudata sertifioinnin sääntöjä: Jos ETA:n ulkopuolella sertifioinnin saanut tuoja ei noudata sertifioinnin sääntöjä, rekisteröidyllä on oltava mahdollisuus nostaa kanne kyseistä yhteisöä vastaan rekisteröidyn vakinaisen asuinpaikan ETA:n valvontaviranomaisessa tai ETA:n tuomioistuimessa vetoamalla edunsaajana olevan kolmannen osapuolen oikeuteensa, mukaan lukien oikeus vahingonkorvaukseen. Sertifioinnin saaneen tuojan on hyväksyttävä rekisteröidyn päätös tehdä näin. Jos tietojen viejä voi joutua vastuuseen sen seurauksena, että tietojen tuoja ei noudata sääntöjä, rekisteröidyillä on myös oltava mahdollisuus nostaa kanne viejää vastaan valvontaviranomaisessa, viejän toimipaikan tuomioistuimessa tai rekisteröidyn asuinpaikan

tuomioistuimessa.[23] Tuojan ja viejän olisi myös hyväksyttävä, että rekisteröityä voi edustaa voittoa tavoittelematon elin, järjestö tai yhdistys yleisen tietosuoja-asetuksen 80 artiklan 1 kohdassa säädetyin edellytyksin.

- Viejän oikeus panna sertifioinnin säännöt täytäntöön sertifioinnin saanutta tuojaa vastaan edunsaajana olevana kolmantena osapuolena.

- Sertifioinnin saaneen tuojan velvollisuus ilmoittaa viejälle ja viejän valvontaviranomaiselle toimenpiteistä, joita sertifiointielin on toteuttanut havaittuaan, että kyseinen tuoja ei ole noudattanut sertifioinnin sääntöjä.

[23] Tämä vastuu ei saisi vaikuttaa mekanismeihin, jotka on tarkoitus panna täytäntöön sertifioinnin mukaisesti sertifiointielimen kanssa, joka voi myös ryhtyä toimiin rekisterinpitäjiä tai henkilötietojen käsittelijöitä vastaan sertifioinnin mukaisesti määräämällä korjaavia toimenpiteitä.

LIITE

A. ESIMERKKEJÄ LISÄTOIMENPITEISTÄ, JOTKA TUOJAN ON TOTEUTETTAVA, KUN SERTIFIOINNIN SOVELTAMISALA KATTAA TIETOJEN KAUTTAKULUN

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

Määritetään salausstandardeja ja salausavaimen turvallisuutta koskevat kriteerit, erityisesti kolmannen maan oikeudellista tilannetta koskevat kriteerit. Jos tuoja voidaan pakottaa luovuttamaan salausavaimet, lisätoimenpidettä ei voida pitää tehokkaana.[24]

Esimerkkitapaus 2: Pseudonymisoitujen tietojen siirto

Pseudonymisoitujen tietojen osalta on määritettävä kriteerit, joilla varmistetaan sellaisten lisätietojen turvallisuus, jotka tarvitaan tietojen yhdistämiseksi tunnistettuun tai tunnistettavissa olevaan henkilöön, erityisesti seuraavat kriteerit:

– Kolmannen maan oikeudellista tilannetta koskevat kriteerit. Jos tuoja voidaan pakottaa antamaan pääsy lisätietoihin tai käyttämään lisätietoja tietojen yhdistämiseksi tunnistettuihin tai tunnistettavissa oleviin henkilöihin, toimenpidettä ei voida pitää tehokkaana.[25]

– Kriteerit, joita sovelletaan sellaisten kolmansien maiden viranomaisten käytettävissä olevien lisätietojen määrittelyyn, jotka saattavat riittää yhdistämään tiedot tunnistettuihin tai tunnistettavissa oleviin henkilöihin.

Esimerkkitapaus 3: Tietojen salaaminen niiden suojaamiseksi kolmannen maan viranomaisten pääsyltä tietoihin, kun siirto viejän ja tuojan välillä tapahtuu kolmannen maan kautta

Salattujen tietojen tapauksessa on määritettävä kaikki kauttakulun turvallisuuteen liittyvät kriteerit. Jos tuoja voidaan pakottaa luovuttamaan salausavaimet salauksen purkamista tai todentamista varten tai muuttamaan kauttakulussa käytettävää komponenttia siten, että sen turvallisuusominaisuudet vaarantuvat, lisätoimenpidettä ei voida pitää tehokkaana.[26]

Esimerkkitapaus 4: Suojattu vastaanottaja

Suojattujen vastaanottajien tapauksessa on määritettävä erioikeuden rajausta koskevat kriteerit. Tällöin käsittelyn on pysyttävä lakisääteisen erioikeuden rajoissa. Tämä koskee myös (ali)käsittelijöiden suorittamaa käsittelyä ja tietojen edelleen siirtämistä: myös näissä tapauksissa tietojen vastaanottajien on kuuluttava erioikeuden piiriin.[27]

---

[24] Liite 2, Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, versio 2.0, esimerkkitapaus 1: Tietojen säilyttäminen varmuuskopiointia ja muita sellaisia tarkoituksia varten, joissa itse tietoihin ei tarvitse päästä, 84 kohta; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[25] Ks. alaviite 24, 86–89 kohta.

[26] Ks. alaviite 24, 90 kohta.

[27] Ks. alaviite 24, 91 kohta.

B. ESIMERKKEJÄ LISÄTOIMENPITEISTÄ, KUN SERTIFIOINTI EI KATA TIETOJEN KAUTTAKULKUA JA VIEJÄN ON SUOJATTAVA TIEDOT

Esimerkkitapaus 2: Pseudonymisoitujen tietojen siirto

Määritetään kriteerit, joita sovelletaan sellaisten kolmansien maiden viranomaisten käytettävissä oleviin lisätietoihin, jotka saattavat riittää yhdistämään tiedot tunnistettuihin tai tunnistettavissa oleviin henkilöihin.

Esimerkkitapaus 3: Tietojen salaaminen niiden suojaamiseksi kolmannen maan viranomaisten pääsyltä tietoihin, kun siirto viejän ja tuojan välillä tapahtuu kolmannen maan kautta

Määritetään kriteerit, jotka liittyvät käytettävän julkisen avaimen varmentamisesta vastaavan viranomaisen tai käytettävän infrastruktuurin luotettavuuteen, todentamiseen tai salauksen purkamiseen käytettävien salausavainten turvallisuuteen ja avainten hallinnan luotettavuuteen sekä asianmukaisesti ylläpidettyjen ohjelmistojen käyttöön (ohjelmissa ei saa olla tunnettuja haavoittuvuuksia).

Jos tuoja voidaan pakottaa luovuttamaan salausavaimet salauksen purkamista tai todentamista varten tai muuttamaan kauttakulussa käytettävää komponenttia siten, että sen turvallisuusominaisuudet vaarantuvat, toimenpidettä ei voida pitää tehokkaana.[28]

Esimerkkitapaus 4: Suojattu vastaanottaja

Suojattujen vastaanottajien tapauksessa on määritettävä erioikeuden rajausta koskevat kriteerit. Tällöin käsittelyn on pysyttävä lakisääteisen erioikeuden rajoissa. Tämä koskee myös (ali)käsittelijöiden suorittamaa käsittelyä ja tietojen edelleen siirtämistä: myös näissä tapauksissa tietojen vastaanottajien on kuuluttava erioikeuden piiriin.[29]

[28] Ks. alaviite 24, 90 kohta.
[29] Ks. alaviite 24, 91 kohta.