Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018

Versio 3.0

4. kesäkuuta 2019

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

Hyväksytty

Versiohistoria

Versio 3.0	4. kesäkuuta 2019	Liitteen 2 lisääminen (liitteen 2 versio 2.0 hyväksyttiin 4. kesäkuuta 2019 julkisen kuulemisen jälkeen)
Versio 2.1	9. huhtikuuta 2019	Suuntaviivoihin tehdyn oikaisun hyväksyminen (45 kohta)
Versio 2.0	23. tammikuuta 2019	Suuntaviivojen hyväksyminen julkisen kuulemisen jälkeen – samana päivänä liite 2 (versio 1.0) hyväksyttiin julkista kuulemista varten
Versio 1.0	25. toukokuuta 2018	Suuntaviivojen hyväksyminen julkista kuulemista varten

Sisällysluettelo

1 Johdanto 5

1.1 Suuntaviivojen soveltamisala 6

1.2 Yleisen tietosuoja-asetuksen mukaisen sertifioinnin tarkoitus 7

1.3 Keskeiset käsitteet 8

1.3.1 ”Sertifioinnin” tulkinta 8

1.3.2 Sertifiointimekanismit, sinetit ja merkit 9

2 Valvontaviranomaisten tehtävä 10

2.1 Valvontaviranomainen sertifiointielimenä 10

2.2 Valvontaviranomaisen muut sertifiointiin liittyvät tehtävät 11

3 Sertifiointielimen tehtävä 12

4 Sertifiointikriteerien hyväksyminen 12

4.1 Toimivaltainen valvontaviranomainen hyväksyy kriteerit 13

4.2 Tietosuojaneuvosto hyväksyy eurooppalaisen tietosuojasinetin kriteerit 13

4.2.1 Hyväksynnän hakeminen 13

4.2.2 Eurooppalaisen tietosuojasinetin kriteerit 14

4.2.3 Akkreditoinnin tehtävä 15

5 Sertifiointikriteerien laatiminen 16

5.1 Mitä voidaan sertifioida yleisen tietosuoja-asetuksen mukaisesti? 16

5.2 Sertifioinnin kohteen määrittely 18

5.3 Arviointimenetelmät ja -metodologiat 19

5.4 Arvioinnin dokumentointi 20

5.5 Tulosten dokumentointi 20

6 Sertifiointikriteerien määrittelyä koskevat suuntaviivat 21

6.1 Olemassa olevat standardit 22

6.2 Kriteerien määrittely 22

6.3 Sertifiointikriteerien voimassaolo 23

Liite 1: Sertifiointiin liittyvät valvontaviranomaisten tehtävät ja valtuudet yleisen tietosuoja-asetuksen mukaisesti 24

Liite 2 25

1 Johdanto 25

2 Sertifiointimekanismin soveltamisala ja arvioinnin kohde 25

3 Yleiset vaatimukset 26

4 Käsittelytoimi, 42 artiklan 1 kohta 26

5 Käsittelyn lainmukaisuus 27

6 Periaatteet, 5 artikla 27
7 Rekisterinpitäjien ja henkilötietojen käsittelijöiden yleiset velvoitteet 27
8 Rekisteröityjen oikeudet 28
9 Luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit 28
10 Suojelun takaavat tekniset ja organisatoriset toimenpiteet 28
11 Muita erityisiä tietosuojaystävällisiä ominaisuuksia 29
12 Kriteerit, joiden tarkoitus on osoittaa asianmukaisten suojatoimien olemassaolo henkilötietojen siirtämisen yhteydessä 30
13 Eurooppalaisen tietosuojasinetin lisäkriteerit 30
14 Kriteerien yleinen arviointi 30

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,

ottaa huomioon 25 päivänä toukokuuta 2018 hyväksytyn työjärjestyksensä 12 ja 22 artiklan,

ottaa huomioon yleisen tietosuoja-asetuksen 70 artiklan 4 kohdan mukaisesti 30 päivän toukokuuta 2018 ja 12 päivän heinäkuuta 2018 välisenä aikana pidetyn, suuntaviivoja koskevan julkisen kuulemisen ja 15 päivän helmikuuta 2019 ja 29 päivän maaliskuuta 2019 välisenä aikana pidetyn, liitettä 2 koskevan julkisen kuulemisen tulokset,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT:

1 JOHDANTO

1. Yleisessä tietosuoja-asetuksessa (asetus 2016/679) säädetään nykyaikaistetusta, tilivelvollisuuteen perustuvasta ja perusoikeuksia noudattavasta tietosuojakehyksestä Euroopassa. Tämän uuden kehyksen kannalta ovat keskeisiä toimenpiteet, jotka helpottavat yleisen tietosuoja-asetuksen säännösten noudattamista. Niihin kuuluvat erityistilanteita koskevat pakolliset vaatimukset (mukaan lukien tietosuojavastaavien nimeäminen ja tietosuojaa koskevien vaikutustenarviointien tekeminen) ja vapaaehtoiset toimenpiteet, kuten käytännesäännöt ja sertifiointimekanismit.
2. Ennen yleisen tietosuoja-asetuksen hyväksymistä tietosuojatyöryhmä vahvisti, että sertifioinnilla voisi olla tietosuojan tilivelvollisuuskehyksessä merkittävä rooli.1 Jotta sertifioinnilla saataisiin luotettavaa näyttöä tietosuojasääntöjen noudattamisesta, olisi laadittava selvät säännöt, joissa esitetään sertifioinnin tarjoamista koskevat vaatimukset.2 Oikeusperusta tällaisten sääntöjen laatimiselle vahvistetaan yleisen tietosuoja-asetuksen 42 artiklassa.
3. Yleisen tietosuoja-asetuksen 42 artiklan 1 kohdassa säädetään seuraavaa:

   "Jäsenvaltiot, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja sekä tietosuojasinettejä ja -merkkejä erityisesti unionin tasolla, minkä tarkoituksena on osoittaa, että rekisterinpitäjät ja

[1] Tietosuojatyöryhmän lausunto 3/2010 tilivelvollisuuden periaatteesta, WP173, 13. heinäkuuta 2010, kohdat 69–71.
[2] Tietosuojatyöryhmän lausunto 3/2010 tilivelvollisuuden periaatteesta, WP173, kohta 69.

henkilötietojen käsittelijät noudattavat käsittelytoimia suorittaessaan tätä asetusta. Mikroyritysten sekä pienten ja keskisuurten yritysten erityistarpeet on otettava huomioon."

4. Sertifiointimekanismit3 voivat parantaa avoimuutta paitsi rekisteröityjen kannalta myös yritysten välisissä suhteissa, esimerkiksi rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä. Yleisen tietosuoja-asetuksen johdanto-osan 100 kappaleessa todetaan, että sertifiointimekanismien käyttöönotto voi tehostaa läpinäkyvyyttä ja asetuksen noudattamista ja rekisteröidyt voivat niiden avulla nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojan tason.4

5. Yleisessä tietosuoja-asetuksessa ei oteta käyttöön rekisterinpitäjien ja henkilötietojen käsittelijöiden sertifiointioikeutta tai -velvollisuutta. Sertifiointi on 42 artiklan 3 kohdan mukaan vapaaehtoista ja auttaa osoittamaan, että yleistä tietosuoja-asetusta noudatetaan. Jäsenvaltioita ja valvontaviranomaisia kehotetaan kannustamaan sertifiointimekanismien perustamiseen, ja ne määrittelevät sidosryhmien sitoutumisen sertifiointiprosessiin ja sertifioinnin elinkaareen.

6. Hyväksyttyjen sertifiointimekanismien noudattaminen on myös asia, joka valvontaviranomaisten on otettava huomioon raskauttavana tai lieventävänä tekijänä, kun ne päättävät hallinnollisen sakon määräämisestä ja sakon määrästä (83 artiklan 2 kohdan j alakohta).5

1.1 Suuntaviivojen soveltamisala

7. Näiden suuntaviivojen soveltamisala on rajallinen; ne eivät ole yleisen tietosuoja-asetuksen mukaista sertifiointia koskeva menettelyohje. Suuntaviivojen ensisijaisena tarkoituksena on määritellä yleiset vaatimukset ja kriteerit, jotka voivat olla kaikentyyppisten yleisen tietosuoja-asetuksen 42 ja 43 artiklan mukaisten sertifiointimekanismien kannalta olennaisia. Tätä tarkoitusta varten suuntaviivoissa

   - tarkastellaan, miksi ja miten sertifiointia voidaan käyttää tilivelvollisuuden toteuttamisen välineenä
   - kerrotaan, mitkä ovat 42 ja 43 artiklan sertifiointia koskevien säännösten keskeiset käsitteet
   - selitetään, mikä on sertifioinnin 42 ja 43 artiklan mukainen soveltamisala sekä sertifioinnin tarkoitus
   - autetaan saavuttamaan mielekäs, yksiselitteinen, mahdollisimman hyvin toistettavissa oleva ja sertifioijasta riippumatta vertailukelpoinen (vertailukelpoisuus) sertifiointitulos.

[3] Näissä suuntaviivoissa käytetään sertifiointimekanismeista ja tietosuojasineteistä ja -merkeistä yhteisnimitystä 'sertifiointimekanismit', ks. kohta 1.3.2.
[4] Johdanto-osan 100 kappaleessa todetaan näin: "Läpinäkyvyyden ja tämän asetuksen noudattamisen tehostamiseksi olisi edistettävä sertifiointimekanismien - - käyttöönottoa, jotta rekisteröidyt voisivat nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojan tason."
[5] Ks. asetuksessa 2016/679 tarkoitettujen hallinnollisten sakkojen soveltamista ja määräämistä koskevat tietosuojatyöryhmän suuntaviivat (WP 253).

8. Yleisessä tietosuoja-asetuksessa esitetään jäsenvaltioille ja valvontaviranomaisille 42 ja 43 artiklan täytäntöönpanoa varten useita keinoja. Suuntaviivoissa annetaan neuvoja 42 ja 43 artiklan säännösten tulkintaan ja täytäntöönpanoon ja autetaan jäsenvaltioita, valvontaviranomaisia ja kansallisia akkreditointielimiä toimimaan yhtenäisemmin ja yhdenmukaisemmin, kun ne ottavat käyttöön sertifiointimekanismeja yleisen tietosuoja-asetuksen mukaisesti.

9. Suuntaviivojen neuvot on tarkoitettu

   - toimivaltaisille valvontaviranomaisille ja Euroopan tietosuojaneuvostolle, jäljempänä ’tietosuojaneuvosto’, silloin kun ne hyväksyvät sertifiointikriteerejä 42 artiklan 5 kohdan, 58 artiklan 3 kohdan f alakohdan ja 70 artiklan 1 kohdan o alakohdan mukaisesti
   - sertifiointielimille, silloin kun ne laativat ja tarkastelevat uudelleen sertifiointikriteerejä, ennen niiden toimittamista toimivaltaiselle valvontaviranomaiselle hyväksyttäväksi 42 artiklan 5 kohdan mukaisesti
   - tietosuojaneuvostolle, silloin kun se hyväksyy eurooppalaisen tietosuojasinetin 42 artiklan 5 kohdan ja 70 artiklan 1 kohdan o alakohdan mukaisesti
   - valvontaviranomaisille, silloin kun ne laativat omia sertifiointikriteerejään
   - Euroopan komissiolle, jolla on valta antaa delegoituja säädöksiä, joissa täsmennetään tietosuojaa koskevien sertifiointimekanismien osalta huomioon otettavat vaatimukset 43 artiklan 8 kohdan mukaisesti
   - tietosuojaneuvostolle, silloin kun se toimittaa Euroopan komissiolle lausunnon sertifiointivaatimuksista 70 artiklan 1 kohdan q alakohdan ja 43 artiklan 8 kohdan mukaisesti
   - kansallisille akkreditointielimille, joiden on otettava huomioon sertifiointikriteerit sertifiointielinten akkreditoinnin osalta EN-ISO/IEC 17065/2012 -standardia noudattaen sekä lisävaatimukset 43 artiklan mukaisesti
   - rekisterinpitäjille ja henkilötietojen käsittelijöille, silloin kun ne määrittelevät omia yleisen tietosuoja-asetuksen noudattamista koskevia strategioitaan ja harkitsevat sertifiointia keinona osoittaa, että ne ovat noudattaneet asetusta.

10. Tietosuojaneuvosto julkaisee erilliset suuntaviivat, jotka koskevat henkilötietojen siirtoon kolmansiin maihin tai kansainvälisille järjestöille käytettävien sertifiointimekanismien hyväksymiskriteerien määrittelyä 42 artiklan 2 kohdan mukaisesti.

1.2 Yleisen tietosuoja-asetuksen mukaisen sertifioinnin tarkoitus

11. Yleisen tietosuoja-asetuksen 42 artiklan 1 kohdan mukaan sertifiointimekanismien käyttöönoton tarkoituksena on ”osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat käsittelytoimia suorittaessaan tätä asetusta”.

12. Yleisessä tietosuoja-asetuksessa esitetään esimerkkejä siitä, missä yhteydessä voidaan osoittaa hyväksyttyjen sertifiointimekanismien avulla, että rekisterinpitäjät ja henkilötietojen käsittelijät täyttävät velvollisuutensa, jotka koskevat

    - tarvittavien teknisten ja organisatoristen toimenpiteiden toteuttamista ja asetuksen noudattamisen osoittamista 24 artiklan 1 ja 3 kohdan, 25 artiklan ja 32 artiklan 1 ja 3 kohdan mukaisesti
    - riittäviä suojatoimia, joihin viitataan 28 artiklan 1 kohdassa (henkilötietojen käsittelijältä rekisterinpitäjälle) ja 4 kohdassa (alihankkijana toimivalta henkilötietojen käsittelijältä henkilötietojen käsittelijälle).

13. Koska sertifiointi ei itsessään todista yleisen tietosuoja-asetuksen noudattamista vaan asetuksen noudattaminen voidaan osoittaa sen avulla, se olisi toteutettava läpinäkyvästi. Asetuksen noudattamisen osoittamiseen tarvitaan sitä tukevaa dokumentaatiota, erityisesti kirjallisia raportteja, joissa ei pelkästään toisteta sitä, miten kriteerit täytetään, vaan myös kuvataan sitä. Jos kriteerit eivät aluksi täyty, dokumentaatiossa on kuvattava korjauksia ja korjaavia toimia ja niiden tarkoituksenmukaisuutta niin, että sertifiointi voidaan niiden perusteella myöntää ja säilyttää. Tähän kuuluu myös sertifioinnin myöntämistä, uusimista tai peruuttamista koskevan yksittäisen päätöksen luonnos. Siinä olisi esitettävä kriteerien soveltamisesta johtuvat syyt, perustelut ja todisteet sekä sertifioinnin aikana tosiseikkojen tai olettamusten perusteella tehdyt johtopäätökset, arvioinnit tai päätelmät.

1.3 Keskeiset käsitteet

14. Seuraavissa kohdissa tarkastellaan 42 ja 43 artiklan keskeisiä käsitteitä. Analyysissä selvitetään yleisen tietosuoja-asetuksen mukaisen sertifioinnin perustermejä ja soveltamisalaa.

1.3.1 ”Sertifioinnin” tulkinta

15. Yleisessä tietosuoja-asetuksessa ei määritellä termiä ’sertifiointi’. Kansainvälisen standardisoimisjärjestön (ISO) yleispätevän määritelmän mukaan sertifiointi tarkoittaa menettelyä, jossa riippumaton elin antaa kirjallisen varmennuksen (sertifikaatin) siitä, että jokin tuote, palvelu tai järjestelmä täyttää tietyt vaatimukset. Sertifiointia kutsutaan myös kolmannen osapuolen suorittamaksi vaatimustenmukaisuuden arvioinniksi, ja sertifiointielimistä voidaan myös käyttää nimitystä vaatimustenmukaisuuden arviointilaitokset. Standardissa EN-ISO/IEC 17000:2004 ”Vaatimustenmukaisuuden arviointi. Sanasto ja yleiset periaatteet” (johon viitataan ISO17065-standardissa) sertifiointi määritellään kolmannen osapuolen toteuttamaksi vahvistamiseksi, joka liittyy tuotteisiin, prosesseihin ja palveluihin.

16. Vahvistaminen tarkoittaa katselmusta seuraavan päätöksen perusteella tehtävää toteamusta, että määriteltyjen vaatimusten täyttäminen on osoitettu (kohta 5.2, ISO 17000:2004).

17. Yleisen tietosuoja-asetuksen 42 ja 43 artiklan mukaisen sertifioinnin yhteydessä sertifioinnilla tarkoitetaan kolmannen osapuolen toteuttamaa vahvistamista, joka liittyy rekisterinpitäjien ja henkilötietojen käsittelijöiden suorittamiin käsittelytoimiin.

1.3.2 Sertifiointimekanismit, sinetit ja merkit

18. Yleisessä tietosuoja-asetuksessa ei määritellä sertifiointimekanismeja, sinettejä ja merkkejä vaan näistä termeistä käytetään yhteisnimitystä. Sertifikaatti on todistus asetuksen noudattamisesta. Sinettiä tai merkkiä voidaan käyttää osoituksena siitä, että sertifiointimenettely on saatettu hyväksytysti päätökseen. Sinetti tai merkki tarkoittaa yleensä logoa tai symbolia, joka osoittaa (sertifikaatin lisäksi), että sertifioinnin kohde on arvioitu riippumattomasti sertifiointimenettelyssä ja että kohde täyttää tietyt normatiivisissa asiakirjoissa, kuten asetuksissa, standardeissa tai teknisissä eritelmissä, esitetyt vaatimukset. Nämä yleiseen tietosuoja-asetukseen liittyvät sertifiointia koskevat vaatimukset on esitetty lisävaatimuksina, jotka täydentävät EN-ISO/IEC 17065/2012 -standardin sisältämiä sertifiointielinten akkreditointisääntöjä ja toimivaltaisen valvontaviranomaisen tai tietosuojaneuvoston hyväksymiä sertifiointikriteerejä. Asetuksen mukainen sertifikaatti, sinetti tai merkki voidaan myöntää vain sillä perusteella, että akkreditoitu sertifiointielin tai toimivaltainen valvontaviranomainen on toteuttanut näytön riippumattoman arvioinnin ja vahvistanut sertifiointikriteerien täyttymisen.

19. Seuraavassa taulukossa esitetään yleisluonteinen esimerkki sertifiointiprosessista.

Rekisterinpitäjä tai henkilötietojen käsittelijä jättää hakemuksen	**Sertifiointielin tekee muodollisen tarkastuksen**	**Arviointi** **Ennakkoarviointi**	**Arviointi** **Arvioinnin kohteen arviointi**	**Arviointi** **Tulosten validointi**	**Tiedot toimivaltaiselle valvontaviranomaiselle**	**Sertifiointi**	**Seuranta**	**Sertifioinnin uusiminen**
Onko arvioinnin kohteen kuvaus yksiselitteinen ja täydellinen myös rajapintojen osalta?	Voidaanko arvioinnin kohteen kuvaus hyväksyä?	Mitä kriteerejä sovelletaan?	Täyttääkö arvioinnin kohde kriteerit?	Onko eritelty kaikki arvioinnin kohteen osalta olennaiset kriteerit?	Onko esitetty perustelut sertifioinnin myöntämiselle tai peruuttamiselle?	Voidaanko sertifikaatti myöntää?	Täyttääkö arvioinnin kohde edelleen kriteerit?	Täyttääkö käsittely edelleen sertifiointikriteerit?
Voidaanko myöntää pääsy arvioinnin kohteen käsittelytoimiin?	Ovatko kaikki asiakirjat täydellisiä ja ajan tasalla?	Mitä arviointimenetelmiä sovelletaan?	Onko arvioinnin kohteen dokumentointi asianmukaista?	Onko arviointi dokumentoitu riittävän hyvin?		Ovatko raportit valmiita julkaistavaksi?	Käytetäänkö sertifikaattia/ sinettiä/ luotettavuusmerkintää asianmukaisesti?	Onko kehittämistä vaativilla osa-alueilla ryhdytty riittäviin toimiin?
42 artiklan 6 kohta	43 artiklan 4 kohta	43 artiklan 4 kohta	42 artiklan 5 kohta, 43 artiklan 4 kohta	43 artiklan 4 kohta	43 artiklan 1 kohta, 43 artiklan 5 kohta	43 artiklan 1 kohta, 42 artiklan 7 kohta	42 artiklan 7 kohta	42 artiklan 7 kohta

2 VALVONTAVIRANOMAISTEN TEHTÄVÄ

20. Yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaan sertifioinnin myöntää akkreditoitu sertifiointielin tai toimivaltainen valvontaviranomainen. Asetuksessa ei säädetä, että sertifioinnin myöntäminen olisi toimivaltaisten valvontaviranomaisten pakollinen tehtävä. Sen sijaan asetus mahdollistaa useita eri toimintamalleja. Valvontaviranomainen voi esimerkiksi valita yhden tai useamman seuraavista vaihtoehdoista:

    - myöntää sertifioinnin itse oman sertifiointimallinsa mukaisesti
    - myöntää sertifioinnin itse oman sertifiointimallinsa mukaisesti mutta delegoida arviointiprosessin kokonaan tai osittain kolmansille osapuolille
    - luoda oman sertifiointimallin ja antaa sertifiointimenettelyn tehtäväksi sertifiointielimille, jotka myöntävät sertifioinnin
    - kannustaa markkinoita kehittämään sertifiointimekanismeja.

21. Valvontaviranomaisen on myös harkittava tehtäväänsä kansallisella tasolla tehtyjen akkreditointimekanismeja koskevien päätösten valossa – erityisesti silloin, jos valvontaviranomaisella itsellään on valtuudet akkreditoida sertifiointielimiä yleisen tietosuoja-asetuksen 43 artiklan 1 kohdan mukaisesti. Näin ollen kukin valvontaviranomainen päättää itse, mitä lähestymistapaa se soveltaa sertifioinnin asetuksen mukaisen laajan tarkoituksen toteuttamiseksi. Tästä päätetään 57 ja 58 artiklan mukaisten tehtävien ja valtuuksien yhteydessä ja lisäksi silloin, kun sertifioinnin katsotaan olevan tekijä, joka on otettava huomioon määrättäessä hallinnollisia sakkoja ja yleisemmin keinona osoittaa, että asetusta on noudatettu.

2.1 Valvontaviranomainen sertifiointielimenä

22. Kun valvontaviranomainen päättää toteuttaa sertifioinnin, sen on arvioitava perusteellisesti omaa asemaansa sille yleisen tietosuoja-asetuksen mukaisesti osoitettujen tehtävien suhteen. Sen on toimittava tehtäviensä suorittamisessa läpinäkyvästi. Sen on myös otettava huomioon erityisesti tutkimuksiin ja täytäntöönpanoon liittyvien valtuuksien erottaminen toisistaan, jotta vältetään mahdolliset eturistiriidat.

23. Kun valvontaviranomainen toimii sertifiointielimenä, sen on varmistettava sertifiointimekanismin asianmukainen perustaminen ja laadittava omat tai mukautetut sertifiointikriteerit. Lisäksi jokaisen sertifiointeja myöntävän valvontaviranomaisen tehtävänä on suorittaa sertifiointien säännöllinen uudelleentarkastelu (57 artiklan 1 kohdan o alakohta) ja peruuttaa sertifioinnit silloin, kun sertifiointia koskevat vaatimukset eivät täyty tai eivät enää täyty (58 artiklan 2 kohdan h alakohta). Näiden vaatimusten täyttämiseksi kannattaa luoda sertifiointimenettely ja laatia prosessin vaatimukset. Jos esimerkiksi kansallisessa lainsäädännössä ei muuta säädetä, yksittäisen hakijaorganisaation kanssa kannattaa myös tehdä sertifiointitoimien tarjoamista koskeva oikeudellisesti täytäntöönpanokelpoinen sopimus. Lisäksi olisi varmistettava tarvittavat järjestelyt arviointien suorittamiseksi, kriteerien noudattamisen seuraamiseksi ja säännöllisen uudelleentarkastelun toteuttamiseksi. Viimeksi mainittuun kuuluvat tiedonsaanti ja/tai pääsy tiloihin, raporttien ja

tulosten dokumentointi ja julkaiseminen sekä valitusten tutkiminen. Valvontaviranomaisen odotetaan myös noudattavan sertifiointielinten akkreditointia koskevissa suuntaviivoissa esitettyjä vaatimuksia 43 artiklan 2 kohdan mukaisten vaatimusten lisäksi.

2.2 Valvontaviranomaisen muut sertifiointiin liittyvät tehtävät

24. Jäsenvaltioissa, joissa sertifiointielimet toimivat, valvontaviranomaisella on sen omista toimista riippumatta seuraavat valtuudet ja tehtävät:

    - sertifiointijärjestelmän kriteerien arviointi ja päätösehdotuksen laatiminen (42 artiklan 5 kohta)
    - päätösehdotuksen antaminen tiedoksi tietosuojaneuvostolle, jos se aikoo hyväksyä sertifiointikriteerit (64 artiklan 1 kohdan c alakohta ja 64 artiklan 7 kohta), ja tietosuojaneuvoston lausunnon ottaminen huomioon (64 artiklan 1 kohdan c alakohta ja 70 artiklan 1 kohdan t alakohta)
    - sertifiointikriteerien hyväksyminen (58 artiklan 3 kohdan f alakohta), ennen kuin akkreditointi ja sertifiointi voidaan toteuttaa (42 artiklan 5 kohta ja 43 artiklan 2 kohdan b alakohta)
    - sertifiointikriteerien julkistaminen (43 artiklan 6 kohta)
    - toimivaltaisena viranomaisena toimiminen EU:n laajuisissa sertifiointijärjestelmissä, mikä voi johtaa tietosuojaneuvoston hyväksymän eurooppalaisen tietosuojasinetin myöntämiseen (42 artiklan 5 kohta ja 70 artiklan 1 kohdan o alakohta)
    - sertifiointielimen määrääminen a) kieltämään sertifioinnin antaminen tai b) peruuttamaan sertifiointi, jos sertifioinnin vaatimukset (sertifiointimenettelyt tai -kriteerit) eivät täyty tai eivät enää täyty (58 artiklan 2 kohdan h alakohta).

25. Yleisessä tietosuoja-asetuksessa annetaan valvontaviranomaisen tehtäväksi hyväksyä sertifiointikriteerit mutta ei laatia kriteerejä. Sertifiointikriteerien hyväksymiseksi 42 artiklan 5 kohdan mukaisesti valvontaviranomaisella pitäisi olla selvä käsitys siitä, mitä on odotettavissa. Tämä koskee erityisesti asetuksen noudattamisen osoittamiseksi tarvittavaa laajuutta ja sisältöä sekä valvontaviranomaisen asetuksen soveltamisen seurantaan ja täytäntöönpanoon liittyviä tehtäviä. Liitteessä esitetään suuntaviivat, joilla varmistetaan yhdenmukaisen lähestymistavan soveltaminen arvioitaessa hyväksyttäviä kriteerejä.

26. Yleisen tietosuoja-asetuksen 43 artiklan 1 kohdassa edellytetään, että ennen sertifioinnin myöntämistä tai uusimista sertifiointielimet tiedottavat siitä valvontaviranomaiselleen, jotta toimivaltainen valvontaviranomainen voi käyttää korjaavia toimivaltuuksiaan 58 artiklan 2 kohdan h alakohdan mukaisesti. Lisäksi asetuksen 43 artiklan 5 kohdassa edellytetään, että sertifiointielimet ilmoittavat toimivaltaiselle valvontaviranomaiselle syyt pyydetyn sertifioinnin myöntämiseen tai peruuttamiseen. Vaikka asetuksen mukaan valvontaviranomaiset voivat päättää, miten nämä tiedot vastaanotetaan, miten niiden vastaanottamisesta ilmoitetaan ja miten niitä tarkastellaan uudelleen ja käsitellään operatiivisesti (tähän voisi kuulua esimerkiksi sertifiointielinten raportoinnin mahdollistavat

tekniset ratkaisut), tietojen käsittelyä sekä sertifiointielimen kustakin onnistuneesta sertifiointihankkeesta antamia raportteja koskevat prosessit ja kriteerit voidaan toteuttaa asetuksen 43 artiklan 1 kohdan mukaisesti. Valvontaviranomainen voi näiden tietojen perusteella käyttää valtuuttaan määrätä sertifiointielin peruuttamaan sertifiointi tai kieltää antamasta sitä (58 artiklan 2 kohdan h alakohta) sekä seurata sertifiointia koskevien vaatimusten ja kriteerien soveltamista ja panna ne täytäntöön asetuksen (57 artiklan 1 kohdan a alakohta ja 58 artiklan 2 kohdan h alakohta) mukaisesti. Tämä tukee eri sertifiointielinten tekemien sertifiointien yhdenmukaistettua lähestymistapaa ja vertailukelpoisuutta ja sitä, että organisaation sertifiointitilanne on valvontaviranomaisten tiedossa.

3 SERTIFIOINTIELIMEN TEHTÄVÄ

27. Sertifiointielimen tehtävänä on myöntää, tarkastella uudelleen, uusia ja peruuttaa sertifiointeja (42 artiklan 5 ja 7 kohta) sertifiointimekanismin ja hyväksyttyjen kriteerien perusteella (43 artiklan 1 kohta). Tämä edellyttää sitä, että sertifiointielin tai sertifiointijärjestelmän omistaja määrittelee ja laatii sertifiointikriteerit ja sertifiointimenettelyt, mukaan lukien noudattamisen seuraamista, uudelleentarkastelua, valitusten käsittelyä ja peruuttamista koskevat menettelyt. Sertifiointikriteerejä tarkastellaan uudelleen osana akkreditointiprosessia, johon liittyvät sertifiointien, sinettien ja merkkien myöntämistä koskevat säännöt ja menettelyt (43 artiklan 2 kohdan c alakohta).

28. Sertifiointimekanismi ja sertifiointikriteerit ovat välttämättömiä, jotta sertifiointielin voidaan akkreditoida 43 artiklan mukaisesti. Sertifiointielimen toimintaan vaikuttavat huomattavasti sertifiointikriteerien soveltamisala ja tyyppi, koska ne vaikuttavat sertifiointimenettelyihin ja päinvastoin. Tietyt kriteerit voivat esimerkiksi edellyttää tiettyjä arviointimenetelmiä, kuten paikalla tehtäviä tarkastuksia ja käytännesääntöjen uudelleentarkastelua. Nämä menettelyt ovat akkreditoinnissa pakollisia, ja niitä kuvataan tarkemmin akkreditointia koskevissa suuntaviivoissa.

29. Yleisessä tietosuoja-asetuksessa edellytetään, että sertifiointielin toimittaa valvontaviranomaisille tietoja erityisesti yksittäisistä sertifioinneista, mikä on sertifiointimekanismin soveltamisen seurannan kannalta välttämätöntä (42 artiklan 7 kohta, 43 artiklan 5 kohta ja 58 artiklan 2 kohdan h alakohta).

4 SERTIFIOINTIKRITEERIEN HYVÄKSYMINEN

30. Sertifiointikriteerit ovat sertifiointimekanismien olennainen osa. Siksi yleisessä tietosuoja-asetuksessa edellytetään, että toimivaltainen valvontaviranomainen hyväksyy sertifiointimekanismin sertifiointikriteerit (42 artiklan 5 kohta ja 43 artiklan 2 kohdan b alakohta). Eurooppalaisen tietosuojasinetin tapauksessa sertifiointikriteerit hyväksyy tietosuojaneuvosto (42 artiklan 5 kohta ja 70 artiklan 1 kohdan o alakohta). Jäljempänä esitellään kumpikin sertifiointikriteerien hyväksymistapa.

31. Tietosuojaneuvoston mukaan sertifiointikriteerit voidaan hyväksyä seuraavista syistä:

- ne vastaavat asianmukaisesti luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä koskevia vaatimuksia ja periaatteita, jotka on vahvistettu asetuksessa (EU) 2016/679
- ne edistävät yleisen tietosuoja-asetuksen johdonmukaista soveltamista.

32. Sertifiointikriteerit hyväksytään, jos ne vastaavat täysin yleiseen tietosuoja-asetukseen sisältyvää vaatimusta siitä, että rekisterinpitäjät ja henkilötietojen käsittelijät voivat sertifiointimekanismin avulla osoittaa asetuksen noudattamisen.

4.1 Toimivaltainen valvontaviranomainen hyväksyy kriteerit

33. Toimivaltaisen valvontaviranomaisen on hyväksyttävä sertifiointikriteerit ennen sertifiointielimen akkreditointiprosessia tai sen aikana. Saman sertifiointielimen ISO 17065 -standardin mukaiset päivitetyt tai täydennetyt järjestelmät tai kriteerit on myös hyväksyttävä ennen täydennettyjen sertifiointimekanismien käyttämistä (42 artiklan 5 kohta ja 43 artiklan 2 kohdan b alakohta). Valvontaviranomaisten on käsiteltävä kaikkia sertifiointikriteerien hyväksymistä koskevia pyyntöjä oikeudenmukaisesti ja syrjimättömästi noudattaen julkisesti käytettävissä olevaa menettelyä, jossa määritellään täytettävät yleiset edellytykset ja hyväksyntäprosessin kuvaus.

34. Sertifiointielin voi myöntää sertifioinnin tietyssä jäsenvaltiossa vain kyseisen jäsenvaltion valvontaviranomaisen hyväksymien kriteerien mukaisesti. Toisin sanoen toimivaltaisen valvontaviranomaisen on hyväksyttävä sertifiointikriteerit, silloin kun sertifiointielimen tarkoituksena on tarjota sertifiointeja ja se saa akkreditoinnin. Euroopan laajuisia sertifiointijärjestelmiä käsitellään seuraavassa kohdassa.

4.2 Tietosuojaneuvosto hyväksyy eurooppalaisen tietosuojasinetin kriteerit

35. Sertifiointielin voi myöntää sertifioinnin myös tietosuojaneuvoston eurooppalaiselle tietosuojasinetille hyväksymien kriteerien mukaisesti. Eurooppalainen tietosuojasinetti voidaan tehdä tietosuojaneuvoston 63 artiklan nojalla hyväksymien sertifiointikriteerien perusteella (42 artiklan 5 kohta). Koska on jo olemassa erilaisia sertifiointi- ja akkreditointikäytäntöjä, tietosuojaneuvoston mielestä on toivottavaa, että pyritään välttämään tietosuojan sertifiointimarkkinoiden hajanaisuutta. Tietosuojaneuvosto toteaa, että 42 artiklan 1 kohdan mukaan jäsenvaltiot, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön sertifiointimekanismeja erityisesti unionin tasolla.

4.2.1 Hyväksynnän hakeminen

36. Kriteerien hyväksymistä 42 artiklan 5 kohdan ja 70 artiklan 1 kohdan o alakohdan mukaisesti koskeva hakemus tietosuojaneuvostolle on toimitettava toimivaltaisen valvontaviranomaisen kautta ja siinä on todettava, että järjestelmän omistaja, ehdokas tai akkreditoitu sertifiointielin aikoo tarjota kriteerit rekisterinpitäjiä ja henkilötietojen käsittelijöitä

koskevassa sertifiointimekanismissa kaikissa jäsenvaltioissa. Toimivaltainen valvontaviranomainen toimittaa tietosuojaneuvostolle luonnoksen, kun se katsoo, että tietosuojaneuvosto voisi hyväksyä kriteerit.

37. Paikka, johon kriteerien hyväksymistä koskeva hakemus toimitetaan, valitaan sertifiointijärjestelmän omistajien tai sertifiointielinten päätoimipaikan perusteella.

38. Jos hakemuksen toimittaa sertifiointielin, se tavallisesti hakee akkreditointia tai sen jäsenvaltion toimivaltainen valvontaviranomainen tai kansallinen akkreditointielin on jo akkreditoinut sen. Jos sertifiointielin on jo akkreditoitu yleisen tietosuoja-asetuksen mukaista sertifiointimekanismia varten, se saattaa osaltaan sujuvoittaa hyväksymisprosessia.

4.2.2 Eurooppalaisen tietosuojasinetin kriteerit

39. Tietosuojaneuvosto koordinoi arviointiprosessia ja hyväksyy vaaditulla tavalla eurooppalaisen tietosuojasinetin kriteerit. Arviointi koskee muun muassa seuraavia osa-alueita: kriteerien soveltamisalaa ja valmiutta toimia yhteisenä sertifiointina. Kun tietosuojaneuvosto on hyväksynyt kriteerit, sertifiointielimen EU:n päätoimipaikan toimivaltaisen valvontaviranomaisen odotetaan käsittelevän itse mekanismia koskevat valitukset ja ilmoittavan niistä muille valvontaviranomaisille. Valvontaviranomaisella on myös toimivalta toteuttaa sertifiointielimeen kohdistuvia toimenpiteitä. Toimivaltainen valvontaviranomainen voi tapauksen mukaan tiedottaa niistä muille valvontaviranomaisille ja tietosuojaneuvostolle.

40. Yhteistä sertifiointia koskevia sertifiointikriteerejä tarvitaan EU:n laajuisesti, ja tähän tarpeeseen olisi vastattava tarjoamalla siihen tarkoitettu mekanismi. Eurooppalaisten sertifiointimekanismien täytyy olla tarkoitettuja käytettäväksi kaikissa jäsenvaltioissa. Eurooppalaisen tietosuojasinetin mekanismin sekä sen kriteerien on 42 artiklan 5 kohdan perusteella oltava mukautettavissa niin, että niissä otetaan tarvittaessa huomioon kansalliset alakohtaiset säännökset, jotka voivat koskea esimerkiksi tietojenkäsittelyä kouluissa, ja niitä on voitava soveltaa Euroopan laajuisesti.

41. Esimerkki: Kansainvälinen koulu, jossa tarjotaan opetusta rekisteröidyille unionissa, sijaitsee jäsenvaltiossa ”A”. Koulu haluaa sertifioida verkkohakuprosessinsa EU:n laajuisen sertifiointijärjestelmän avulla saadakseen eurooppalaisen tietosuojasinetin. Koulun tavoitteena on hakea käsittelytoimien sertifiointia jäsenvaltioon ”B” sijoittautuneelta sertifiointielimeltä eurooppalaisen tietosuojasinetin perusteella. Asiaankuuluvassa mekanismissa suunnitelluissa ja dokumentoiduissa sinetin kriteereissä on voitava ottaa huomioon jäsenvaltiossa ”A” kouluihin sovellettavat säännökset. Kriteereissä olisi myös vaadittava, että koulun verkkohakuprosessissa annetaan tietoja jäsenvaltion sovellettavista tietosuojavaatimuksista, jotka saattavat poiketa muiden jäsenvaltioiden vastaavista vaatimuksista, ja otetaan ne huomioon. Esimerkkejä tästä ovat se, että hakua varten toimitetaan henkilötietojen sarjoja, kuten esikoulussa annettuja arvosanoja tai koetuloksia, erilaiset säilytysajat, taloutta koskevien tai biometristen tietojen kerääminen tai käsittely ja jatkokäsittelyn rajoitukset.

- Eurooppalaisen tietosuojasinetin mekanismin korkean tason kriteerejä ovat muun muassa

- tietosuojaneuvoston hyväksymät kriteerit
- soveltaminen kaikilla lainkäyttöalueilla tarvittaessa kansallisen lainsäädännön vaatimusten ja alakohtaisten säännösten mukaisesti
-

- yhdenmukaistetut kriteerit, joita voidaan mukauttaa vastaamaan kansallisia vaatimuksia
  - sertifiointimekanismin kuvaus, jossa määritellään
  - sertifiointijärjestelyt ja tunnustetaan yleiseurooppalaiset vaatimukset
  - menettelyt ratkaisujen varmistamiseksi ja tarjoamiseksi kansallisille muunnelmille sekä sen varmistamiseksi, että sinetti auttaa osoittamaan yleisen tietosuoja-asetuksen noudattamisen
  - kaikille asiaankuuluville valvontaviranomaisille tarkoitettujen raporttien kieli.

42. Eurooppalaisen tietosuojasinetin kriteerejä koskevia neuvoja on myös liitteessä.

4.2.3 Akkreditoinnin tehtävä

43. Kuten kohdassa 4.2.1 kerrottiin, jos kriteerien on todettu soveltuvan yhteiseen sertifiointiin ja tietosuojaneuvosto on hyväksynyt ne sellaisiksi 42 artiklan 5 kohdan mukaisesti, sertifiointielimet voidaan akkreditoida suorittamaan sertifiointi näiden kriteerien mukaisesti unionin tasolla.

44. Järjestelmät, jotka on tarkoitettu tarjottavaksi vain tietyissä jäsenvaltioissa, eivät ole mahdollisia EU:n sinetin hakijoita. Akkreditointi eurooppalaisen tietosuojasinetin soveltamisalalle edellyttää akkreditointia siinä jäsenvaltiossa, jossa sijaitsee sen sertifiointielimen päätoimipaikka, joka aikoo käyttää järjestelmää eli joka vastaa sertifiointien myöntämisestä ja johtaa yksiköidensä ja tytäryhtiöidensä sertifiointitoimia muissa jäsenvaltioissa. Jos muut toimipaikat tai toimistot johtavat tai suorittavat sertifiointeja itsenäisesti, kukin näistä toimipaikoista ja toimistoista tarvitsee erillisen akkreditoinnin jäsenvaltiossa, johon ne ovat sijoittautuneet. Toisin sanoen akkreditointi tarvitaan vain siinä jäsenvaltiossa, jossa sertifiointielimen päätoimipaikka sijaitsee, jos vain päätoimipaikka myöntää sertifiointeja. Jos sen sijaan sertifiointielimen muut toimipaikat myöntävät myös sertifiointeja, nämä toimipaikat on myös akkreditoitava.

45. Näin ollen jos sertifiointielintä ei ole akkreditoitu suorittamaan sertifiointia eurooppalaisen tietosuojasinetin mukaisesti, tietosuojaneuvoston hyväksymiä kriteerejä ei voida käyttää eikä sinettiä voida tarjota.

5 SERTIFIOINTIKRITEERIEN LAATIMINEN

46. Yleisessä tietosuoja-asetuksessa vahvistettiin kehys sertifiointikriteerien laatimiselle. Sertifiointimenettelyä koskevia perusvaatimuksia käsitellään 42 ja 43 artiklassa, mutta sertifiointimenettelyjen kannalta olennaisten kriteerien määrittelemiseksi sertifiointikriteerien on perustuttava myös yleisen tietosuoja-asetuksen periaatteisiin ja sääntöihin ja niiden on autettava antamaan varmuus siitä, että ne täyttyvät.

47. Sertifiointikriteerien laatimisessa painopisteen olisi oltava niiden todennettavuudessa, merkitsevyydessä ja soveltuvuudessa asetuksen noudattamisen osoittamiseen. Sertifiointikriteerit olisi muotoiltava niin, että ne ovat selviä ja ymmärrettäviä ja että niitä voidaan soveltaa käytännössä.

48. Sertifiointikriteerien laadinnassa on otettava huomioon muun muassa seuraavat asetuksen noudattamisen näkökohdat, jotka tukevat tarvittaessa käsittelytoimien arviointia:

    - käsittelyn lainmukaisuus 6 artiklan mukaisesti
    - tietojen käsittelyä koskevat periaatteet 5 artiklan mukaisesti
    - rekisteröityjen 12–23 artiklan mukaiset oikeudet
    - velvollisuus ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle 33 artiklan mukaisesti
    - sisäänrakennetun ja oletusarvoisen tietosuojan velvoite 25 artiklan mukaisesti
    - onko 35 artiklan 7 kohdan d alakohdan mukainen tietosuojaa koskeva vaikutustenarviointi tehty tarvittaessa
    - onko 32 artiklan mukaiset asianmukaiset tekniset ja organisatoriset toimenpiteet toteutettu.

49. Se, miten laajasti nämä seikat näkyvät kriteereissä, voi vaihdella sertifioinnin soveltamisalan mukaan. Siihen voivat kuulua käsittelytoimien tyyppi ja sertifioinnin kohteen ala (esim. terveysala).

5.1 Mitä voidaan sertifioida yleisen tietosuoja-asetuksen mukaisesti?

50. Tietosuojaneuvosto katsoo, että sertifioinnin yleisen tietosuoja-asetuksen mukainen soveltamisala on laaja niin kauan kuin painopiste on siinä, että rekisterinpitäjiä ja henkilötietojen käsittelijöitä autetaan osoittamaan asetuksen noudattaminen käsittelytoimissa (42 artiklan 1 kohta).

51. Kun arvioidaan käsittelytoimea, on otettava soveltuvin osin huomioon kolme keskeistä osatekijää:

    1. henkilötiedot (asetuksen aineellinen soveltamisala)

2. tekniset järjestelmät – infrastruktuuri, kuten laitteet ja ohjelmistot, joita käytetään henkilötietojen käsittelyyn sekä

3. käsittelytoimiin liittyvät prosessit ja menettelyt.

52. Jokainen käsittelytoimissa käytettävä osatekijä on arvioitava määriteltyjen kriteerien mukaan. Vaikutusta voi olla ainakin neljällä merkittävällä tekijällä: 1) rekisterinpitäjän tai henkilötietojen käsittelijän organisaatiolla ja oikeudellisella rakenteella, 2) osastolla, ympäristöllä ja käsittelytoimiin osallistuvilla ihmisillä, 3) arvioitavien osien teknisellä kuvauksella ja 4) käsittelytoimia tukevalla IT-infrastruktuurilla, kuten käyttöjärjestelmillä, virtuaalijärjestelmillä, tietokannoilla, todentamis- ja valtuutusjärjestelmillä, reitittimillä ja palomuureilla, tallennusjärjestelmillä, viestintäinfrastruktuurilla tai internetyhteydellä ja niihin liittyvillä teknisillä toimenpiteillä.

53. Kaikki kolme keskeistä osatekijää ovat sertifiointimenettelyjen ja -kriteerien suunnittelun kannalta olennaisia. Niiden käytön laajuus voi vaihdella sertifioinnin kohteen mukaan. Esimerkiksi joissakin tapauksissa jotkin osatekijät voidaan jättää huomiotta, jos arvioidaan, että ne eivät ole sertifioinnin kohteen kannalta olennaisia.

54. Yleisessä tietosuoja-asetuksessa annetaan lisäohjeita siitä, miten voidaan määritellä tarkemmin, mitä yleisen tietosuoja-asetuksen mukaan voidaan sertifioida. Asetuksen 42 artiklan 7 kohdasta seuraa, että asetuksen mukaisia sertifiointeja myönnetään vain rekisterinpitäjille tai henkilötietojen käsittelijöille. Näin ollen niiden ulkopuolelle jää esimerkiksi tietosuojavastaavien sertifiointi. Asetuksen 43 artiklan 1 kohdan b alakohdassa viitataan ISO 17065 -standardiin, jolla mahdollistetaan tuotteiden, palveluiden ja prosessien vaatimustenmukaisuutta arvioivien sertifiointielinten akkreditointi. Käsittelytoimen tai toimien sarjan tuloksena voi olla ISO 17065 -standardin terminologian mukainen tuote tai palvelu, joka voidaan sertifioida. Esimerkiksi työntekijöitä koskevien tietojen käsittely palkanmaksua tai lomien hallinnointia varten koostuu asetuksessa tarkoitetussa merkityksessä toimien sarjasta ja sen tuloksena voi olla ISO-terminologian mukainen tuote, prosessi tai palvelu.

55. Näiden seikkojen perusteella tietosuojaneuvosto katsoo, että yleisen tietosuoja-asetuksen mukaisen sertifioinnin soveltamisala kattaa käsittelytoimet tai toimien sarjat. Ne voivat muodostua organisatoristen toimenpiteiden kaltaisista hallintoprosesseista, jotka ovat siten käsittelytoimen olennaisia osia (esim. hallintoprosessi, joka perustetaan valitusten käsittelyä varten osana palkanmaksuun tarvittavaa työntekijöiden tietojen käsittelyä).

56. Jotta voidaan arvioida, täyttääkö käsittelytoimi sertifiointikriteerit, on tarkasteltava jotain käyttötilannetta. Esimerkiksi se, onko jonkin teknisen infrastruktuurin käyttö käsittelytoimessa kriteerien mukaista, riippuu siitä, minkä luokan tietojen käsittelyyn se on suunniteltu. Organisatoriset toimenpiteet ovat sidoksissa tietojen luokkiin ja määriin sekä käsittelyssä käytettyyn tekniseen infrastruktuuriin ottaen huomioon käsittelyn luonne, laajuus, sisältö ja tarkoitukset sekä rekisteröityjen oikeuksia ja vapauksia koskevat riskit.

57. Lisäksi on muistettava, että IT-sovellukset voivat vaihdella paljon, vaikka niillä olisi samat käsittelytarkoitukset. Siksi tämä on otettava huomioon sertifiointimekanismien soveltamisalan määrittelyssä ja sertifiointikriteerien laatimisessa. Sertifioinnin soveltamisalan

ja kriteerien ei siis pitäisi olla niin suppeita, että ei voitaisi käyttää eri tavalla suunniteltuja IT-sovelluksia.

5.2 Sertifioinnin kohteen määrittely

58. Sertifiointimekanismin soveltamisala on sertifiointimekanismin alaisissa yksittäisissä sertifiointihankkeissa erotettava arvioinnin kohteesta. Sertifiointimekanismissa voidaan määritellä soveltamisala joko yleisesti tai suhteessa tiettyyn käsittelytoimien tyyppiin tai alaan. Näin voidaan määritellä, mitkä sertifioinnin kohteet kuuluvat sertifiointimekanismin soveltamisalaan (esimerkiksi digitaalisen kassaholvin sisältämien henkilötietojen turvallinen säilytys ja suojelu). Joka tapauksessa asetuksen noudattamisen luotettava, mielekäs arviointi voidaan tehdä vain, jos sertifiointihankkeen yksittäinen kohde kuvaillaan tarkasti. On kuvailtava selvästi, mitä käsittelytoimia sertifioinnin kohde sisältää, sekä se, mitä perusosatekijöitä eli tietoja, prosesseja ja teknistä infrastruktuuria arvioidaan ja mitä ei. Tässä yhteydessä on aina otettava huomioon ja kuvailtava myös rajapinnat muihin prosesseihin. Selvää on, että tuntematonta ei voida arvioida eikä näin ollen myöskään sertifioida. Joka tapauksessa yksittäisen sertifioinnin kohteen on oltava mielekäs sertifioinnista välitetyn viestin tai siinä taikka siitä esitetyn väittämän suhteen eikä se saisi johtaa käyttäjää, asiakasta tai kuluttajaa harhaan.

59. [Esimerkki 1]

Pankki tarjoaa asiakkailleen sivuston verkkopankin käyttöä varten. Tässä palvelussa voi tehdä tilisiirtoja, ostaa osakkeita, antaa pysyväistoimeksiantoja ja hallinnoida tilejä. Pankki haluaa sertifioida yleisiin kriteereihin perustuvan ja yleiseen soveltamisalaan kuuluvan tietosuojan sertifiointimekanismin mukaisesti seuraavat:

a) Turvallinen sisäänkirjautuminen

Turvallinen sisäänkirjautuminen on käsittelytoimi, joka on loppukäyttäjän kannalta ymmärrettävä ja tietosuojan näkökulmasta olennainen, koska sillä on suuri merkitys asiaan liittyvien henkilötietojen turvallisuuden varmistamisessa. Tämä käsittelytoimi on välttämätön turvallisen sisäänkirjautumisen varmistamiseksi ja voi siten olla mielekäs arvioinnin kohde, jos sertifikaatissa ilmaistaan selvästi, että vain sisäänkirjautumisen käsittelytoimi on sertifioitu.

b) Verkon edustaohjelma

Verkon edustaohjelma (front-end) voi olla tietosuojan näkökulmasta olennainen, mutta se ei ole loppukäyttäjälle ymmärrettävä eikä siksi mielekäs arvioinnin kohde. Lisäksi käyttäjälle ei ole selvää, mitkä verkkosivuston palvelut ja siten käsittelytoimet sertifiointi käsittää.

c) Verkkopankkitoiminta

Verkon edustaohjelma (front-end) ja taustaohjelma (back-end) ovat verkkopankkipalvelun käsittelytoimia, jotka voivat olla käyttäjän kannalta mielekkäitä. Tässä yhteydessä kumpikin on sisällytettävä arvioinnin kohteeseen.

Käsittelytoimet, jotka eivät liity suoraan verkkopankkipalvelun tarjoamiseen, kuten rahanpesun ehkäisemiseksi suoritettavat käsittelytoimet, voidaan jättää arvioinnin kohteen ulkopuolelle.

Pankin sivustonsa kautta tarjoamat verkkopankkipalvelut voivat kuitenkin myös sisältää muita palveluja, jotka puolestaan vaativat omat käsittelytoimensa. Tässä yhteydessä muihin palveluihin voi kuulua esimerkiksi vakuutustuotteen tarjoaminen. Koska tämä lisäpalvelu ei liity suoraan verkkopankkipalvelujen tarjoamiseen, se voidaan jättää arvioinnin kohteen ulkopuolelle. Jos lisäpalvelu (vakuutus) jätetään arvioinnin kohteen ulkopuolelle, sivustoon integroidut tämän palvelun liittymät ovat osa arvioinnin kohdetta ja siksi ne on kuvailtava, jotta palvelut voitaisiin erottaa selvästi toisistaan. Tällainen kuvaus on välttämätön mahdollisten kahden palvelun välisten tiedonsiirtojen tunnistamiseksi ja arvioimiseksi.

60. [Esimerkki 2]

    Pankki tarjoaa asiakkailleen palvelua, jonka avulla he voivat kerätä eri tileihin ja luottokortteihin liittyviä tietoja eri pankeista (tilien yhdistelmä). Pankki haluaa sertifioida palvelunsa yleisen tietosuoja-asetuksen mukaisesti. Toimivaltainen valvontaviranomainen on hyväksynyt tietyt sertifiointikriteerit, jotka koskevat tämän tyyppistä toimintaa. Sertifiointimekanismin soveltamisalaan kuuluvat vain seuraavat asetuksen noudattamiseen liittyvät näkökohdat:

    - käyttäjän todentaminen sekä
    - hyväksyttävät tavat hankkia yhdistettäviä tietoja muilta pankeilta tai muista palveluista.

    Koska tämän sertifiointimekanismin soveltamisala määrää arvioinnin kohteen, ei ole mahdollista mielekkäästi kaventaa arvioinnin kohdetta ehdotetun soveltamisalan mukaiseksi ja sertifioida vain tietyt ominaisuudet tai yksittäinen käsittelytoimi. Tässä skenaariossa arvioinnin kohteen on vastattava tiettyä soveltamisalaa.

5.3 Arviointimenetelmät ja -metodologiat

61. Arviointi, joka auttaa osoittamaan, että käsittelytoimissa noudatetaan asetusta, edellyttää arviointimenetelmien ja -metodologioiden tunnistamista ja määrittelyä. Sillä, onko arvioitavat tiedot kerätty vain dokumentaatiosta (joka ei yksinään riitä) vai onko ne kerätty aktiivisesti paikalla ja suoraan tai välillisesti, on merkitystä. Se, millä tavalla tiedot kerätään, vaikuttaa sertifioinnin merkittävyyteen ja olisi siksi määriteltävä ja kuvailtava.

    Sertifiointien myöntämistä koskeviin menettelyihin ja säännölliseen uudelleentarkasteluun pitäisi sisältyä eritelmät, joiden mukaan määritellään arvioinnin tarkoituksenmukainen taso (perusteellisuus ja yksityiskohtaisuus), jotta sertifiointikriteerit täyttyvät. Lisäksi niihin pitäisi sisältyä seuraavat asiat:

    - tiedot ja erittelyt esimerkiksi sovelletuista arviointimenetelmistä ja paikalla tehtävien tarkastusten aikana tai dokumentaatiosta tehdyistä havainnoista

- arviointimenetelmät, jotka koskevat käsittelytoimia (tiedot, järjestelmät ja prosessit), sekä käsittelyn tarkoitus
- tietoluokkien, suojelutarpeiden sekä sen määrittely, osallistuuko sertifiointiin henkilötietojen käsittelijöitä tai kolmansia osapuolia
- tehtävien määrittely ja tehtävien ja vastuiden mukaisesti määritellyn pääsynvalvontamekanismin olemassaolo.

62. Arvioinnin perusteellisuus vaikuttaa sertifioinnin merkittävyyteen ja arvoon. Jos arviointi on vähemmän perusteellinen käytännön syistä tai kustannusten vähentämiseksi, tietosuojan sertifioinnin merkittävyys vähenee. Toisaalta arvioinnin yksityiskohtaisuutta koskevat päätökset voivat ylittää hakijan taloudelliset resurssit ja usein myös arvioijien ja tarkastajien resurssit. Asetuksen noudattamisen osoittamista varten ei välttämättä aina ole ratkaisevaa tehdä hyvin yksityiskohtaista analyysiä IT-järjestelmistä, jotta sertifiointi olisi vielä merkittävä.

5.4 Arvioinnin dokumentointi

63. Sertifiointi olisi dokumentoitava perusteellisesti ja kattavasti. Dokumentaation puute tarkoittaa, että asianmukaista arviointia ei voida tehdä. Sertifioinnin dokumentaation olennainen tehtävä on, että sillä varmistetaan sertifiointimekanismin mukaisen arviointiprosessin läpinäkyvyys. Dokumentaatio antaa vastauksia kysymyksiin, jotka koskevat lainsäädännön vaatimuksia. Sertifiointimekanismissa pitäisi varmistaa standardoitujen dokumentointimenetelmien käyttö. Sen jälkeen arviointi mahdollistaa sertifioinnin dokumentaation vertailun todellisen tilanteen kanssa ja sertifiointikriteerien perusteella.

64. Sertifioinnin kohteen ja menetelmän kattava dokumentaatio lisää läpinäkyvyyttä. Asetuksen 43 artiklan 2 kohdan c alakohdan mukaan sertifiointimekanismeissa pitäisi vahvistaa menettelyjä, jotka mahdollistavat sertifiointien tarkastelun. Jotta valvontaviranomainen voi arvioida, voidaanko sertifiointi tunnustaa muodollisissa tutkimuksissa ja miten laajasti se voidaan tehdä, tarkoituksenmukaisin viestintäkeino voi olla yksityiskohtainen dokumentaatio. Siksi arvioinnin aikana laaditussa dokumentaatiossa pitäisi keskittyä kolmeen tärkeimpään näkökohtaan:
    - käytetyt arviointimenetelmät ovat yhtenäisiä ja johdonmukaisia
    - arviointimenetelmillä pyritään osoittamaan, että sertifioinnin kohde täyttää sertifiointikriteerit ja on siten asetuksen mukainen
    - riippumaton ja puolueeton sertifiointielin on validoinut arvioinnin tulokset.

5.5 Tulosten dokumentointi

65. Johdanto-osan 100 kappaleessa kerrotaan sertifioinnin käyttöönoton tavoitteista.

”Läpinäkyvyyden ja tämän asetuksen noudattamisen tehostamiseksi olisi edistettävä

sertifiointimekanismien sekä tietosuojasinettien ja -merkkien käyttöönottoa, jotta rekisteröidyt voisivat nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojan tason."

66. Tulosten dokumentoinnin ja niistä tiedottamisen läpinäkyvyys on tärkeää. Rekisteröidyille (heidän roolissaan kuluttajina tai asiakkaina) suunnattuja sertifiointimekanismeja, sinettejä tai merkkejä käyttävien sertifiointielinten pitäisi antaa helposti saatavilla olevaa, ymmärrettävässä muodossa olevaa ja mielekästä tietoa sertifioiduista käsittelytoimista. Näitä julkisia tietoja ovat vähintään

    - arvioinnin kohteen kuvaus
    - viittaus arvioinnin kohteeseen sovellettaviin hyväksyttyihin kriteereihin
    - kriteerien arviointimenetelmä (paikalla tehtävä arviointi, dokumentointi jne.)
    - sertifioinnin voimassaoloaika
    - ja niiden avulla valvontaviranomaisten ja yleisön olisi pystyttävä vertailemaan tuloksia.

6 SERTIFIOINTIKRITEERIEN MÄÄRITTELYÄ KOSKEVAT SUUNTAVIIVAT

67. Sertifiointikriteerit ovat sertifiointimekanismin olennainen osa. Sertifiointimenettelyyn kuuluvat vaatimukset siitä, miten, kenen toteuttamana ja miten laajasti ja yksityiskohtaisesti arviointi tehdään yksittäisissä sertifiointihankkeissa, jotka koskevat tiettyä kohdetta eli arvioinnin kohdetta. Sertifiointikriteerit muodostavat nimelliset vaatimukset, joiden täyttymistä arvioinnin kohteessa määritellyssä tosiasiallisessa käsittelytoiminnassa arvioidaan. Näissä sertifiointikriteerien määrittelyä koskevissa suuntaviivoissa annetaan yleisiä neuvoja, jotka auttavat arvioimaan sertifiointikriteerejä hyväksymistä varten.

    - Tiettyä sertifiointikriteeriä hyväksyttäessä tai määriteltäessä olisi otettava huomioon seuraavat yleiset seikat. Sertifiointikriteerien pitäisi olla
    - yhdenmukaisia ja todennettavia
    - tarkastettavissa, jotta voidaan helpottaa yleisen tietosuoja-asetuksen mukaista käsittelytoimien arviointia määrittelemällä erityisesti tavoitteet ja antamalla opastusta niiden saavuttamiseksi
    - kohdeyleisön (esim. yritysten välisen ja yritysten ja asiakkaiden välisen toiminnan) kannalta olennaisia
    - muut standardit (kuten ISO-standardit ja kansallisen tason standardit) huomioon ottavia ja tarvittaessa yhteentoimivia niiden kanssa
    - joustavia ja skaalattavissa sovellettavaksi erityyppisiin ja -kokoisiin organisaatioihin, kuten mikroyrityksiin sekä pieniin ja keskisuuriin yrityksiin 42 artiklan 1 kohdan mukaisesti ja riskiperusteiseen lähestymistapaan johdanto-osan 77 kappaleen mukaisesti.

68. Pieni paikallinen yritys, kuten vähittäiskauppias, suorittaa yleensä vähemmän monimutkaisia käsittelytoimia kuin suuri monikansallinen vähittäiskauppias. Käsittelytoimien lainmukaisuutta koskevat vaatimukset ovat samat, mutta on otettava huomioon tietojenkäsittelyn laajuus ja monimutkaisuus. Siksi sertifiointimekanismien ja niiden kriteerien on oltava skaalattavissa kunkin käsittelytoimen mukaan.

6.1 Olemassa olevat standardit

69. Sertifiointielinten on harkittava, miten tietyissä kriteereissä otetaan huomioon olemassa olevat asiaankuuluvat välineet, kuten käytännesäännöt, tekniset standardit tai kansalliset sääntely- ja lainsäädäntöaloitteet. Ihannetapauksessa kriteerit ovat yhteentoimivia olemassa olevien standardien kanssa, mikä voi auttaa rekisterinpitäjää tai henkilötietojen käsittelijää täyttämään yleisen tietosuoja-asetuksen mukaiset velvollisuutensa. Teollisuusstandardeissa painopiste on usein organisaation suojelemisessa uhkilta ja turvallisuudessa, kun taas yleinen tietosuoja-asetus on tarkoitettu luonnollisten henkilöiden perusoikeuksien suojeluun. Nämä erilaiset näkökulmat on otettava huomioon, jos kriteerejä tai sertifiointimekanismeja laaditaan tai hyväksytään teollisuusstandardien pohjalta.

6.2 Kriteerien määrittely

70. Sertifiointikriteerien täytyy vastata sertifiointimekanismin tai -järjestelmän sertifiointilausuntoa (viesti tai väittämä) ja synnyttämiään odotuksia. Sertifiointimekanismin nimi voi jo määrittää soveltamisalan ja vaikuttaa kriteerien määrittelyyn.

71. [Esimerkki 3]

    ”HealthPrivacyMark” -nimellä toimivan mekanismin soveltamisala olisi rajoitettava terveysalaan. Sinetin nimi synnyttää odotuksen siitä, että on tutkittu terveystietoihin liittyviä tietosuojavaatimuksia. Vastaavasti tämän mekanismin kriteerien on oltava tämän alan tietosuojavaatimusten arvioimisen kannalta tarkoituksenmukaisia.

72. [Esimerkki 4]

    Mekanismissa, joka liittyy tietojenkäsittelyn hallintojärjestelmiä koskevien käsittelytoimien sertifiointiin, olisi määriteltävä kriteerit, jotka mahdollistavat hallintoprosessien ja sen teknisten ja organisatoristen tukitoimenpiteiden tunnustamisen ja arvioimisen.

73. [Esimerkki 5]

    Pilvipalveluihin liittyvän mekanismin kriteereissä on otettava huomioon erityiset tekniset vaatimukset, jotka ovat pilvipalvelujen käytön kannalta välttämättömiä. Jos palvelimet esimerkiksi sijaitsevat EU:n ulkopuolella, kriteereissä on otettava huomioon yleisen tietosuoja-asetuksen V luvussa vahvistetut tietojen siirtämistä kolmansiin maihin koskevat edellytykset.

74. Erilaisia arvioinnin kohteita eri aloilla ja/tai jäsenvaltioissa varten laadittujen kriteerien olisi oltava sovellettavissa eri skenaarioihin, mahdollistettava pieniin, keskisuuriin tai suuriin

käsittelytoimiin sopivien tarkoituksenmukaisten toimenpiteiden tunnistaminen ja kuvastettava luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyviä riskejä, joiden todennäköisyydet ja vakavuusasteet vaihtelevat yleisen tietosuoja-asetuksen mukaisesti. Näin ollen näitä kriteerejä täydentävien sertifiointimenettelyjen (esim. dokumentointiin, testaukseen tai arviointimenetelmään ja perusteellisuuteen liittyvien) on vastattava näihin tarpeisiin. Niiden puitteissa on hyväksyttävä ja otettava käyttöön sääntöjä esimerkiksi asiaankuuluvien kriteerien soveltamiseksi yksittäisissä sertifiointihankkeissa. Kriteerien on helpotettava sen arvioimista, onko asianmukaisten teknisten ja organisatoristen toimenpiteiden täytäntöönpanolle riittävät takeet.

6.3 Sertifiointikriteerien voimassaolo

75. Vaikka sertifiointikriteerien on oltava luotettavia ja kestettävä aikaa, niiden ei pitäisi olla kiveen hakattuja. Niitä on tarkasteltava uudelleen esimerkiksi silloin, kun

- lainsäädäntöä muutetaan
- ehtoja ja säännöksiä tulkitaan Euroopan ihmisoikeustuomioistuimen päätöksissä
- tekniikka on kehittynyt.

Euroopan tietosuojaneuvoston puolesta

Puheenjohtaja

(Andrea Jelinek)

LIITE 1: SERTIFIOINTIIN LIITTYVÄT VALVONTAVIRANOMAISTEN TEHTÄVÄT JA VALTUUDET YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI

	Säännökset	Vaatimukset
Tehtävät	43 artiklan 6 kohta	Valvontaviranomaisen on julkaistava 42 artiklan 5 kohdassa tarkoitetut kriteerit helposti saatavilla olevassa muodossa ja toimitettava ne tietosuojaneuvostolle.
	57 artiklan 1 kohdan n alakohta	Valvontaviranomaisen on hyväksyttävä sertifiointikriteerejä 42 artiklan 5 kohdan nojalla.
	57 artiklan 1 kohdan o alakohta	Valvontaviranomaisen on tarvittaessa (eli silloin kun se myöntää sertifioinnin) toteutettava 42 artiklan 7 kohdan mukaisesti myönnetyn sertifioinnin säännöllinen uudelleentarkastelu.
	64 artiklan 1 kohdan c alakohta	Valvontaviranomaisen on annettava tietosuojaneuvostolle tiedoksi päätösehdotus, jonka tarkoituksena on hyväksyä 42 artiklan 5 kohdassa tarkoitetut sertifiointikriteerit.
Valtuudet	58 artiklan 1 kohdan c alakohta	Valvontaviranomaisella on valtuudet tarkastella 42 artiklan 7 kohdan mukaista sertifiointia uudelleen.
	58 artiklan 2 kohdan h alakohta	Valvontaviranomaisella on valtuudet peruuttaa tai määrätä sertifiointielin peruuttamaan sertifiointi tai kieltää sertifiointielintä antamasta sertifiointia.
	58 artiklan 3 kohdan e alakohta	Valvontaviranomaisella on valtuudet akkreditoida sertifiointielimet.
	58 artiklan 3 kohdan f alakohta	Valvontaviranomaisella on valtuudet myöntää sertifiointeja ja hyväksyä sertifiointikriteerejä.
	58 artiklan 3 kohdan e alakohta	Valvontaviranomaisella on valtuudet akkreditoida sertifiointielimet.
	58 artiklan 3 kohdan f alakohta	Valvontaviranomaisella on valtuudet myöntää sertifiointeja ja hyväksyä sertifiointikriteerejä.

LIITE 2

1 JOHDANTO

Liitteessä 2 annetaan ohjeita 42 artiklan 5 kohdan mukaisten sertifiointikriteerien tarkasteluun ja arviointiin. Siinä määritetään seikkoja, joita tietosuojaviranomainen ja tietosuojaneuvosto tarkastelevat ja soveltavat sertifiointimekanismin sertifiointikriteerien hyväksymiseksi. Sertifiointielinten ja sertifiointijärjestelmän omistajien, jotka haluavat laatia ja esittää kriteerejä hyväksyttäviksi, olisi otettava huomioon nämä kysymykset. Luettelo ei ole tyhjentävä vaan sisältää seikat, joihin ainakin pitäisi kiinnittää huomiota. Kaikkia kysymyksiä ei voida aina soveltaa, mutta ne pitäisi ottaa huomioon kriteerejä laadittaessa. Sitä, miksi kriteerit eivät kata tiettyjä näkökohtia, on ehkä perusteltava. Jotkin kysymykset saattavat toistua, koska ne esitetään eri näkökulmista. Näitä ohjeita olisi tarkasteltava yleisessä tietosuoja-asetuksessa ja mahdollisesti kansallisessa lainsäädännössä säädettyjen oikeudellisten vaatimusten pohjalta.

2 SERTIFIOINTIMEKANISMIN SOVELTAMISALA JA ARVIOINNIN KOHDE

a. Onko sertifiointimekanismin (jonka kohdalla tietosuojakriteerejä on tarkoitus käyttää) soveltamisala kuvailtu selkeästi?

b. Onko sertifiointimekanismin soveltamisala selkeä ja mielekäs kohdeyleisön kannalta vai onko se harhaanjohtava?

- *Esimerkki: ”Trusted Company Seal” -sinetti antaa ymmärtää, että koko yrityksen käsittelytoimet on tarkastettu, vaikka sertifiointi koskee vain tiettyjä käsittelytoimia, esimerkiksi verkkomaksuprosessia. Soveltamisala on siksi harhaanjohtava.*

c. Onko sertifiointimekanismin soveltamisalassa otettu huomioon käsittelytoimien kaikki olennaiset näkökohdat?

- *Esimerkki: Terveysalan ”Privacy Health Mark” -tietosuojamerkin on katettava kaikki terveyttä koskevat arviointitiedot, jotta 9 artiklan mukaisiin vaatimuksiin voidaan vastata.*

d. Mahdollistaako sertifiointimekanismin soveltamisala mielekkään tietosuojasertifioinnin, jossa otetaan huomioon asiaankuuluvien käsittelytoimien luonne, sisältö ja riskit?

- *Esimerkki: Jos sertifiointimekanismin soveltamisala keskittyy ainoastaan käsittelytoimien tiettyihin näkökohtiin, kuten tietojen keräämiseen, mutta ei muihin käsittelytoimiin, kuten käsittelyyn mainontaprofiilien luomiseksi tai rekisteröityjen oikeuksien hallinnoimiseksi, se ei ole mielekäs rekisteröityjen kannalta.*

e. Kattaako sertifiointimekanismin soveltamisala henkilötietojen käsittelyn kyseisessä soveltamismaassa vai koskeeko se rajatylittävää käsittelyä ja/tai rajatylittäviä siirtoja?

f. Kuvaillaanko sertifiointikriteereissä riittävästi sitä, miten arvioinnin kohde olisi määriteltävä?

- *Esimerkki: Soveltamisalaltaan yleinen ”Privacy Seal ” -tietosuojasinetti, joka edellyttää ainoastaan ”sertifioitavan käsittelyn yksilöintiä”, ei tarjoa riittävän selkeitä ohjeita arvioinnin kohteen määrittämisestä ja kuvailemisesta.*

- *Esimerkki: Soveltamisalaltaan rajatun, turvallista säilyttämistä koskevan ”Privacy Vault Seal” -sinetin kriteereissä olisi kuvailtava yksityiskohtaisesti tämän soveltamisalan noudattamisen vaatimukset, esimerkiksi säilön (vault) määritelmä, järjestelmävaatimukset sekä pakolliset tekniset ja organisatoriset toimenpiteet. Tässä tapauksessa soveltamisalassa voidaan selkeästi määrittää arvioinnin kohde.*

    (1) Edellytetäänkö kriteereissä, että arvioinnin kohde sisältää kaikkien olennaisten käsittelytoimien yksilöinnin, tietovirtojen kuvauksen ja arvioinnin kohteen soveltamisen alueen määrityksen?

        - *Esimerkki: Sertifiointimekanismi tarjoaa rekisterinpitäjien yleisen tietosuoja-asetuksen alaisten käsittelytoimien sertifiointia erittelemättä tarkemmin soveltamisen aluetta (yleinen soveltamisala). Mekanismin käyttämät kriteerit edellyttävät, että hakemuksen tekevä rekisterinpitäjä määrittää kohteena olevan käsittelytoimen (arvioinnin kohteen) käytössä olevien tietotyyppien, järjestelmien ja prosessien osalta.*

    (2) Edellytetäänkö kriteereissä, että hakija ilmoittaa selvästi, missä arvioinnin kohteena oleva käsittely alkaa ja päättyy? Edellytetäänkö kriteereissä, että arvioinnin kohde sisältää rajapinnat, joiden osaltatoisistaan riippuvaiset käsittelytoimet eivät sisälly arvioinnin kohteeseen? Ja onko tätä perusteltu riittävästi?

        - *Esimerkki: Arvioinnin kohde, jossa kuvaillaan riittävän yksityiskohtaisesti verkkopohjaisen palvelun käsittelytoimea, kuten käyttäjien rekisteröintiä, palvelun tarjoamista, laskutusta, IP-osoitteiden kirjaamista sekä rajapintoja suhteessa käyttäjiin ja kolmansiin osapuoliin, pois lukien palvelinten ylläpitäminen (mutta mukaan lukien käsittelyä ja teknisiä ja organisatorisia toimenpiteitä koskevat sopimukset).*

g. Takaavatko kriteerit, että (yksittäiset) arvioinnin kohteet ovat ymmärrettäviä kohdeyleisölle ja tarvittaessa myös rekisteröidyille?

3 YLEISET VAATIMUKSET

a. Onko kaikki kriteeriluettelossa (eli kaikissa sertifiointikriteereissä) käytetyt olennaiset käsitteet määritetty, selitetty ja kuvailtu?

b. Onko kaikki normatiiviset viiteasiakirjat määritetty?

c. Sisältävätkö kriteerit sertifiointimekanismin soveltamisalan kattamien tietosuojavelvoitteiden, menettelyjen ja käsittelyn määritelmät?

4 KÄSITTELYTOIMI, 42 ARTIKLAN 1 KOHTA

Käsitelläänkö kriteereissä käsittelytoimien kaikkia sertifiointimekanismin soveltamisalan (yleinen tai rajattu) kannalta olennaisia osatekijöitä (tietoja, järjestelmiä ja prosesseja)?

a. Edellytetäänkö kriteereissä käsittelyn oikeusperustojen määrittämistä arvioinnin kohteen osalta?

b. Huomioidaanko kriteereissä arvioinnin kohteen osalta käsittelyn olennaiset vaiheet ja tietojen koko elinkaari, mukaan lukien tietojen poistaminen ja/tai anonymisointi?

c. Edellytetäänkö kriteereissä arvioinnin kohteen osalta mahdollisuutta siirtää tietoja järjestelmästä toiseen?

d. Mahdollistavatko kriteerit arvioinnin kohteen osalta tietyntyyppisten käsittelytoimien, kuten automatisoidun päätöksenteon tai profiloinnin, tunnistamisen ja huomioon ottamisen?

e. Mahdollistavatko kriteerit arvioinnin kohteen osalta erityisten tietoryhmien tunnistamisen?

f. Mahdollistavatko kriteerit yksittäisten käsittelytoimien riskien ja rekisteröityjen oikeuksien ja vapauksien suojelutarpeen arvioimisen ja edellytetäänkö niissä sitä?

g. Mahdollistavatko kriteerit luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien asianmukaisen huomioimisen ja edellytetäänkö niissä sitä?

…

5 KÄSITTELYN LAINMUKAISUUS

a. Vaaditaanko kriteereissä käsittelyn lainmukaisuuden tarkistamista yksittäisten käsittelytoimien kohdalla käsittelyn tarkoituksen ja tarpeellisuuden osalta?

b. Vaaditaanko kriteereissä yksittäisten käsittelytoimien oikeusperustan kaikkien vaatimusten tarkistamista?

6 PERIAATTEET, 5 ARTIKLA

a. Käsitelläänkö kriteereissä asianmukaisesti kaikkia 5 artiklan mukaisia tietosuojaperiaatteita?

b. Vaaditaanko kriteereissä tietojen minimoinnin osoittamista yksittäisten arvioinnin kohteiden osalta?

…

7 REKISTERINPITÄJIEN JA HENKILÖTIETOJEN KÄSITTELIJÖIDEN YLEISET VELVOITTEET

a. Vaaditaanko kriteereissä näyttöä henkilötietojen käsittelijöiden ja rekisterinpitäjien välisistä sopimuksista?

b. Arvioidaanko rekisterinpitäjän ja henkilötietojen käsittelijän välisiä sopimuksia?

c. Otetaanko kriteereissä huomioon IV luvun mukaiset rekisterinpitäjän velvoitteet?

d. Edellytetäänkö kriteereissä näyttöä rekisterinpitäjän täytäntöön panemien teknisten ja organisatoristen toimenpiteiden tarkistamisesta ja päivittämisestä 24 artiklan 1 kohdan mukaisesti?

e. Varmistetaanko kriteereillä, että organisaatio on arvioinut, olisiko sen nimitettävä tietosuojavastaava, kuten 37 artiklassa edellytetään? Täyttääkö mahdollinen tietosuojavastaava 37–39 artiklassa säädetyt vaatimukset?

f. Varmistetaanko kriteereillä, että seloste käsittelytoimista vaaditaan 30 artiklan 5 kohdan mukaisesti ja että selosteessa käsitellään asianmukaisesti 30 artiklan vaatimuksia?

8 REKISTERÖITYJEN OIKEUDET

a. Käsitelläänkö kriteereissä asianmukaisesti rekisteröityjen oikeutta saada tietoja, ja vaaditaanko niissä vastaavien toimenpiteiden toteuttamista?

b. Edellytetäänkö kriteereissä, että rekisteröidyille annetaan asianmukainen tai jopa laajempi pääsy tietoihinsa ja oikeus valvoa niitä, tietojen siirtäminen järjestelmästä toiseen mukaan luettuna?

c. Edellytetäänkö kriteereissä sellaisten toimenpiteiden toteuttamista, joiden avulla käsittelytoimeen voidaan puuttua rekisteröityjen oikeuksien turvaamiseksi ja oikaisujen, poistamisen tai rajoitusten mahdollistamiseksi?

…

9 LUONNOLLISTEN HENKILÖIDEN OIKEUKSIIN JA VAPAUKSIIN KOHDISTUVAT RISKIT

a. Mahdollistavatko kriteerit luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien arvioimisen ja edellytetäänkö niissä sitä?

b. Tarjoavatko kriteerit tunnustetun riskinarviointimenetelmän tai edellytetäänkö niissä sellaista? Jos vastaus on kyllä, niin onko menetelmä oikeasuhteinen?

c. Mahdollistavatko kriteerit suunniteltujen käsittelytoimien luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvan vaikutuksen arvioimisen ja edellytetäänkö niissä sitä?

d. Edellytetäänkö kriteereissä ennakkokuulemista niistä jäljellä olevista riskeistä, joita ei voitu pienentää, tietosuojaa koskevan vaikutustenarvioinnin tulosten pohjalta?

10 SUOJELUN TAKAAVAT TEKNISET JA ORGANISATORISET TOIMENPITEET

a. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, jotka takaavat käsittelytoimien luottamuksellisuuden?

b. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, jotka takaavat käsittelytoimien eheyden?

c. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, jotka takaavat käsittelytoimien käytettävyyden?

d. Edellytetäänkö kriteereissä sellaisten toimenpiteiden soveltamista, jotka takaavat käsittelytoimien läpinäkyvyyden seuraavien seikkojen osalta:

e. osoitusvelvollisuus?

f. rekisteröityjen oikeudet?

g. yksittäisten käsittelytoimien arvioiminen, esimerkiksi algoritmien läpinäkyvyyttä varten?

h. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, jotka takaavat rekisteröityjen oikeudet, esimerkiksi kyvyn antaa tietoja tai oikeuden tietojen siirtämiseen järjestelmästä toiseen?

i. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, joiden avulla käsittelytoimeen voidaan puuttua rekisteröityjen oikeuksien turvaamiseksi ja oikaisujen, poistamisen tai rajoitusten mahdollistamiseksi?

j. Edellytetäänkö kriteereissä sellaisten toimenpiteiden soveltamista, joiden avulla käsittelytoimeen voidaan puuttua järjestelmän tai prosessin korjaamiseksi tai tarkastamiseksi?

k. Edellytetäänkö kriteereissä sellaisten teknisten ja organisatoristen toimenpiteiden soveltamista, joiden avulla voidaan taata tietojen minimointi, esimerkiksi tietojen irrottamista tai erottamista rekisteröidystä, anonymisointia tai pseudonymisointia tai tietojärjestelmien eristämistä?

l. Edellytetäänkö kriteereissä teknisiä toimenpiteitä oletusarvoisen tietosuojan panemiseksi täytäntöön?

m. Edellytetäänkö kriteereissä teknisiä ja organisatorisia toimenpiteitä sisäänrakennetun tietosuojan panemiseksi täytäntöön, esimerkiksi tietosuojan hallinnointijärjestelmää tietosuojavaatimusten osoittamiseksi, niistä ilmoittamiseksi, niiden valvomiseksi ja täytäntöön panemiseksi?

n. Edellytetäänkö kriteereissä teknisiä ja organisatorisia toimenpiteitä, joiden avulla järjestetään määräaikaista koulutusta henkilöstölle, jolla on pysyvä tai säännöllinen pääsy henkilötietoihin?

o. Edellytetäänkö kriteereissä uudelleentarkastelutoimenpiteitä?

p. Edellytetäänkö kriteereissä itsearviointia / sisäisiä tarkastuksia?

q. Edellytetäänkö kriteereissä toimenpiteitä sen takaamiseksi, että henkilötietojen tietoturvaloukkauksen ilmoittamiseen liittyvät velvoitteet täytetään ajoissa ja riittävän laajasti?

r. Edellytetäänkö kriteereissä häiriötilanteiden hallintaan liittyvien menettelyjen käyttöönottoa ja todentamista?

s. Edellytetäänkö kriteereissä esiin tulevien tietosuoja- ja teknologiaseikkojen seuraamista ja järjestelmän päivittämistä tarpeen mukaan?

…

11 MUITA ERITYISIÄ TIETOSUOJAYSTÄVÄLLISIÄ OMINAISUUKSIA

a. Edellytetäänkö kriteereissä tietosuojaa tehostavien tekniikoiden käyttöönottoa? Tähän voisi kuulua kriteereitä, jotka edellyttävät tietosuojan tehostamista poistamalla tai vähentämällä henkilötietoja ja/tai tietosuojariskiä.

- *Esimerkki: Kriteereissä, jotka edellyttävät yhdistämismahdollisuuksien minimoimista siten, että käytetään käyttäjäkeskeistä henkilöllisyyden hallintaa, kuten ominaisuuspohjaista valtuutusta, organisaatiokeskeisen henkilöllisyyden hallinnan sijaan, otettaisiin huomioon tietosuojaa tehostava tekniikka.*

b. Edellytetäänkö kriteereissä rekisteröityjen oman valvonnan tehostamista itsemääräämisoikeuden ja valinnanvapauden helpottamiseksi?

…

12 KRITEERIT, JOIDEN TARKOITUS ON OSOITTAA ASIANMUKAISTEN SUOJATOIMIEN OLEMASSAOLO HENKILÖTIETOJEN SIIRTÄMISEN YHTEYDESSÄ

Kriteerejä käsitellään 42 artiklan 2 kohtaa koskevissa tulevissa suuntaviivoissa.

13 EUROOPPALAISEN TIETOSUOJASINETIN LISÄKRITEERIT

a. Onko kriteerien tarkoitus kattaa kaikki jäsenvaltiot?

b. Voidaanko kriteereissä ottaa huomioon jäsenvaltioiden tietosuojalainsäädäntö tai -skenaariot?

c. Edellytetäänkö kriteereissä yksittäisten arvioinnin kohteiden arviointia jäsenvaltioiden alakohtaisen tietosuojalainsäädännön osalta?

d. Edellytetäänkö kriteereissä, että rekisterinpitäjä tai henkilötietojen käsittelijä antaa rekisteröidyille ja asianomaisille osapuolille jäsenvaltioiden kielillä tietoja

e. käsittelystä / arvioinnin kohteesta?

f. käsittelyn / arvioinnin kohteen dokumentoinnista?

g. arvioinnin tuloksista?

…

14 KRITEERIEN YLEINEN ARVIOINTI

a. Kattavatko kriteerit kokonaan sertifiointimekanismin soveltamisalan (eli kokonaisvaltaiset kriteerit) riittävien takuiden antamiseksi siitä, että sertifiointiin voi luottaa?

- *Esimerkki: Jos sertifiointimekanismin soveltamisalassa keskitytään terveyteen liittyviin käsittelytoimiin, tietosuojan korkea taso pitäisi taata määrittämällä kriteerejä, jotka takaavat esimerkiksi perusteellisen arvioinnin ja sisäänrakennettua yksityisyydensuojaa ja oletusarvoista yksityisyydensuojaa koskevien periaatteiden soveltamisen.*

b. Ovatko kriteerit suhteessa sertifiointimekanismin soveltamisalaan kuuluvan käsittelytoimen laajuuteen, tietojen arkaluonteisuuteen ja käsittelyn riskiin?

c. Onko todennäköistä, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat tietosuojasääntöjä paremmin kriteerien ansiosta?

d. Hyötyvätkö rekisteröidyt tiedonsaantioikeuksiensa osalta, mukaan luettuna toivottujen tulosten selittäminen rekisteröidyille?