Suuntaviivat 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen (2016/679) 43 artiklan mukaisesti

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	Lisättiin liite 1 (julkisen kuulemisen jälkeen 4.6.2019 hyväksytyn liitteen 1 versio 2.0)
Versio 2.0	4. joulukuuta 2018	Hyväksyttiin suuntaviivat julkisen kuulemisen jälkeen – Samana päivänä hyväksyttiin liite 1 (versio 1.0) julkista kuulemista varten
Versio 1.0	6. helmikuuta 2018	Tietosuojatyöryhmä hyväksyi suuntaviivat (versio julkista kuulemista varten). Tietosuojaneuvosto hyväksyi kyseisen version 25. toukokuuta 2018.

Sisällys

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 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon suuntaviivoista helmikuussa 2018 järjestetyn julkisen kuulemisen tulokset ja liitteestä 14. joulukuuta 2018 ja 1. helmikuuta 2019 välisenä aikana järjestetyn kuulemisen tulokset edellä mainitun asetuksen 70 artiklan 4 kohdan mukaisesti,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT:

1 JOHDANTO

1. Yleinen tietosuoja-asetus (asetus (EU) 2016/679, jäljempänä ’tietosuoja-asetus’), joka tuli voimaan 25. toukokuuta 2018, tarjoaa osoitusvelvollisuuteen ja perusoikeuksiin perustuvan nykyaikaistetun kehyksen tietosuojaa koskevien sääntöjen noudattamiselle Euroopassa. Tässä uudessa kehyksessä ovat keskeisiä erilaiset toimenpiteet, joilla helpotetaan tietosuoja-asetuksen säännösten noudattamista. Niitä ovat muun muassa pakolliset vaatimukset tietyissä olosuhteissa (muun muassa tietosuojavastaavien nimittäminen ja tietosuojaa koskevien vaikutustenarviointien tekeminen) ja vapaaehtoiset toimenpiteet, kuten käytännesäännöt ja sertifiointimekanismit.

2. Sertifiointimekanismien ja tietosuojasinettien ja -merkkien käyttöönoton yhteydessä tietosuoja-asetuksen 43 artiklan 1 kohdassa vaaditaan jäsenvaltioita varmistamaan, että 42 artiklan 1 kohdan mukaisen sertifioinnin myöntävät sertifiointielimet on akkreditoinut toimivaltainen valvontaviranomainen tai kansallinen akkreditointielin tai molemmat. Jos akkreditoinnin on tehnyt kansallinen akkreditointielin standardin ISO/IEC 17065/2012 mukaisesti, on sovellettava myös toimivaltaisen valvontaviranomaisen vahvistamia lisävaatimuksia.

3. Tarkoituksenmukaiset sertifiointimekanismit voivat edistää tietosuoja-asetuksen noudattamista ja läpinäkyvyyttä rekisteröityjen kannalta ja yritystenvälisissä suhteissa, esimerkiksi rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä. Rekisterinpitäjät ja henkilötietojen käsittelijät hyötyvät riippumattoman kolmannen osapuolen antamasta todistuksesta, jonka tarkoituksena on osoittaa, että niiden käsittelytoimet ovat vaatimusten mukaisia.[1]

4. Tässä yhteydessä Euroopan tietosuojaneuvosto (jäljempänä ’tietosuojaneuvosto’) toteaa, että akkreditoinnista on annettava suuntaviivat. Akkreditoinnin erityinen arvo ja merkitys on

[1] Tietosuoja-asetuksen johdanto-osan 100 kappaleessa todetaan, että sertifiointimekanismien käyttöönotolla voidaan lisätä läpinäkyvyyttä ja asetuksen noudattamista ja antaa rekisteröidyille mahdollisuus arvioida asianomaisten tuotteiden ja palvelujen tietosuojan tasoa.

siinä, että se tarjoaa sertifiointielinten pätevyydestä luotettavan lausunnon, jolla voidaan luoda luottamusta sertifiointimekanismiin.

5. Suuntaviivojen tarkoituksena on antaa ohjeistusta siitä, miten tietosuoja-asetuksen 43 artiklan säännöksiä pitäisi tulkita ja miten ne pitäisi panna täytäntöön. Niiden tarkoituksena on erityisesti auttaa jäsenvaltioita, valvontaviranomaisia ja kansallisia akkreditointielimiä ottamaan käyttöön johdonmukainen ja yhdenmukaistettu perustaso niiden sertifiointielinten akkreditoinnissa, jotka myöntävät sertifioinnin tietosuoja-asetuksen mukaisesti.

2 SUUNTAVIIVOJEN SOVELTAMISALA

6. Näissä suuntaviivoissa

- esitetään akkreditoinnin tarkoitus tietosuoja-asetuksen yhteydessä
- selitetään reitit, jotka ovat käytettävissä sertifiointielinten akkreditointia varten 43 artiklan 1 kohdan mukaisesti, ja määritetään keskeiset pohdittavat kysymykset
- tarjotaan kehys akkreditoinnin lisävaatimusten vahvistamiselle, kun akkreditoinnin suorittaa kansallinen akkreditointielin, ja
- tarjotaan kehys akkreditointivaatimusten vahvistamiselle, kun akkreditoinnin suorittaa valvontaviranomainen.

7. Suuntaviivat eivät ole menettelyopas sertifiointielinten akkreditoimiseksi tietosuoja-asetuksen mukaisesti. Niissä ei laadita uutta teknistä standardia sertifiointielinten akkreditoimiseksi asetuksen tarkoituksia varten.

8. Suuntaviivat on tarkoitettu

- jäsenvaltioille, joiden on varmistettava, että valvontaviranomainen ja/tai kansallinen akkreditointielin akkreditoi sertifiointielimet
- kansallisille akkreditointielimille, jotka suorittavat sertifiointielinten akkreditointeja 43 artiklan 1 kohdan b alakohdan mukaisesti
- standardin ISO/IEC 17065/2012[2] vaatimuksia täydentävät lisävaatimukset määrittelevälle toimivaltaiselle valvontaviranomaiselle, kun kansallinen akkreditointielin suorittaa akkreditoinnin 43 artiklan 1 kohdan b alakohdan mukaisesti
- tietosuojaneuvostolle, kun se antaa lausunnon toimivaltaisen valvontaviranomaisen akkreditointivaatimuksista ja hyväksyy ne 43 artiklan 3 kohdan, 70 artiklan 1 kohdan p alakohdan ja 64 artiklan 1 kohdan c alakohdan mukaisesti
- akkreditointivaatimukset määrittävälle toimivaltaiselle valvontaviranomaiselle, kun valvontaviranomainen suorittaa akkreditoinnin 43 artiklan 1 kohdan a alakohdan mukaisesti

- muille sidosryhmille, kuten mahdollisille sertifiointielimille tai sertifiointijärjestelmän omistajille[3], jotka laativat sertifiointikriteerejä ja -menettelyjä.

[2] Kansainvälinen standardisoimisjärjestö: Vaatimustenmukaisuuden arviointi. Vaatimukset tuotteita, prosesseja ja palveluja sertifioiville elimille.

9. Määritelmät

10. Seuraavien määritelmien tarkoituksena on edistää yhteistä käsitystä akkreditointiprosessin perustekijöistä. Niitä on pidettävä viitteellisinä, eikä niihin voi vedota ehdottomina. Nämä määritelmät perustuvat voimassa oleviin sääntelykehyksiin ja standardeihin, erityisesti tietosuoja-asetuksen asiaankuuluviin säännöksiin ja standardiin ISO/IEC 17065/2012.

11. Näissä suuntaviivoissa käytetään seuraavia määritelmiä:

12. sertifiointielinten *'akkreditointi'*, katso kohta 3, joka koskee akkreditoinnin tulkintaa tietosuoja-asetuksen 43 artiklan tarkoituksia varten;

13. *'lisävaatimuksilla'* tarkoitetaan toimivaltaisen valvontaviranomaisen vahvistamia vaatimuksia, joiden perusteella akkreditointi suoritetaan[4];

14. *'sertifioinnilla'* tarkoitetaan arviointia ja puolueettoman kolmannen osapuolen todistusta[5] siitä, että sertifiointikriteerien täyttäminen on osoitettu;

15. *'sertifiointielimellä'* tarkoitetaan kolmannen osapuolen vaatimustenmukaisuuden[6] arviointielintä[7], joka käyttää sertifiointimekanismeja[8];

16. *'sertifiointijärjestelmällä'* tarkoitetaan sertifiointijärjestelmää, joka liittyy tiettyihin tuotteisiin, prosesseihin ja palveluihin, joihin sovelletaan samoja täsmennettyjä vaatimuksia, erityisiä sääntöjä ja menettelyjä;[9]

17. *'kriteereillä'* tai *'sertifiointikriteereillä'* tarkoitetaan kriteereitä, joiden perusteella sertifiointi (vaatimustenmukaisuuden arviointi) tehdään;[10]

18. *'kansallisella akkreditointielimellä'* tarkoitetaan jäsenvaltion ainoaa elintä, joka on nimetty Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 mukaisesti ja joka suorittaa akkreditointia valtiolle kuuluvaa julkista valtaa käyttäen.[11]

---

[3] Järjestelmän omistaja on tunnistettavissa oleva organisaatio, joka on laatinut sertifiointikriteerit ja -vaatimukset, joiden perusteella vaatimustenmukaisuutta on määrä arvioida. Akkreditointi koskee organisaatiota, joka tekee arvioinnin (43 artiklan 4 kohta) sertifiointijärjestelmän vaatimusten perusteella ja antaa todistukset (ts. sertifiointielin eli vaatimustenmukaisuutta arvioiva elin). Arvioinnit tekevä organisaatio voisi olla sama organisaatio, joka on kehittänyt järjestelmän ja omistaa sen, mutta käytössä voi olla järjestelyjä, joissa yksi organisaatio omistaa järjestelmän ja toinen (tai useampi) tekee arviointeja.

[4] Tietosuoja-asetuksen 43 artiklan 1, 3 ja 6 kohta.

[5] Standardin ISO 17000 mukaan kolmannen osapuolen todistusta (sertifiointia) sovelletaan kaikkiin vaatimustenmukaisuuden arvioinnin kohteisiin (kohta 5.5) lukuun ottamatta itse vaatimustenmukaisuutta arvioivia elimiä, joihin sovelletaan akkreditointia (kohta 5.6).

[6] Kolmannen osapuolen vaatimustenmukaisuuden arvioinnista vastaa organisaatio, joka on riippumaton henkilöstä tai organisaatiosta, joka tarjoaa kohteen, ja kyseisen kohteen käyttäjien eduista (ks. ISO 17000, kohta 2.4).

[7] Ks. ISO 17000, kohta 2.5: vaatimustenmukaisuuden arviointipalveluja suorittava elin; ISO 17011: vaatimustenmukaisuuden arviointipalveluja suorittava elin, joka voi olla akkreditoinnin kohde; ISO 17065, kohta 3.12.

[8] Tietosuoja-asetuksen 42 artiklan 1 ja 5 kohta.

[9] Ks. kohta 3.9 yhdessä standardin ISO 17065 liitteen B kanssa.

[10] Ks. tietosuoja-asetuksen 42 artiklan 5 kohta.

[11] Ks. asetuksen (EY) N:o 765/2008 2 artiklan 11 kohta.

3 ”AKKREDITOINNIN” TULKINTA TIETOSUOJA-ASETUKSEN 43 ARTIKLAN TARKOITUKSIA VARTEN

19. Tietosuoja-asetuksessa ei määritellä akkreditointia. Akkreditointeihin sovellettavia yleisiä vaatimuksia koskevan asetuksen (EY) N:o 765/2008 2 artiklan 10 kohdan mukaan akkreditoinnilla tarkoitetaan

20. ”kansallisen akkreditointielimen antamaa todistusta siitä, että vaatimustenmukaisuuden arviointilaitos täyttää tiettyä vaatimustenmukaisuuden arviointia koskevat, yhdenmukaistetuilla standardeilla vahvistetut vaatimukset ja tarvittaessa muut vaatimukset, mukaan luettuna ne, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa”.

21. Standardin ISO/IEC 17011 mukaan

22. akkreditoinnilla viitataan kolmannen osapuolen antamaan todistukseen, joka liittyy vaatimustenmukaisuutta arvioivaan elimeen ja jossa annetaan virallinen osoitus sen pätevyydestä suorittaa erityisiä vaatimustenmukaisuuden arviointitehtäviä.

23. Tietosuoja-asetuksen 43 artiklan 1 kohdassa säädetään seuraavaa:

24. ”Sertifioinnin myöntää ja uusii sertifiointielin, jolla on tietosuojaan liittyvä asianmukaisen tason asiantuntemus, sen jälkeen kun se on tiedottanut valvontaviranomaiselle valvontaviranomaisen 58 artiklan 2 kohdan h alakohdan mukaisten valtuuksien käyttämisen mahdollistamiseksi, sanotun kuitenkaan rajoittamatta toimivaltaisen valvontaviranomaisen 57 ja 58 artiklan mukaisia tehtäviä ja valtuuksia. Jäsenvaltioiden on säädettävä siitä, akkreditoiko nämä sertifiointielimet yksi tai molemmat seuraavista:

    a) 55 tai 56 artiklan nojalla toimivaltainen valvontaviranomainen;
    b) Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 mukaisesti nimitetty kansallinen akkreditointielin noudattaen EN-ISO/IEC 17065/2012 -standardia ja 55 tai 56 artiklan nojalla toimivaltaisen valvontaviranomaisen vahvistamia lisävaatimuksia.”

25. Tietosuoja-asetuksen osalta akkreditointivaatimusten perustana ovat

- standardi ISO/IEC 17065/2012 ja lisävaatimukset, jotka vahvistaa 43 artiklan 1 kohdan b alakohdan mukaisesti toimivaltainen valvontaviranomainen, kun akkreditoinnin suorittaa kansallinen akkreditointielin, ja valvontaviranomainen, kun se suorittaa akkreditoinnin itse.

26. Molemmissa tapauksissa vahvistettujen vaatimusten on katettava 43 artiklan 2 kohdassa tarkoitetut vaatimukset.

27. Tietosuojaneuvosto toteaa, että akkreditoinnin tarkoituksena on antaa luotettava lausunto tietyn elimen pätevyydestä sertifioinnin (vaatimustenmukaisuuden arviointiin liittyvien toimenpiteiden) toteuttamiseen.[12] Tietosuoja-asetuksen mukaisesti akkreditoinnin katsotaan tarkoittavan seuraavaa:

[12] Vrt. asetuksen (EY) N:o 765/2008 johdanto-osan 15 kappale.

28. kansallisen akkreditointielimen ja/tai valvontaviranomaisen todistusta[13] siitä, että sertifiointielin[14] on pätevä toteuttamaan sertifioinnin tietosuoja-asetuksen 42 ja 43 artiklan mukaisesti ottaen huomioon standardin ISO/IEC 17065/2012 ja valvontaviranomaisen ja tietosuojaneuvoston vahvistamat lisävaatimukset.

4 AKKREDITOINTI TIETOSUOJA-ASETUKSEN 43 ARTIKLAN 1 KOHDAN MUKAISESTI

29. Tietosuoja-asetuksen 43 artiklan 1 kohdassa todetaan, että sertifiointielinten akkreditointiin on useita vaihtoehtoja. Tietosuoja-asetuksessa vaaditaan valvontaviranomaisia ja jäsenvaltioita määrittämään sertifiointielinten akkreditointimenettely. Tässä kohdassa esitetään reitit 43 artiklassa tarkoitettua akkreditointia varten.

4.1 Jäsenvaltioiden tehtävät

30. Tietosuoja-asetuksen 43 artiklan 1 kohdan mukaan jäsenvaltioiden on *varmistettava*, että sertifiointielimet akkreditoidaan, mutta kukin jäsenvaltio saa itse päättää, kuka vastaa akkreditointiin johtavan arvioinnin tekemisestä. Tietosuoja-asetuksen 43 artiklan 1 kohdan nojalla käytössä on kolme vaihtoehtoa. Akkreditoinnin voi toteuttaa

1) ainoastaan valvontaviranomainen omien vaatimustensa mukaisesti;
2) ainoastaan asetuksen (EY) N:o 765/2008 mukaisesti ja standardin ISO/IEC 17065/2012 ja toimivaltaisen valvontaviranomaisen vahvistamien lisävaatimusten mukaisesti nimetty kansallinen akkreditointielin; tai
3) sekä valvontaviranomainen että kansallinen akkreditointielin (kaikkien edellä kohdassa 2 lueteltujen vaatimusten mukaisesti).

31. Kukin jäsenvaltio päättää itse, toteuttaako nämä akkreditoinnit kansallinen akkreditointielin vai valvontaviranomainen vai molemmat yhdessä, mutta sen on joka tapauksessa varmistettava riittävät resurssit[15].

4.2 Vuorovaikutus asetuksen (EY) N:o 765/2008 kanssa

32. Tietosuojaneuvosto huomauttaa, että asetuksen (EY) N:o 765/2008 2 artiklan 11 kohdassa määritetään kansallinen akkreditointielin jäsenvaltion *ainoaksi* elimeksi, joka suorittaa akkreditointia valtiolle kuuluvaa julkista valtaa käyttäen.

33. Kyseisen 2 artiklan 11 kohdan voidaan katsoa olevan ristiriidassa tietosuoja-asetuksen 43 artiklan 1 kohdan kanssa, koska siinä sallitaan myös muun elimen kuin jäsenvaltion kansallisen akkreditointielimen suorittama akkreditointi. Tietosuojaneuvosto katsoo, että EU:n lainsäädännön tarkoituksena on ollut tehdä poikkeus yleiseen periaatteeseen, jonka mukaan akkreditoinnin suorittaa yksinomaan kansallinen akkreditointielin, antamalla valvontaviranomaisille samat valtuudet sertifiointielinten akkreditoinnissa. Siksi 43 artiklan 1 kohta on erityissäännös suhteessa asetuksen (EY) N:o 765/2008 2 artiklan 11 kohtaan.

---

[13] Vrt. tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista 9 päivänä heinäkuuta 2008 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 10 kohta.
[14] Vrt. standardin ISO 17011 mukainen määritelmä akkreditoinnista.
[15] Ks. asetuksen (EY) N:o 765/2008 4 artiklan 9 kohta.

4.3 Kansallisen akkreditointielimen tehtävät

34. Tietosuoja-asetuksen 43 artiklan 1 kohdan b alakohdassa säädetään, että kansallinen akkreditointielin akkreditoi sertifiointielimet noudattaen standardia ISO/IEC 17065/2012 ja toimivaltaisen valvontaviranomaisen vahvistamia lisävaatimuksia.

35. Selvyyden vuoksi tietosuojaneuvosto huomauttaa, että nimenomainen viittaus 43 artiklan 3 kohdan 1 alakohdan b alakohtaan tarkoittaa, että ”näillä vaatimuksilla” tarkoitetaan toimivaltaisen valvontaviranomaisen 43 artiklan 1 kohdan b alakohdan mukaisesti vahvistamia ”lisävaatimuksia” ja 43 artiklan 2 kohdassa tarkoitettuja vaatimuksia.

36. Akkreditointiprosessissa kansallisten akkreditointielinten on noudatettava valvontaviranomaisten määrittämiä lisävaatimuksia.

37. Sertifiointielin, jolla on standardiin ISO/IEC 17065/2012 perustuva voimassa oleva akkreditointi muiden kuin tietosuoja-asetukseen liittyvien sertifiointijärjestelmien osalta ja joka haluaa laajentaa akkreditointinsa soveltamisalaa kattamaan tietosuoja-asetuksen mukaisesti myönnetyt akkreditoinnit, on täytettävä valvontaviranomaisen vahvistamat lisävaatimukset, jos akkreditoinnin suorittaa kansallinen akkreditointielin. Jos vain toimivaltainen valvontaviranomainen suorittaa tietosuoja-asetuksen mukaisen sertifiointielimen akkreditoinnin, akkreditointia hakevan sertifiointielimen on täytettävä asiaankuuluvan valvontaviranomaisen asettamat vaatimukset.

4.4 Valvontaviranomaisen tehtävät

38. Tietosuojaneuvosto huomauttaa, että 57 artiklan 1 kohdan q alakohdassa säädetään, että valvontaviranomaisen on akkreditoitava sertifiointielin 43 artiklan mukaisesti, koska 57 artiklan ja 58 artiklan 3 kohdan e alakohdan mukaisessa valvontaviranomaisen tehtävässä valvontaviranomaisella on hyväksymis- ja neuvontavaltuudet akkreditoida sertifiointielimet 43 artiklan mukaisesti. Tietosuoja-asetuksen 43 artiklan 1 kohdan sanamuoto sallii jonkin verran joustavuutta, ja valvontaviranomaisen akkreditointitoiminta olisi tulkittava tehtäväksi vain soveltuvin osin. Jäsenvaltioiden lainsäädännössä voidaan selkeyttää tätä kohtaa. Kansallisen akkreditointielimen suorittamassa akkreditointiprosessissa sertifiointielimen on kuitenkin 43 artiklan 2 kohdan a alakohdan mukaisesti osoitettava riippumattomuutensa ja asiantuntemuksensa tarjoamansa sertifiointimekanismin kohteeseen nähden toimivaltaista valvontaviranomaista tyydyttävällä tavalla.[16]

39. Jos jäsenvaltio määrää, että valvontaviranomaisen on akkreditoitava sertifiointielimet, valvontaviranomaisen olisi vahvistettava akkreditointivaatimukset, muun muassa 43 artiklan 2 kohdassa täsmennetyt vaatimukset. Kansallisten akkreditointielinten suorittamaan sertifiointielinten akkreditointiin liittyviin velvoitteisiin verrattuna 43 artiklassa annetaan vähemmän ohjeita akkreditointia koskevista vaatimuksista, kun valvontaviranomainen suorittaa akkreditoinnin itse. Akkreditointia koskevan yhdenmukaistetun lähestymistavan edistämiseksi valvontaviranomaisen käyttämien akkreditointikriteerien pohjana pitäisi olla standardi ISO/IEC 17065, ja niitä pitäisi täydentää valvontaviranomaisen 43 artiklan 1 kohdan b alakohdan mukaisesti vahvistamilla lisävaatimuksilla. Tietosuojaneuvosto huomauttaa, että 43 artiklan 2 kohdan a–e alakohdat perustuvat standardin ISO 17065 vaatimuksiin ja että niissä täsmennetään näitä vaatimuksia. Näin edistetään johdonmukaisuutta.

---

[16] Valvontaviranomaisen 43 artiklan 1 kohdan b alakohdan mukaisesti vahvistamissa lisävaatimuksissa olisi täsmennettävä riippumattomuutta ja asiantuntemusta koskevat vaatimukset. Ks. myös suuntaviivojen liite 1.

40. Jos jäsenvaltio määrää, että kansallisten akkreditointielinten on akkreditoitava sertifiointielimet, valvontaviranomaisen on vahvistettava lisävaatimuksia, joilla täydennetään asetuksessa (EY) N:o 765/2008 (jossa 3–14 artiklat liittyvät vaatimustenmukaisuuden arviointielinten akkreditoinnin järjestämiseen ja toimintaan) tarkoitettuja voimassa olevia akkreditointikäytäntöjä, ja teknisiä sääntöjä, joissa kuvataan sertifiointielinten menetelmät ja menettelyt. Asetuksessa (EY) N:o 765/2008 annetaan tämän osalta lisäohjeistusta: asetuksen 2 artiklan 10 kohdassa määritetään akkreditointi ja viitataan yhdenmukaistettuihin standardeihin ja muihin vaatimuksiin, mukaan luettuna niihin, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa. Sen vuoksi valvontaviranomaisen vahvistamien lisävaatimusten pitäisi sisältää erityisiä vaatimuksia, ja niissä pitäisi keskittyä muun muassa sertifiointielinten riippumattomuuden ja tietosuoja-asiantuntemuksen tason arvioinnin helpottamiseen. Tämä koskee esimerkiksi niiden kykyä arvioida ja sertifioida rekisterinpitäjien ja henkilötietojen käsittelijöiden henkilötietojenkäsittelytoimia 42 artiklan 1 kohdan mukaisesti. Tämä sisältää alakohtaisissa ohjelmissa vaaditun pätevyyden luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojelun ja erityisesti heidän henkilötietojen suojaa koskevan oikeutensa osalta.[17] Näiden suuntaviivojen liitteestä voi olla apua toimivaltaisille valvontaviranomaisille niiden vahvistaessa lisävaatimuksia 43 artiklan 1 kohdan b alakohdan ja 3 kohdan mukaisesti.

41. Tietosuoja-asetuksen 43 artiklan 6 kohdan mukaan ”[v]alvontaviranomainen julkistaa tämän artiklan 3 kohdassa tarkoitetut vaatimukset ja 42 artiklan 5 kohdassa tarkoitetut kriteerit helposti saatavilla olevassa muodossa”. Näin ollen kaikki valvontaviranomaisen hyväksymät kriteerit ja vaatimukset on julkaistava avoimuuden takaamiseksi. Sertifiointielinten laadun ja niiden nauttiman luottamuksen kannalta olisi toivottavaa, että kaikki akkreditointia koskevat vaatimukset olisivat heti yleisön saatavilla.

4.5 Sertifiointielimenä toimiva valvontaviranomainen

42. Tietosuoja-asetuksen 42 artiklan 5 kohdan mukaan valvontaviranomainen voi myöntää sertifiointeja, mutta asetuksessa siltä ei edellytetä akkreditointia asetuksen (EY) N:o 765/2008 vaatimusten täyttämiseksi. Tietosuojaneuvosto huomauttaa, että valvontaviranomaisilla on 43 artiklan 1 kohdan a alakohdan ja erityisesti 58 artiklan 2 kohdan h alakohdan ja 3 kohdan a, e ja f alakohdan nojalla valtuudet suorittaa sekä akkreditointeja että sertifiointeja, antaa neuvoja, tarvittaessa peruuttaa sertifiointeja ja kieltää sertifiointielintä antamasta sertifiointia.

43. Joissakin tilanteissa akkreditointi- ja sertifiointitehtävien ja -velvollisuuksien erottaminen on asianmukaista tai tarpeellista, esimerkiksi silloin, jos jäsenvaltiossa on sekä valvontaviranomainen että muita sertifiointielimiä ja molemmat myöntävät samanlaisia sertifiointeja. Valvontaviranomaisten olisi sen vuoksi toteutettava riittäviä organisatorisia toimenpiteitä tietosuoja-asetuksen mukaisten tehtävien erottamiseksi, jotta sertifiointimekanismien käyttö voidaan vakiinnuttaa ja sitä voidaan helpottaa. Samalla niiden olisi toteutettava varotoimenpiteitä näistä tehtävistä mahdollisesti johtuvien eturistiriitojen välttämiseksi. Jäsenvaltioiden ja valvontaviranomaisten olisi lisäksi pidettävä mielessä yhdenmukaistettu EU:n taso, kun ne muotoilevat kansallisia lakeja ja menettelyjä, jotka liittyvät tietosuoja-asetuksen mukaiseen akkreditointiin ja sertifiointiin.

4.6 Akkreditointivaatimukset

[17] Tietosuoja-asetuksen 1 artiklan 2 kohta.

44. Näiden suuntaviivojen liitteessä on ohjeistusta siitä, miten akkreditoinnin lisävaatimukset voidaan määrittää. Siinä esitetään tietosuoja-asetuksen asiaankuuluvat säännökset ja ehdotetaan vaatimuksia, jotka valvontaviranomaisten ja kansallisten akkreditointielinten olisi otettava huomioon tietosuoja-asetuksen noudattamisen varmistamiseksi.

45. Kuten edellä todetaan, jos kansallinen akkreditointielin akkreditoi sertifiointielimet asetuksen (EY) N:o 765/2008 mukaisesti, asiaankuuluva akkreditointistandardi on ISO/IEC 17065/2012, jota täydennetään valvontaviranomaisen vahvistamilla lisävaatimuksilla. Tietosuoja-asetuksen 43 artiklan 2 kohta perustuu standardin ISO/IEC 17065/2012 yleisiin määräyksiin, ja siinä otetaan huomioon asetuksen mukainen perusoikeuksien suoja. Liitteen kehyksessä käytetään 43 artiklan 2 kohtaa ja standardia ISO/IEC 17065/2012 perustana vaatimusten määrittämiselle sekä lisäkriteereille, jotka liittyvät sertifiointielinten tietosuoja-asiantuntemuksen sekä sen arviointiin, pystyvätkö ne kunnioittamaan tietosuoja-asetukseen kirjattuja henkilötietojen käsittelyä koskevia luonnollisten henkilöiden oikeuksia ja vapauksia. Tietosuojaneuvosto huomauttaa, että se keskittyy erityisesti varmistamaan, että sertifiointielimillä on asianmukainen tietosuoja-asiantuntemuksen taso 43 artiklan 1 kohdan mukaisesti.

46. Valvontaviranomaisen vahvistamia akkreditoinnin lisävaatimuksia sovelletaan kaikkiin akkreditointia pyytäviin sertifiointielimiin. Akkreditointielin arvioi, onko kyseinen sertifiointielin pätevä suorittamaan sertifiointitoimintaa lisävaatimusten ja sertifioinnin kohteen mukaisesti. Arvioinnissa viitataan niihin sertifioinnin erityisiin aloihin tai alueisiin, joille sertifiointielin akkreditoidaan.

47. Tietosuojaneuvosto huomauttaa myös, että standardin ISO/IEC 17065/2012 vaatimusten lisäksi tarvitaan myös erityisasiantuntemusta tietosuojan alalla, jos muut ulkopuoliset elimet, kuten laboratoriot tai auditoijat, suorittavat akkreditoidun sertifiointielimen puolesta sertifiointitoiminnan osia tai komponentteja. Tällöin ulkopuolisten elinten akkreditointi tietosuoja-asetuksen mukaisesti ei ole mahdollista. Jotta näiden elinten sopivuus toimimiseen akkreditoitujen sertifiointielinten puolesta voitaisiin varmistaa, akkreditoidun sertifiointielimen on varmistettava, että myös kyseisellä ulkopuolisella elimellä on todistetusti akkreditoidulta elimeltä vaadittu tietosuoja-asiantuntemus asiaankuuluvan toiminnan osalta.

48. Näiden suuntaviivojen liitteessä esitettyjen akkreditoinnin lisävaatimusten määrittämiskehys ei ole menettelykäsikirja kansallisen akkreditointielimen tai valvontaviranomaisen suorittamaa akkreditointiprosessia varten. Siinä annetaan ohjeita rakenteesta ja menetelmistä, ja se on siten työkalupakki valvontaviranomaisille akkreditoinnin lisävaatimusten määrittämiseksi.

LIITE 1

Liitteessä 1 annetaan ohjeita akkreditoinnin lisävaatimusten määrittelyä varten standardin ISO/IEC 17065/2012 osalta tietosuoja-asetuksen 43 artiklan 1 kohdan b alakohdan ja 3 kohdan mukaisesti.

Tässä liitteessä esitetään ehdotetut vaatimukset, jotka tietosuojavalvontaviranomaisen on laadittava ja joita sovelletaan kansallisen akkreditointielimen tai toimivaltaisen valvontaviranomaisen suorittamassa akkreditoinnissa.[18] Nämä lisävaatimukset on ilmoitettava tietosuojaneuvostolle ennen niiden hyväksymistä 64 artiklan 1 kohdan c alakohdan mukaisesti.

Tätä liitettä olisi luettava yhdessä standardin ISO/IEC 17065/2012 kanssa. Liitteessä käytetty kohtien numerointi vastaa standardin ISO/IEC 17065/2012 kohtien numeroita. Kun akkreditoinnin suorittavat valvontaviranomaiset 43 artiklan 1 kohdan a alakohdan nojalla, hyvä käytäntö olisi noudattaa tätä lähestymistapaa aina, kun se on tarkoituksenmukaista. Tämä tukee EU:n yhdenmukaistettua akkreditointia.

Toimivaltainen valvontaviranomainen voi kansallisen lainsäädännön salliessa määrittää muitakin lisävaatimuksia mistä tahansa standardiin ISO/IEC 17065/2012 kuuluvasta asiasta riippumatta seuraavista sitä koskevista ohjeista tai niiden puuttumisesta.

0 ALKUSANAT

[Tässä kohdassa esitetään kansallisen akkreditointielimen ja tietosuojavalvontaviranomaisen mahdollisesti sopimat yhteistyöehdot, esim. kuka vastaa hakemusten vastaanottamisesta tai miten hyväksytyt kriteerit tunnustetaan akkreditointiprosessissa.]

1 SOVELTAMISALA[19]

Standardin ISO/IEC 17065/2012 soveltamisalaa sovelletaan tietosuoja-asetuksen mukaisesti. Lisätietoa on akkreditointia ja sertifiointia koskevissa suuntaviivoissa. Sertifiointimekanismin soveltamisala (esim. käsittelytoimia suorittavan pilvipalvelun sertifiointi) olisi otettava huomioon kansallisen akkreditointielimen ja toimivaltaisen valvontaviranomaisen suorittamassa arvioinnissa akkreditointimenettelyn aikana. Tämä koskee erityisesti kriteerejä, asiantuntemusta ja arviointimenetelmiä. Standardin ISO/IEC 17065/2012 laaja soveltamisala, joka kattaa tuotteet, prosessit ja palvelut, ei saisi alentaa tai syrjäyttää tietosuoja-asetuksen vaatimuksia. Niinpä esimerkiksi hallintamekanismi ei voi olla sertifiointimekanismin ainoa osatekijä, koska sertifioinnin on katettava myös henkilötietojen käsittely eli käsittelytoimet. Tietosuoja-asetuksen 42 artiklan 1 kohdan mukaisesti tietosuojaa koskevaa sertifiointia sovelletaan ainoastaan rekisterinpitäjien ja henkilötietojen käsittelijöiden käsittelytoimiin.

[18] Sertifiointikriteerien hyväksymisprosessi, ks. sertifiointia koskevien suuntaviivojen kohta 4.
[19] Numerointi viittaa standardiin ISO/IEC 17065/2012.

2 VIITTAUKSET SÄÄNNÖKSIIN JA MÄÄRÄYKSIIN

Tietosuoja-asetus on ensisijainen standardiin ISO/IEC 17065/2012 nähden. Jos lisävaatimuksissa tai sertifiointimekanismissa viitataan muihin ISO-standardeihin, niitä on tulkittava tietosuoja-asetuksessa vahvistettujen vaatimusten mukaisesti.

3 TERMIT JA MÄÄRITELMÄT

Tässä liitteessä sovelletaan akkreditoinnista annetuissa suuntaviivoissa (WP 261) ja sertifioinnista annetuissa suuntaviivoissa (EDPB 1/2018) käytettyjä termejä ja määritelmiä, ja ne ovat ensisijaisia ISO-määritelmiin nähden.

4 YLEISET AKKREDITOINTIVAATIMUKSET

4.1 Oikeudelliset asiat ja sopimusasiat

4.1.1 Oikeudellinen vastuu

Sertifiointielimen olisi voitava osoittaa kansalliselle akkreditointielimelle tai toimivaltaiselle valvontaviranomaiselle (milloin tahansa), että sillä on käytössään ajantasaiset menettelyt, joilla se osoittaa noudattavansa akkreditointiehdoissa vahvistettuja oikeudellisia velvollisuuksia, mukaan lukien asetuksen (EU) 2016/679 soveltamista koskevat lisävaatimukset. Koska sertifiointielin on itse rekisterinpitäjä tai henkilötietojen käsittelijä, se on voitava osoittaa, että sen menettelyt ja toimenpiteet ovat asetuksen (EU) 2016/679 mukaisia varsinkin sen rekisteröidessä ja käsitellessä asiakasorganisaation henkilötietoja osana sertifiointiprosessia.

Toimivaltainen valvontaviranomainen voi päättää lisätä vaatimuksia ja menettelyjä tarkistaakseen ennen akkreditointia, että sertifiointielimet noudattavat yleistä tietosuoja-asetusta

4.1.2 Sertifiointisopimus

Sertifiointisopimuksen vähimmäisvaatimuksia on täydennettävä seuraavassa luetelluilla seikoilla.

Sertifiointielimen on osoitettava standardin ISO/IEC 17065/2012 vaatimusten lisäksi, että sen sertifiointisopimuksissa

1. edellytetään hakijan aina noudattavan sekä standardin ISO/IEC 17065/2012 kohdan 4.1.2.2 alakohdassa a tarkoitettuja yleisiä sertifiointivaatimuksia että toimivaltaisen valvontaviranomaisen tai tietosuojaneuvoston 43 artiklan 2 kohdan b alakohdan ja 5 kohdan mukaisesti hyväksymiä kriteerejä;
2. edellytetään hakijan sallivan toimivaltaiselle valvontaviranomaiselle täyden avoimuuden sertifiointimenettelyn suhteen, mukaan lukien tietosuojan noudattamiseen 42 artiklan 7 kohdan ja 58 artiklan 1 kohdan c alakohdan mukaisesti liittyvät luottamukselliset sopimusasiat;
3. ei kavenneta hakijan vastuuta noudattaa asetusta (EU) 2016/679 eikä rajoiteta 42 artiklan 5 kohdan nojalla toimivaltaisen valvontaviranomaisen tehtäviä ja valtuuksia;
4. edellytetään hakijan toimittavan sertifiointielimelle 42 artiklan 6 kohdan mukaisesti kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot sekä pääsyn käsittelytoimiinsa;

5. edellytetään hakijan noudattavan asiassa sovellettavia määräaikoja ja menettelyjä. Sertifiointisopimuksessa on määrättävä, että esimerkiksi sertifiointiohjelmasta tai muista määräyksistä johtuvia määräaikoja ja menettelyjä on noudatettava;
6. vahvistetaan standardin ISO/IEC 17065/2012 kohdan 4.1.2.2 alakohdan c alakohdan 1 osalta pätevyyttä, uusimista ja peruuttamista koskevat säännöt 42 artiklan 7 kohdan ja 43 artiklan 4 kohdan mukaisesti, mukaan lukien säännöt uudelleenarvioinnin tai tarkastelun tarkoituksenmukaisista määräajoista (säännöllisyys) 42 artiklan 7 kohdan mukaisesti;
7. sallitaan sertifiointielimen luovuttaa kaikki sertifioinnin myöntämiseen tarvittavat tiedot 42 artiklan 8 kohdan ja 43 artiklan 5 kohdan mukaisesti;
8. on säännöt tarvittavista varotoimista valitusten tutkimiseksi kohdan 4.1.2.2 alakohdan c alakohdassa 2 ja lisäksi alakohdassa j tarkoitetulla tavalla sekä yksiselitteisiä lausuntoja valitusten käsittelyn rakenteesta ja menettelystä 43 artiklan 2 kohdan d alakohdan mukaisesti;
9. olisi standardin ISO/IEC 17065/2012 kohdassa 4.1.2.2 tarkoitettujen vähimmäisvaatimusten lisäksi käsiteltävä kaikkia asiakkaalle koituvia seurauksia, jos sertifiointielimen akkreditoinnin peruuttamisen tai lykkäämisen seuraukset vaikuttavat asiakkaaseen;
10. edellytetään hakijaa ilmoittamaan sertifiointielimelle merkittävistä muutoksista sen tosiasialliseen tai oikeudelliseen tilanteeseen sekä sertifioinnin kohteena oleviin tuotteisiinsa, prosesseihinsa ja palveluihinsa.

4.1.3 Tietosuojasinettien ja -merkkien käyttö

Sertifikaattien, sinettien ja merkkien käytössä on noudatettava 42 ja 43 artiklaa sekä akkreditoinnista ja sertifioinnista annettuja suuntaviivoja.

4.2 Puolueettomuuden hallinta

Akkreditointielimen on varmistettava, että standardin ISO/IEC 17065/2012 kohdassa 4.2 olevan vaatimuksen lisäksi

1. sertifiointielin noudattaa toimivaltaisen valvontaviranomaisen lisävaatimuksia (43 artiklan 1 kohdan b alakohdan mukaisesti)
    a. toimittaa 43 artiklan 2 kohdan a alakohdan mukaisesti erillisen näytön riippumattomuudestaan. Tämä koskee erityisesti näyttöä sertifiointielimen rahoituksesta siltä osin kuin on kyse puolueettomuusvakuutuksesta;
    b. sen tehtävät ja velvollisuudet eivät johda eturistiriitaan 43 artiklan 2 kohdan e alakohdan mukaisesti;
2. sertifiointielimellä ei ole merkityksellistä kytköstä arvioimaansa asiakkaaseen.

4.3 Korvausvastuu ja rahoitus

Akkreditointielimen on standardin ISO/IEC 17065/2012 kohdassa 4.3.1 esitetyn vaatimuksen lisäksi varmistettava säännöllisesti, että sertifiointielimellä on käytössään asianmukaiset toimenpiteet (esim. vakuutus tai vararahasto) korvausvastuunsa kattamiseksi niillä maantieteellisillä alueilla, joilla se toimii.

4.4 Syrjimättömyyttä koskevat ehdot

Valvontaviranomainen voi laatia lisävaatimuksia kansallisen lainsäädännön sen salliessa.

4.5 Luottamuksellisuus

Valvontaviranomainen voi laatia lisävaatimuksia kansallisen lainsäädännön sen salliessa.

4.6 Julkisesti saatavilla olevat tiedot

Akkreditointielimen on standardin ISO/IEC 17065/2012 kohdassa 4.6 esitetyn vaatimuksen lisäksi edellytettävä sertifiointielimeltä vähintäänkin, että

1. kaikki hyväksyttyjen, 42 artiklan 5 kohdassa tarkoitetulla tavalla käytettyjen kriteerien (voimassa olevat ja aikaisemmat) versiot samoin kuin kaikki sertifiointimenettelyt julkaistaan, että ne ovat julkisesti helposti saatavilla ja että niissä ilmoitetaan yleensä niiden voimassaoloaika;
2. tiedot valitusten käsittelymenettelyistä ja muutoksenhausta julkaistaan 43 artiklan 2 kohdan d kohdan mukaisesti.

5 RAKENTEELLISET VAATIMUKSET, 43 ARTIKLAN 4 KOHTA [ASIANMUKAINEN ARVIOINTI]

5.1 Organisaatiorakenne ja ylin johto

Valvontaviranomainen voi laatia lisävaatimuksia.

5.2 Mekanismit puolueettomuuden takaamiseksi

Valvontaviranomainen voi laatia lisävaatimuksia.

6 RESURSSIVAATIMUKSET

6.1 Sertifiointielimen henkilöstö

Akkreditointielimen on standardin ISO/IEC 17065/2012 kohdassa 6 esitetyn vaatimuksen lisäksi varmistettava, että kunkin sertifiointielimen henkilöstön jäsenet

1. ovat osoittaneet omaavansa tietosuojaan liittyvää asianmukaista ja ajantasaista asiantuntemusta (tietämystä ja kokemusta) 43 artiklan 1 kohdan mukaisesti;
2. ovat riippumattomia, heillä on ajantasaista asiantuntemusta sertifioinnin kohteesta 43 artiklan 2 kohdan a alakohdan mukaisesti ja heillä ei ole eturistiriitoja 43 artiklan 2 kohdan e alakohdan mukaisesti;
3. sitoutuvat 43 artiklan 2 kohdan b alakohdan mukaisesti noudattamaan 42 artiklan 5 kohdassa tarkoitettuja kriteerejä;
4. omaavat asianmukaista tietämystä ja kokemusta tietosuojalainsäädännön soveltamisesta;
5. omaavat asianmukaista tietämystä ja kokemusta tietosuojaan liittyvistä teknisistä ja organisatorista toimenpiteistä tilanteen mukaan;
6. pystyvät osoittamaan, että heillä on kokemusta lisävaatimuksissa 6.1.1, 6.1.4 ja 6.1.5 mainituilta aloilta.

Teknistä asiantuntemusta omaava henkilöstö:

- Henkilöstön jäsenillä on oltava asianomaisella teknisen asiantuntemuksen alalla vähintään 6. tason EQF-pätevyys[20] tai asianomaiseen säänneltyyn ammattiin liittyvä tunnustettu ja suojattu ammattinimike (esim. diplomi-insinööri) tai huomattavaa ammattikokemusta.
- *Sertifiointipäätöksistä vastaavan henkilöstön* jäsenillä on oltava huomattavaa ammattikokemusta tietosuojatoimenpiteiden määrittelystä ja toteuttamisesta.
- *Arvioinneista vastaavan henkilöstön* jäsenillä on oltava ammattikokemusta tietojen teknisestä suojaamisesta sekä tietämystä ja kokemusta vastaavasta menettelystä (esim. sertifioinnit/tarkastukset) ja heidän on oltava rekisteröityjä asiassa sovellettavien vaatimusten mukaisesti.

Henkilöstön jäsenten on ammattitaitoaan jatkuvasti kehittämällä osoitettava ylläpitävänsä alakohtaista teknistä ja tarkastuksiin liittyvä osaamista.

Oikeudellista asiantuntemusta omaava henkilöstö:

- Oikeustieteen opintoja EU:n tai valtion hyväksymässä yliopistossa vähintään kahdeksan lukukauden ajalta, mukaan lukien maisteritutkinto (LLM) tai vastaava, tai huomattavaa ammattikokemusta.
- *Sertifiointipäätöksistä vastaavan henkilöstön* jäsenten on osoitettava, että heillä on huomattavaa ammattikokemusta tietosuojaoikeudesta, ja heidän on oltava rekisteröityjä jäsenvaltion vaatimusten mukaisesti.
- *Arvioinneista vastaavan henkilöstön* jäsenten on osoitettava, että heillä on vähintään kahden vuoden ammattikokemus tietosuojaoikeudesta sekä tietämystä ja kokemusta vastaavista menettelyistä (esim. sertifioinnit/tarkastukset), ja heidän on oltava rekisteröityjä, jos jäsenvaltio sitä edellyttää.
    - Henkilöstön jäsenten on ammattitaitoaan jatkuvasti kehittämällä osoitettava ylläpitävänsä alakohtaista teknistä ja tarkastuksiin liittyvä osaamista.

6.2 Arviointiresurssit

Valvontaviranomainen voi laatia lisävaatimuksia kansallisen lainsäädännön sen salliessa.

7 PROSESSIVAATIMUKSET, 43 ARTIKLAN 2 KOHDAN C JA D ALAKOHTA

7.1 Yleistä

Akkreditointielimen on standardin ISO/IEC 17065/2012 kohdassa 7.1 esitetyn vaatimuksen lisäksi

1. varmistettava, että sertifiointielimet noudattavat hakemusta jättäessään toimivaltaisen valvontaviranomaisen lisävaatimuksia (43 artiklan 1 kohdan b alakohdan mukaisesti), jotta tehtävät ja velvollisuudet eivät johda eturistiriitaan 43 artiklan 2 kohdan b alakohdan mukaisesti;
2. ilmoitettava asianomaiselle toimivaltaiselle valvontaviranomaiselle ennen kuin sertifiointielin alkaa käyttää hyväksyttyä eurooppalaista tietosuojasinettiä uudessa jäsenvaltiossa sivutoimistosta käsin.

7.2 Hakemus

Standardin ISO/IEC 17065/2012 kohdassa 7.2 esitetyn lisäksi on edellytettävä, että hakemuksessa

[20] Ks. tutkintojen ja tutkintotasojen vertailuun tarkoitettu väline osoitteessa https://ec.europa.eu/ploteus/en/compare?

1. kuvataan sertifioinnin kohde (arvioinnin kohde) yksityiskohtaisesti. Tämä käsittää myös rajapinnat, siirrot muihin järjestelmiin ja järjestöihin, protokollat ja muut takeet;
2. täsmennetään, käytetäänkö henkilötietojen käsittelijöitä, ja kuvataan heidän vastuunsa ja tehtävänsä, jos hakija on henkilötietojen käsittelijä. Lisäksi hakemuksen on sisällettävä asiaankuuluvat rekisterinpitäjän tai henkilötietojen käsittelijän sopimus/sopimukset.

7.3 Hakemuksen tarkastelu

Standardin ISO/IEC 17065/2012 kohdassa 7.3 esitetyn lisäksi on edellytettävä, että

1. sertifiointisopimuksessa määrätään sitovista arviointimenetelmistä arvioinnin kohteen osalta;
2. asiantuntemuksen riittävyyttä koskevassa kohdan 7.3 alakohdassa e tarkoitetussa arvioinnissa otetaan huomioon sekä tekninen että oikeudellinen asiantuntemus tietosuojasta tarkoituksenmukaisessa laajuudessa.

7.4 Arviointi

Standardin ISO/IEC 17065/2012 kohdassa 7.4 esitetyn lisäksi sertifiointimekanismeissa on kuvattava riittävät menetelmät sen arvioimiseen, täyttävätkö käsittelytoimet sertifiointikriteerit, soveltuvin osin esimerkiksi seuraavat:

1. menetelmä käsittelytoimien tarpeellisuuden ja oikeasuhteisuuden arvioimiseksi niiden tarkoitukseen ja asianomaisiin rekisteröityihin nähden;
2. menetelmä kaikkien rekisterinpitäjän ja henkilötietojen käsittelijän tarkastelemien riskien laajuuden, sisällön ja arvioinnin arvioimiseksi oikeudellisten seuraamusten osalta tietosuoja-asetuksen 30, 32, 35 ja 36 artiklan mukaisesti ja teknisten ja organisatoristen toimenpiteiden määrittelyn osalta tietosuoja-asetuksen 24, 25 ja 32 artiklan mukaisesti, siltä osin kuin edellä mainittuja artikloja sovelletaan sertifioinnin kohteeseen, ja
3. menetelmä oikeussuojakeinojen arvioimiseksi, mukaan lukien takeet, suojatoimet ja menetelmät, joilla varmistetaan, että henkilötiedot suojataan, kun niiden käsittely liittyy sertifioinnin kohteeseen, sekä sen osoittamiseksi, että kriteerien oikeudelliset vaatimukset täyttyvät; sekä
4. menetelmiä koskevat asiakirjat ja päätelmät.

Sertifiointielin olisi velvoitettava varmistamaan, että nämä arviointimenetelmät on standardoitu ja että niitä sovelletaan yleisesti. Tämä tarkoittaa, että vastaavia arviointimenetelmiä käytetään vastaavanlaisissa arvioinnin kohteissa. Sertifiointielimen on perusteltava kaikki poikkeamat tästä menetelmästä.

Standardin ISO/IEC 17065/2012 kohdassa 7.4.2 esitetyn lisäksi arviointi olisi sallittava ulkopuolisille asiantuntijoille, jotka sertifiointielin on tunnustanut.

Standardin ISO/IEC 17065/2012 kohdassa 7.4.5 esitetyn lisäksi olisi mahdollistettava se, että voimassa olevaan sertifiointiin sisällytetään tietosuoja-asetuksen 42 ja 43 artiklan mukaisesti sellainen tietosuojaa koskeva sertifiointi, joka kattaa jo osan sertifioinnin kohteesta. Se ei kuitenkaan riitä korvaamaan (osittaisia) arviointeja kokonaan. Sertifiointielin on velvollinen tarkastamaan, että kriteerejä noudatetaan. Tunnustaminen edellyttää joka tapauksessa, että saatavilla on koko arviointikertomus tai tietoja, joiden avulla voidaan arvioida edellistä sertifiointitoimintoa ja sen tuloksia. Sertifiointilausuntoa tai vastaavaa sertifiointitodistusta ei tulisi pitää asiakirjana, jolla kertomus voidaan korvata.

Standardin ISO/IEC 17065/2012 kohdassa 7.4.6 esitetyn lisäksi sertifiointielin olisi velvoitettava esittämään sertifiointimekanismissaan yksityiskohtaisesti, miten kohdassa 7.4.6 vaadittavat tiedot auttavat asiakasta (sertifioinnin hakijaa) ymmärtämään poikkeamia sertifiointimekanismista. Tässä yhteydessä olisi määriteltävä ainakin tällaisten tietojen luonne ja ajoitus.

Standardin ISO/IEC 17065/2012 kohdassa 7.4.9 esitetyn lisäksi olisi vaadittava, että tietosuojavalvontaviranomainen saa pyynnöstä käyttöönsä kaikki asiakirjat ilman rajoituksia.

7.5 Tarkastelu

Standardin ISO/IEC 17065/2012 kohdassa 7.5 esitetyn lisäksi vaaditaan menettelyt sertifiointien myöntämistä, määräaikaistarkastelua ja peruuttamista varten 43 artiklan 2 ja 3 kohdan mukaisesti.

7.6 Sertifiointipäätös

Standardin ISO/IEC 17065/2012 kohdassa 7.6.1 esitetyn lisäksi sertifiointielin olisi velvoitettava esittämään menettelyissään yksityiskohtaisesti, miten sen riippumattomuus ja vastuu varmistetaan yksittäisissä sertifiointipäätöksissä.

7.7 Sertifiointiasiakirjat

Standardin ISO/IEC 17065/2012 kohdan 7.7.1. alakohdassa e esitetyn lisäksi ja tietosuoja-asetuksen 42 artiklan 7 kohdan mukaisesti olisi vaadittava, että sertifioinnin voimassaoloaika ei ylitä kolmea vuotta.

Standardin ISO/IEC 17065/2012 kohdan 7.7.1. alakohdassa e esitetyn lisäksi olisi vaadittava, että myös aiotun, kohdassa 7.9 tarkoitetun seurannan ajankohta dokumentoidaan.

Standardin ISO/IEC 17065/2012 kohdan 7.7.1. alakohdassa f esitetyn lisäksi sertifiointielin olisi velvoitettava nimeämään sertifioinnin kohde sertifiointiasiakirjoissa (ja ilmoittamaan tarvittaessa niiden versio tai vastaavat ominaisuudet).

7.8 Sertifioitujen tuotteiden hakemisto

Standardin ISO/IEC 17065/2012 kohdassa 7.8 esitetyn lisäksi sertifiointielin olisi velvoitettava pitämään sertifioituja tuotteita, prosesseja ja palveluja koskevat tiedot sisäisesti ja julkisesti saatavilla. Sertifiointielin toimittaa julkisesti saataville tiivistelmän arviointikertomuksesta. Tiivistelmän tarkoituksena on lisätä avoimuutta siitä, mitä on sertifioitu ja miten se on arvioitu. Siinä selitetään muun muassa seuraavat:

a) sertifioinnin soveltamisala ja kuvaus sertifioinnin kohteesta (arvioinnin kohde),

b) asiassa sovellettavat sertifiointikriteerit (ml. versio tai toiminnallinen status),

c) arviointimenetelmät ja tehdyt testit, ja

d) tulos/tulokset.

Standardin ISO/IEC 17065/2012 kohdassa 7.8 esitetyn lisäksi ja tietosuoja-asetuksen 43 artiklan 5 kohdan mukaisesti sertifiointielimen on ilmoitettava toimivaltaisille valvontaviranomaisille syyt sertifioinnin myöntämiselle tai peruuttamiselle.

7.9 Valvonta

Standardin ISO/IEC 17065/2012 kohtien 7.9.1, 7.9.2 ja 7.9.3 lisäksi ja tietosuoja-asetuksen 43 artiklan 2 kohdan c alakohdan mukaisesti olisi vaadittava, että säännölliset seurantatoimenpiteet ovat pakollisia sertifioinnin säilyttämiseksi seurantajakson ajan.

7.10 Sertifiointiin vaikuttavat muutokset

Standardin EN ISO/IEC 17065/2012 kohdissa 7.10.1 ja 7.10.2 esitetyn lisäksi sertifiointielimen on tarkasteltava seuraavia sertifiointiin vaikuttavia muutoksia: muutokset tietosuojalainsäädäntöön, 43 artiklan 8 ja 9 kohdan mukaisesti annetut Euroopan komission delegoidut säädökset, tietosuojaneuvoston päätökset ja tietosuojaan liittyvät tuomioistuimen päätökset. Muutosmenettelyistä on sovittava, ja ne voivat käsittää esimerkiksi siirtymäkaudet, toimivaltaisen valvontaviranomaisen suorittaman hyväksyntämenettelyn, sertifiointikohteen uudelleenarvioinnin ja aiheelliset toimenpiteet sertifioinnin peruuttamiseksi, jos sertifioitu käsittelytoimi ei enää täytä ajantasaisia kriteerejä.

7.11 Sertifioinnin päättäminen, rajoittaminen, keskeyttäminen ja peruuttaminen

Standardin ISO/IEC 17065/2012 kohdassa 7.11.1 esitetyn lisäksi sertifiointielin olisi velvoitettava ilmoittamaan toimivaltaiselle valvontaviranomaiselle ja tarvittaessa kansalliselle akkreditointielimelle toteutetuista toimenpiteistä sekä sertifioinnin jatkamisesta, rajoittamisesta, keskeyttämisestä ja peruuttamisesta välittömästi ja kirjallisesti.

Sertifiointielimen on 58 artiklan 2 kohdan h alakohdan mukaisesti hyväksyttävä toimivaltaisen valvontaviranomaisen päätökset ja määräykset peruuttaa sertifiointi tai olla myöntämättä sitä asiakkaalle (hakijalle), jos sertifiointivaatimus ei (enää) täyty.

7.12 Arkisto

Sertifiointielin olisi velvoitettava säilyttämään kaikki asiakirjat täydellisinä, ymmärrettävinä, ajantasaisina ja tarkastuskelpoisina.

7.13 Valitukset ja muutoksenhaut, 43 artiklan 2 kohdan d alakohta

Standardin ISO/IEC 17065/2012 kohdassa 7.13.1 esitetyn lisäksi sertifiointielin olisi velvoitettava määrittelemään,

a) kuka voi tehdä valituksia tai esittää vastalauseita,

b) kuka sertifiointielimessä voi käsitellä ne,

c) mitä varmistuksia siinä yhteydessä tehdään ja

d) mitkä ovat asianomaisten osapuolten mahdollisuudet tulla kuulluiksi.

Standardin ISO/IEC 17065/2012 kohdassa 7.13.2 esitetyn lisäksi sertifiointielin olisi velvoitettava määrittelemään,

a) miten ja kenelle vahvistus on annettava,

b) vahvistamisen määräajat ja

c) mitä prosesseja on jälkeenpäin käynnistettävä.

Standardin ISO/IEC 17065/2012 kohdassa 7.13.1 esitetyn lisäksi sertifiointielimen on määriteltävä, miten sertifiointi ja muutoksenhakujen ja valitusten käsittely pidetään erillisinä toimintoina.

8 HALLINTAJÄRJESTELMÄN VAATIMUKSET

Hallintajärjestelmän yleisvaatimuksena on standardin ISO/IEC 17065/2012 luvun 8 mukaan se, että akkreditoitu sertifiointielin täyttää kaikki edeltävien lukujen vaatimukset sertifiointimekanismin soveltamisalalla ja että vaatimusten täyttäminen dokumentoidaan ja sitä arvioidaan, valvotaan ja seurataan riippumattomasti.

Hallinnan perusperiaatteena on määritellä järjestelmä, jonka mukaan sen tavoitteet asetetaan tuloksellisesti ja tehokkaasti. Tavoitteena on varsinkin sertifiointipalvelujen suorittaminen tarkoitustenmukaisten eritelmien avulla. Tämä edellyttää, että akkreditointivaatimusten täyttäminen sertifiointielimen toimesta on avointa ja todennettavissa ja että vaatimuksia noudatetaan koko ajan.

Tätä tarkoitusta varten hallintajärjestelmässä on täsmennettävä menetelmät kyseisten vaatimusten täyttämiseksi ja valvomiseksi tietosuojamääräyksiä noudattaen sekä niiden tarkastamiseksi jatkuvasti yhdessä akkreditoidun elimen kanssa.

Näiden hallinnointiperiaatteiden ja niiden dokumentoidun noudattamisen on oltava avointa ja akkreditoidun sertifiointielimen on ilmoitettava siitä akkreditointimenettelyn ja 58 artiklan mukaisesti ja sen jälkeen tietosuojavalvontaviranomaisen pyynnöstä milloin tahansa tietosuojaa koskevien tarkastelujen muodossa tehtävän tutkimuksen aikana 58 artiklan 1 kohdan b alakohdan mukaisesti tai 42 artiklan 7 kohdan mukaisesti myönnetyn sertifioinnin uudelleentarkastelun aikana 58 artiklan 1 kohdan c alakohdan mukaisesti.

Akkreditoidun sertifiointielimen on pidettävä jatkuvasti ja pysyvällä tavalla julkisesti saatavilla tiedot siitä, mitkä sertifioinnit on suoritettu milläkin perusteella (tai mitä sertifiointimekanismia tai -ohjelmaa käyttäen), miten pitkään sertifioinnit ovat voimassa missäkin kehyksessä ja millä edellytyksin (johdanto-osan 100 kappale).

8.1 Hallintajärjestelmän yleiset vaatimukset

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.2 Hallintajärjestelmän dokumentointi

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.3 Asiakirjojen hallinta

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.4 Arkiston hallinta

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.5 Hallintajärjestelmän uudelleentarkastelu

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.6 Sisäiset tarkastukset

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.7 Korjaavat toimenpiteet

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

8.8 Ennaltaehkäisevät toimenpiteet

Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.

9 YLIMÄÄRÄISET LISÄVAATIMUKSET21

9.1 Arviointimenetelmien päivittäminen

Sertifiointielimen on laadittava menettelyt kohdassa 7.4 tarkoitetun arvioinnin yhteydessä sovellettavien arviointimenetelmien päivittämiseen. Menetelmiä on päivitettävä aina, kun oikeudellinen kehys, asiaankuuluva(t) riski(t) ja teknisten ja organisatoristen toimenpiteiden tekniikan taso ja täytäntöönpanokustannukset muuttuvat.

9.2 Asiantuntemuksen ylläpitäminen

Sertifiointielinten on laadittava menettelyt työntekijöidensä koulutuksen varmistamiseksi, jotta he voivat päivittää osaamistaan kohdassa 9.1 mainitut muutokset huomioon ottaen.

9.3 Vastuut ja toimivaltuudet

9.3.1 Sertifiointielimen ja sen asiakkaiden välinen viestintä

On vahvistettava menettelyt asianmukaisten menettelyjen ja viestintärakenteiden käyttöön ottamiseksi sertifiointielimen ja sen asiakkaiden välillä. Tähän on kuuluttava

1. tehtävien ja vastuiden dokumentoinnista huolehtiminen akkreditoidun sertifiointielimen toimesta seuraavia tarkoituksia varten:
    a. tietopyynnöt,
    b. yhteydenpito siinä tapauksessa, että sertifioinnista tehdään valitus;
2. hakuprosessista huolehtiminen seuraavia tarkoituksia varten:
    a. hakemuksen käsittelyvaiheesta tiedottaminen,
    b. toimivaltaisen valvontaviranomaisen tekemät arvioinnit seuraavista:
        i. palaute,
        ii. toimivaltaisen valvontaviranomaisen päätökset.

9.3.2 Arviointitoimintojen dokumentointi

Valvontaviranomainen voi laatia lisävaatimuksia.

9.3.3 Valitusten käsittely

Hallintajärjestelmään on kuuluttava sen erottamattomana osana myös valitusten käsittely, jonka on täytettävä varsinkin standardin ISO/IEC 17065/2012 kohdan 4.1.2.2 alakohdassa c, kohdan 4.1.2.2 alakohdassa j, kohdan 4.6 alakohdassa d ja kohdassa 7.13 esitetyt vaatimukset.

Valitukset ja vastalauseet olisi toimitettava toimivaltaisen valvontaviranomaisen tietoon.

9.3.4 Peruuttamisen hallinnointi

Menettelyt, jotka liittyvät akkreditoinnin keskeyttämiseen tai peruuttamiseen, olisi vietävä osaksi sertifiointielimen hallintajärjestelmää, mukaan lukien ilmoitukset asiakkaille.

---

[21] Toimivaltainen valvontaviranomainen voi täsmentää ja laatia uusia lisävaatimuksia, jos kansallinen lainsäädäntö sen sallii.