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

Hyväksytty 4. joulukuuta 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,

ON ANTANUT SEURAAVAT OHJEET:

1 JOHDANTO

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

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

Tarkoituksenmukaiset sertifiointimekanismit voivat edistää yleisen 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 käsittelytoiminta on säännösten mukaista.[1].

Tässä yhteydessä Euroopan tietosuojaneuvosto toteaa, että akkreditoinnista on annettava ohjeet. Akkreditoinnin erityinen arvo ja merkitys on siinä, että se tarjoaa sertifiointielinten pätevyydestä luotettavan lausunnon, jolla voidaan luoda luottamusta sertifiointimekanismiin.

Ohjeiden tarkoituksena on antaa opastusta siinä, miten yleisen tietosuoja-asetuksen 43 artiklan säännöksiä pitäisi tulkita ja panna täytäntöön. Niiden tarkoituksena on erityisesti auttaa jäsenvaltioita, valvontaviranomaisia ja kansallisia akkreditointielimiä ottamaan käyttöön johdonmukainen ja yhdenmukaistettu perustaso niiden sertifiointielinten akkreditoinnille, jotka myöntävät sertifioinnin yleisen tietosuoja-asetuksen mukaisesti.

[1] Yleisen tietosuoja-asetuksen johdanto-osan 100 kappaleessa todetaan, että sertifiointimekanismien käyttöönotolla voidaan tehostaa läpinäkyvyyttä ja asetuksen noudattamista ja antaa rekisteröidyille mahdollisuus arvioida asianomaisten tuotteiden ja palvelujen tietosuojan taso.

2 OHJEIDEN SOVELTAMISALA

Näissä ohjeissa

- esitetään akkreditoinnin tarkoitus yleisen 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 kansallinen akkreditointielin käsittelee akkreditointia, ja
- tarjotaan kehys akkreditointivaatimusten vahvistamiselle, kun valvontaviranomainen käsittelee akkreditointia.

Ohjeet eivät ole menettelyopas sertifiointielinten akkreditoinnille yleisen tietosuoja-asetuksen mukaisesti. Niissä ei laadita uutta teknistä standardia sertifiointielinten akkreditoimiseksi yleisen tietosuoja-asetuksen tarkoituksia varten.

Ohjeet on tarkoitettu

- jäsenvaltioille, joiden on varmistettava, että valvontaviranomainen ja/tai kansallinen akkreditointielin akkreditoi sertifiointielimet
- kansallisille akkreditointielimille, jotka tekevät sertifiointielinten akkreditointeja 43 artiklan 1 kohdan b alakohdan mukaisesti
- standardissa ISO/IEC 17065/2012[2] tarkoitetut lisävaatimukset täsmentävälle toimivaltaiselle valvontaviranomaiselle, kun kansallinen akkreditointielin tekee akkreditoinnin 43 artiklan 1 kohdan b alakohdan mukaisesti
- Euroopan tietosuojaneuvostolle, kun se antaa lausunnon toimivaltaisen valvontaviranomaisten akkreditointivaatimuksista ja hyväksyy ne 43 artiklan 3 kohdan, 70 artiklan 1 kohdan p alakohdan ja 64 artiklan 1 kohdan c alakohdan mukaisesti
- akkreditointivaatimukset täsmentävälle toimivaltaiselle valvontaviranomaiselle, kun valvontaviranomainen tekee akkreditoinnin 43 artiklan 1 kohdan a alakohdan mukaisesti
- muille sidosryhmille, kuten mahdollisille sertifiointielimille tai sertifiointijärjestelmän omistajille, jotka laativat sertifiointivaatimuksia ja -menettelyjä[3].

Määritelmät

Seuraavien määritelmien tarkoituksena on edistää yhteistä käsitystä akkreditointiprosessin perustekijöistä. Niitä on pidettävä viitteellisinä, eikä niihin saa vedota ehdottomina. Nämä määritelmät

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

[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 (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 kuin yksi) tekee arviointeja.

perustuvat voimassa oleviin sääntelykehyksiin ja standardeihin, erityisesti yleisen tietosuoja-asetuksen asiaankuuluviin säännöksiin ja standardiin ISO/IEC 17065/2012.

Näissä ohjeissa käytetään seuraavia määritelmiä:

sertifiointielinten *akkreditointi*, katso kohta 3, joka koskee akkreditoinnin tulkintaa yleisen tietosuoja-asetuksen 43 artiklan tarkoituksia varten

lisävaatimuksilla tarkoitetaan toimivaltaisen valvontaviranomaisen vahvistamia vaatimuksia, joiden perusteella akkreditointi tehdään[4]

sertifioinnilla tarkoitetaan arviointia ja puolueettoman kolmannen osapuolen todistusta[5] siitä, että sertifiointikriteerien täyttäminen on osoitettu

sertifiointielimellä tarkoitetaan kolmannen osapuolen vaatimustenmukaisuuden[6] arviointielintä[7], joka käyttää sertifiointimekanismeja[8]

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

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

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

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

Yleisessä tietosuoja-asetuksessa ei määritellä akkreditointia. Akkreditointeihin sovellettavia yleisiä vaatimuksia koskevan asetuksen (EY) N:o 765/2006 2 artiklan 10 kohdassa määritellään akkreditointi

[4] 43 artiklan 1, 3 ja 6 kohta.
[5] Huomaa, että 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] Yleisen tietosuoja-asetuksen 42 artiklan 1 ja 5 kohta.
[9] Ks. kohta 3.9 yhdessä standardin ISO 17065 liitteen B kanssa.

[10] Ks. 42 artiklan 5 kohta.
[11] Ks. asetuksen 765/2008/EY 2 artiklan 11 kohta.

”kansallisen akkreditointielimen antamaksi todistukseksi 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”

Standardin ISO/IEC 17011 mukaan

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

tietosuoja-asetuksen 43 artiklan 1 kohdan mukaan

”sertifioinnin myöntää ja uusii sertifiointielin, jolla on tietosuojaan liittyvä asianmukaisen tason asiantuntemus, sen jälkeen kun se on tiedottanut 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.”

Yleisen 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 tekee kansallinen akkreditointielin, ja valvontaviranomainen, kun se tekee akkreditoinnin itse.

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

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

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

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

4 AKKREDITOINTI YLEISEN TIETOSUOJA-ASETUKSEN 43 ARTIKLAN 1 KOHDAN MUKAISESTI

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

4.1 Jäsenvaltioiden tehtävät

Asetuksen 43 artiklan 1 kohdassa vaaditaan, että jäsenvaltioiden *on varmistuttava* siitä, että sertifiointielimet akkreditoidaan. Kyseisen artiklan kohdan mukaan jäsenvaltioiden on säädettävä siitä, kuka vastaa akkreditoinnin tekemisestä. Asetuksen 43 artiklan 1 kohdan nojalla käytössä on kolme vaihtoehtoa. Akkreditoinnin voi toteuttaa

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

Kunkin jäsenvaltion on päätettävä itse, toteuttaako nämä akkreditoinnit kansallinen akkreditointielin vai valvontaviranomainen vai molemmat yhdessä, mutta joka tapauksessa sen on varmistettava riittävät resurssit[15].

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

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

Tämän 2 artiklan 11 kohdan voidaan katsoa olevan ristiriidassa yleisen 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 tekee yksinomaan kansallinen akkreditointielin, antamalla valvontaviranomaisille samat valtuudet sertifiointielinten akkreditoinnissa. Siksi 43 artiklan 1 kohta on erityissäännös suhteessa asetuksen 765/2008 2 artiklan 11 kohtaan.

4.3 Kansallisen akkreditointielimen tehtävät

Yleisen 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.

[15] Ks. asetuksen (EY) N:o 765/2008 4 artiklan 9 kohta.

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.

Akkreditointiprosessissa kansallisten akkreditointielinten on sovellettava lisävaatimuksia, joista valvontaviranomaiset säätävät.

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

4.4 Valvontaviranomaisen tehtävät

Euroopan 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. 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 toteuttamassa akkreditointiprosessissa sertifiointielimen on kuitenkin 43 artiklan 2 kohdan a alakohdan mukaisesti osoitettava riippumattomuutensa ja asiantuntemuksensa sertifioinnin kohteeseen nähden toimivaltaista valvontaviranomaista tyydyttävällä tavalla[16].

Jos jäsenvaltio määrää, että valvontaviranomaisen on akkreditoitava sertifiointielimet, valvontaviranomaisen olisi vahvistettava akkreditointivaatimukset, muun muassa 43 artiklan 2 kohdassa täsmennetyt vaatimukset. Kansallisten akkreditointielinten toteuttamaan sertifiointielimen akkreditointiin liittyviin velvoitteisiin verrattuna 43 artiklassa annetaan vähemmän ohjeita akkreditointia koskevista vaatimuksista, kun valvontaviranomainen tekee akkreditoinnin itse. Akkreditointia koskevan yhdenmukaisen toimintamallin 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. Euroopan tietosuojaneuvosto huomauttaa, että 43 artiklan 2 kohdan a–e alakohdat perustuvat standardin ISO 17065 vaatimuksiin ja niissä täsmennetään näitä vaatimuksia. Näin edistetään johdonmukaisuutta.

Jos jäsenvaltio määrää, että kansallisten akkreditointielinten on akkreditoitava sertifiointielimet, valvontaviranomaisen on vahvistettava lisävaatimuksia, joilla täydennetään asetuksessa (EY) N:o 765/2008 (jossa artiklat 3–14 liittyvät vaatimustenmukaisuuden arviointielinten akkreditoinnin

[16] Valvontaviranomaisen 43 artiklan 1 kohdan b alakohdan mukaisesti vahvistamissa lisävaatimuksissa on täsmennettävä riippumattomuutta ja asiantuntemusta koskevia vaatimuksia. Ks. myös ohjeiden liite 1.

järjestämiseen ja toimintaan) säädettyjä voimassa olevia akkreditointikäytäntöjä, ja teknisiä sääntöjä, joissa kuvataan sertifiointielinten menetelmät ja menettelyt. Asetuksessa (EY) N:o 765/2008 annetaan tämän osalta lisää ohjeita: asetuksen 2 artiklan 10 kohdassa määritetään akkreditointi ja viitataan ”yhdenmukaistettuihin standardeihin ja tarvittaessa muihin vaatimuksiin, mukaan luettuna niihin, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa”. Sen vuoksi valvontaviranomaisen vahvistamien lisävaatimusten pitäisi sisältää erityisvaatimukset, 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 järjestelmissä vaaditun pätevyyden luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojelun ja erityisesti heidän henkilötietojen suojaa koskevan oikeutensa osalta[17] Näiden ohjeiden liite voi auttaa antamaan tietoa toimivaltaisille valvontaviranomaisille, kun ne vahvistavat ”lisävaatimuksia” 43 artiklan 1 kohdan b alakohdan ja 3 kohdan mukaisesti.

Asetuksen 43 artiklan 6 kohdassa säädetään, että ”[V]alvontaviranomainen julkistaa tämän artiklan 3 kohdassa tarkoitetut vaatimukset ja 42 artiklan 5 kohdassa tarkoitetut sertifiointikriteerit helposti saatavilla olevassa muodossa”. Näin ollen kaikki valvontaviranomaisen hyväksymät kriteerit ja vaatimukset on julkaistava avoimuuden takaamiseksi. Sertifiointielinten laadun ja niiden saaman luottamuksen kannalta olisi toivottavaa, että kaikki akkreditointia koskevat vaatimukset olisivat heti yleisön saatavilla.

4.5 Sertifiointielimenä toimiva valvontaviranomainen

Yleisen tietosuoja-asetuksen 42 artiklan 5 kohdassa säädetään, että valvontaviranomainen voi myöntää sertifiointeja, mutta asetuksessa ei edellytetä siltä akkreditointia asetuksen (EY) N:o 765/2008 vaatimusten täyttämiseksi. Euroopan tietosuojaneuvosto huomauttaa, että 43 artiklan 1 kohdan a alakohdan ja erityisesti 58 artiklan 2 kohdan h alakohdan ja 3 kohdan a ja e–f alakohdan nojalla valvontaviranomaiset saavat valtuudet toteuttaa sekä akkreditoinnin että sertifioinnin ja samalla antaa neuvontaa ja soveltuvin osin peruuttaa sertifioinnit tai kieltää sertifiointielintä antamasta sertifiointia.

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 yleisen tietosuoja-asetuksen mukaisten tehtävien erottamiseksi, jotta sertifiointimekanismien käyttö voidaan juurruttaa ja sitä voidaan helpottaa. Niiden olisi samalla 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 yleisen tietosuoja-asetuksen mukaiseen akkreditointiin ja sertifiointiin.

4.6 Akkreditointivaatimukset

Näiden ohjeiden liitteessä on neuvoja siitä, miten akkreditoinnin lisävaatimukset voidaan määrittää. Siinä esitetään yleisen tietosuoja-asetuksen asiaankuuluvat säännökset ja ehdotetaan vaatimuksia,

[17] Yleisen tietosuoja-asetuksen 1 artiklan 2 kohta.

jotka valvontaviranomaisten ja kansallisten akkreditointielinten olisi otettava huomioon yleisen tietosuoja-asetuksen noudattamisen varmistamiseksi.

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. Asetuksen 43 artiklan 2 kohta perustuu standardin ISO/IEC 17065/2012 yleisiin säännöksiin ja siinä otetaan huomioon yleisen tietosuoja-asetuksen mukainen perusoikeuksien suoja. Liitteen rungossa käytetään 43 artiklan 2 kohtaa ja standardia ISO/IEC 17065/2012 perustana vaatimusten määrittämiselle sekä lisäkriteereille, jotka liittyvät sertifiointielinten tietosuoja-asiantuntemuksen arviointiin ja sen arviointiin, pystyvätkö ne noudattamaan yleisessä tietosuoja-asetuksessa vahvistettuja 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.

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

Euroopan 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 osia tai komponentteja sertifiointitoiminnasta. Näissä tapauksissa näiden ulkopuolisten elinten akkreditointi itse yleisen 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.

Näiden ohjeiden 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.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)