

Tietosuojaneuvoston lausunto (64 artikla)



Lausunto 4/2020 Yhdistyneen kuningaskunnan toimivaltaisen valvontaviranomaisen päätösluonnoksesta, joka koskee sertifiointielimen akkreditointivaatimusten hyväksymistä yleisen tietosuoja-asetuksen 43 artiklan 3 kohdan mukaisesti

Annettu 29. tammikuuta 2020

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

Sisällysluettelo

1	Tiivistelmä tosiseikoista.....	4
2	Arviointi	5
2.1	Annettua päätösluonnosta koskeva Euroopan tietosuojaneuvoston yleinen perustelu... 5	
2.2	Seuraavien asioiden yhdenmukaista arviointia koskevien akkreditointivaatimusten arvioinnin painopisteet (yleisen tietosuoja-asetuksen 43 artiklan 2 kohta ja Euroopan tietosuojaneuvoston ohjeiden liite 1):	6
2.2.1	JOHDANTO (akkreditoinnin lisävaatimusten luonnoksen 0 luku).....	7
2.2.2	AKKREDITOINNIN YLEISET VAATIMUKSET (akkreditoinnin lisävaatimusten luonnoksen 4 luku).....	7
2.2.3	RESURSSIVAATIMUKSET (akkreditoinnin lisävaatimuksen luonnoksen 6 luku).....	7
2.2.4	MENETELMÄVAATIMUKSET, 43 ARTIKLAN 2 KOHDAN C JA D ALAKOHTA (akkreditoinnin lisävaatimusten luonnoksen 7 luku).....	8
3	Johtopäätökset/suositukset	9
4	Loppuhuomautukset	10

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') 63 artiklan, 64 artiklan 1 kohdan c alakohdan ja 3–8 kohdan sekä 43 artiklan 3 kohdan,

ottaa huomioon luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta annetun direktiivin (EU) 2016/680 (jäljempänä 'poliisidirektiivi') 51 artiklan 1 kohdan b alakohdan,

ottaa huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018¹,

ottaa huomioon 25 päivänä toukokuuta 2018 hyväksytyt työjärjestyksensä 10 ja 22 artiklan,

sekä katsoo seuraavaa:

(1) Tietosuojaneuvoston tärkeimpänä tehtävänä on varmistaa asetuksen 2016/679 (jäljempänä 'yleinen tietosuoja-asetus') yhdenmukainen soveltaminen koko Euroopan talousalueella. Yleisen tietosuoja-asetuksen 64 artiklan 1 kohdan mukaan tietosuojaneuvosto antaa lausunnon aina, kun valvontaviranomainen aikoo hyväksyä sertifiointielinten akkreditointivaatimukset 43 artiklan nojalla. Tämän lausunnon tarkoituksena on näin ollen luoda yhdenmukainen toimintamalli, joka koskee sertifiointielimen akkreditointiin sovellettavia tietosuojaviranomaisen tai kansallisen akkreditointielimen vaatimuksia. Vaikka yleinen tietosuoja-asetus ei aseta tiettyä vaatimusten sarjaa akkreditoinnille, se kuitenkin kannustaa yhdenmukaisuuteen. Tietosuojaneuvosto pyrkii saavuttamaan tämän tavoitteen lausunnoissaan ensinnäkin kannustamalla valvontaviranomaisia laatimaan akkreditointivaatimukset sertifiointielinten akkreditoinnista annettujen Euroopan tietosuojaneuvoston ohjeiden liitteessä kuvatun rakenteen mukaisesti ja toiseksi analysoimalla niitä käyttämällä Euroopan tietosuojaneuvoston mallia, mikä mahdollistaa vaatimusten vertailuanalyysin (ISO 17065 -standardin ja sertifiointielinten akkreditoinnista annettujen Euroopan tietosuojaneuvoston ohjeiden pohjalta).

(2) Yleisen tietosuoja-asetuksen 43 artiklan mukaisesti toimivaltaiset valvontaviranomaiset hyväksyvät akkreditointivaatimukset. Niiden on kuitenkin sovellettava yhdenmukaisuusmekanismia luottamuksen herättämiseksi sertifiointimekanismiin erityisesti asettamalla korkea vaatimustaso.

(3) Vaikka akkreditointivaatimukseen sovelletaan yhdenmukaisuusmekanismia, vaatimusten ei tarvitse olla identtisiä. Toimivaltaisilla valvontaviranomaisilla on kansallisen tai alueellisen tason harkintavaltaa, ja niiden on otettava huomioon paikallinen lainsäädäntö. Euroopan tietosuojaneuvoston lausunnon tarkoituksena ei ole asettaa EU:n laajuisia yhteisiä vaatimuksia vaan

¹ Viittauksilla "unioniin" tarkoitetaan kauttaaltaan tässä lausunnossa viittauksia ETAan.

pikemminkin välttää merkittäviä epäjohtonmukaisuuksia, jotka voivat vaikuttaa esimerkiksi luottamukseen akkreditoitujen sertifiointielinten itsenäisyyttä tai asiantuntemusta kohtaan.

(4) Ohjeet 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen (2016/679) 43 artiklan mukaisesti (jäljempänä 'ohjeet') ja "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" [Ohjeet 1/2018 sertifiointinista ja sertifiointikriteerien määrittämisestä asetuksen 2016/679 42 ja 43 artiklan mukaisesti] toimivat ohjenuorana yhdenmukaisuusmekanismin yhteydessä.

(5) 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 tietoa akkreditointia koskevista vaatimuksista, kun valvontaviranomainen tekee akkreditoinnin itse. Akkreditointia koskevan yhdenmukaisen toimintamallin edistämiseksi valvontaviranomaisen käyttämien akkreditointivaatimusten pohjana pitäisi olla ISO/IEC 17065 -standardi, ja niitä pitäisi täydentää valvontaviranomaisen 43 artiklan 1 kohdan b alakohdan mukaisesti vahvistamalla lisävaatimuksilla. Euroopan tietosuojaneuvosto toteaa, että 43 artiklan 2 kohdan a–e alakohta perustuu ISO 17065 -standardin vaatimuksiin ja täsmentää niitä. Näin edistetään johdonmukaisuutta.²

(6) Euroopan tietosuojaneuvosto antaa lausunnon yleisen tietosuoja-asetuksen 64 artiklan 1 kohdan c alakohdan ja 3 ja 8 kohdan nojalla, luettuina yhdessä Euroopan tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan kanssa, kahdeksan viikon kuluessa ensimmäisestä arkipäivästä sen jälkeen, kun puheenjohtaja ja toimivaltainen valvontaviranomainen ovat päättäneet, että asiakirja on valmis. Määräaika voidaan jatkaa puheenjohtajan päätöksellä kuudella viikolla ottaen huomioon asian monimutkaisuuden.

ON ANTANUT LAUSUNNON:

1 TIIVISTELMÄ TOSISEIKOISTA

1. Yhdistyneen kuningaskunnan valvontaviranomainen on toimittanut akkreditointivaatimusten luonnoksen Euroopan tietosuojaneuvostolle 43 artiklan 1 kohdan b alakohdan mukaisesti. Asiakirja lähetettiin 25. lokakuuta 2019, kun oli annettu päätös siitä, että se on valmis. Yhdistyneen kuningaskunnan kansallinen akkreditointielin (UKAS) akkreditoi sertifiointielimiä, jotka suorittavat sertifiointeja yleisen tietosuoja-asetuksen sertifiointikriteerien mukaan. Tämä tarkoittaa sitä, että Yhdistyneen kuningaskunnan kansallinen akkreditointielin käyttää sertifiointielinten akkreditoinnissa ISO 17065 -standardia ja valvontaviranomaisen asettamia lisävaatimuksia, kun valvontaviranomainen on hyväksynyt ne tietosuojaneuvoston vaatimusluonnoksesta antaman lausunnon jälkeen.

² Ohjeiden 39 kohta:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

2. Tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan mukaisesti käsiteltävän asian monimutkaisuuden vuoksi tietosuojaneuvosto on päättänyt jatkaa alkuperäistä kahdeksan viikon hyväksymisaikaa kuudella viikolla.

2 ARVIOINTI

2.1 Annettua päätösluonnosta koskeva Euroopan tietosuojaneuvoston yleinen perustelu

3. Lausunnon tarkoituksena on arvioida valvontaviranomaisten laatimia akkreditointivaatimuksia joko suhteessa ISO 17065 -standardiin tai kaikkiin vaatimuksiin, jotta kansallinen akkreditointielin tai valvontaviranomainen voisi yleisen tietosuoja-asetuksen 43 artiklan 1 kohdan mukaisesti akkreditoida sertifiointielimen, joka vastaa sertifiointien myöntämisestä ja uusimisesta yleisen tietosuoja-asetuksen 42 artiklan mukaisesti. Tämä ei rajoita toimivaltaisen valvontaviranomaisen tehtäviä ja valtuuksia. Tässä tapauksessa tietosuojaneuvosto toteaa, että Yhdistyneen kuningaskunnan valvontaviranomainen on päättänyt turvautua kansalliseen akkreditointielimeen akkreditoinnin myöntämiseksi ja laatinut ohjeiden mukaisia lisävaatimuksia, joita kansallinen akkreditointielimen on noudatettava akkreditoinnin myöntämisessä.
4. Yhdistyneen kuningaskunnan valvontaviranomaisen akkreditointia koskevien lisävaatimusten arvioinnin tarkoituksena on tarkastella sitä, miten vaatimukset eroavat ohjeista ja erityisesti liitteestä (lisäykset tai poistot). Euroopan tietosuojaneuvoston lausunto keskittyy myös kaikkiin asioihin, jotka voivat vaikuttaa sertifiointielinten akkreditointia koskevaan yhdenmukaiseen lähestymistapaan.
5. On huomattava, että sertifiointielinten akkreditointia koskevien ohjeiden tarkoituksena on auttaa valvontaviranomaisia akkreditointivaatimusten määrittelyssä. Ohjeiden liite ei sinänsä sisällä akkreditointivaatimuksia. Siksi valvontaviranomaisen on määriteltävä sertifiointielinten akkreditointivaatimukset siten, että niitä on mahdollista soveltaa yhdenmukaisesti käytännössä, kuten valvontaviranomaisen toimintayhteydessä vaaditaan.
6. Tietosuojaneuvosto myöntää, että kansallisille akkreditointielimille on niiden asiantuntemus huomioon ottaen myönnettävä liikkumavaraa, kun ne määrittelevät tiettyjä sovellettaviin akkreditointivaatimuksiin sisältyviä erityissäännöksiä. Tietosuojaneuvosto pitää kuitenkin tarpeellisena painottaa sitä, että mahdolliset lisävaatimukset on määriteltävä siten, että niiden vaadittava yhdenmukainen käytännön soveltaminen ja uudelleenarviointi on mahdollista.
7. Tietosuojaneuvosto huomauttaa, että ISO-standardit, erityisesti ISO 17065, ovat teollis- ja tekijänoikeuksien alaisia, minkä vuoksi se ei siteeraa kyseisen asiakirjan tekstiä tässä lausunnossa. Siksi tietosuojaneuvosto on päättänyt tarvittaessa viitata ISO-standardin tiettyihin osiin kuitenkin jäljentämättä tekstiä.
8. Tietosuojaneuvosto on tehnyt arvioinnin ohjeiden liitteessä 1 kuvatun rakenteen mukaisesti. Jos lausunnossa ei mainita Yhdistyneen kuningaskunnan valvontaviranomaisen akkreditointivaatimusten luonnoksen tiettyä lukua, tietosuojaneuvostolla ei ole siitä huomautuksia eikä se pyydä Yhdistyneen kuningaskunnan valvontaviranomaista ryhtymään lisätoimiin.
9. Tämä lausunto ei käsittele niitä Yhdistyneen kuningaskunnan valvontaviranomaisen toimittamia kohtia, jotka eivät kuulu yleisen tietosuoja-asetuksen 43 artiklan 2 kohdan soveltamisalaan, kuten

viittaukset kansalliseen lainsäädäntöön. Tietosuojaneuvosto kuitenkin toteaa, että kansallisen lainsäädännön pitäisi noudattaa yleistä tietosuojasetusta tarvittaessa.

2.2 Seuraavien asioiden yhdenmukaista arviointia koskevien akkreditointivaatimusten arvioinnin painopisteet (yleisen tietosuojasetuksen 43 artiklan 2 kohta ja Euroopan tietosuojaneuvoston ohjeiden liite 1):

- a. kaikkien ohjeiden liitteessä mainittujen keskeisten alueiden käsittely ja mahdolliset poikkeamat liitteestä
- b. sertifiointielimen riippumattomuus
- c. sertifiointielimen eturistiriidat
- d. sertifiointielimen asiantuntemus
- e. asianmukaiset takeet, joilla varmistetaan se, että sertifiointielin soveltaa asianmukaisesti yleisen tietosuojasetuksen sertifiointikriteerejä
- f. yleisen tietosuojasetuksen mukaisen sertifiointin myöntämis-, määräaikaistarkastelu- ja peruuttamismenettelyt ja
- g. sertifiointin rikkomista koskevien valitusten läpinäkyvä käsittely.

10. Ottaen huomioon, että

- a. yleisen tietosuojasetuksen 43 artiklan 2 kohdassa on luettelo akkreditointia koskevista vaatimuksista, jotka sertifiointielimen on täytettävä saadakseen akkreditoinnin,
- b. yleisen tietosuojasetuksen 43 artiklan 3 kohdan mukaan sertifiointielinten akkreditointivaatimusten on oltava toimivaltaisen valvontaviranomaisen hyväksymiä,
- c. yleisen tietosuojasetuksen 57 artiklan 1 kohdan p ja q alakohdan mukaan toimivaltaisen valvontaviranomaisen on laadittava ja julkaistava sertifiointielimiä koskevat akkreditointivaatimukset ja ne voivat päättää suorittaa sertifiointielinten akkreditoinnin itse,
- d. yleisen tietosuojasetuksen 64 artiklan 1 kohdan c alakohdan mukaan tietosuojaneuvosto antaa lausunnon aina, kun toimivaltainen valvontaviranomainen aikoo hyväksyä sertifiointielimen akkreditointivaatimukset 43 artiklan 3 kohdan nojalla,
- e. jos akkreditoinnin on tehnyt kansallinen akkreditointielin ISO/IEC 17065/2012 -standardin mukaisesti, on sovellettava myös toimivaltaisen valvontaviranomaisen vahvistamia lisävaatimuksia,
- f. sertifiointielinten akkreditointia koskevien ohjeiden liite 1 sisältää ehdotetut vaatimukset, jotka tietosuojaviranomaisen on laadittava ja joita sovelletaan kansallisen akkreditointielimen tekemän sertifiointielimen akkreditoinnin aikana,

tietosuojaneuvosto esittää seuraavan lausunnon:

2.2.1 JOHDANTO (akkreditoinnin lisävaatimusten luonnoksen 0 luku)

11. Tietosuojaneuvosto myöntää, että kansallisen akkreditointielimen ja tietosuojaviranomaisen suhdetta säätelevät yhteistyöehdot eivät ole itsessään edellytys sertifiointielinten akkreditoinnille. Tietosuojaneuvosto katsoo kuitenkin kattavuuden ja avoimuuden vuoksi, että mikäli tällaiset yhteistyöehdot on laadittu, ne on julkaistava valvontaviranomaisen sopivaksi katsomassa muodossa.
12. Tietosuojaneuvosto panee merkille, että Yhdistyneen kuningaskunnan valvontaviranomainen ottaa käyttöön tällaiset yhteistyöehdot kansallisen akkreditointielimensä kanssa ja että lopulliset ehdot julkaistaan Yhdistyneen kuningaskunnan valvontaviranomaisen verkkosivustolla.

2.2.2 AKKREDITOINNIN YLEISET VAATIMUKSET (akkreditoinnin lisävaatimusten luonnoksen 4 luku)

13. Tietosuojaneuvosto panee merkille, että oikeudellista vastuuta koskevassa vaatimuksessa (4.1.1 kohta) Yhdistyneen kuningaskunnan valvontaviranomainen vaatii, että akkreditoitavan sertifiointielimen *"pitäisi kyetä toimittamaan todisteet akkreditointiprosessin aikana vaadittavasta yleisen tietosuoja-asetuksen ja Yhdistyneen kuningaskunnan vuoden 2018 tietosuojalain noudattamisesta"*. Tämän vaatimuksen asianmukaisen arvioinnin ja toimeenpanon varmistamiseksi tietosuojaneuvosto kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista korvaamaan ilmaisun *"pitäisi kyetä toimittamaan todisteet"* ilmaisulla *"on toimitettava todisteet"*. Tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen muuttaa luonnosta vastaavasti.
14. Sertifiointisopimuksen (4.1.2 kohta) ja erityisesti vaatimuksen numero 8 (liitteessä oleva numero 9) osalta tietosuojaneuvosto panee merkille, että Yhdistyneen kuningaskunnan valvontaviranomainen on muotoillut uudelleen osan ohjeiden liitteessä 1 tarkoitetusta vaatimuksesta. Yhdistyneen kuningaskunnan valvontaviranomainen on kuitenkin poistanut ilmaisun [tarvittaessa] *"asiakkaaseen kohdistuvat vaikutukset olisi myös huomioitava"*. Tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen lisää edellä mainitun vaatimuksen puuttuvan osan.
15. Tietosuojaneuvosto huomauttaa tietosuojasinettien ja -merkkien käytöstä (4.1.3 kohta), että Yhdistyneen kuningaskunnan valvontaviranomainen vaatii, että jäljennös *"sinetistä/merkistä/logosta on toimitettava ICO:lle arkistointia varten"*. Koska sinettejä, merkkejä ja logoja käsittelee sertifiointielimen lisäksi myös järjestelmän omistaja, tietosuojaneuvosto kehottaa, että Yhdistyneen kuningaskunnan valvontaviranomainen viittaa myös mahdollisiin Yhdistyneen kuningaskunnan valvontaviranomaisen hyväksymien sertifiointijärjestelmien mukaisiin sinetteihin, merkkeihin ja logoihin.

2.2.3 RESURSSIVAATIMUKSET (akkreditoinnin lisävaatimuksen luonnoksen 6 luku)

16. Sertifiointielimen henkilöstön (6.1 kohta) ja erityisesti 6 alakohdan osalta tietosuojaneuvosto panee merkille, että Yhdistyneen kuningaskunnan valvontaviranomainen on todennut, että *"sertifiointipäätöksistä vastaavalla henkilöstöllä on oltava merkittävää tietosuojatoimenpiteiden määrittämiseen ja toteuttamiseen liittyvää ammatillista kokemusta"*. Tietosuojaneuvosto kuitenkin katsoo, että vaikka sertifiointipäätöksiä tekevillä henkilöstön jäsenillä ei välttämättä ole itsellään *"merkittävää tietosuojatoimenpiteiden määrittämiseen ja toteuttamiseen liittyvää ammatillista"*

kokemusta”, heillä on ainakin oltava mahdollisuus konsultoida tällaista asiantuntijaa tietoon perustuvan päätöksen tekemiseksi. Merkittävä ammatillinen kokemus tällaisten toimenpiteiden toteuttamisesta ei ainakaan varhaisessa vaiheessa ole todennäköisesti kovin yleistä kyseisellä alalla. Siksi tietosuojaneuvosto kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista vaatimaan, että sertifiointielin määrittelee ja selventää sertifiointijärjestelmän kannalta asianmukaiset ammatillista kokemusta koskevat vaatimukset.

2.2.4 MENETELMÄVAATIMUKSET, 43 ARTIKLAN 2 KOHDAN C JA D ALAKOHTA (akkreditoinnin lisävaatimusten luonnoksen 7 luku)

17. Menetelmävaatimuksia koskevan yleisen kohdan (7.1 kohta) ja erityisesti sen 4 alakohdan osalta tietosuojaneuvosto panee merkille lisävaatimuksen, jonka mukaan akkreditointielimen on varmistettava, että sertifiointielin suorittaa tutkimuksen tai auditoinnin tapauksissa, joissa tietosuojan noudattaminen on asetettu kyseenalaiseksi. Tietosuojaneuvosto ymmärtää, että tietosuojan noudattamisella viitataan sertifiointiin haltijaan. Asia on kuitenkin täsmennettävä selvästi vaatimuksissa. Tietosuojaneuvosto katsoo lisäksi, että Yhdistyneen kuningaskunnan valvontaviranomaisen on esitettävä yksityiskohtaisesti, että tällaisen tutkimuksen on oltava yhteydessä sertifiointiin alaan ja arvioinnin kohteeseen. Siksi tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen muuttaa vaatimusta vastaavasti ja ilmoittaa selvästi, että tietosuojan noudattamisella viitataan sertifiointiin haltijaan, ja määrittää, että tutkimuksen on oltava yhteydessä sertifiointiin alaan ja arvioinnin kohteeseen.
18. Menetelmävaatimusten soveltamisen (7.2 kohta) osalta tietosuojaneuvosto panee merkille, että sertifiointielimen on tarpeen määrittää *”käytetäänkö henkilötietojen käsittelijöitä, ja kun henkilötietojen käsittelijät toimivat hakijana, niiden vastuut ja tehtävät on kuvattava, ja hakemuksen on sisällettävä asianmukaiset rekisterinpitäjän / henkilötietojen käsittelijän sopimukset”*. Vaikka tietosuojaneuvosto toteaa, että Yhdistyneen kuningaskunnan valvontaviranomainen on käyttänyt liitteen 1 sanamuotoa, se myös kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista harkitsemaan, pitäisikö samassa yhteydessä myös viitata yhteisiin rekisterinpitäjiin ja niitä koskeviin erityisjärjestelyihin.
19. Arviointimenetelmien (7.4 kohta) osalta tietosuojaneuvosto panee merkille Yhdistyneen kuningaskunnan valvontaviranomaisen laatiman lisävaatimuksen, jonka mukaan *”ISO 17065 -standardin 7.4.5 kohdan lisäksi säädetään, että samaan sertifiointiin kohteeseen liittyvä voimassa oleva sertifiointi voidaan huomioida osana uutta arviointia [...]”*. Tältä osin tietosuojaneuvosto katsoo, että tapauksissa, joissa voimassa oleva sertifiointi otetaan huomioon osana uutta arviointia, on tarpeen selventää edelleen, että kyseisen sertifiointiin ala on myös arvioitava yksityiskohtaisesti sen osalta, onko se asianmukaisten sertifiointikriteerien mukainen. Siksi tietosuojaneuvosto kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista selventämään sanamuotoa vastaavasti.
20. Virkkeen *”Koko arviointiraportti tai aiemman sertifiointitoiminnan arvioinnin mahdollistavat tiedot ja sen tulokset voidaan ottaa huomioon.”* osalta tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen korvaa ilmaisun *”voidaan”* ilmaisulla *”täytyy”*, mikäli sertifiointielin päättää ottaa huomioon voimassa olevan sertifiointiin. Tietosuojaneuvosto katsoo myös, että olisi selvempää viitata yksinkertaisesti *”sertifiointiin”* eikä *”sertifiointitoimintaan”*, ja suosittaa Yhdistyneen kuningaskunnan valvontaviranomaista muuttamaan luonnosta vastaavasti. Viittaus *”aiempaan sertifiointiin”* voi olla lisäksi harhaanjohtava, sillä se ei viittaa selvästi voimassa

olevaan sertifiointiin, jonka sertifiointielin aikoo ottaa huomioon osana omaa arviointiaan. Tietosuojaneuvosto suosittaa Yhdistyneen kuningaskunnan valvontaviranomaista muuttamaan sanamuotoa selventääkseen, että viittaus koskee voimassa olevaa sertifiointia. Tietosuojaneuvosto toteaa lopuksi, että sertifiointielimen pitäisi saada käyttöönsä arviointiraportti ja muut asiaan liittyvät sertifiointitoiminnan arvioinnin mahdollistavat tiedot, jotta se voisi tehdä tietoon perustuvan päätöksen. Siksi tietosuojaneuvosto kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista selventämään sanamuotoa vastaavasti.

21. Ilmaisulla ”ISO 17065 -standardin 7.4.6 kohdan lisäksi” alkavan kappaleen osalta tietosuojaneuvosto katsoo, että Yhdistyneen kuningaskunnan valvontaviranomaisen viittaus ”sen sertifiointimekanismiin” tarkoittaa itse asiassa ”sertifiointijärjestelmää”. Siksi se suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen muuttaa sanamuodon vastaavasti.
22. Sertifiointiin vaikuttavien muutosten (7.10 kohta) ja erityisesti neljännen luetelmakohdan (”Euroopan tietosuojaneuvoston päätökset”) osalta tietosuojaneuvosto myöntää, että Yhdistyneen kuningaskunnan valvontaviranomainen on käyttänyt liitteen 1 sanamuotoa. Sen varmistamiseksi, että ilmaisun ”Euroopan tietosuojaneuvoston päätökset” merkitys ymmärretään selvästi, tietosuojaneuvosto kuitenkin kehottaa Yhdistyneen kuningaskunnan valvontaviranomaista selventämään viittausta. Esimerkiksi voidaan viitata ”asiakirjoihin, jotka Euroopan tietosuojaneuvosto on hyväksynyt”.

3 JOHTOPÄÄTÖKSET/SUOSITUKSET

23. Yhdistyneen kuningaskunnan valvontaviranomaisen akkreditointivaatimusten luonnos voi johtaa sertifiointielinten akkreditoinnin epäjohdonmukaiseen soveltamiseen, ja on tehtävä seuraavat muutokset:
24. Akkreditoinnin yleisten vaatimusten osalta tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen
 1. korvaa 4.1.1 kohdassa ilmaisun ”pitäisi kyetä toimittamaan todisteet” ilmaisulla ”on toimitettava todisteet”
 2. lisää 4.1.2 kohtaan vaatimuksen puuttuvan osan, jotta se olisi yhdenmukainen ohjeiden liitteen 1 tekstin kanssa.
25. Menetelmävaatimusten osalta tietosuojaneuvosto suosittaa, että Yhdistyneen kuningaskunnan valvontaviranomainen
 1. muuttaa 7.1 kohtaa täsmentääkseen, että tietosuojan noudattamisella viitataan sertifiointin haltijaan ja että tutkimuksen on oltava yhteydessä sertifiointin alaan ja arvioinnin kohteeseen
 2. muuttaa 7.4 kohtaa korvaamalla ilmaisun ”voidaan” ilmaisulla ”täytyy” ja ilmaisun ”sertifiointitoiminta” ilmaisulla ”sertifiointi”
 3. korvaa viittauksen ”sertifiointimekanismiin” viittauksella ”sertifiointijärjestelmään”.

4 LOPPUHUOMAUTUKSET

26. Tämä lausunto osoitetaan Yhdistyneen kuningaskunnan valvontaviranomaiselle ja julkaistaan yleisen tietosuoja-asetuksen 64 artiklan 5 kohdan b alakohdan mukaisesti.
27. Yleisen tietosuoja-asetuksen 64 artiklan 7 ja 8 kohdan mukaisesti valvontaviranomainen ilmoittaa tietosuojaneuvoston puheenjohtajalle sähköisesti kahden viikon kuluessa lausunnon saamisesta, pitäytyykö se ehdottamassaan luettelossa vai muuttaako se sitä. Saman ajanjakson kuluessa sen on toimitettava korjattu luetteloehdotus tai, mikäli se ei aio noudattaa tietosuojaneuvoston lausuntoa kokonaisuudessaan tai osittain, sen on toimitettava asianmukaiset perustelut.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)