Lausunto 15/2020, joka koskee Saksan toimivaltaisten valvontaviranomaisten luonnosta päätökseksi sertifiointielimen akkreditointivaatimusten hyväksymisestä yleisen tietosuoja-asetuksen 43 artiklan 3 kohdan mukaisesti

Annettu 25. toukokuuta 2020

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

Annettu

Sisällysluettelo

1 TIIVISTELMÄ TOSISEIKOISTA.....4

2 ARVIOINTI.....5

2.1 Toimitettua päätösluonnosta koskeva Euroopan tietosuojaneuvoston yleinen perustelu....5

2.2 Pääpainopisteet sen arvioinnille (yleisen tietosuoja-asetuksen 43 artiklan 2 kohta ja Euroopan tietosuojaneuvoston ohjeiden liite 1), että akkreditointivaatimuksilla määrätään seuraavien yhdenmukaisesta arvioinnista: 6

2.2.1 JOHDANTO.....6

2.2.2 TERMIT JA MÄÄRITELMÄT.....7

2.2.3 YLEISET HUOMAUTUKSET 7

2.2.4 AKKREDITOINNIN YLEISET VAATIMUKSET (akkreditointivaatimusten luonnoksen 4 luku)7

2.2.5 RESURSSIVAATIMUKSET (akkreditointivaatimusten luonnoksen 6 luku) 8

2.2.6 MENETTELYVAATIMUKSET (akkreditointivaatimusten luonnoksen 7 luku).....9

2.2.7 MUUT LISÄVAATIMUKSET 12

3 PÄÄTELMÄT/SUOSITUKSET 12

4 LOPPUHUOMAUTUKSET.....13

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, 64 artiklan 3–8 kohdan ja 43 artiklan 3 kohdan,

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 154/2018[1],

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

sekä katsoo seuraavaa:

(1) Tietosuojaneuvoston tärkeimpänä tehtävänä on varmistaa asetuksen (EU) 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 mukaisesti. Tämän lausunnon tarkoituksena on näin ollen saada aikaan yhdenmukainen toimintamalli niiden vaatimusten osalta, joita tietosuojan valvontaviranomainen tai kansallinen akkreditointielin soveltaa sertifiointielimen akkreditointiin. Vaikka yleisessä tietosuoja-asetuksessa ei aseteta tiettyjä vaatimuksia akkreditoinnille, siinä kuitenkin kannustetaan yhdenmukaisuuteen. Tietosuojaneuvosto pyrkii saavuttamaan tämän tavoitteen lausunnoillaan ensinnäkin kannustamalla valvontaviranomaisia laatimaan akkreditointivaatimuksensa sertifiointielinten akkreditointia koskevien Euroopan tietosuojaneuvoston ohjeiden 4/2018 liitteessä 1 esitetyn rakenteen mukaisesti ja toiseksi analysoimalla niitä käyttämällä Euroopan tietosuojaneuvoston mallia, joka mahdollistaa vaatimusten vertailun (standardin ISO 17065 ja sertifiointielinten akkreditointia koskevien Euroopan tietosuojaneuvoston ohjeiden mukaisesti).

(2) Yleisen tietosuoja-asetuksen 43 artiklan mukaisesti toimivaltaiset valvontaviranomaiset hyväksyvät akkreditointivaatimukset. Niiden on kuitenkin sovellettava yhdenmukaisuusmekanismia, jotta sertifiointimekanismia kohtaan saadaan aikaan luottamusta. Tämä tehdään etenkin asettamalla korkea vaatimustaso.

(3) Vaikka akkreditointivaatimuksiin sovelletaan yhdenmukaisuusmekanismia, vaatimusten ei tarvitse olla identtisiä. Toimivaltaisilla valvontaviranomaisilla on kansallista tai alueellista harkintavaltaa, ja niiden on otettava huomioon myös paikallinen lainsäädäntö. Euroopan tietosuojaneuvoston lausunnon tarkoituksena ei ole määrittää EU:n laajuisia yhteisiä vaatimuksia vaan pikemminkin välttää merkittäviä epäjohdonmukaisuuksia, jotka voivat vaikuttaa esimerkiksi luottamukseen akkreditoitujen sertifiointielinten riippumattomuutta tai asiantuntemusta kohtaan.

(4) Yhdenmukaisuusmekanismissa käytetään ohjenuorana ohjeita 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen (2016/679) 43 artiklan mukaisesti, jäljempänä 'ohjeet',

[1] Viittauksilla "unioniin" tarkoitetaan tässä lausunnossa viittauksia ETA:han.

Annettu

ja ohjeita 1/2018 sertifioinnista ja sertifiointikriteerien määrittämisestä asetuksen 2016/679 42 ja 43 artiklan mukaisesti.

(5) Jos jäsenvaltio määrää, että valvontaviranomaisen on akkreditoitava sertifiointielimet, valvontaviranomaisen on vahvistettava akkreditointivaatimukset, muun muassa 43 artiklan 2 kohdassa täsmennetyt vaatimukset. Kansallisten akkreditointielinten toteuttamaan sertifiointielinten 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 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 alakohta perustuu standardin ISO 17065 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. Määräaikaa voidaan jatkaa puheenjohtajan päätöksellä kuudella viikolla asian monimutkaisuuden huomioon ottaen.

ON ANTANUT LAUSUNNON:

1 TIIVISTELMÄ TOSISEIKOISTA

1. Saksan liittovaltion ja osavaltioiden valvontaviranomaiset, jäljempänä ’Saksan valvontaviranomaiset’, ovat toimittaneet akkreditointivaatimusten luonnoksen Euroopan tietosuojaneuvostolle 43 artiklan 1 kohdan b alakohdan mukaisesti. Asiakirja todettiin täydelliseksi 13. helmikuuta 2020. Saksan kansallinen akkreditointielin, DAkkS, akkreditoi sertifiointielimiä, jotka suorittavat sertifiointeja yleisen tietosuoja-asetuksen sertifiointikriteerien mukaisesti. Tämä tarkoittaa, että kansallinen akkreditointielin käyttää sertifiointielinten akkreditoinnissa ISO 17065 -standardia ja Saksan valvontaviranomaisten asettamia lisävaatimuksia, kun Saksan valvontaviranomaiset ovat hyväksyneet ne vaatimusten luonnosta koskevan tietosuojaneuvoston lausunnon jälkeen.
2. Tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan mukaisesti puheenjohtaja päätti käsiteltävänä olevan asian monimutkaisuuden vuoksi jatkaa alkuperäistä kahdeksan viikon hyväksymisaikaa kuudella viikolla.

[2] Ohjeet 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen 43 artiklan mukaisesti, 39 kohta. Saatavilla osoitteessa https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_fi

Annettu

2 ARVIOINTI

2.1 Toimitettua päätösluonnosta koskeva Euroopan tietosuojaneuvoston yleinen perustelu

3. Lausunnon tarkoituksena on arvioida valvontaviranomaisen 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 vaikuta toimivaltaisen valvontaviranomaisen tehtäviin ja valtuuksiin. Tässä tapauksessa tietosuojaneuvosto toteaa, että Saksan valvontaviranomaiset ovat päättäneet turvautua Saksan kansallisen akkreditointielimen eli DAkkS:n ja toimivaltaisen valvontaviranomaisen toteuttamaan yhteiseen akkreditointiprosessiin akkreditoinnin myöntämiseksi ja laatineet ohjeiden mukaisia lisävaatimuksia, joita on noudatettava akkreditoinnin myöntämisessä.

4. Saksan valvontaviranomaisten akkreditointia koskevien lisävaatimusten arvioinnin tarkoituksena on tarkastella sitä, miten vaatimukset eroavat ohjeista ja erityisesti ohjeiden liitteestä 1 (lisäykset tai poistot). Euroopan tietosuojaneuvoston lausunnossa keskitytään myös kaikkiin näkökohtiin, jotka voivat vaikuttaa sertifiointielinten akkreditointia koskevaan yhdenmukaiseen lähestymistapaan.

5. On huomattava, että sertifiointielinten akkreditointia koskevien ohjeiden tavoitteena on auttaa valvontaviranomaisia akkreditointivaatimustensa määrittämisessä. Ohjeiden liite ei sellaisenaan muodosta akkreditointivaatimuksia. Siksi valvontaviranomaisten on määritettävä sertifiointielimiä koskevat akkreditointivaatimukset siten, että niitä voidaan soveltaa käytännössä ja johdonmukaisesti valvontaviranomaisten toimintaympäristön edellyttämällä tavalla.

6. Tietosuojaneuvosto tunnustaa, että kansallisille akkreditointielimille ja toimivaltaisille valvontaviranomaisille on niiden asiantuntemus huomioon ottaen myönnettävä soveltuvissa tapauksissa liikkumavaraa, kun ne määrittelevät tiettyjä sovellettaviin akkreditointivaatimuksiin sisältyviä erityissäännöksiä. Tietosuojaneuvosto pitää kuitenkin tarpeellisena painottaa sitä, että mahdolliset lisävaatimukset on määriteltävä siten, että niiden yhdenmukainen käytännön soveltaminen ja uudelleenarviointi on mahdollista tarpeen mukaan.

7. Tietosuojaneuvosto huomauttaa, että ISO-standardit, erityisesti ISO 17065, ovat teollis- ja tekijänoikeuksien alaisia, minkä vuoksi se ei siteeraa kyseisen asiakirjan tekstiä tässä lausunnossa. Näin ollen tietosuojaneuvosto on päättänyt tarvittaessa viitata ISO-standardin tiettyihin osiin toistamatta tekstiä kuitenkaan sellaisenaan.

8. Tietosuojaneuvosto on tehnyt arviointinsa ohjeiden liitteessä 1 (jäljempänä ’liite’) kuvatun rakenteen mukaisesti. Siltä osin kuin lausunnossa ei mainita tiettyjä osia Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksesta, tietosuojaneuvostolla ei ole niistä huomautuksia eikä se pyydä Saksan valvontaviranomaisia ryhtymään lisätoimiin.

9. Tässä lausunnossa ei käsitellä niitä Saksan valvontaviranomaisten toimittamia kohtia, jotka eivät kuulu yleisen tietosuoja-asetuksen 43 artiklan 2 kohdan soveltamisalaan, kuten viittaukset kansalliseen lainsäädäntöön. Tietosuojaneuvosto toteaa kuitenkin, että kansallisen lainsäädännön tulisi olla tarpeellisilta osin linjassa yleisen tietosuoja-asetuksen kanssa.

2.2 Pääpainopisteet sen arvioinnille (yleisen tietosuoja-asetuksen 43 artiklan 2 kohta ja Euroopan tietosuojaneuvoston ohjeiden liite 1), että akkreditointivaatimuksilla määrätään seuraavien yhdenmukaisesta arvioinnista:

1) ohjeiden liitteessä mainittujen kaikkien keskeisten aiheiden käsittely ja mahdolliset poikkeamat liitteestä

2) sertifiointielimen riippumattomuus

3) sertifiointielimen eturistiriidat

4) sertifiointielimen asiantuntemus

5) asianmukaiset suojatoimet sen varmistamiseksi, että sertifiointielin soveltaa yleisen tietosuoja-asetuksen sertifiointikriteerejä asianmukaisesti

6) menettelyt yleisen tietosuoja-asetuksen mukaisen sertifioinnin myöntämistä, määräaikaisarviointia ja peruuttamista varten ja

7) sertifiointia koskevista rikkomuksista tehtyjen kantelujen avoin käsittely.

10. Ottaen huomioon, että

a. yleisen tietosuoja-asetuksen 43 artiklan 2 kohdassa on luettelo akkreditointia koskevista vaatimuksista, jotka sertifiointielimen on täytettävä saadakseen akkreditoinnin,

b. yleisen tietosuoja-asetuksen 43 artiklan 3 kohdan mukaan sertifiointielinten akkreditointivaatimusten on oltava toimivaltaisen valvontaviranomaisen hyväksymiä,

c. yleisen tietosuoja-asetuksen 57 artiklan 1 kohdan p ja q alakohdan mukaan toimivaltaisen valvontaviranomaisen on laadittava ja julkaistava sertifiointielinten akkreditointivaatimukset, ja se voi päättää suorittaa sertifiointielinten akkreditoinnin itse,

d. yleisen tietosuoja-asetuksen 64 artiklan 1 kohdan c alakohdan mukaan tietosuojaneuvosto antaa lausunnon aina, kun valvontaviranomainen aikoo hyväksyä sertifiointielimen akkreditointivaatimukset 43 artiklan 3 kohdan nojalla,

e. jos akkreditoinnin tekee 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

11. Tietosuojaneuvosto myöntää, että kansallisen akkreditointielimen ja tietosuojaviranomaisen suhdetta säätelevät yhteistyöehdot eivät ole itsessään edellytys sertifiointielinten akkreditoinnille.

Annettu

Tietosuojaneuvosto katsoo kuitenkin kattavuuden ja avoimuuden vuoksi, että mikäli tällaiset yhteistyöehdot on laadittu, ne on julkaistava valvontaviranomaisen sopivaksi katsomassa muodossa.

2.2.2 TERMIT JA MÄÄRITELMÄT

12. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnokseen sisältyvässä luvussa 3 (”Määritelmät”) määritetään, minkätyyppiset sertifiointijärjestelmät ovat sallittuja, ja täsmennetään, että niiden on täytettävä standardin DIN EN ISO / IEC 17065 vaatimukset. Tähän liittyen on huomautettava, että jo Euroopan tietosuojaneuvoston ohjeiden 5.1 ja 5.2 kohdassa määritetään kattavasti, mitä yleisen tietosuoja-asetuksen nojalla voi sertifioida. Niinpä tietosuojaneuvosto tunnustaa, että Saksan valvontaviranomaisten tarkoituksena ei ole rajoittaa ohjeissa määritettyä ja että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 3 lukuun sisältyvät väitteet on katsottava sovellettaviksi kyseisten akkreditointivaatimusten yhteydessä.

2.2.3 YLEISET HUOMAUTUKSET

13. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen osiossa ”yleiset huomautukset” viitataan Euroopan tietosuojaneuvoston toteuttamaan sertifiointikriteerien ”vahvistukseen” ”yleisen tietosuoja-asetuksen 63 artiklan ja 64 artiklan 1 kohdan c alakohdan mukaisesti”. Tietosuojaneuvosto huomauttaa, että yleisessä tietosuoja-asetuksessa ei anneta Euroopan tietosuojaneuvostolle toimivaltaa ”vahvistaa” sertifiointikriteerejä. Euroopan tietosuojaneuvosto voi kuitenkin edellä mainittujen artiklojen nojalla hyväksyä sertifiointikriteerit. Näin ollen tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset poistavat viittauksen ”Euroopan tietosuojaneuvoston vahvistukseen”, jotta luonnoksen sanamuoto vastaisi yleistä tietosuoja-asetusta.

2.2.4 AKKREDITOINNIN YLEISET VAATIMUKSET (akkreditointivaatimusten luonnoksen 4 luku)

14. Oikeudellista vastuuta koskevan vaatimuksen (Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.1 kohta) osalta tietosuojaneuvosto toteaa Saksan valvontaviranomaisten määrittävän lisäasiakirjassa, että sertifiointielimellä odotetaan olevan käytössään ajantasaiset menettelyt ja että asiaan liittyen ei näin ollen tarvitse lisätä muita vaatimuksia. Tietosuojaneuvosto katsoo kuitenkin, ettei odotus sido sertifiointielimiä siihen, että niillä olisi tällaiset menettelyt. Ohjeiden liitteen 4.1.1 kohdassa määritetyn mukaisesti sertifiointielimillä on oltava ajantasaiset menettelyt, jotka osoittavat akkreditoinnin ehdoissa määritettyjen oikeudellisten vastuiden noudattamisen. Lisäksi sertifiointielimen on voitava esittää todisteet yleisen tietosuoja-asetuksen mukaisista menettelyistä ja toimenpiteistä erityisesti asiakasorganisaation henkilötietojen hallintaan ja käsittelyyn osana sertifiointiprosessia. Näin ollen tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset muuttavat luonnosta vaatimuksiksi ja yhdenmukaistavat sitä ohjeiden kanssa.

15. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.1.2.2 alakohdan (”sertifiointisopimus”) osalta tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnokseen ei sisälly velvollisuutta mahdollistaa menettelyjen täydellistä läpinäkyvyyttä toimivaltaiselle valvontaviranomaiselle sertifiointimenettelyn suhteen, mikä koskee myös sopimuksella luottamuksellisiksi määritettyjä asioita. Vaatimusten luonnoksessa ei myöskään viitata hakijan velvollisuuteen tarjota sertifiointielimelle pääsy tarkastelemaan sen käsittelytoimia.

Annettu

Tietosuojaneuvosto suositteleekin, että Saksan valvontaviranomaiset sisällyttävät luonnokseensa edellä mainitut velvollisuudet.

16. Tietosuojaneuvosto huomauttaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.1.2.2 alakohtaan ei sisälly nimenomaista viittausta toimivaltaisen valvontaviranomaisen tehtäviin ja valtuuksiin (liitteen 4.1.2 kohdan kolmas sisennys). Tietosuojaneuvosto katsoo, että kyseinen viittaus olisi lisättävä vaatimusten luonnokseen, ja suosittelee näin ollen, että Saksan valvontaviranomaiset muuttavat luonnosta vastaavasti.

17. Lisäksi Saksan valvontaviranomaisten sertifiointisopimusta koskevien vaatimusten luonnokseen ei sisälly velvollisuutta mahdollistaa sertifiointielimelle kaikkien sellaisten tietojen luovuttaminen, jotka ovat tarpeen sertifioinnin myöntämiseksi yleisen tietosuoja-asetuksen 42 artiklan 8 kohdan ja 43 artiklan 5 kohdan mukaisesti (liitteen 4.1.2 kohdan seitsemäs sisennys). Vaikka kyseinen velvollisuus sisältyykin Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen prosessinhallintaa koskevaan osioon, tietosuojaneuvosto katsoo, että sen pitäisi olla osa sertifiointisopimusta velvollisuuden sitovan luonteen vahvistamiseksi. Näin ollen tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset sisällyttävät edellä mainitun velvollisuuden osaksi sertifiointisopimuksen elementtejä.

18. Liitteen mukaan hakijan on ilmoitettava sertifiointielimelle merkittävistä muutoksista tosiasiallisessa tai oikeudellisessa tilanteessaan sekä tuotteissaan, prosesseissaan ja palveluissaan, joita sertifiointi koskee (liitteen 4.1.2 kohdan kymmenes sisennys). Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.1.2.2 alakohdan kuudenteen sisennykseen sisältyy kuitenkin vain velvollisuus ilmoittaa sertifiointielimelle merkittävistä muutoksista tosiasiallisissa tai oikeudellisissa olosuhteissa. Tuotteita, prosesseja ja palveluja ei mainita siinä erikseen. Tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset lisäävät kyseisen viittauksen liitteen mukaisesti.

19. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.2.7 alakohdan (”käsittelyn puolueettomuus”) osalta tietosuojaneuvosto suosittelee, että vahvistetaan erilliseen oikeushenkilöön kuuluviin tai sellaisen hallitsemiin sertifiointielimiin sovellettavia kriteerejä sen huomioimiseksi, että minkä tahansa tyyppinen sertifiointielimen ja oikeushenkilön välinen taloudellinen suhde voi ominaisuuksistaan riippuen vaikuttaa sertifiointitoimien puolueettomuuteen.

20. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 4.6 kohdan (”julkisesti saatavilla olevat tiedot”) osalta tietosuojaneuvosto huomauttaa, että siinä ei viitata hyväksyttyjen kriteerien kaikkien versioiden ja sertifiointimenettelyjen julkaisuun. Näin ollen tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia muuttamaan akkreditointivaatimusten luonnosta siten, että julkaisun todetaan nimenomaisesti käsittävän kaikki hyväksyttyjen kriteerien versiot ja sertifiointimenettelyt. Lisäksi tietosuojaneuvosto huomauttaa 4.6 kohdan toisessa kappaleessa todettavan, että ”sertifiointielimen käyttämät sertifiointijärjestelmät yleisen tietosuoja-asetuksen 42 artiklan 5 kohdan mukaisesti hyväksytyt kriteerit ja soveltamisen sallittu kesto *on yleisesti julkaistava*.” Monitulkintaisuuden välttämiseksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia poistamaan sanan ”yleisesti” sekä lisäämään sanan ”ja” ilmauksen ”sertifiointijärjestelmät” jälkeen.

2.2.5 RESURSSIVAATIMUKSET (akkreditointivaatimusten luonnoksen 6 luku)

21. Asiantuntemusta koskevien vaatimusten ja erityisesti Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 6.1.2.1 alakohdan (”henkilöstön pätevyys”) osalta

tietosuojaneuvosto huomauttaa, että luetelluilla toiminta-alueilla vaaditun osaamisen yhteydessä ei täsmennetä, että osaamisen on oltava merkityksellistä ja asianmukaista. Jotta voidaan varmistaa yhdenmukaisuus liitteessä vaaditun asiantuntemuksen tason kanssa, tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset yhdenmukaistavat sanamuotoa ohjeiden kanssa edellyttämällä merkityksellistä ja asianmukaista osaamista.

22. Lisäksi tietosuojaneuvosto toteaa, että sellaista henkilöstöä koskeviin vaatimuksiin, jolla on teknistä asiantuntemusta ja joka vastaa päätöksenteosta, sisältyy vähintään seitsemän vuotta ammatillista kokemusta tai viisi vuotta tekniseen tietosuojaan liittyvää ammatillista kokemusta henkilöstön koulutustason mukaan, kun taas arvioinneista vastaavalla henkilöstöllä tulisi olla neljän vuoden ammatillinen kokemus tai kahden vuoden tekniseen tietosuojaan liittyvä ammatillinen kokemus sekä kokemusta testausmenettelystä koulutustasonsa mukaan. Samoin henkilöstöllä, jolla on oikeudellista asiantuntemusta ja joka tekee päätöksiä, on oltava vähintään viiden vuoden ammatillinen kokemus tietosuojalainsäädännön alalta, kun taas arvioinneista vastaavalla henkilöstöllä on oltava vähintään kahden vuoden kokemus tietosuojalainsäädännön ja tarkastusmenettelyjen alalta. Tietosuojaneuvosto toteaa, että päätöksenteosta vastaavalta henkilöstöltä ja arvioinnista vastaavalta henkilöstöltä edellytettävän ammatillisen kokemuksen vähimmäisvuosimäärässä on merkittävä ero. Tähän liittyen tietosuojaneuvosto katsoo, että arvioijien ja päätöksentekijöiden osaamista koskevat vaatimukset tulisi räätälöidä ottamalla huomioon heidän suorittamansa erilaiset tehtävät eikä niinkään kokemusvuodet. Tietosuojaneuvoston näkemys on, että arvioijilla tulisi olla enemmän erikoisalan asiantuntemusta ja ammatillista kokemusta teknisistä menettelyistä (esimerkiksi tarkastuksista ja sertifioinneista), kun taas päätöksentekijöillä tulisi olla yleisluontoisempi ja kattavampi asiantuntemus sekä ammatillista kokemusta tietosuojan alalta. Tämän perusteella tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia antamaan enemmän painoarvoa arvioijien ja päätöksentekijöiden erilaiselle olennaiselle osaamiselle ja/tai kokemukselle sekä pienentämään heiltä edellytettävien kokemusvuosien määrien välistä eroa.

23. Lisäksi tietosuojaneuvosto katsoo, että sertifiointia koskevan aihealueen kannalta merkityksellisiin hallintajärjestelmiin liittyvä osaaminen tulisi laajentaa standardiin ISO/IEC 27701:2019 – turvallisuustekniikat – laajennus standardeihin ISO/IEC 27001 ja ISO/IEC 27002 tietosuojan hallintaa varten – vaatimukset ja ohjeet, ja kannustaa Saksan valvontaviranomaisia sisällyttämään vaatimuksiin kyseisen viittauksen.

24. Teknisen henkilöstön koulutusvaatimusten osalta tietosuojaneuvosto katsoo, että aineiden luettelo on jo räätälöity liitteessä vaaditun teknisen asiantuntemuksen mukaiseksi. Näin ollen tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia poistamaan viittauksen ”luonnontieteisiin” teknisen henkilöstön yliopistokoulutusta koskevasta aineiden luettelosta.

2.2.6 MENETTELYVAATIMUKSET (akkreditointivaatimusten luonnoksen 7 luku)

25. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7 luvussa viitataan useasti termiin ”sen kriteerit” (esim. kohdat 7.4, 7.6, 7.11 ja 7.13). Monitulkintaisuuden välttämiseksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia selventämään kyseisen termin merkitystä esimerkiksi lisäämällä selityksen liitteeseen 1 (sanasto).

26. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.1 kohdan (”yleiset tiedot”) osalta tietosuojaneuvosto toteaa, että kohtaan ei sisälly nimenomaista viittausta sertifiointielimen velvollisuuteen noudattaa lisävaatimuksia. Vaikka kyseinen velvollisuus voitaisiinkin päätellä

vaatimusten luonnoksen tekstistä, tietosuojaneuvosto katsoo, että nimenomainen viittaus edellä mainittuun velvollisuuteen olisi lisättävä. Niinpä tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset muuttavat luonnosta vastaavasti.

27. Tietosuojaneuvosto huomauttaa, että Saksan valvontaviranomaisten lisävaatimusten luonnokseen ei sisälly viittausta hyväksytyn eurooppalaisen tietosuojasinetin käyttöön liitteen 7.1.2 kohdan mukaisesti. Tietosuojaneuvoston näkemyksen mukaan kyseinen viittaus olisi lisättävä ottaen huomioon erityisesti, että eurooppalaisia tietosuojasinettejä myöntävän sertifiointielimen akkreditointi saatetaan joutua suorittamaan kussakin niistä jäsenvaltioista, johon sertifiointielin on sijoittautunut.[3] Niinpä tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset lisäävät edellä mainitun viittauksen. Vaatimusten luonnoksessa voitaisiin todeta esimerkiksi seuraavaa: *”Toimivaltaiselle valvontaviranomaiselle on ilmoitettava, ennen kuin sertifiointielin alkaa käyttää hyväksyttyä eurooppalaista tietosuojasinettiä uudessa jäsenvaltiossa sivuyksiköstä käsin.”*

28. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.2 kohdassa (”hakeminen”) kuvataan tilanne, jossa tietojenkäsittelytoimien suorittamiseen käytetään tietojen käsittelijöitä, ohjeiden liitteen mukaisesti. Tietosuojaneuvosto huomauttaa kuitenkin, että tietojen käsittelijöitä käytettäessä hakemukseen on sisällyttävä asianmukaiset rekisterinpitäjän / tietojen käsittelijän sopimukset liitteessä määritetyn mukaisesti. Näin ollen tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset yhdenmukaistavat sanamuotoa ohjeiden mukaiseksi sisällyttämällä mukaan viittauksen rekisterinpitäjän / tietojen käsittelijän sopimuksiin. Lisäksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia harkitsemaan, olisiko tässä tapauksessa mainittava myös yhteisrekisterinpitäjät ja heitä koskevat erityisjärjestelyt.

29. Tietosuojaneuvosto toteaa Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.2 kohdassa määritettävän, että ”rekisterinpitäjä ja tietojen käsittelijä ovat oikeutettuja hakemaan sertifiointia”. Tietojen käsittelijöiden mahdollisuus hakea sertifiointia riippuu kyseessä olevasta sertifiointijärjestelmästä. Näin ollen ja epäselvyyksien välttämiseksi tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset poistavat edellä olevan maininnan tai selventävät, että tietojen käsittelijöiden mahdollisuus sertifiointiin riippuu sertifiointijärjestelmän laajuudesta.

30. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.3 kohdan (”hakemusten arviointi”) osalta tietosuojaneuvosto huomauttaa Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksessa todettavan, että ”suunnitellut arviointimenetelmät ovat sopimuksella määrättyjä [...]”. Sen selventämiseksi, että kyseessä on vaatimus, tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia laatimaan ensimmäisen kappaleen uudelleen selventääkseen, että arviointimenetelmien on sisällyttävä sertifiointisopimukseen, eli muuttamaan vaatimuksen muotoon ”suunniteltujen arviointimenetelmien on oltava sopimuksella määrättyjä [...]”. Lisäksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia vaihtamaan standardin ISO 17065 kohtaan 7.3.1.b tehdyn viittauksen tilalle viittauksen standardin ISO 17065 kohtaan 7.3 sanamuodon yhdenmukaistamiseksi liitteen kanssa. Tietosuojaneuvosto panee myös merkille, että neljännessä kappaleessa viitataan asianmukaiseen tekniseen ja oikeudelliseen osaamiseen. Selkeyden vuoksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia lisäämään tähän yhteyteen ilmaisun ”tietosuojan alalla”.

31. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.4 kohtaan (”arviointimenetelmät”) ei sisälly sertifiointielimen velvollisuutta kuvata riittävät

[3] Katso tähän liittyen ohjeissa 1/2018 oleva 44 kohta.

Annettu

arviointimenetelmät sen määrittämiseksi, ovatko käsittelytoimet sertifiointikriteerien mukaisia. Tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset muuttavat luonnosta vaatimuksiksi lisäämällä kyseisen maininnan. Lisäys voisi olla esimerkiksi seuraavanlainen: *”Sertifiointielimen on varmistettava, että sertifioinnin myöntämiseen käytettävissä mekanismeissa kuvataan riittävät arviointimenetelmät sen määrittämiseksi, ovatko käsittelytoimet sertifiointikriteerien mukaisia*”. Arviointimenetelmissä käsiteltävän ensimmäisen aihealueen osalta tietosuojaneuvosto katsoo lisäksi, että tarpeellisuutta ja oikeasuhteisuutta on soveltuvissa tapauksissa arvioitava myös suhteessa kyseessä oleviin rekisteröityihin. Tietosuojaneuvosto toteaa vielä, että menetelmien ja löydösten dokumentointia ei mainita. Niinpä tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia muuttamaan luonnosta ja lisäämään kyseisen maininnan erikseen.

32. Olemassa olevien sertifiointien (Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.4 kohta) osalta tietosuojaneuvosto katsoo, että neljäs sisennys sivulla 13 johtaa sekaannukseen, sillä on epäselvää, mikä yhteys nykyisen ja aikaisemman sertifioinnin voimassaoloaikojen välillä on ja miten ne sopivat toisiinsa. Lisäksi toisen akkreditoidun sertifiointielimen aikaisemmin myöntämän sertifioinnin voimassaolon kyseenalaistaminen ei vaikuta toteuttamiskelpoiselta. Yhteenvetona kappaletta olisi hyvä selkeyttää mainittujen eri elementtien välisen suhteen osalta. Tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset muuttavat luonnosta erityisesti sen selventämiseksi, että yleisen tietosuoja-asetuksen mukaisen sertifioinnin voimassaolon kesto ei saa riippua muuntyyppisten sertifiointien voimassaolosta.

33. Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.5 kohdan (”arvotus”) osalta tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia muuttamaan osion nimeksi ”arviointi”.

34. Sertifiointiin vaikuttavien muutosten (Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.10 kohta) osalta tietosuojaneuvosto panee merkille, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksessa todetaan seuraavaa: ”asiakkaalle ilmoitetaan viipymättä häneen vaikuttavista oikeudellisen kehyksen muutoksista”. Tietosuojaneuvosto ottaa huomioon tarpeen säilyttää sertifiointielimen puolueettomuus ja kannustaa Saksan valvontaviranomaisia muotoilemaan virkkeen uudelleen sen selventämiseksi, että asiakkaalle toimitetaan viipymättä yleisiä tietoja muutoksista, jotka voivat vaikuttaa häneen. Lisäksi sen varmistamiseksi, että ilmaisun ”Euroopan tietosuojaneuvoston päätökset” merkitys ymmärretään selvästi, tietosuojaneuvosto kehottaa Saksan valvontaviranomaisia selventämään kyseistä viittausta. Ne voivat viitata esimerkiksi ”Euroopan tietosuojaneuvoston antamiin asiakirjoihin”.

35. Tietosuojaneuvosto toteaa, että Saksan valvontaviranomaisten akkreditointivaatimusten luonnoksen 7.11 kohtaan (”sertifioinnin päättäminen, rajoittaminen, keskeyttäminen tai peruuttaminen”) ei sisälly sertifiointielimen velvollisuutta hyväksyä Saksan valvontaviranomaisten antamat päätökset ja määräykset, jotka koskevat hakijalle myönnetyn sertifioinnin peruuttamista tai sertifioinnin myöntämättä jättämistä, mikäli sertifiointivaatimukset eivät täyty tai lakkaavat täyttymästä. Tietosuojaneuvosto suositteleekin, että Saksan valvontaviranomaiset sisällyttävät vaatimuksiin kyseisen velvollisuuden. Lisäksi tietosuojaneuvosto kannustaa Saksan valvontaviranomaisia korvaamaan osan otsikossa olevan sanan ”rajoittaminen” sanalla ”vähentäminen” ohjeiden liitteen mukaisesti.

Annettu

2.2.7 MUUT LISÄVAATIMUKSET

36. Saksan valvontaviranomaisten akkreditointivaatimusten 8.11.3 alakohdan (”valitusten käsittely”) osalta tietosuojaneuvosto kehottaa Saksan valvontaviranomaisia korvaamaan ilmaisun ”oikeutetut valitukset” ilmaisulla ”perustellut valitukset” selkeyden lisäämiseksi.

3 PÄÄTELMÄT/SUOSITUKSET

37. Saksan liittovaltion ja osavaltioiden valvontaviranomaisten akkreditointivaatimusten luonnos voi johtaa sertifiointielinten akkreditoinnin epäyhdenmukaiseen soveltamiseen ja edellyttää seuraavien muutosten tekemistä:

38. ”Yleisten huomautusten” osalta tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset

    1) poistavat viittauksen ”Euroopan tietosuojaneuvoston vahvistukseen”, jotta luonnoksen sanamuoto vastaa yleistä tietosuoja-asetusta.

39. ”Yleisten akkreditointivaatimusten” osalta tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset

    1) muuttavat oikeudellista vastuuta koskevia vaatimuksia (4.1 alakohta) yhdenmukaistaakseen niitä ohjeiden kanssa

    2) muuttavat 4.1.2.2 alakohtaa sisällyttääkseen sertifiointisopimukseen velvollisuuden mahdollistaa Saksan valvontaviranomaisille sertifiointimenettelyn suhteen täydellinen avoimuus ja tarjota sertifiointielimelle pääsy hakijan käsittelytoimiin

    3) sisällyttävät 4.1.2.2 alakohtaan nimenomaisen viittauksen toimivaltaisen valvontaviranomaisen tehtäviin ja valtuuksiin liitteen mukaisesti

    4) sisällyttävät osaksi sertifiointisopimuksen elementtejä velvollisuuden mahdollistaa sertifiointielimelle kaikkien sellaisten tietojen luovuttaminen, jotka ovat tarpeen sertifioinnin myöntämiseksi yleisen tietosuoja-asetuksen 42 artiklan 8 kohdan ja 43 artiklan 5 kohdan mukaisesti

    5) sisällyttävät nimenomaisen viittauksen ”tuotteisiin, prosesseihin ja palveluihin, joita sertifiointi koskee,” 4.1.2.2 alakohdan kuudenteen sisennykseen

    6) vahvistavat 4.2.7 alakohdassa erilliseen oikeushenkilöön kuuluviin tai sellaisen hallitsemiin sertifiointielimiin sovellettavia kriteerejä sen huomioimiseksi, että minkä tahansa tyyppinen sertifiointielimen ja oikeushenkilön välinen taloudellinen suhde voi ominaisuuksistaan riippuen vaikuttaa sertifiointitoimien puolueettomuuteen.

40. ”Resurssivaatimusten” osalta tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset

    1) yhdenmukaistavat 6.1.2.1 alakohdan sanamuotoa ohjeiden kanssa edellyttämällä merkityksellistä ja asianmukaista osaamista.

41. ”Menettelyvaatimusten” osalta tietosuojaneuvosto suosittelee, että Saksan valvontaviranomaiset

Annettu

1) muuttavat 7.1 kohtaa siten, että se sisältää nimenomaisen viittauksen sertifiointielimen velvollisuuteen noudattaa lisävaatimuksia

2) lisäävät viittauksen hyväksytyn eurooppalaisen tietosuojasinetin käyttöön

3) yhdenmukaistavat 7.2 kohdan sanamuotoa ohjeiden mukaiseksi sisällyttämällä mukaan viittauksen rekisterinpitäjän / tietojen käsittelijän sopimuksiin

4) sisällyttävät 7.4 kohtaan sertifiointielimen velvollisuuden kuvata riittävät arviointimenetelmät sen määrittämiseksi, ovatko käsittelytoimet sertifiointikriteerien mukaisia

5) selventävät 7.4 kohdassa, että yleisen tietosuoja-asetuksen mukaisen sertifioinnin voimassaolon kesto ei saa riippua muuntyyppisten sertifiointien voimassaolosta

6) sisällyttävät 7.11 kohtaan sertifiointielimen velvollisuuden hyväksyä Saksan valvontaviranomaisten antamat päätökset ja määräykset, jotka koskevat hakijalle myönnetyn sertifioinnin peruuttamista tai sertifioinnin myöntämättä jättämistä, mikäli sertifiointivaatimukset lakkaavat täyttymästä.

4 LOPPUHUOMAUTUKSET

42. Tämä lausunto osoitetaan Saksan liittovaltion ja osavaltioiden valvontaviranomaisille ja julkaistaan yleisen tietosuoja-asetuksen 64 artiklan 5 kohdan b alakohdan mukaisesti.

43. Yleisen tietosuoja-asetuksen 64 artiklan 7 ja 8 kohdan mukaisesti Saksan valvontaviranomaiset ilmoittavat tietosuojaneuvoston puheenjohtajalle sähköisesti kahden viikon kuluessa lausunnon saamisesta, pitäytyvätkö ne päätösehdotuksessaan vai muuttavatko ne sitä. Saman ajanjakson kuluessa niiden on toimitettava korjattu päätösehdotus tai, mikäli ne eivät aio noudattaa tietosuojaneuvoston lausuntoa kokonaisuudessaan tai osittain, niiden on toimitettava siitä asianmukaiset perustelut.

44. Saksan valvontaviranomaiset ilmoittavat lopullisesta päätöksestä tietosuojaneuvostolle, joka sisällyttää sen rekisteriinsä yhdenmukaisuusmekanismissa käsitellyissä asioissa tehdyistä päätöksistä, yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan y alakohdan mukaisesti.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)

Annettu