Lausunto 5/2020, joka koskee Luxemburgin toimivaltaisen valvontaviranomaisen luonnosta päätökseksi sertifiointielimen akkreditointivaatimusten hyväksymisestä 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.

Annettu

Sisällysluettelo

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 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 2016/680/EU, jäljempänä 'poliisidirektiivi', 51 artiklan 1b kohdan,

ottaa huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETAn 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 mukaisesti tietosuojaneuvosto antaa lausunnon aina, kun valvontaviranomainen aikoo hyväksyä vaatimukset 43 artiklan mukaisen sertifiointielimen akkreditoimiseksi. 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 aseta yksiä vaatimuksia akkreditoinnille, siinä kuitenkin kannustetaan yhdenmukaisuuteen. Tietosuojaneuvosto pyrkii saavuttamaan tämän tavoitteen lausunnoillaan ensinnäkin kannustamalla valvontaviranomaisia laatimaan akkreditointivaatimuksensa tietosuojaneuvoston sertifiointielinten akkreditointia koskevien ohjeiden liitteessä esitetyn rakenteen mukaisesti ja toiseksi arvioimalla niitä käyttämällä tietosuojaneuvoston mallia, jossa vaatimuksia voidaan vertailla (standardin ISO 17065 ja sertifiointielinten akkreditointia koskevien tietosuojaneuvoston ohjeiden mukaisesti).

(2) Toimivaltaisten valvontaviranomaisten on yleisen tietosuoja-asetuksen 43 artiklan mukaan hyväksyttävä akkreditointivaatimukset. Niiden on kuitenkin sovellettava yhdenmukaisuusmekanismia, jotta sertifiointimekanismia kohtaan pystytään luomaan luottamusta. Se tehdään etenkin laatimalla korkeatasoisia vaatimuksia.

(3) Vaikka akkreditointivaatimuksiin sovelletaan yhdenmukaisuusmekanismia, se ei tarkoita, että vaatimusten pitäisi olla samanlaisia. Toimivaltaisilla valvontaviranomaisilla on kansallista tai alueellista harkintavaltaa, ja niiden on otettava huomioon paikallinen lainsäädäntönsä. Tietosuojaneuvoston lausunnon tarkoituksena ei ole saada aikaan yksiä yhtenäisiä EU:n vaatimuksia vaan välttää

[1] Viittaukset "unioniin" tulee ymmärtää kauttaaltaan tässä lausunnossa myös viittauksina ETAan.

huomattavia epäyhdenmukaisuuksia, 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', 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 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 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.[2]

(6) Tietosuojaneuvosto antaa lausunnon yleisen tietosuoja-asetuksen 64 artiklan 1 kohdan c alakohdan sekä 3–8 kohdan nojalla, luettuna 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 ottaen huomioon asian monimutkaisuus.

ON ANTANUT LAUSUNNON:

1 TIIVISTELMÄ TOSISEIKOISTA

1. Luxemburgin valvontaviranomainen on toimittanut akkreditointivaatimustensa luonnoksen tietosuojaneuvostolle 43 artiklan 1 kohdan a alakohdan mukaisesti. Se julkaistiin 25. lokakuuta 2019, kun oli tehty päätös, että asiakirja on valmis. Luxemburgin valvontaviranomainen tekee sertifiointielinten sertifiointiakkreditoinnin yleisen tietosuoja-asetuksen sertifiointikriteerien mukaisesti.
2. Tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan mukaisesti puheenjohtaja päätti käsiteltävänä olevan asian monimutkaisuuden vuoksi jatkaa alkuperäistä kahdeksan viikon hyväksymisaikaa kuudella viikolla.

[2] Ohjeiden 39 kohta: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

2 ARVIOINTI

2.1 Tietosuojaneuvoston yleinen perustelu toimitetusta akkreditointivaatimusten luonnoksesta

Tämän lausunnon tarkoituksena on arvioida valvontaviranomaisen laatimia akkreditointivaatimuksia. Niillä voidaan joko täydentää standardia ISO 17065 tai ne voivat muodostaa itse kokonaiset vaatimukset. Vaatimusten nojalla kansallinen akkreditointielin tai valvontaviranomainen voi yleisen tietosuoja-asetuksen 43 artiklan 1 kohdan mukaisesti akkreditoida sertifiointielimen, joka vastaa sertifioinnin myöntämisestä ja uusimisesta yleisen tietosuoja-asetuksen 42 artiklan mukaisesti. Tämä ei vaikuta toimivaltaisen valvontaviranomaisen tehtäviin ja valtuuksiin. Tässä nimenomaisessa tapauksessa tietosuojaneuvosto panee merkille, että Luxemburgin valvontaviranomaiselle on kansallisessa lainsäädännössä annettu tehtäväksi sertifiointielinten akkreditointi. Luxemburgin valvontaviranomainen on laatinut tätä varten nimenomaisesti sertifiointielinten akkreditointiin tarkoitettuja vaatimuksia sekä sertifiointikriteereitä, jotka on vielä hyväksyttävä virallisesti.

Akkreditointivaatimusten arvioinnin tarkoituksena on tutkia muutoksia (lisäyksiä tai poistoja) ohjeisiin ja erityisesti liitteeseen verrattuna. Tietosuojaneuvoston lausunnossa keskitytään lisäksi kaikkiin näkökohtiin, jotka voivat vaikuttaa sertifiointielinten akkreditoinnin yhdenmukaiseen toimintamalliin.

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

Tietosuojaneuvosto on tehnyt arviointinsa ohjeiden liitteessä 1 esitetyn rakenteen mukaisesti. Vaikka tässä lausunnossa ei käsitellä Luxemburgin valvontaviranomaisen akkreditointivaatimuksia koskevan luonnoksen tiettyä osaa, sitä ei pidä tulkita niin, että tietosuojaneuvostolla ei ole huomautuksia tai että se ei pyydä Luxemburgin valvontaviranomaista toteuttamaan lisätoimenpiteitä. Tietosuojaneuvosto panee merkille, että Luxemburgin valvontaviranomainen on toimittanut tietoja avuksi akkreditointivaatimusten luonnoksen arvioinnissa. Tietosuojaneuvoston lausunnossa käsitellään kuitenkin vain akkreditointivaatimusten luonnosta.

Lausunnossa ei myöskään käsitellä niitä Luxemburgin valvontaviranomaisen toimittamia kohtia, jotka eivät kuulu yleisen tietosuoja-asetuksen 43 artiklan 2 kohdan soveltamisalaan, kuten viittauksia kansalliseen lainsäädäntöön. Tietosuojaneuvosto kuitenkin toteaa, että kansallisen lainsäädännön tulisi olla linjassa yleisen tietosuoja-asetuksen kanssa tarpeellisilta kohdiltaan.

2.2 Arvioinnin keskeiset kohdat (yleisen tietosuoja-asetuksen 43 artiklan 2 kohta ja tietosuojaneuvoston ohjeiden liite 1) siitä, että akkreditointivaatimuksissa määrätään seuraavien yhdenmukaisesta arvioinnista:

a. ohjeiden liitteessä esitettyjen kaikkien keskeisten alojen käsittely ja liitteestä poikkeamisen huomioon ottaminen

b. sertifiointielimen riippumattomuus

c. sertifiointielimen eturistiriidat

d. sertifiointielimen asiantuntemus

e. asianmukaiset suojatoimet, joilla varmistetaan, että sertifiointielin soveltaa asianmukaisesti yleisen tietosuoja-asetuksen sertifiointikriteereitä

f. menettelyt yleisen tietosuoja-asetuksen mukaisen sertifioinnin myöntämistä, määräaikaisarviointia ja peruuttamista varten ja

g. sertifiointia koskevista rikkomuksista tehtyjen kantelujen avoin käsittely.

3. 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 toimivaltaisen valvontaviranomaisen on hyväksyttävä sertifiointielinten akkreditointi;

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

d. yleisen tietosuoja-asetuksen 64 artiklan 1 kohdan c alakohdan mukaan tietosuojaneuvoston on annettava lausunto, kun valvontaviranomainen aikoo hyväksyä kriteerit 43 artiklan 3 kohdan mukaisen sertifiointielimen akkreditoimiseksi;

tietosuojaneuvosto esittää seuraavan lausunnon:

2.2.1 YLEISET HUOMAUTUKSET

4. Tietosuojaneuvosto panee merkille, että akkreditointivaatimusten luonnoksessa ei täysin noudateta ohjeiden liitteessä 1 esitettyä rakennetta. Siitä puuttuvat esimerkiksi soveltamisalaa sekä käsitteitä ja määritelmiä koskevat jaksot. Tietosuojaneuvosto panee tämän osalta merkille, että asiakirjassa ei käytetä joitakin käsitteitä, esimerkiksi ”asiakasta” ja ”hakijaa” kauttaaltaan yhdenmukaisesti. Selvyyden vuoksi käsitteiden olisi mahdollisuuksien mukaan vastattava ohjeiden ja liitteen määritelmiä, ja niitä olisi käytettävä yhdenmukaisesti. Arvioinnin helpottamiseksi tietosuojaneuvosto kannustaa näin ollen Luxemburgin valvontaviranomaista noudattamaan akkreditointivaatimusten luonnoksessa [ohjeiden] liitettä 1 ja lisäämään puuttuvat osat.

5. Tietosuojaneuvosto huomauttaa, että asiakirjassa on kauttaaltaan useita viittauksia ”tämän sertifiointimekanismin” vaatimuksiin (esimerkiksi vaatimus 4.6.4) tai sertifiointielimiin, jotka on akkreditoitu ”sertifiointimekanismin nojalla” (esimerkiksi vaatimus 2.2.2). Viittaus sertifiointimekanismiin näyttää olevan luonnoksen ongelma. Niin ollen tietosuojaneuvosto kannustaa Luxemburgin valvontaviranomaista laatimaan viitteet uudelleen, jotta kävisi ilmi, että sertifiointielimet akkreditoidaan valvontaviranomaisen hyväksymien vaatimusten perusteella.

6. Niin ikään asiakirjassa kauttaaltaan (esimerkiksi vaatimuksessa 1.1.1.2) käytetty viittaus ”tässä sertifiointimekanismissa esitettyihin vaatimuksiin” on hämmentävä. Sitä asianmukaisempi viittaus voisi olla ”sertifiointimekanismissa esitetyt kriteerit”. Siksi tietosuojaneuvosto kannustaa Luxemburgin valvontaviranomaista selkeyttämään kaikkia viittauksia ”sertifiointimekanismiin” kauttaaltaan asiakirjassa.

7. Tietosuojaneuvosto huomauttaa, että useissa vaatimuksissa (esim. 3.2.1.1 ja 4.1.2) viitataan ”asianomaisiin kansainvälisiin standardeihin”, ”asianomaiseen standardiin” tai ”nimenomaiseen

standardiin". Tällaisia standardeja ei kuitenkaan ole määritelty eikä siksi ole selvää, mihin standardeihin viitataan. Tietosuojaneuvosto kehottaa siksi Luxemburgin valvontaviranomaista selkeyttämään näiden standardien merkitystä. Tämä voidaan tehdä esimerkiksi soveltamisalaa tai käsitteitä ja määritelmiä koskevissa jaksoissa.

2.2.2 YLEISET AKKREDITOINTIVAATIMUKSET

8. Tietosuojaneuvosto panee merkille, että Luxemburgin valvontaviranomaisen vaatimuksessa 1.1.1.1 viitataan toiseen standardiin ("ISAE 3000"), jota tietosuojaneuvosto ei ole arvioinut. Siten tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen selkeyttää, etteivät vaatimukset ole ohitettavissa millään ulkoisella standardilla, kuten ISAE 3000:lla.

9. Tietosuojaneuvosto panee merkille, että vaatimukset 1.6 jaksossa eivät sisällä sertifiointielimen velvollisuutta julkaista ja antaa helposti yleisesti saataville kaikki hyväksyttyjen kriteerien versiot ja kaikki sertifiointimenettelyt ohjeiden liitteen (4.6 jakso) mukaisesti. Tietosuojaneuvosto panee merkille, että Luxemburgin valvontaviranomainen voi olla sertifiointijärjestelyn omistaja, mutta katsoo, että olisi hyödyllistä lisätä asianmukainen viittaus, jotta voidaan varmistaa, että kriteerit ovat ajan tasalla ja helposti saatavilla itse sertifiointielimen kautta. Tämän osalta tietosuojaneuvosto katsoo, että jos tiedot annetaan saataville vain pyynnöstä, kuten vaatimuksessa 1.6.1 todetaan, Luxemburgin valvontaviranomainen asettaa tiukemman vaatimuksen kuin liitteessä, jonka mukaan tiedot on annettava helposti julkisesti saataville. Tietosuojaneuvosto suosittelee siksi, että Luxemburgin valvontaviranomainen muuttaa vaatimusta siten, että se sisältää sertifiointielimen velvollisuuden antaa helposti julkisesti saataville kaikki hyväksyttyjen kriteerien versiot ja kaikki sertifiointimenettelyt ohjeiden liitteen mukaisesti.

10. Tietosuojaneuvosto panee merkille, että vaatimuksessa 1.2.4 viitataan "sertifioituun prosessiin". Tietosuojaneuvosto katsoo, että ohjeiden mukaisesti voitaisiin käyttää täsmällisempää sanamuotoa, kuten "sertifioidut käsittelytoimet". Näin sertifioinnin soveltamisalasta saadaan laajempi, kuten yleisessä tietosuoja-asetuksessa säädetään. Tietosuojaneuvosto kannustaa näin ollen Luxemburgin valvontaviranomaista muuttamaan luonnosta esitetyn mukaisesti.

2.2.3 RESURSSIVAATIMUKSET

11. Tietosuojaneuvosto panee merkille, että vaatimuksessa 3.1.1.2 vaikuttaa olevan toistoa ja epäselvyyttä. Erilaisten käsitteiden käyttö ei myöskään ole avuksi. Esimerkiksi kolmas kohta kuulostaa siltä kuin toimeksiannosta vastaava kumppani tekisi päätöksen soveltuvuudesta pelkästään oman arviointinsa perusteella. Tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen laatii vaatimuksen uudelleen, jotta siitä tulee selkeämpi ja ymmärrettävämpi, ja käyttää siinä käsitteitä yhdenmukaisesti.

2.2.4 MENETTELYJÄ KOSKEVAT VAATIMUKSET

12. Tietosuojaneuvosto huomauttaa, että vaatimuksessa 4.2.1 on useita esimerkkejä tarvittavista tiedoista. Kahden ensimmäisen annetun esimerkin pitäisi kuitenkin olla itsessään vaatimuksia ohjeiden liitteessä 1 olevan 7.2 jakson mukaisesti. Tietosuojaneuvosto kannustaa siksi Luxemburgin valvontaviranomaista muuttamaan sanamuotoa ja sisällyttämään edellä mainitut esimerkit siihen vaatimuksina.

13. Luxemburgin valvontaviranomaisen akkreditointivaatimusten 4.4 jakson (arviointi) osalta tietosuojaneuvosto katsoo, että akkreditointivaatimuksiin pitäisi sisältyä sertifiointielimen velvollisuus varmistaa, että käytössä on arviointimenetelmät ja että nämä sertifiointimekanismissa kuvatut arviointimenetelmät on vakioitu ja ne ovat yleisesti sovellettavissa. Näin varmistettaisiin, että

vertailukelpoisia arviointikohteita varten käytetään vertailukelpoisia arviointimenetelmiä. Sertifiointielimen pitäisi perustella kaikki poikkeamat näistä arviointimenetelmistä. Tietosuojaneuvosto suosittelee siksi, että Luxemburgin valvontaviranomainen muuttaa luonnosta, jotta edellä mainittu sertifiointielimen velvollisuus voidaan sisällyttää siihen.

14. Tietosuojaneuvosto panee lisäksi merkille, että vaatimuksessa 4.4.2 todetaan, että vaikka ulkoistaminen ei ole sallittua, sertifiointielin voi käyttää tietyillä aloilla ulkopuolisia asiantuntijoita. Tämän osalta on tärkeää selventää, että sertifiointielimellä säilyy vastuu päätöksenteosta, vaikka se käyttääkin ulkopuolisia asiantuntijoita. Tietosuojaneuvosto suosittelee näin ollen, että Luxemburgin valvontaviranomainen muuttaa vaatimuksen 4.4.2 sanamuotoa vastaavasti.

15. Tietosuojaneuvosto huomauttaa, että Luxemburgin valvontaviranomaisen akkreditointivaatimusten 4.7 jaksossa (”sertifiointiasiakirjat”) ei käsitellä liitteen vaatimusta valvontajakson dokumentoinnista (7.9 jakso). Tietosuojaneuvosto kannustaa siksi Luxemburgin valvontaviranomaista sisällyttämään vaatimukseen valvontaa käsittelevässä 7.9 jaksossa tarkoitetun valvontajakson.

16. Luxemburgin valvontaviranomaisen akkreditointivaatimusten 4.8 jakson (”sertifioitujen käsittelytoimien hakemisto”) vaatimuksessa 4.8.1 todetaan, että tiedot annetaan yleisölle ”pyynnöstä”. Tietosuojaneuvosto katsoo, että liitteessä 1 olevassa 7.8 jaksossa esitetty avoimuusvelvoite täytettäisiin paremmin, jos sertifiointielin antaisi tiedot saataville ennakoivasti. Tietosuojaneuvosto suosittelee siksi, että Luxemburgin valvontaviranomainen muuttaa luonnosta siten, että sertifiointielimen on annettava julkisesti saataville ohjeiden liitteessä 1 olevassa 7.8 jaksossa tarkoitetut tiedot.

17. Tietosuojaneuvosto panee merkille, että 4.8 jaksossa on valvontaa koskeva otsikko mutta ei vaatimuksia. Tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen selventää, miten valvonta toteutetaan.

18. Tietosuojaneuvosto panee merkille, että sertifioinnin päättämisen, supistamisen, keskeyttämisen tai peruuttamisen (4.10 alajakso) osalta ei viitata sertifiointielimen velvollisuuteen hyväksyä toimivaltaisen valvontaviranomaisen päätöksiä tai määräyksiä peruuttaa asiakkaan (hakijan) sertifiointi tai kieltää sen myöntäminen, jos sertifiointivaatimukset eivät enää täyty. Tämä velvollisuus esitetään yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan h alakohdassa sekä liitteessä 1 olevassa 7.11 jaksossa. Tietosuojaneuvosto suosittelee siksi, että Luxemburgin valvontaviranomainen muuttaa akkreditointivaatimuksia siten, että niissä yksilöidään sertifioinnin peruuttamista, päättämistä, supistamista tai keskeyttämistä koskevat säännöt.

19. Tietosuojaneuvosto panee merkille, että liitteen 9 jaksossa, jossa on yleisiä otsakkeita, ei ole vaatimuksia. Esimerkiksi akkreditoinnin keskeyttämistä tai peruuttamista koskevaa 9.3.4 jaksoa ei käsitellä tässä. Nämä ovat tärkeitä otsakkeita, jotka edellyttävät, että asiaankuuluviin jaksoihin tai vaatimuksiin lisätään ristiviittauksia. Tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen selventää, missä vaatimuksia käsitellään.

3 JOHTOPÄÄTÖKSET / SUOSITUKSET

20. Luxemburgin valvontaviranomaisen akkreditointivaatimusten luonnos voi johtaa sertifiointielinten akkreditoinnin epäyhdenmukaiseen soveltamiseen ja edellyttää seuraavien muutosten tekemistä:

21. Yleisinä huomautuksina tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen

    1. selkeyttää useissa vaatimuksissa (esim. 3.2.1.1 ja 4.1.2) viitatun käsitteen ”vakio” merkitystä Tämä voidaan tehdä esimerkiksi soveltamisalaa tai käsitteitä ja määritelmiä koskevissa osissa.

22. ”Yleisten akkreditointivaatimusten” osalta tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen

    1. selkeyttää, että vaatimuksia ei voida ohittaa millään ulkoisella standardilla, kuten ISAE 3000:lla

    2. muuttaa vaatimusta 1.6 siten, että se sisältää sertifiointielimen velvollisuuden julkaista ja antaa helposti julkisesti saataville kaikki hyväksyttyjen kriteerien versiot ja kaikki sertifiointimenettelyt ohjeiden liitteen mukaisesti.

23. ”Resurssivaatimusten” osalta tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen

    1. laatii vaatimuksen 3.1.1.2 uudelleen, jotta siitä tulisi selkeämpi ja ymmärrettävämpi, ja käyttää siinä käsitteitä yhdenmukaisesti.

24. ”Menettelyjä koskevien vaatimusten” osalta tietosuojaneuvosto suosittelee, että Luxemburgin valvontaviranomainen

    1. muuttaa 4.4 jaksoa siten, että siihen sisältyy sertifiointielimen velvollisuus varmistaa, että käytössä on arviointimenetelmät ja että nämä sertifiointimekanismissa kuvatut arviointimenetelmät on vakioitu ja ne ovat yleisesti sovellettavissa. Sertifiointielimen pitäisi perustella kaikki poikkeamat arviointimenetelmistä

    2. muuttaa vaatimuksen 4.4.2 sanamuotoa, jotta kävisi selväksi, että sertifiointielimellä säilyy vastuu päätöksenteosta, vaikka se käyttääkin ulkopuolisia asiantuntijoita

    3. muuttaa akkreditointivaatimustensa luonnoksen 4.8 jaksoa siten, että sertifiointielimen on annettava julkisesti saataville ohjeiden liitteessä 1 olevassa 7.8 jaksossa tarkoitetut tiedot

    4. selkeyttää 4.8 jaksossa, miten valvonta toteutetaan

    5. muuttaa 4.10 alajaksoa, jotta voitaisiin täsmentää sertifioinnin peruuttamista, päättämistä, supistamista tai keskeyttämistä koskevia sääntöjä.

4 LOPPUHUOMAUTUKSET

25. Tämä lausunto osoitetaan Luxemburgin valvontaviranomaiselle ja se tuodaan julkiseksi yleisen tietosuoja-asetuksen 64 artiklan kohdan 5b mukaisesti.

26. Yleisen tietosuoja-asetuksen 64 artiklan 7 ja 8 kohdan mukaisesti valvontaviranomainen ilmoittaa tietosuojaneuvoston puheenjohtajalle sähköisesti kahden viikon kuluessa lausunnon saamisesta,

pitäytyykö se vaatimusehdotuksessaan vai muuttaako se sitä. Saman ajanjakson kuluessa sen on toimitettava korjattu vaatimusehdotus tai, mikäli se ei aio noudattaa tietosuojaneuvoston lausuntoa kokonaisuudessaan tai osittain, sen on toimitettava asianmukaiset perustelut.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)