Lausunto 16/2020 Tšekin tasavallan toimivaltaisen valvontaviranomaisen päätösluonnoksesta, joka koskee sertifiointielimen akkreditointivaatimusten hyväksymistä 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

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 vaatimukset 43 artiklan mukaisten sertifiointielinten 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 aseteta yksiä vaatimuksia akkreditoinnille, siinä kuitenkin kannustetaan yhdenmukaisuuteen. Tietosuojaneuvosto pyrkii saavuttamaan tämän tavoitteen lausunnoillaan ensinnäkin kannustamalla valvontaviranomaisia laatimaan akkreditointivaatimuksensa sertifiointielinten akkreditointia koskevien tietosuojaneuvoston suuntaviivojen liitteessä esitetyn rakenteen mukaisesti ja toiseksi arvioimalla niitä käyttämällä tietosuojaneuvoston mallia, jossa vaatimuksia voidaan vertailla (standardin ISO 17065 ja sertifiointielinten akkreditointia koskevien tietosuojaneuvoston suuntaviivojen 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 suuntaviivoja 4/2018 sertifiointielinten akkreditoinnista yleisen tietosuoja-asetuksen (2016/679) 43 artiklan mukaisesti, jäljempänä

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

Annettu

’suuntaviivat’, ja suuntaviivoja 1/2018 sertifioinnista ja sertifiointikriteerien määrittelemisestä 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. Tšekin valvontaviranomainen on toimittanut akkreditointivaatimusten luonnoksen Euroopan tietosuojaneuvostolle 43 artiklan 1 kohdan b alakohdan mukaisesti. Asiakirja todettiin täydelliseksi 17. helmikuuta 2020. Tšekin kansallinen akkreditointielin (NAB) akkreditoi sertifiointielimiä, jotka suorittavat sertifiointeja yleisen tietosuoja-asetuksen sertifiointikriteerien mukaan. Tämä tarkoittaa sitä, että Tšekin kansallinen akkreditointielin käyttää sertifiointielinten akkreditoinnissa ISO 17065 -standardia ja valvontaviranomaisen asettamia lisävaatimuksia, kun Tšekin valvontaviranomainen on hyväksynyt ne tietosuojaneuvoston vaatimusluonnoksesta antaman 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] Suuntaviivat 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 Euroopan tietosuojaneuvoston yleiset perustelut sille toimitetun päätösluonnoksen osalta

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 Tšekin valvontaviranomainen on päättänyt turvautua kansalliseen akkreditointielimeen akkreditoinnin myöntämiseksi ja laatinut suuntaviivojen mukaisia lisävaatimuksia, joita kansallisen akkreditointielimen on noudatettava akkreditoinnin myöntämisessä.

4. Tšekin valvontaviranomaisen akkreditointia koskevien lisävaatimusten arvioinnin tarkoituksena on tarkastella sitä, miten vaatimukset eroavat suuntaviivoista ja erityisesti 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 suuntaviivojen tavoitteena on auttaa valvontaviranomaisia akkreditointivaatimustensa määrittämisessä. Suuntaviivojen liite ei sellaisenaan muodosta akkreditointivaatimuksia. Siksi valvontaviranomaisen on määritettävä sertifiointielimiä koskevat akkreditointivaatimukset siten, että niitä voidaan soveltaa käytännössä ja johdonmukaisesti valvontaviranomaisen toimintaympäristön edellyttämällä tavalla.

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 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 suuntaviivojen liitteessä 1, jäljempänä ’liite’, kuvatun rakenteen mukaisesti. Jos Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen jokin tietty kohta jätetään lausunnossa mainitsematta, tietosuojaneuvostolla ei ole sitä koskevia huomautuksia eikä se pyydä Tšekin valvontaviranomaista ryhtymään lisätoimiin.

9. Tässä lausunnossa ei käsitellä niitä Tšekin valvontaviranomaisen 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 Arvioinnin keskeiset kohdat (yleisen tietosuoja-asetuksen 43 artiklan 2 kohta ja tietosuojaneuvoston suuntaviivojen liite 1) siitä, että akkreditointivaatimuksissa määrätään seuraavien yhdenmukaisesta arvioinnista:

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

b. sertifiointielimen riippumattomuus

c. sertifiointielimen eturistiriidat

d. sertifiointielimen asiantuntemus

e. asianmukaiset suojatoimet sen varmistamiseksi, että sertifiointielin soveltaa yleisen tietosuoja-asetuksen sertifiointikriteerejä asianmukaisesti

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

g. 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 suuntaviivojen 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 YLEISET HUOMAUTUKSET

12. Tietosuojaneuvosto panee merkille, että akkreditointivaatimusten luonnoksessa ei täysin noudateta suuntaviivojen liitteessä 1 esitettyä rakennetta. Siitä puuttuvat esimerkiksi soveltamisalaa sekä käsitteitä ja määritelmiä koskevat luvut. Selkeyden vuoksi ja vaatimusten arvioinnin helpottamiseksi tietosuojaneuvosto katsoo tältä osin, että asiakirjan numerointia ja yleistä rakennetta voitaisiin parantaa. Arvioinnin helpottamiseksi tietosuojaneuvosto kehottaa Tšekin valvontaviranomaista noudattamaan akkreditointivaatimusten luonnoksessa liitteen rakennetta ja lisäämään puuttuvat luvut, jotka ovat erityisen tärkeitä koko asiakirjassa käytettyjen termien määrittelyn kannalta. Lisäksi tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa viitataan useaan otteeseen ISO 17065 -standardin vastaavaan osaan tai liitteen vastaaviin osiin täsmentämättä kuitenkaan näitä viittauksia. Tietosuojaneuvosto kehottaa näin ollen Tšekin valvontaviranomaista selventämään viittauksia ISO 17065 -standardin ja liitteen osiin.

13. Tietosuojaneuvosto panee merkille, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa käytetään useaan otteeseen termiä ”arvioitu objekti” (esim. 3.2.1.2.1.2.10, 3.2.1.2.6.3.1, 3.2.1.2.8.1.6.3, 3.2.1.2.10.4.1, 3.1.2.10.7.3.1, 3.1.2.10.7.3.2 ja 3.2.1.2.10.10.2 kohdassa). Tietosuojaneuvoston käsityksen mukaan tätä termiä käytetään synonyymina termille ”arvioinnin kohde”. Selkeyden vuoksi tietosuojaneuvosto kuitenkin kehottaa Tšekin valvontaviranomaista käyttämään johdonmukaisesti termiä ”arvioinnin kohde”.

14. Tietosuojaneuvosto toteaa, että monia vaatimuksia ei ole muotoiltu sertifiointielimen velvoitteiksi (esim. 3.2.1.2.2 ja 3.2.1.2.3 kohta). Tietosuojaneuvosto kehottaa Tšekin valvontaviranomaista laatimaan kyseiset vaatimukset uudelleen ja selventämään niiden pakollisuuden aloittamalla ne ilmaisulla ”sertifiointielimen on [...]”.

2.2.3 YLEISET AKKREDITOINTIVAATIMUKSET

15. Tietosuojaneuvosto toteaa sertifiointisopimuksen (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2 kohta) osalta, että 3.2.1.2.1.2.2 alakohdassa ei viitata ”luottamuksellisiin sopimusasioihin”, joihin valvontaviranomaisella on myös oikeus tutustua. Sen vuoksi tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen muuttaa luonnosta sisällyttämällä siihen velvoitteen antaa valvontaviranomaiselle oikeus tutustua myös luottamuksellisiin sopimusasioihin.

16. Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2.8 alakohdan osalta tietosuojaneuvosto toteaa, että siinä jää epäselväksi, kenelle tiedot on annettava. Tietoneuvosto kehottaa sen vuoksi Tšekin valvontaviranomaista selventämään, kenen on määrä olla tietojen vastaanottaja. Mainittujen tietojen on liitteessä olevan 4.1.2 kohdan 7 alakohdan mukaisesti lisäksi oltava ”sertifioinnin myöntämiseen tarvittavia”. Tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen korvaa ilmaisun ”sertifioinnin myöntämistä koskevat tiedot” ilmaisulla ”sertifioinnin myöntämiseen tarvittavat tiedot”.

17. Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2.9 alakohdan osalta on epäselvää, minkä tyyppisiä tietoja tietosuojaneuvostolle on määrä toimittaa välittömästi. Yleisen tietosuoja-asetuksen 42 artiklan 8 kohdassa säädetään tietosuojaneuvoston velvollisuudesta koota

muun muassa kaikki sertifiointimekanismit. Tässä yhteydessä oletetaan, että toimivaltaiset valvontaviranomaiset toimittavat asiaankuuluvat tiedot tietosuojaneuvostolle, joka sen jälkeen julkaisee ne julkisessa rekisterissä. Sen vuoksi tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen selventää vaatimusten luonnoksen 3.2.1.2.1.2.9 alakohtaa siten, että se vastaa yleisen tietosuoja-asetuksen 42 artiklan 8 kohtaa.

18. Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2.12 alakohdan osalta tietosuojaneuvosto panee merkille, että Tšekin valvontaviranomainen on muotoillut uudelleen osan liitteessä esitettyä vaatimusta. Tšekin valvontaviranomainen on kuitenkin poistanut ilmaisun [tarvittaessa] ”lisäksi käsiteltävä asiakkaalle koituvia seurauksia”. Tietosuojaneuvosto suosittelee sen vuoksi, että Tšekin valvontaviranomainen lisää luonnokseen edellä mainitun puuttuvan vaatimuksen osan.

19. Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2.13 alakohdassa asetetaan lisäksi velvollisuus ”sisällyttää hakijan sitoumus ilmoittaa sertifiointielimelle kaikista muutoksista, jotka voivat vaikuttaa siihen, onko sertifioinnin kohde sertifiointikriteerien mukainen”. Tietosuojaneuvosto katsoo tämän muotoilun olevan liian yleisluonteinen ja suosittelee, että Tšekin valvontaviranomainen muuttaa vaatimusten luonnosta sisällyttäen siihen ilmaisun ”kaikki muutokset sen tosiasiallisessa tai oikeudellisessa tilanteessa ja sen tuotteissa, prosesseissa ja palveluissa, joita sertifiointi koskee”.

20. Tietosuojasinettien ja -merkkien käytön (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.3 kohta) osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen vaatimusten luonnoksessa vahvistetaan, että sertifiointisopimukseen on sisällytettävä ”sertifikaattien, sinettien ja merkkien käyttöä koskevia sääntöjä, jos sertifiointijärjestelmän omistaja niin edellyttää”. Sama sanamuoto on 3.2.1.2.1.2.14 alakohdassa. Tietosuojaneuvosto katsoo, että ISO 17065 -standardin kohdan 4.1.2.2 alakohta I kattaa jo tämän velvoitteen eikä sitä sen vuoksi pitäisi sisällyttää sertifiointijärjestelmään (ks. myös ISO 17065 -standardin kohta 4.1.3). Tietosuojaneuvosto suosittelee näin ollen selvyyden vuoksi, että Tšekin valvontaviranomainen poistaa edellä mainitut kohdat.

21. Tšekin valvontaviranomaisen mallissa antamien tietojen mukaan voidaan puolueettomuuden hallintaa koskevien vaatimusten osalta todeta, että ISO 17065 -standardin kohta 4.2 kattaa riittävästi liitteessä olevan 4.2.1.b) ja 4.2.2 kohdan. Tietosuojaneuvosto katsoo kuitenkin, että nämä vaatimukset on nimenomaisesti sisällytettävä valvontaviranomaisten liitteen mukaisesti laatimaan akkreditointivaatimusten luonnokseen. Tietosuojaneuvosto suosittelee näin ollen, että Tšekin valvontaviranomainen sisällyttää luonnokseen liitteessä esitetyt puolueettomuuden hallintaa koskevat puuttuvat vaatimukset.

22. Korvausvastuuta ja rahoitusta koskevan vaatimuksen (Tšekin valvontaviranomaisen vaatimusten luonnoksen 3.2.1.2.3.1 kohta) osalta tietosuojaneuvosto kehottaa Tšekin valvontaviranomaista täsmentämään, että sen täyttäminen on varmistettava säännöllisesti.

2.2.4 RESURSSIVAATIMUKSET

23. Sertifiointielimen henkilöstön (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.8.1.6 kohta) osalta tietosuojaneuvosto toteaa, että arvioinneista vastaavaa henkilöstöä koskeviin vaatimuksiin (3.2.1.2.8.1.6.3 alakohta) kuuluu ”*viiden vuoden käytännön kokemus sekä vähintään kymmenen suoritettua tarkastusta, jotka on tehty sertifiointitoiminnan puitteissa samalla*

tai vastaavalla alalla [...] tai viiden vuoden käytännön kokemus sellaisten kohteiden sertifioinnista, joihin sertifiointielin on keskittynyt)". Vastaavasti päätöksenteosta vastaavaa henkilöstöä koskeviin vaatimuksiin (3.2.1.2.8.1.6.4 alakohta) sisältyy *"vähintään viiden vuoden käytännön kokemus sekä vähintään kymmenen suoritettua tarkastusta, jotka on tehty sertifiointitoiminnan puitteissa samalla tai vastaavalla alalla"*. Tietosuojaneuvosto katsoo, että arvioijien ja päätöksentekijöiden asiantuntemusta koskevat vaatimukset olisi räätälöitävä ottaen huomioon näiden hoitamat erilaiset tehtävät. Tältä osin tietosuojaneuvosto katsoo, 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 kehottaa Tšekin valvontaviranomaista laatimaan tämän alakohdan uudelleen ja ottamaan huomioon, että arvioijilta vaaditaan erilaista olennaista tietämystä ja/tai kokemusta kuin päätöksentekijöiltä.

24. Tietosuojaneuvosto panee lisäksi merkille, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.9.1 kohdassa todetaan, että ulkoistaminen ei ole sallittua sertifiointitoiminnassa. Seuraavassa kohdassa sallitaan kuitenkin ulkopuolisten tarkastajien ja ulkopuolisten asiantuntijoiden käyttö arvioinnissa, ellei kyseessä ole sertifiointitoiminta. Tietosuojaneuvosto katsoo, että akkreditointivaatimusten luonnoksessa olisi täsmennettävä, milloin "kyseessä on sertifiointitoiminta", tai selvennettävä, että sertifiointielimellä säilyy vastuu päätöksenteosta, vaikka se käyttääkin ulkopuolisia asiantuntijoita. Näin ollen tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen muuttaa luonnosta vastaavasti.

2.2.5 PROSESSIVAATIMUKSET

25. Tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen lisävaatimusten luonnoksen 3.2.1.2.10.1.1 kohdassa viitataan "kaikkiin eturistiriitoja koskeviin lisävaatimuksiin (7.1 kohdan 1 alakohta)". Tšekin valvontaviranomaisen lisävaatimusten luonnokseen ei kuitenkaan sisälly eturistiriitaa koskevia lisävaatimuksia. Tietosuojaneuvosto kehottaa näin ollen Tšekin valvontaviranomaista muuttamaan luonnosta sekaannusten välttämiseksi.

26. Soveltamista koskevien vaatimusten osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.10.2.3 alakohdassa edellytetään ilmeisesti, että siirrettyjä tietoja koskevat tiedot toimitetaan hakemuksessa vain silloin, kun siirto tehdään kolmanteen maahan tai kansainväliselle järjestölle. Tietosuojaneuvosto korostaa kuitenkin, että hakemuksessa on aina oltava kuvaus tiedoista, jotka siirretään muihin järjestelmiin tai järjestöihin niiden sijainnista riippumatta. Tietosuojaneuvosto suosittelee näin ollen, että Tšekin valvontaviranomainen muuttaa sanamuotoa sekaannusten välttämiseksi.

27. Tietosuojaneuvosto panee merkille, että velvoitteessa määrätä sertifiointisopimuksessa sitovista arviointimenetelmistä (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.1.2.6 kohta) ei viitata arvioinnin kohteeseen kuten suuntaviivojen liitteessä olevan 7.3 kohdan 1 alakohdassa. Tietosuojaneuvosto kehottaa selkeyden vuoksi Tšekin valvontaviranomaista sisällyttämään velvoitteeseen kyseisen viittauksen.

28. Tietosuojaneuvosto toteaa lisäksi, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa varaudutaan tilanteeseen, jossa henkilötietojen käsittelijöitä käytetään suorittamaan henkilötietojenkäsittelytoimia suuntaviivojen liitteen mukaisesti (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.10.2 kohta). Tietosuojaneuvosto kehottaa Tšekin

valvontaviranomaista harkitsemaan, olisiko tässä tapauksessa mainittava myös yhteisrekisterinpitäjät ja niitä koskevat erityisjärjestelyt.

29. Arviointia koskevien vaatimusten (Tšekin valvontaviranomaisen vaatimusten luonnoksen 3.2.1.2.10.4 kohta) osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimuksiin ei sisälly sertifiointielimen velvollisuutta esittää sertifiointimekanismissaan yksityiskohtaisesti, miten hakijalle toimitetaan ISO 17065 -standardin kohdassa 7.4.6 vaadittavat tiedot, jotka koskevat poikkeamia sertifiointimekanismista. Liitteen (7.4 alakohdan) mukaisesti on määriteltävä ainakin tällaisten tietojen luonne ja ajoitus. Tietosuojaneuvosto suosittelee näin ollen, että Tšekin valvontaviranomainen lisää vaatimuksiin edellä mainitun velvollisuuden.

30. Tšekin valvontaviranomaisen vaatimusten luonnoksen 3.2.1.2.10.4.2 alakohta näyttää lisäksi rajoittavan testaukseen, auditointiin ja tarkastuksiin liittyviä arviointimenetelmiä. Tietosuojaneuvosto katsoo, että muitakin arviointimenetelmiä voitaisiin käyttää, ja kehottaa siksi Tšekin valvontaviranomaista muuttamaan luonnosta ja tekemään selväksi, että luettelo ei ole tyhjentävä.

31. Tietosuojaneuvosto katsoo Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.10.4.4.1.4 alakohdan osalta, että vaatimuksissa olisi todettava selvästi sertifiointielimen olevan velvollinen tarkastamaan, että kriteerejä noudatetaan. Tietosuojaneuvosto kehottaa Tšekin valvontaviranomaista muuttamaan luonnosta vastaavasti.

32. Tarkastelua koskevien vaatimusten (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.10.5 alakohta) osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa ei viitata velvoitteeseen vahvistaa menettelyjä sertifiointien myöntämistä ja peruuttamista varten. Tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen muuttaa luonnosta vastaavasti.

33. Sertifiointiasiakirjoja koskevien vaatimusten osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.1.2.10.7.2 kohdassa todetaan, että sertifiointielimen on täsmennettävä, että seuranta on sertifioinnin voimassaolon edellytys ”jos seurantaa edellytetään sertifiointijärjestelmässä [...]”. Tietosuojaneuvosto katsoo, että yleisen tietosuoja-asetuksen mukaisen sertifioinnin tapauksessa valvontatoimet ovat aina pakollisia ja suosittelee sen vuoksi, että Tšekin valvontaviranomainen sisällyttää vaatimuksiin tämän velvoitteen.

34. Mitä tulee sertifioitujen tuotteiden hakemistoa koskeviin vaatimuksiin (Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksen 3.2.1.2.10.8 kohta ja liitteessä oleva 7.8 kohta) ja erityisesti velvoitteeseen ilmoittaa toimivaltaiselle valvontaviranomaiselle syyt sertifioinnin myöntämiselle tai peruuttamiselle, tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa viitataan 3.2.1.2.10.4.5 kohtaan. Kyseinen kohta koskee kuitenkin velvoitetta saattaa arviointiasiakirjat pyynnöstä Tšekin valvontaviranomaisen saataville, kun taas suuntaviivojen liitteessä olevan 7.8 kohdan mukaiseen vaatimukseen sisältyy velvoite ilmoittaa valvontaviranomaiselle ennakoivasti syyt sertifioinnin myöntämiselle tai peruuttamiselle. Näin ollen tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen muuttaa luonnosta vastaavasti.

35. Sertifiointiin vaikuttavien muutosten osalta tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnoksessa ei sovittavien menettelyjen yhteydessä mainita toimivaltaisen valvontaviranomaisen suorittamaa hyväksyntämenettelyä, johon viitataan suuntaviivojen liitteessä (sivu 19). Tietosuojaneuvosto toteaa, että liitteessä olevassa 7.10 kohdassa esitetty luettelo ei ole pakollinen. Yhdenmukaisuuden vuoksi tietosuojaneuvosto kuitenkin kehottaa

Annettu

Tšekin valvontaviranomaista lisäämään luonnokseen viittauksen valvontaviranomaisen suorittamaan hyväksyntämenettelyyn.

36. Tietosuojaneuvosto toteaa, että Tšekin valvontaviranomaisen akkreditointivaatimusten luonnokseen ei selkeästi sisälly sertifiointielimen velvollisuutta hyväksyä toimivaltaisen valvontaviranomaisen antamat päätökset ja määräykset, jotka koskevat hakijalle myönnetyn sertifioinnin peruuttamista tai sertifioinnin myöntämättä jättämistä, mikäli sertifiointivaatimukset lakkaavat täyttymästä. Tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen sisällyttää kyseisen velvollisuuden selkeästi akkreditointivaatimusten luonnokseen. Sertifioinnin päättämisen, rajoittamisen, keskeyttämisen tai peruuttamisen osalta tietosuojaneuvosto toteaa, että vaatimusten luonnoksen 3.2.1.2.10.10.2 ja 3.2.1.2.10.10.3 kohdassa viitataan ”aloitteeseen”. Jos tässä tarkoitetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan h alakohdassa säädettyjä valvontaviranomaisen antamia ”päätöksiä ja määräyksiä”, tietosuojaneuvosto kehottaa Tšekin valvontaviranomaista käyttämään samaa terminologiaa kuin yleisessä tietosuoja-asetuksessa ja viittaamaan ”päätöksiin ja määräyksiin”.

2.2.6 HALLINTAJÄRJESTELMÄ

37. Tietosuojaneuvosto katsoo, että Tšekin valvontaviranomaisen lisävaatimusten luonnoksen 3.2.1.2.11 kohtaan ei sisälly sertifiointielimen velvoitetta, jonka mukaan sen on ”pidettävä jatkuvasti ja pysyvällä tavalla julkisesti saatavilla tiedot siitä, mitkä sertifioinnit on suoritettu milläkin perusteella, miten pitkään sertifioinnit ovat voimassa missäkin kehyksessä ja millä edellytyksin”, kuten liitteessä olevassa 8 kohdassa mainitaan. Tietosuojaneuvosto suosittelee näin ollen, että Tšekin valvontaviranomainen muuttaa vaatimusten luonnosta sisällyttämällä siihen edellä mainitun viittauksen.

3 JOHTOPÄÄTÖKSET / SUOSITUKSET

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

39. ”Yleisten akkreditointivaatimusten” osalta tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen

    1) sisällyttää 3.2.1.2.1.2 kohtaan velvoitteen antaa valvontaviranomaiselle oikeus tutustua ”luottamuksellisiin sopimusasioihin”

    2) korvaa 3.2.1.2.1.2.8 alakohdassa ilmaisun ”sertifioinnin myöntämistä koskevat tiedot” ilmaisulla ”sertifioinnin myöntämiseen tarvittavat tiedot”

    3) selventää 3.2.1.2.1.2.9 alakohtaa siten, että se vastaa yleisen tietosuoja-asetuksen 42 artiklan 8 kohtaa

    4) lisää 3.2.1.2.1.2.12 alakohtaan ilmaisun [tarvittaessa] ”lisäksi käsiteltävä asiakkaalle koituvia seurauksia”

    5) muuttaa 3.2.1.2.1.2.13 alakohtaa siten, että siihen sisällytetään ilmaisu ”kaikki muutokset sen tosiasiallisessa tai oikeudellisessa tilanteessa ja sen tuotteissa, prosesseissa ja palveluissa, joita sertifiointi koskee”

    6) poistaa 3.2.1.2.1.3 kohdan ja 3.2.1.2.1.2.14 alakohdan

Annettu

7) sisällyttää luonnokseen liitteessä esitetyt puolueettomuuden hallintaa koskevat puuttuvat vaatimukset.

40. ”Resurssivaatimusten” osalta tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen

1) muuttaa 3.2.1.2.9.1 kohtaa siten, että siinä täsmennetään, milloin ”kyseessä on sertifiointitoiminta”, tai selvennetään, että sertifiointielimellä säilyy vastuu päätöksenteosta, vaikka se käyttääkin ulkopuolisia asiantuntijoita.

41. ”Prosessivaatimusten” osalta tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen

1) sisällyttää 3.2.1.2.10.4 kohtaan sertifiointielimen velvollisuuden esittää sertifiointimekanismissaan yksityiskohtaisesti, miten hakijalle toimitetaan ISO 17065 -standardin kohdassa 7.4.6 vaadittavat tiedot, jotka koskevat poikkeamia sertifiointimekanismista

2) muuttaa 3.2.1.2.10.5 kohtaa siten, että siinä viitataan velvoitteeseen vahvistaa menettelyjä sertifiointien myöntämistä ja peruuttamista varten

3) muuttaa 3.1.2.10.7.2 kohtaa sen huomioon ottamiseksi, että valvontatoimet ovat aina pakollisia yleisen tietosuoja-asetuksen mukaisen sertifioinnin tapauksessa

4) muuttaa 3.2.1.2.10.8 kohtaa siten, että siinä otetaan huomioon sertifiointielimen velvoite ilmoittaa valvontaviranomaiselle ennakoivasti syyt sertifioinnin myöntämiselle tai peruuttamiselle

5) sisällyttää luonnokseen sertifiointielimen velvollisuuden hyväksyä toimivaltaisen valvontaviranomaisen antamat päätökset ja määräykset, jotka koskevat hakijalle myönnetyn sertifioinnin peruuttamista tai sertifioinnin myöntämättä jättämistä, mikäli sertifiointivaatimukset lakkaavat täyttymästä.

42. ”Hallintajärjestelmän” osalta tietosuojaneuvosto suosittelee, että Tšekin valvontaviranomainen

1) sisällyttää luonnokseen sertifiointielimen velvoitteen, jonka mukaan sen on ”pidettävä jatkuvasti ja pysyvällä tavalla julkisesti saatavilla tiedot siitä, mitkä sertifioinnit on suoritettu milläkin perusteella, miten pitkään sertifioinnit ovat voimassa missäkin kehyksessä ja millä edellytyksin”, kuten liitteessä olevassa 8 kohdassa mainitaan.

4 LOPPUHUOMAUTUKSET

43. Tämä lausunto osoitetaan Tšekin valvontaviranomaiselle ja se julkaistaan yleisen tietosuoja-asetuksen 64 artiklan 5 kohdan b alakohdan mukaisesti.

44. Yleisen tietosuoja-asetuksen 64 artiklan 7 ja 8 kohdan mukaisesti Tšekin 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.

Annettu

45. Tšekin valvontaviranomainen ilmoittaa lopullisesta päätöksestä tietosuojaneuvostolle, joka sisällyttää sen rekisteriinsä päätöksistä, kun asia on käsitelty yhdenmukaisuusmekanismissa yleisen tietosuoja-asetuksen 70 artiklan 1 kohdan y alakohdan mukaisesti.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)

Annettu