Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

29.3.2022

MÄÄRÄYS 1/2022: MÄÄRÄYS TIETOTURVALLISUUSTODISTUKSEN MYÖNTÄMISEEN LIITTYVISTÄ MENETTELYISTÄ SERTIFIOINTIEN LOPPUUN SAATTAMISEKSI

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)
32 § 4 momentti, 34 § 4 momentti ja 35 § 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat, jotka ovat käynnistäneet sertifioinnin aiempien säädösten voimassa ollessa ennen 1.9.2021, ja joiden aiempi vaatimustenmukaisuustodistus on vanhenemassa määräyksen voimassaoloaikana tai vanhentunut.

Kansaneläkelaitos

Tietoturvallisuuden arviointilaitokset

Voimaantulo

Määräys tulee voimaan 29. päivänä maaliskuuta 2022 ja se on voimassa 31.12.2022 saakka.

Sisällys

1 Määräyksen tarkoitus

Tällä määräyksellä määrätään poikkeuksista ja täsmennyksistä THL:n määräysten 4/2021 ja 5/2021 mukaisiin menettelyihin.

Määräyksellä määrätään määräaikaiset, 31.12.2022 saakka voimassa olevat menettelyt, joita vaatimustenmukaisuuden osoittamisessa noudatetaan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (jäljempänä asiakastietolaki) (784/2021) sekä sen nojalla annettujen THL:n määräysten 4/2021 ja 5/2021 voimaantulokaudella niille luokkaan A kuuluville tietojärjestelmille, joille on myönnetty aiemman asiakastietolain (159/2007) mukainen vaatimustenmukaisuustodistus, ja joille on käynnistetty todistuksen uudistamiseksi sertifiointiin aiempien säädösten perusteella käytettyjen menettelyjen ja vaatimusten voimassa ollessa. Soveltamisala kuvataan tarkemmin luvussa 2.

Tietojärjestelmien sertifiointiin ja rekisteröintiin liittyvät säännökset ovat eräiltä osin muuttuneet uuden asiakastietolain (784/2021) tultua voimaan 1.11.2021. Aiemman asiakastietolain mukaista vaatimustenmukaisuustodistusta vastaa voimassa olevassa asiakastietolaissa todistus tietoturvallisuuden arvioinnista (tietoturvallisuustodistus).

THL:n määräyksen 4/2021 (määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista, annettu 9.12.2021) kohtaa, jossa määrätään aiempien menettelyjen mukaisesta sertifioinnista, ei voida sellaisenaan soveltaa määräysten voimaantulokaudella (ks. tämän määräyksen liite 1 kohta 7). Kyseinen kohta koskee tietojärjestelmiä, joille on aiemmin hyväksytysti suoritettu tietoturvallisuuden arviointi, ja jotka on ilmoitettu yhteistestaukseen ennen 1.9.2021.

Tietoturvallisuuden arviointi on asiakastietolaissa säädetty edellytys tietojärjestelmän käyttöönotolle ja tarpeellinen tuotantokäyttöön tarkoitettujen tietojärjestelmien tietoturvallisuuden ja tietosuojan varmistamiseksi. Tietoturvallisuustodistus kirjoitetaan vain suoritetuista tietoturvallisuuden arvioinneista. Väliaikaisen tietoturvallisuustodistuksen kirjoittaminen ilman uutta tietoturvallisuuden arviointia ei ole mahdollista voimassa olevan asiakastietolain perusteella. Voimaantulokauden menettelyjä on tarpeen tarkentaa sertifiointien loppuun saattamisen varmistamiseksi siten, että tietojärjestelmien käyttöönotot ovat mahdollisia tietoturvallisuusvaatimukset ja muut voimassa olevan lain asettamat vaatimukset täyttäen.

2 Määräyksen soveltamisala ja THL:n toimivalta antaa määräyksiä

Määräys koskee sosiaali- ja terveydenhuollon asiakas- tai potilastietoja käsittelevien tietojärjestelmien vaatimustenmukaisuuden osoittamisessa noudatettavia menettelyjä, joista säädetään asiakastietolain 7 luvussa Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset.

Tämä määräys koskee tietojärjestelmä ja tietojärjestelmäpalvelujen tuottajia, jotka täyttävät kaikki seuraavat ehdot:

1. tietojärjestelmäpalvelun tuottaja on hakeutunut ennen 1.9.2021 yhteistestaamaan luokkaan A kuuluvaa tietojärjestelmää;
2. tietojärjestelmälle on suoritettu aiemmin tietoturvallisuuden arviointi aiemman asiakastietolain (159/2007) mukaisesti;
3. tietojärjestelmäpalvelun tuottaja on uudistamassa tietojärjestelmälle osana sertifiointia aiemman lain voimassa ollessa kirjoitetun vaatimustenmukaisuustodistuksen voimassa olevan lain mukaiseksi tietoturvallisuustodistukseksi; ja

4. tietojärjestelmäpalvelun tuottaja ja Kela ovat testaamassa yhtä tai useampaa seuraavista Kelan Kanta-yhteistestauksen kokonaisuuksista: määrittelyversion tasonnosto 2014–2016, Resepti-palvelun alaikäisen puolesta-asiointi, potilastiedon arkiston alaikäisen puolesta-asiointi.

Näiltä tietojärjestelmiltä edellytetään tietoturvallisuustodistukseen tarvittavaa tietoturvallisuuden arviointia, ja niihin voidaan soveltaa määräyksen 4/2021 luvun 12 mukaisesti aiemmin voimassa olleita vaatimuksia ja menettelyjä.

Terveyden ja hyvinvoinnin laitoksella on valtuus antaa määräyksiä tämän määräyksen soveltamisalalla seuraavasti: vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä (asiakastietolaki 35 § 3 mom.); mitkä ovat tietojärjestelmien olennaisten vaatimusten merkittäviä poikkeamia ja miten niitä koskevat ilmoitukset tehdään (asiakastietolaki 32 § 4 mom.) sekä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä (asiakastietolaki 34 § 4 mom.).

Tuotantokäyttöönoton edellytyksistä säädetään muun muassa asiakastietolain (784/2021) 31 §:ssä. Tietojärjestelmän käyttöönoton edellytyksenä on muun muassa voimassa oleva todistus tietoturvallisuuden arvioinnista. Tietojärjestelmää ei voida ottaa tuotantokäyttöön, jos sen aiempi vaatimustenmukaisuustodistus on vanhentunut, tai jos tietojärjestelmästä ei ole ajantasaisia tietoja Valviran tietojärjestelmärekisterissä. Tämä määräys ei vaikuta edellä mainittuihin tuotantokäytön edellytyksiin, jotka koskevat sekä tietojärjestelmäpalvelujen tuottajia että sosiaali- ja terveydenhuollon palvelunantajia. Määräys tai sen perustana olevat valtuutussäännökset eivät kohdistu siihen, millä aikataululla palvelunantajat ottavat käyttöön uusia järjestelmäversioita. Määräys kuitenkin kohdistuu järjestelmien sertifiointiin ja siinä käytettäviin menettelyihin, joiden avulla tuotantokäyttöönoton edellytyksiä voidaan täyttää.

Määräys ei koske hyvinvointisovelluksia.

Tässä määräyksessä käytetyt määritelmät ovat THL:n määräyksen 4/2021 luvun 3 mukaiset.

3 Vaatimustenmukaisuuden osoittamisen väliaikaiset menettelyt sertifioinnissa

Vaatimustenmukaisuuden osoittamisessa tulee noudattaa joko THL:n määräysten 4/2021 ja 5/2021 mukaista menettelyä tai tämän määräyksen mukaista menettelyä.

Tämän määräyksen mukaisella menettelyllä tarkoitetaan seuraavaa.

1. Tietoturvallisuuden arvioinnista annettava todistus voidaan myöntää tietoturvallisuuden arviointilaitoksen suorittaman tietoturvallisuuden arvioinnin pohjalta ennen kuin vaaditut, käynnissä olevat yhteistestaukset (Kelan yhteistestauslausunto) ovat hyväksytysti valmistuneet. Näin myönnetystä todistuksesta käytetään tässä määräyksessä nimitystä ”määräaikainen tietoturvallisuustodistus”.

2. Tietoturvallisuuden arvioinnista annettavaan todistukseen on tällöin merkittävä selvästi ”Todistus on määräaikainen kesken olevien yhteistestausten loppuun suorittamiseksi ja edellyttää yhteistestatun järjestelmäversion tietoturvallisuuden uutta arviointia ja uuden todistuksen kirjoittamista.”. Todistuksessa ei eritellä sitä, mitkä yhteistestaukset ovat kesken.

3. Kohdassa 1 tarkoitettu todistus voidaan kirjoittaa voimassa olevaksi enintään 31.12.2022 saakka, johon mennessä on kirjoitettava uusi enintään kolme vuotta asiakastietolain voimaan tulosta voimassa oleva todistus tietoturvallisuuden arvioinnista.

4. Kohtien 1–3 mukaisen tietoturvallisuuden arvioinnin jälkeen järjestelmä on rekisteröitävä Valviran tietojärjestelmärekisteriin.

5. THL:n määräyksessä 5/2021 (luku 10.4, kohta 6) on määritelty, että tuotantokäytössä toimivan järjestelmän ominaisuuksien perustuminen vanhentuneisiin määrittelyversioihin on merkittävä poikkeama[1]. Kyseinen merkittävä poikkeama ei ole tuotantokäyttöönoton estävä tämän määräyksen voimassaoloaikana, jos järjestelmään sovelletaan tämän määräyksen mukaista menettelyä.

6. Järjestelmän tuotantokäytössä toimivan version käyttöönotto on mahdollista myös muilla palvelunantajilla kuin niillä, jotka järjestelmää tällä hetkellä käyttävät tai tilanteissa, joissa järjestelmää käyttävän palvelunantajan organisaatio muuttuu. Käyttöönoton edellytyksenä on voimassa olevan lain mukaisesti yllä kuvatun mukainen voimassa oleva todistus tietoturvallisuuden arvioinnista ja järjestelmän rekisteröinti Valviran tietojärjestelmärekisteriin.

7. Käynnissä olevat yhteistestaukset on suoritettava loppuun voimassa olevien yhteentoimivuusvaatimusten todentamiseksi seuraavien yhteistestauksessa läpikäytävien testauskokonaisuuksien osalta: määrittelyversion tasonnosto 2014–2016, Resepti-palvelun alaikäisen puolesta-asiointi, potilastiedon arkiston alaikäisen puolesta-asiointi. Tietoturvallisuuden arviointi on suoritettava uudelleen yhteistestauksen valmistumisen jälkeen järjestelmäversioon, joka on yhteistestattu tai vastaa yhteistestattua tietoturvallisuusvaatimusten toteutumisen osalta.

8. Kohdan 7 mukaisen tietoturvallisuuden arvioinnin jälkeen järjestelmä on rekisteröitävä uudelleen Valviran tietojärjestelmärekisteriin. Rekisteröinnin yhteydessä tietojärjestelmäpalvelun tuottajan on ilmoitettava Valviralle tiedot hyväksytysti suoritetuista yhteistestauksista ja suoritetusta uudesta tietoturvallisuuden arvioinnista kuten määräyksessä 4/2021 määrätään.

9. Tietoturvallisuuden arvioinnissa kohdissa 1–3 ja 7 sovelletaan määräyksen 4/2021 luvussa 12 kuvatulla tavalla joko järjestelmän sertifiointiprosessin käynnistyessä voimassa olleita määräyksen 1/2015 tietoturvallisuusvaatimuksia tai määräyksen 5/2021 mukaisia tietoturvallisuusvaatimuksia.

10. Määräyksen mukaista menettelyä käyttävissä järjestelmissä käytetään määräyksen 2/2016 liitteen 4 mukaista järjestelmälomaketta, ei määräyksen 5/2021 liitteen 4 mukaista järjestelmälomaketta, kun tietojärjestelmän tiedot ilmoitetaan yhteistestaukseen, tietoturvallisuuden arviointiin sekä Valviran tietojärjestelmärekisteriin. Järjestelmälomakkeen kohtaan ”Järjestelmän luokka” merkitään kuitenkin määräyksen 4/2021 mukainen järjestelmän tarkempi luokka (esimerkiksi A2 tai A3). Yhdelle tietojärjestelmän versiolle käytetään vain yhtä versiota järjestelmälomakkeesta. Määräyksen 5/2021 mukaista lomaketta käytetään kuitenkin viimeistään siinä vaiheessa, järjestelmälle kohdan 7 mukaisesti myönnettyä tietoturvallisuustodistusta ollaan myöhemmin uudistamassa määräyksen 5/2021 vaatimusten mukaisesti.

[1] Tuotantokäytössä toimivassa järjestelmässä toteutettujen ominaisuuksien perustuminen vanhentuneeseen määritysversioon, jonka voimassaolo on päättynyt tai tuki Kanta-palveluissa on poistunut tai poistumassa siten, että järjestelmässä ei ole pystytty tai ei pystytä siirtymään voimassa olevien vaatimusten mukaiseen toteutukseen säännösten tai valvontaviranomaisen edellyttämässä määräajassa.

Edellä kuvattua menettelyä vaatimustenmukaisuuden osoittamisessa voidaan soveltaa tämän määräyksen voimassa ollessa 31.12.2022 saakka. Muiden kuin tässä määräyksessä täsmennettyjen menettelyiden ja seikkojen osalta sertifioinnissa toimitaan määräysten 4/2021 ja 5/2021 mukaisesti.

Jos tietojärjestelmäpalvelun tuottaja toimii tässä määräyksessä kuvatun menettelytavan mukaisesti, sen on ilmoitettava asiasta kirjallisesti tietoturvallisuuden arviointilaitokselle, Kelalle ja Valviralle ennen tietoturvallisuuden arvioinnin käynnistämistä, kuitenkin viimeistään 9.6.2022. Tietojärjestelmäpalvelun tuottajan tulee ilmoittaa tässä yhteydessä, käytetäänkö tietoturvallisuuden arvioinnissa määräyksen 1/2015 vai määräyksen 5/2021 mukaisia vaatimuksia sekä kohdan 1 että kohdan 7 mukaisen arvioinnin osalta[2].

Jos tietojärjestelmäpalvelun tuottaja toimii tässä määräyksessä kuvatun menettelytavan mukaisesti, sen on ilmoitettava asiasta kirjallisesti viimeistään 9.6.2022 niille asiakkaanaan toimiville palvelunantajille, joiden tuotantokäyttöönottoihin asia liittyy. Tässä yhteydessä tietojärjestelmäpalvelun tuottajan on ilmaistava, että järjestelmässä ei ole hyväksytysti yhteistestattu kohdan 7 mukaisiin testauskokonaisuuksiin liittyviä vaatimuksia.

4 Määräyksen suhde muihin määräyksiin

Tämän määräyksen liitteessä 1 on eritelty yksityiskohtaisesti ne THL:n määräysten 4/2021 ja 5/2021 kohdat, joita ei sovelleta tai joita sovelletaan poikkeavasti tämän määräyksen kohteena oleviin tietojärjestelmiin sekä määrätty miten mainittuja kohtia on sovellettava kyseisissä tietojärjestelmissä.

Kaikkia tämän määräyksen liitteessä 1 eriteltyjä määräysten 4/2021 ja 5/2021 kohtia sovelletaan muutettuina siten kuin liitteessä 1 on määrätty. Tämän määräyksen liitteen 1 mukainen soveltaminen kohdistuu vain luvussa 2 määritellyt ehdot täyttäviin tietojärjestelmiin, jotka käyttävät tämän määräyksen luvun 3 mukaisia menettelyitä määräyksen voimassaoloaikana. Tämä määräys ei vaikuta muiden määräysten ja säännösten sisältöihin tai määräaikoihin muuten kuin luvuissa 3 ja 4 sekä liitteessä 1 on kuvattu. Myös määräysten 4/2021 ja 5/2021 sisältämissä *liitteissä* olevia seikkoja sovelletaan tämän määräyksen ja liitteen 1 mukaisesti.

5 Ohjaus ja neuvonta

Terveyden ja hyvinvoinnin laitos ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa. Lisätietoja olennaisista vaatimuksista ja sertifiointiprosessista löytyy myös THL:n verkkosivustolta ja Kanta.fi-verkkosivustolta.

Kansaneläkelaitos ohjaa Kanta-palveluihin liittyvien tietojärjestelmien käyttöönottoja.

6 Voimaantulo

Tämä määräys tulee voimaan 29. päivänä maaliskuuta 2022 ja on voimassa 31.12.2022 saakka.

[2] Sekä määräyksen 1/2015 että määräyksen 5/2021 mukaisten vaatimusten käyttäminen tietoturvallisuuden arvioinnin kriteereinä on mahdollista tämän määräyksen voimassa ollessa. Jos tietoturvallisuuden arvioinnin kriteereinä kohdassa 7 käytetään määräyksen 1/2015 mukaisia vaatimuksia, tietoturvallisuustodistus voidaan kirjoittaa voimassa olevaksi enintään kolmen vuoden ajaksi asiakastietolain voimaantulosta määräyksen 4/2021 luvun 12 mukaisesti. Jos kriteereinä käytetään määräyksen 5/2021 mukaisia vaatimuksia, tietoturvallisuustodistus voidaan kirjoittaa voimassa olevaksi enintään kolmen vuoden ajaksi todistuksen myöntämisestä, ks. myös liite 1 kohta 7.

Sirpa Soini
Osastonjohtaja

Jarmo Kärki
Yksikönpäällikkö,

Jakelu

Kansaneläkelaitos
Tietoturvallisuuden arviointilaitokset
Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat
Sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat
Sosiaali- ja terveydenhuollon palvelunantajat
Sosiaali- ja terveysministeriö
Suomen Kuntaliitto ry
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
Liikenne- ja viestintävirasto Traficom
Tietosuojavaltuutetun toimisto
Aluehallintovirastot

Tämä määräys on julkaistu viranomaisten määräyskokoelmissa

https://www.finlex.fi/fi/viranomaiset/normi/561001/ (FINLEX ® - Viranomaisten määräyskokoelmat: Terveyden ja hyvinvoinnin laitos) ja saatavissa:

Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä

Internet-osoitteesta https://thl.fi/fi/web/tiedonhallinta-sosiaalija-terveysalalla/maaraykset-ja-maarittelyt/maaraykset

Liite 1. Poikkeukset ja täsmennykset THL:n määräysten 4/2021 ja 5/2021 mukaisiin menettelyihin

Kaikkia liitteen poikkeuksia ja täsmennyksiä noudatetaan vain tämän määräyksen 1/2022 voimassaoloaikana ja vain tämän määräyksen kohderyhmärajausten mukaisesti.

1.

Alkuperäisteksti (THL:n määräys 4/2021 luku 7.3. kappale 10): *Tietoturvallisuustodistus tulisi kirjoittaa kolme vuotta voimassa olevaksi, ellei viranomaisten määräyksistä tai ohjeista johtuen tai tiedossa olevan olennaisten vaatimusten tai muiden säännösten uudistamisen vuoksi lyhyempi voimassaolo ole välttämätön.*

Täsmennys: Määräaikainen tietoturvallisuustodistus sertifioinnin loppuun saattamiseksi voidaan kirjoittaa tämän määräyksen luvun 3 mukaisesti 31.12.2022 saakka voimassa olevaksi. Yhteistestatun version tietoturvallisuuden arvioinnista kirjoitettava todistus tulisi kirjoittaa voimassa olevaksi määräyksen 4/2021 mukaisesti kolme vuotta asiakastietolain voimaan tulosta, jos arvioinnissa käytetään määräyksen 1/2015 mukaisia kriteerejä ja kolme vuotta todistuksen myöntämisestä, jos arvioinnissa käytetään määräyksen 5/2021 mukaisia kriteerejä.

2.

Alkuperäisteksti (THL:n määräys 4/2021 luku 7.3. kappale 11 ja 12)*: Luokkaan A2 ja A3 kuuluvalle järjestelmälle voidaan kirjoittaa tietoturvallisuustodistus vasta sen jälkeen, kun järjestelmä on hyväksytysti läpäissyt yhteistestauksen. Jos luokan A2 tai A3 tietojärjestelmä on sertifioitavana siten, että sille suoritetaan sekä yhteistestaus että tietoturvallisuuden arviointi, on tietojärjestelmäpalvelun tuottajan huolehdittava siitä, että yhteistestauksen ja tietoturvallisuuden arvioinnin kohteena on sama järjestelmäversio tai sellainen versio, jossa yhteistestattaviin olennaisiin vaatimuksiin liittyvät mahdolliset järjestelmämuutokset eivät vaikuta arvioitaviin tietoturvavaatimuksiin. Ennen tietoturvallisuustodistuksen antamista luokkaan A2 tai A3 kuuluvalle järjestelmälle tietoturvallisuuden arviointilaitos varmistaa tietojärjestelmäpalvelun tuottajalta ja Kelalta, että yhteistestauksen kohteena olevaan järjestelmään ei ole tulossa muutoksia, jotka voisivat vaikuttaa tietoturvavaatimusten toteuttamiseen.*

Poikkeus: Ei sovelleta luvun 3 mukaiseen määräaikaiseen tietoturvallisuustodistukseen: määräaikainen tietoturvallisuustodistus voidaan kirjoittaa tietoturvallisuuden hyväksytyn arvioinnin jälkeen, vaikka käynnissä olevan yhteistestauksen osalta ei ole saatavilla Kelan lausuntoa hyväksytysti suoritetusta yhteistestauksesta. Alkuperäistekstin mukaista kohtaa sovelletaan määräaikaisen todistuksen jälkeen myönnettävään yhteistestatun version tietoturvallisuustodistukseen.

3.

Alkuperäisteksti (THL:n määräys 4/2021 luku 8 kappale 2)*: Mikäli tietojärjestelmä kuuluu luokkaan A1, A2 tai A3 ja on sertifioitava, rekisteröinti Valviran tietojärjestelmien rekisteriin edellyttää sitä, että järjestelmän käyttötarkoitusta vastaavat olennaiset vaatimukset on hyväksytysti todennettu yhteistestauksessa ja tietoturvallisuuden arvioinnissa. Tällöin ilmoitus ja järjestelmälomake toimitetaan Valviraan, kun järjestelmään kohdistuva yhteistestaus tai tietoturvallisuuden arviointi on suoritettu loppuun hyväksytysti.*

Poikkeus: Rekisteröinti tehdään tämän määräyksen luvun 3 kohdan 4 mukaisesti nojautuen määräaikaiseen tietoturvallisuustodistukseen. Rekisteröinti on uudistettava luvun 3 ja määräyksen 4/2021 mukaisesti yhteistestatulle järjestelmäversiolle, kun yhteistestaus suhteessa uusimpiin määrittelyversioihin ja yhteistestatun version tietoturvallisuuden arviointi on suoritettu.

4.

Alkuperäisteksti (THL:n määräys 4/2021 luku 9 kappale 1)*: Sekä luokkaan A että B kuuluvan tietojärjestelmän on täytettävä järjestelmän käyttötarkoitusta vastaavat olennaiset vaatimukset (ks. luku 6) ennen kuin järjestelmä voidaan ottaa tuotantokäyttöön. Tuotantokäyttöönoton edellytykset on kuvattu asiakastietolain 31 §:ssä.*

Täsmennys: Kohtaa sovelletaan siten, että meneillään olevien tämän määräyksen luvussa 2 ilmaistujen yhteistestausten kohteena olevien vaatimusten perustuminen tietojärjestelmässä aiempiin määrittelyversioihin ei muodosta sellaista merkittävää poikkeamaa, joka estää käyttöönoton. Meneillään olevien yhteistestausten kohteena olevat vaatimukset on täytettävä ja niiden yhteistestaus saatettava hyväksytysti loppuun ennen tämän määräyksen voimassaolon päättymistä ja ennen luvun 3 mukaisen määräaikaisen tietoturvallisuustodistuksen voimassaolon päättymistä. Ks. myös kohta 3.

5.

Alkuperäisteksti (THL:n määräys 4/2021 luku 9 kappale 4): *Kanta-palveluihin liitettävän luokan A tietojärjestelmän on oltava hyväksytysti yhteistestattu voimassa olevien määrittelyjen mukaisesti, jotta se voidaan liittää Kanta-palveluihin. Yhteistestaus suoritetaan järjestelmän käyttötarkoituksen mukaisessa laajuudessa (ks. tämän määräyksen luku 6). Niistä toiminnoista ja tietosisällöistä, jotka liittyvät järjestelmässä Kanta-palvelujen kautta toteutettaviin ominaisuuksiin ja jotka sisältyvät Kanta-palvelujen yhteistestauksen testauskokonaisuuksiin on oltava lausunto yhteistestauksen hyväksymisestä Kelalta. Järjestelmätoteutuksen, yhteistestauksen ja puoltavan lausunnon on perustuttava sellaisiin määrittelyihin ja määrittelyversioihin, joita kulloinkin edellytetään Kanta-palveluihin liittyvältä järjestelmältä.*

Poikkeus: Sovelletaan siten, että määräyksen kohderyhmään kuuluvalta Kanta-palveluihin liitettävältä järjestelmältä edellytetään määräyksen luvun 3 mukaisen menettelyn kohdissa 1-6 sitä, että se jo toimii tuotantokäytössä aiemmin hyväksytysti yhteistestattujen ja Kanta-palveluissa tällä hetkellä tuettujen määrittelyjen mukaisesti, ja uudempien Kanta-palveluissa edellytettävien määrittelyversioiden mukainen yhteistestaus niissä tämän määräyksen luvun 3 kohdan 7 mukaisissa vaatimuksissa jotka sisältyvät järjestelmän käyttötarkoitukseen on käynnistetty.

6.

Alkuperäisteksti (THL:n määräys 4/2021 luku 10 kappale 3): *Tietojärjestelmä on tarvittaessa yhteistestattava suhteessa voimassa oleviin tai yhteistestauksessa edellytettäviin määrittelyihin ennen tietoturvallisuuden arvioinnista annettavan uusitun todistusten myöntämistä.*

Poikkeus: Ei sovelleta määräaikaiseen tietoturvallisuustodistukseen, ks. luku 3.

7.

Alkuperäisteksti (THL:n määräys 4/2021 luku 12 kappale 5): *Määräyksessä kuvattuja luokittelu- ja sertifiointimenettelyjä sovelletaan kaikkiin sertifioitaviin järjestelmiin viimeistään kuusi kuukautta määräyksen voimaantulosta alkaen. Järjestelmälle, jonka yhteistestaus on käynnistetty ennen 1.9.2021 voidaan suorittaa sertifiointiprosessi loppuun kuuden kuukauden kuluessa määräyksen voimaantulosta niiden vaatimusten, säädösten ja menettelyjen mukaisesti, jotka olivat voimassa prosessin käynnistyessä. Tietoturvallisuustodistus on tällöin mahdollista kirjoittaa voimassa olevaksi enintään kolmen vuoden ajaksi asiakastietolain voimaantulosta, ja todistuksessa on oltava selvä merkintä siitä, että arviointi on suoritettu lain 159/2007 vaatimusten mukaisesti. (…) Järjestelmät, joiden aiemman (lain 159/2007 mukaisen) vaatimustenmukaisuustodistuksen voimassaolo päättyy yli 6*

kk tämän määräyksen voimaantulosta tai sen jälkeen, on todennettava olennaiset vaatimukset tämän määräyksen ja määräyksen 5/2021 mukaisesti ennen vaatimustenmukaisuustodistuksen voimassaolon päättymistä.

Poikkeus: Määräyksen 4/2021 mukaisia menettelyjä sovelletaan tämän määräyksen kohteena oleviin tietojärjestelmiin tässä määräyksessä kuvatuin tarkennuksin ja poikkeuksin tämän määräyksen voimassaoloaikana. Järjestelmälle, jonka yhteistestaus on käynnistetty ennen 1.9.2021 voidaan suorittaa sertifiointiprosessi loppuun tämän määräyksen voimassaoloaikana, ei pelkästään kuuden kuukauden kuluessa määräyksen 4/2021 voimaantulosta. Täsmennys: Jos luvun 3 kohdan 7 mukainen tietoturvallisuuden arviointi suoritetaan aiemmin voimassa olleiden vaatimusten pohjalta, vaatimustenmukaisuustodistus voidaan kirjoittaa voimassa olevaksi määräyksen 4/2021 mukaisesti enintään kolmen vuoden ajaksi voimassa olevan asiakastietolain voimaantulosta.

8.

Alkuperäisteksti (THL:n määräys 4/2021 luku 12 kappale 8): *Aiemman asiakastietolain 159/2007 sekä THL:n määräysten 1/2015 ja 2/2016 nojalla sertifioitujen järjestelmien vaatimustenmukaisuustodistus on uudistettava tämän määräyksen mukaiseksi tietoturvallisuustodistukseksi ennen aiemman lain mukaisen vaatimustenmukaisuustodistuksen voimassaolon päättymistä, kuitenkin viimeistään kolmen vuoden kuluessa asiakastietolain voimaantulosta. Uudistamisen yhteydessä tietojärjestelmäpalvelun tuottajan on varmistettava, että järjestelmään on toteutettu ja sertifioitu kaikki sen käyttötarkoitusta vastaavat olennaiset vaatimukset.*

Poikkeus: Tämän määräyksen kohderyhmään kuuluvissa järjestelmissä kyseessä on jo vanhentuneen tai vanhenevan aiemman lain nojalla myönnetyn todistuksen uudistaminen voimassa olevan lain mukaiseksi tietoturvallisuustodistukseksi. Aiempi vaatimustenmukaisuustodistus on uudistettava voimassa olevan asiakastietolain ja määräyksen 4/2021 mukaiseksi tietoturvallisuustodistukseksi tämän määräyksen luvussa 3 kuvatulla tavalla ja aikataululla, mitä ennen voidaan kirjoittaa tämän määräyksen luvun 3 mukaisesti voimassa oleva määräaikainen tietoturvallisuustodistus.

9.

Alkuperäisteksti (THL:n määräys 5/2021 luku 7 kappale 6 ja 8): *Järjestelmän käyttötarkoitukseen sisältyvien profiilien edellyttämien vaatimusten toteuttaminen tai täyttäminen sekä niiden todentaminen yhteistestauksessa tai tietoturvallisuuden arvioinnissa siltä osin kuin vaatimukset ovat sertifioinnissa todennettavia on edellytys luokan A tietojärjestelmien hyväksytylle sertifioinnille ja tuotantokäyttöönotolle.*

Mikäli kyseessä on luokan A tietojärjestelmä, rekisteröinti Valviran tietojärjestelmärekisteriin edellyttää sitä, että profiilin mukaisiin toimintoihin liittyvät yhteentoimivuuden ja tietoturvallisuuden vaatimukset on hyväksytysti todennettu yhteistestauksessa ja tietoturvallisuuden arvioinnissa ja että tietojärjestelmä on saanut tietoturvallisuustodistuksen.

Täsmennys: Sovelletaan yhteistestattavien vaatimusten osalta tämän määräyksen luvun 3 sekä tämän liitteen kohtien 2, 3, 4, 5 ja 6 mukaisesti.

10.

Alkuperäisteksti (THL:n määräys 5/2021 luku 8 kohta 13, kappale 7 ja kappale 13): *Kanta-palveluihin liittyviin määrityksiin liittyvät järjestelmää koskevat toiminnalliset vaatimukset (toiminnot ja tietosisällöt, kohdat 3–8), on toteutettu, täytetty ja dokumentoitu siten, että järjestelmälle voidaan hyväksytysti suorittaa tarvittavat yhteistestaukset Kelan Kanta-palvelujen yhteistestauksen ohjeiden mukaisesti.*

Luokan A2 tai A3 tietojärjestelmän tuotantokäyttöönotto edellyttää sitä, että kaikki järjestelmän Kanta-palveluihin liittyvät toiminnot ja tietosisällöt, joihin kohdistuu yhteistestauksen sisältöjä, on hyväksytysti yhteistestattu (ks. myös määräys 4/2021 luku 9).

Tietojärjestelmäpalvelun tuottajan on seurattava asiakastietolain 32 § mukaisesti olennaisten vaatimusten muutoksia ja tehtävä muutosten edellyttämät korjaukset. Jos muutokset edellyttävät uutta yhteistestausta tai uutta tietoturvallisuuden arviointia, nämä toimenpiteet on suoritettava ennen muutokset sisältävän tietojärjestelmän version tuotantokäyttöön ottamista.

Täsmennys: Sovelletaan yhteistestattavien vaatimusten osalta tämän määräyksen luvun 3 sekä tämän liitteen kohtien 2, 3, 4, 5, 6 ja 9 mukaisesti.

11.

Alkuperäisteksti (THL:n määräys 5/2021 luku 8 kappale 14) *Tietojärjestelmäpalvelun tuottajan on tarkistettava vähintään tietoturvallisuustodistuksen uusimiseen hakeutuessaan, että tietojärjestelmässä on yhteistestattu Kanta-palveluihin liittyvät ominaisuudet voimassa olevien määritysten ja määritysversioiden mukaisesti määräys 4/2021 luvun 10 mukaisesti.*

Poikkeus: Sovelletaan luvun 3 ja tämän liitteen kohdan 4 mukaisesti: kohtaa ei sovelleta niihin vaatimuksiin, jotka ovat käynnissä olevan yhteistestauksen kohteena, kun järjestelmälle ollaan hakemassa määräaikaista tietoturvallisuustodistusta.

12.

Alkuperäisteksti (THL:n määräys 5/2021 luku 10.3 kohta 1): *Tuotantokäytössä olevan tai sertifioitavan järjestelmän tulee toteuttaa kukin järjestelmään toteutettu olennainen vaatimus voimassa olevien määritysten mukaisesti, jos määritys sisältää järjestelmän luokkaa ja käyttötarkoitusta vastaavia vaatimuksia.*

Täsmennys: Sovelletaan luvun 3 ja tämän liitteen kohdan 4 mukaisesti: kohtaa sovelletaan yhteistestauksen kohteena olevien vaatimusten osalta niihin järjestelmiin joissa käytetään tämän määräyksen mukaista menettelyä vain luvun 3 mukaisen menettelyn kohdissa 7-8, kun yhteistaus ja tietoturvallisuuden arviointi suoritetaan loppuun tämän määräyksen mukaisten määräaikojen puitteissa.

13.

Alkuperäisteksti (THL:n määräys 5/2021 luku 10.4 kohta 5): *Tuotantokäytössä toimivan järjestelmän vaatimustenmukaisuustodistuksen tai tietoturvallisuuden arviointitodistuksen vanheneminen, erityisesti todistuksen uusimisen pitkittyessä tietojärjestelmän valmistajasta tai tietojärjestelmäpalvelun tuottajasta johtuvista syistä.*

Täsmennys: Vanheneva tai vanhentunut vaatimustenmukaisuustodistus voidaan uudistaa määräaikaisesti ennen yhteistestauksen ja yhteistestatun version tietoturvallisuuden arvioinnin loppuun saattamista tämän määräyksen luvun 3 mukaisesti. Valvira päättää merkittävien poikkeamien merkitsemisestä tietojärjestelmärekisteriin.

14.

Alkuperäisteksti (THL:n määräys 5/2021 luku 10.4 kohta 6): *Tuotantokäytössä toimivassa järjestelmässä toteutettujen ominaisuuksien perustuminen vanhentuneeseen määritysversioon, jonka voimassaolo on päättynyt tai tuki Kanta-palveluissa on poistunut tai poistumassa siten, että järjestelmässä ei ole pystytty tai ei pystytä siirtymään*

voimassa olevien vaatimusten mukaiseen toteutukseen säännösten tai valvontaviranomaisen edellyttämässä määräajassa.

Täsmennys: Kyseinen seikka ei ole käyttöönoton estävä merkittävä poikkeama tämän määräyksen voimassaoloaikana määräyksen kohderyhmään kuuluvissa tietojärjestelmissä, mikäli uudempi määritysversio on järjestelmälle suoritettavassa sertifioinnissa käynnissä olevan yhteistestauksen kohteena. Valvira voi kuitenkin merkitä tietojärjestelmärekisteriin merkittävän poikkeaman.

15. Alkuperäisteksti (THL:n määräys 5/2021 luku 10.4 kappale 3 ja 4): *Mikäli osana sertifiointiprosessia havaitaan sellainen poikkeama olennaisista vaatimuksista, joka johtaisi merkittävään poikkeamaan tuotantokäytössä, ei sertifiointia voida hyväksytysti suorittaa loppuun ennen kuin poikkeaman aiheuttava seikka on korjattu tai poikkeamasta koituvat virhetilanteet muulla tavoin estetty. Vaatimukset, jotka eivät täyty tai täyttyvät puutteellisesti voivat aiheuttaa korjaustarpeen ennen yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä, kuten luvussa 10.2 on kuvattu.*

Täsmennys: Sovelletaan määräaikaiseen tietoturvallisuustodistukseen ja määräyksen mukaista menettelyä käyttävään järjestelmään luvun 3 ja tämän liitteen kohdan 13 sekä muiden liitteen 1 kohtien mukaisesti: määräaikaisen tietoturvallisuustodistuksen myöntämisen yhteydessä ei tarkastella niitä vaatimuksia, jotka ovat käynnissä olevien yhteistestausten kohteena. Sekä määräaikaiseen tietoturvallisuustodistukseen tähtäävässä että yhteistestatulle versiolle suoritettavassa tietoturvallisuusvaatimusten arvioinnissa on tietoturvallisuusvaatimukset täytettävä alkuperäistekstin mukaisesti.