Tietopalvelut
Sote-tieto ja -tiedonhallinta

9.12.2021

MÄÄRÄYS SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN LUOKITTELUSTA JA SERTIFIOINNISTA

VANHENTUNUT

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) 29 §:n 4 momentti, 32 §:n 4 momentti, 34 § 4 momentti ja 35 §:n 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat ja tietojärjestelmien valmistajat
Asiakastietojen välityspalvelujen tuottajat
Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Kansaneläkelaitos
Tietoturvallisuuden arviointilaitokset
Välittäjät

Voimaantulo

Määräys tulee voimaan 9. päivänä joulukuuta 2021 ja se on voimassa toistaiseksi.

Tämä määräys kumoaa aiemmat THL:n määräykset 1/2015 ja 2/2016. Aiemmat määräykset on annettu asiakastietolain 159/2007 nojalla. Lailla 784/2021 on kumottu laki 159/2007.

Sisällys

VANHENTUNUT

1 Määräyksen tarkoitus

Tämä määräys kuvaa sosiaali- ja terveydenhuollon tietojärjestelmien luokittelussa sekä niihin kohdistuvien olennaisten vaatimusten toteuttamisessa sekä sertifioinnissa käytettävät menettelyt ja vastuut. Määräys ohjaa tietojärjestelmien vaatimustenmukaista toteuttamista, järjestelmiltä edellytettävien selvitysten antamista, sertifiointiin kuuluvaa yhteistestausta ja tietoturvallisuuden arviointia sekä järjestelmien rekisteröintiä ja käyttöönottoa.

2 Määräyksen soveltamisala

Määräys koskee sosiaali- ja terveydenhuollon asiakas- tai potilastietoja käsittelevien tietojärjestelmien luokittelussa ja vaatimustenmukaisuuden osoittamisessa noudatettavia menettelyjä sekä annettavan selvityksen sisältöä (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, jäljempänä asiakastietolaki, 7 luku ”Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset”). Terveyden ja hyvinvoinnin laitoksella (jäljempänä THL) on asiakastietolain 34 §:n 4 momentin perusteella valtuus antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä. Asiakastietolain 35 §:n 3 momentin perusteella THL:lla on valtuus antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä. Asiakastietolain 29 §:n 4 momentin perusteella THL voi antaa määräyksiä tietojärjestelmien luokkien määräytymisestä.

Tämä määräys koskee:

- valtakunnallisiin tietojärjestelmäpalveluihin (Kanta-palvelut) liitettäviksi tarkoitettuja asiakas- ja potilastietoja käsitteleviä tietojärjestelmiä (luokka A),
- muita käyttötarkoituksensa perusteella sertifioitavia tietojärjestelmiä ja välittäjien palveluja (luokka A),
- muita sosiaali- ja terveydenhuollon järjestelmiä, joiden käyttötarkoituksena on asiakas- ja potilastietojen käsittely (luokka B).

3 Määritelmät

Tässä määräyksessä tarkoitetaan:

- *Asiakastietojen välityspalvelulla* sosiaali- ja terveydenhuollon organisaation tai apteekin Kanta-palveluihin liittymisessä hyödyntämää tietojärjestelmää tai osajärjestelmää, jonka kautta teknisesti siirretään toisen tietojärjestelmän tai osajärjestelmän tuottamia asiakastietoja Kanta-palveluihin tai hyödynnetään toisella tietojärjestelmällä tai osajärjestelmällä Kanta-palveluissa olevia asiakastietoja ja jossa ei ole Kanta-palveluihin liittyvän tietojärjestelmän loppukäyttäjille suunnattuja ominaisuuksia. Lisätietoja ks. Liite 1.
- *Kanta-palveluilla* sosiaali- ja terveydenhuollon valtakunnallisia tietojärjestelmäpalveluita, joita ovat asiakastietolain 6 §:n mukaiset Kansaneläkelaitoksen (jäljempänä Kela) tuottamat tietojärjestelmäpalvelut.
- *Olennaisella vaatimuksella* asiakastietolain 34 §:n mukaista tietojärjestelmän toiminnallisuuteen, yhteentoimivuuteen tai tietoturvallisuuteen kohdistuvaa kansallisesti asetettua vaatimusta, joka voi perustua vaatimuksessa viitattuihin lähdedokumentteihin, kuten eri säädöksiin tai määrityksiin.

VANHENTUNUT

- *Osajärjestelmällä* tietojärjestelmää tai sitä vastaavaan käyttöön suunniteltua ja toteutettua ohjelmistoa, joka toimii osana laajempaa tietojärjestelmää tai tietojärjestelmäkokonaisuutta ja joka on tarkoitettu liitettäväksi muihin asiakastietoja käsitteleviin tietojärjestelmiin tai osajärjestelmiin. Osajärjestelmä voidaan sertifioida ja ottaa käyttöön osana laajempaa tietojärjestelmäkokonaisuutta ja rekisteröidä erikseen, mikäli osajärjestelmän käyttötarkoitus ja siihen kohdistuvat olennaiset vaatimukset on kuvattu ja todennettu vastaavasti kuin yleisesti tietojärjestelmillä ja osajärjestelmän liittyminen muihin tietojärjestelmiin tai osajärjestelmiin on kuvattu määräysten mukaisesti.

- *Palvelunantajalla* asiakastietolain 3 §:n 1 momentissa tarkoitettua palvelunantajaa:
    - terveydenhuollon toimintayksikköä (potilaslaki (785/1992) 2 § 1 mom. 4) kohta)
    - työnantajaa (työterveyshuoltolaki (1383/2001) 7 § 2 mom.)
    - itsenäisenä ammatinharjoittajana toimivaa terveydenhuollon ammattihenkilöä (laki yksityisestä terveydenhuollosta (152/1990) 2 § 3 mom.)
    - sosiaalihuollon asiakasasiakirjalain (254/2015) 3 §:n 3 kohdan mukaan sosiaalihuoltoa tai sosiaalipalveluja järjestävää, tuottavaa tai toteuttavaa viranomaista taikka yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tarkoitettua palvelujen tuottajaa
    - asiakastietolain mukaisen määritelmän lisäksi tässä määräyksessä palvelunantajaan kohdistuvat velvoitteet koskevat vastaavalla tavalla ja lain sähköisestä lääkemääräyksestä (61/2007) mukaisessa laajuudessa myös lääkelain (395/1987) 38 §:n mukaista apteekkia.

- *Profiililla* dokumenttia, jossa kuvataan tiettyyn käyttötarkoitukseen käytettävään tietojärjestelmään kohdistuvat kansalliset vähimmäisvaatimukset järjestelmässä toteutettavien toimintojen, tietosisältöjen ja tietoturvavaatimusten suhteen.

- *Sertifioinnilla* menettelyä, jolla todennetaan tietojärjestelmän täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset (asiakastietolaki 3 §). Luokkaan A kuuluvien järjestelmien vaatimusten todentaminen tehdään tietoturvallisuuden arvioinnin ja tarvittaessa yhteistestauksen kautta. Järjestelmälle hyväksytysti suoritetun yhteistestauksen tuloksista ja tietoturvallisuuden arviointia koskevan todistuksen voimassaolosta tehdään merkinnät Sosiaali- ja terveysalan lupa- ja valvontaviraston (jäljempänä Valvira) tietojärjestelmärekisteriin.

- *Tietojärjestelmällä* tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja (asiakastietolaki 3 §).

- *Tietojärjestelmän valmistajalla* tahoa, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta (asiakastietolaki 3 §), riippumatta siitä toimiiko tämä taho myös tietojärjestelmäpalvelun tuottajana.

- *Tietojärjestelmäpalvelun tuottajalla* tahoa, joka tarjoaa tai toteuttaa palvelunantajalle tietojärjestelmää, jossa käsitellään asiakas- tai hyvinvointitietoa ja joka vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista (asiakastietolaki 3 §). Tietojärjestelmäpalvelun tuottaja voi vastata myös osajärjestelmien integroinnista.

- *Tietoturvallisuuden arvioinnilla* sertifiointiprosessin osaa, jossa hyväksytty tietoturvallisuuden arviointilaitos todentaa tietoturvavaatimukset tuottaen asiakastietolain 37 §:ssä tarkoitetun todistuksen tietoturvallisuuden arvioinnista.

VANHENTUNUT

- *Todentamisella* menettelyä, jolla osoitetaan, että järjestelmä täyttää sille asetettuja vaatimuksia. Todentamistapoja ovat mm. ohjelmiston testaus, tietojärjestelmän dokumentaation tai ohjeiden läpikäynti tai ohjelmiston tuottamien sanomien, lokien tai muiden tuotosten läpikäynti. Todentamiseen voi liittyä myös ohjelmiston valmistajan tai tietojärjestelmäpalvelujen tuottajan dokumentoitu haastattelu. Todentamista käsitellään tarkemmin THL:n määräyksen 5/2021 luvussa 10.

- *Todistuksella tietoturvallisuuden arvioinnista* tai *tietoturvallisuustodistuksella* hyväksytyn arviointilaitoksen antamaa todistusta siitä, että tietojärjestelmä tai osajärjestelmä on hyväksytysti läpäissyt tietoturvallisuuden arvioinnin.

- *Toiminnolla* tietojärjestelmään toteutettua toiminnallisuutta tai tietosisältöä, joka vastaa sisällöllisesti THL:n määräyksen 5/2021 liitteen 2 luokituksessa kuvattua olennaisiin toiminnallisiin vaatimuksiin kuuluvaa toimintoa tai tietosisältöä.

- *Yhteistestauksella* asiakastietolain 36 §:n mukaista Kelan järjestämää yhteentoimivuuden testausta, jossa osoitetaan tietojärjestelmän yhteentoimivuus Kanta-palvelujen ja muihin niihin liitettyjen tietojärjestelmien kanssa. Yhteistestauksen tuloksena Kela tuottaa yhteistestausraportin ja antaa puoltavan lausunnon yhteentoimivuutta koskevien vaatimusten täyttymisestä (yhteistestauslausunto), kun testattavat vaatimukset on hyväksytysti todennettu.

4 Määräyksen rajaukset ja suhde muihin määräyksiin ja dokumentteihin

THL on antanut asiakas- ja potilastietojen käsittelyyn tarkoitettujen järjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista erillisen määräyksen (THL:n määräys 5/2021: määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista vaatimuksista, jäljempänä määräys 5).

THL on antanut erillisen määräyksen Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (määräys 3/2021).

Tässä määräyksessä ei kuvata asiakastietolain 3 §:n mukaisten hyvinvointisovellusten olennaisia vaatimuksia tai niihin liittyviä sertifiointimenettelyjä. Mikäli kyseessä on tietojärjestelmä, joka täyttää myös hyvinvointisovelluksen määritelmän, sovelletaan sen sertifiointiin a) ensisijaisesti ja palvelunantajan henkilörekisteriin kuuluvien asiakastietojen käsittelyn osalta tätä määräystä sekä määräystä 5/2021 ja b) toissijaisesti ja hyvinvointitietojen käsittelyn ominaisuuksien osalta THL:n määräystä 6/2021.

Tällä määräyksellä on kumottu THL:n aiemmin antamat määräykset 1/2015 määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset ja 2/2016 määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista vaatimuksista. Tämä määräys korvaa kyseissä määräyksissä aiempien säädösten mukaiset tietojärjestelmien luokitteluun ja sertifiointiin sekä olennaisiin vaatimuksiin liittyneet sisällöt.

Tämä määräys tai sen voimaantuloaika ja siirtymäsäännökset eivät vaikuta asiakastietolain 52 §:ssä säädettyihin palvelunantajien velvoitteiden määräaikoihin liittyä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi.

Määräys koskee sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitettuja tietojärjestelmiä. Luokkiin B, A1, A2 tai A3 kuuluva järjestelmä, osajärjestelmä tai siihen kuuluva ohjelmisto voi olla *lääkinnällinen laite* tai laitteessa voi olla osia/moduuleja, joilla on lääkinnällinen käyttötarkoitus. Näiden laitteiden ja ohjelmistojen vaatimustenmukaisuus tulee todentaa lääkinnällisistä laitteista annetun Euroopan parlamentin ja neuvoston

VANHENTUNUT

asetuksen (EU) 2017/745[1] mukaisesti, ja laitteet tulee ilmoittaa Lääkealan turvallisuus- ja kehittämiskeskus Fimean rekisteriin. Tämä määräys ja määräys 5/2021 ovat riippumattomia siitä, millä tavoin ohjelmistoja tai laitteita luokitellaan lääkinnällisten laitteiden säädösten perusteella. Tietojärjestelmän valmistajan on otettava erikseen kantaa siihen, onko järjestelmä tai osa siitä lääkinnälliseksi laitteeksi luokiteltava.

Tämän määräyksen ja määräyksen 5/2021 tarkoittamalla sertifioinnilla ei tarkoiteta luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (*yleinen tietosuoja-asetus*) [2] 42-44 artiklojen mukaista vapaaehtoista rekisterinpitäjään tai henkilötietojen käsittelijään kohdistuvaa sertifiointia. Tämän määräyksen mukaista sertifiointia ei siten pidetä selvityksenä tietosuoja-asetuksen noudattamisesta tai tietosuoja-asetuksessa säädetyn osoitusvelvollisuuden toteuttamisesta. Asiakastietolaissa säädetty sertifiointi ei vaikuta tietosuojavaltuutetun toimiston toimivaltuuksiin tietosuojalainsäädännön perusteella.

Tähän määräykseen on koottu myös aiempiin määräyksiin liittyneiden erillisten ohjeiden sisältöä. Vanhentuneet ohjeet merkitään kumotuiksi määräysten voimaantulon yhteydessä.

5 Tietojärjestelmien luokittelu

Sosiaali- ja terveydenhuollon tietojärjestelmät luokitellaan luokkiin A ja B. *Luokittelusta vastaa tietojärjestelmäpalvelun tuottaja.* Luokittelu vaikuttaa siihen, millaisia sertifioinnin ja rekisteröinnin toimenpiteitä (ks. luku 7) järjestelmälle on suoritettava.

Luokittelun lisäksi tietojärjestelmäpalvelun tuottajan on arvioitava tietojärjestelmään ja sen kautta tehtävään asiakastietojen käsittelyyn liittyvät riskit ja suunniteltava ja mitoitettava järjestelmän tietoturvallisuus riskiarvion mukaisesti. Tietojärjestelmien sertifioinnin ja olennaisten vaatimusten näkökulmasta *riskitason* ja *asiakastietojen käsittelyn laajamittaisuuden* arviointi on tehtävä tämän määräyksen liitteessä 1 kuvatuilla perusteilla.

Luokkaan A kuuluvat järjestelmät, jotka liittyvät suoraan tai välityspalvelun kautta Kanta-palveluihin tai tuottavat asiakirjoja, jotka välitetään Kanta-palveluihin, tai joiden käyttötarkoitus on muutoin sellainen, että niissä on todennettava tietoturvavaatimusten täyttäminen. A-luokka jaetaan edelleen A1, A2 ja A3-luokkiin, jotka erotellaan toisistaan järjestelmän käyttötarkoituksen, järjestelmässä käsiteltyjen asiakastietojen luonteen ja laajuuden sekä järjestelmän riskitason ja kriittisyyden perusteella.

- A1: Ulkoista tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta. Luokkaan A1 kuuluvat asiakastietojen välityspalvelut sekä järjestelmät tai osajärjestelmät, joiden yhteentoimivuuden vaatimukset on todennettu toisen järjestelmän kautta, mutta joihin kohdistuu todennettavia tietoturvavaatimuksia. Luokkaan A1 kuuluvat myös sellaiset tietojärjestelmät tai osajärjestelmät, joihin sisältyy asiakas- ja potilastietojen laajamittaista säilyttämistä tai käsittelyä, vaikka ne eivät liittyisi Kanta-palveluihin tai kuuluisi luokkiin A2 tai A3. Luokan A1 tietojärjestelmän riskitaso voi olla perustaso tai korkea riskitaso.

- A2: Yhteistestausta ja tietoturvallisuuden arviointia vaativat, rajattua tietosisältöä tai käyttötarkoitusta palvelevat järjestelmät. Järjestelmät ovat Kanta-palvelujen rajapintoihin suoraan liittyviä tai Kanta-

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta.

[2] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

VANHENTUNUT

palveluihin toimitettavia asiakirjoja tuottavia tai käyttäviä. Luokan A2 järjestelmän avulla ei voida yksin täyttää kaikkia sote-palveluja tuottavaan organisaatioon kohdistuvia vaatimuksia esimerkiksi kaikkien toiminnassa tarvittavien tietosisältöjen tai kaikkien Kanta-palveluihin liittyvien velvoitteiden osalta. Luokkaan kuuluvat esimerkiksi a) vain hallinnollisia tietoja Kanta-palveluihin tallentavat tai hyödyntävät järjestelmät; b) Kanta-palveluihin liittyvät tietyn erikoisalan tai osaston hoidollista tietoa sisältävät erillisjärjestelmät, joiden lisäksi organisaatiossa käytetään luokkaan A3 kuuluvaa perusjärjestelmää tai c) Kanta-palveluihin liittyvät osajärjestelmät, jotka toteuttavat modulaarisessa järjestelmäkokonaisuudessa rajatun toiminnallisuuden tai hallinnollisen tai hoidollisen tietosisällön. Luokan A2 tietojärjestelmän riskitaso voi olla korkea tai perustaso.

- A3: Yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, sosiaali- ja terveydenhuollon palveluja tuottavaan organisaatioon kohdistuvat vaatimukset kattavasti tai Kanta-liittymisvelvoitteiden osalta täysin täyttävät pääjärjestelmät, joissa käsitellään laajasti hoidollisia tai palvelujen sisältöön liittyviä asiakastietoja. Luokan A3 tietojärjestelmän riskitaso on oletusarvoisesti korkea.

    - *Kriittisiä luokan A3 järjestelmiä* ne luokan A3 tietojärjestelmät, joita käytetään erikoissairaanhoidossa tai kuntien tai hyvinvointialueiden sairaaloissa tai julkisen perusterveydenhuollon avosairaanhoidossa päivystysvastuun toteuttamisessa ja ensihoidossa taudinmääritykseen, sairauksien tutkimukseen ja hoitoon ja näihin liittyvien asiakastietojen hallintaan. Kriittisten järjestelmien joukkoa on mahdollista laajentaa myöhemmin.

Luokat A1, A2 ja A3 ohjaavat sitä, millaisella tasolla ja millä menettelyillä (testaus, dokumentointi, validointi jne.) järjestelmiin kohdistuvat vaatimukset on todennettava sertifiointiin kuuluvassa yhteistestauksessa tai tietoturvallisuuden arvioinnissa tämän määräyksen luvun 7 mukaisesti.

Kanta-palveluilta edellytetään aina ulkoista tietoturvallisuuden arviointia. Kanta-palveluilta, jotka sisältävät sosiaali- ja terveydenhuollon palvelunantajille tai asiakkaille tarkoitettuja käyttöliittymiä edellytetään soveltuvin osin tason A3 mukaista sertifiointia. Näitä toimenpiteitä on mahdollista yhdistää Tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaisiin Kelalle viranomaistoimijana suoritettaviin tietoturvallisuuden arviointeihin.

Luokkaan B kuuluvat järjestelmät, jotka on tarkoitettu asiakas- tai potilastietojen käsittelyyn, mutta jotka eivät liity suoraan Kanta-palveluihin ja joihin kohdistuvat tietoturvavaatimukset täytetään ja todennetaan muiden järjestelmien tai järjestelmää hyödyntävän palvelunantajan tietoturvallisuussuunnitelman mukaisten toimenpiteiden kautta. Luokkaan B kuuluvat myös sellaiset asiakastietojen käsittelyyn tarkoitetut järjestelmät, jotka toimivat kaikilta osin teknisesti ja fyysisesti suojatussa käyttöympäristössä tai ovat osa laajempaa laitteista ja ohjelmistoista koostuvaa lääkinnällisten laitteiden kokonaisuutta. Edellä kuvattuihin tietojärjestelmiin voivat kuulua lääkinnällisten laitteiden säädösten mukaisesti lääkinnällisiksi laitteiksi[3] luokkiin I, IIa, IIb tai III luokiteltavat ohjelmistot. Kyseiset järjestelmät voivat kuulua luokkaan B, jos niiden potilasturvallisuus- ja laaturiskeihin varautuminen tapahtuu lääkinnällisten laitteiden vaatimusten ja sertifiointien mukaisesti ja jos kyseiset vaatimukset ja sertifioinnit sekä käyttäjäorganisaatioiden tietoturvasuunnitelmat kattavat järjestelmällä tehtävän asiakastietojen käsittelyn tietoturvallisuuden. Luokassa B voivat toimia myös järjestelmät, jotka tuottavat tai käyttävät hyvin suppeasti yksittäisiä asiakastietoihin liittyviä tietoja.

Esimerkkejä erityyppisten järjestelmien luokittelusta on tämän määräyksen liitteessä 1.

[3] Lääkinnällisistä laitteista annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/745 artiklan 2 mukaisen lääkinnällisen laitteen määritelmän mukaisesti.

VANHENTUNUT

Mikäli tietojärjestelmäpalvelun tuottajana on muu taho kuin tietojärjestelmän tai osajärjestelmän alkuperäinen valmistaja, on valmistajan ja tietojärjestelmäpalvelun tuottajan keskenään sovittava siitä, kuka vastaa järjestelmän käyttötarkoituksen kuvaamisesta, luokittelusta, rekisteröinnistä ja olennaisten vaatimusten seurannasta. Luokkaan A kuuluvissa järjestelmissä on sovittava myös olennaisten vaatimusten sertifioinnista ja todentamisesta ja vaatimustenmukaisuuden uudistamisesta.

Tietojärjestelmä voi nojautua toisen valmistajan tai tietojärjestelmäpalvelun tuottajan tietojärjestelmään tai kolmannen osapuolen alustaan tai palveluun olennaisten vaatimusten täyttämisessä. Tietojärjestelmäpalvelun tuottajan on huolehdittava siitä, että tietojärjestelmän vaatimustenmukaisuus voidaan todentaa ja kuvata myös näissä tapauksissa. Tämä voi tapahtua osana tietojärjestelmästä annettavaa selvitystä tai sertifiointia joko sertifioitavana tai rekisteröitävänä olevassa tietojärjestelmässä tai viittaamalla aiemmin suoritettuun voimassa olevaan sertifiointiin tai rekisteröintiin, jossa kyseisen ratkaisun vaatimustenmukaisuus on kuvattu tai todennettu.

6 Tietojärjestelmän käyttötarkoituksen kuvaaminen ja selvitys olennaisten vaatimusten täyttämisestä

Luokkaan A ja luokkaan B kuuluvan tietojärjestelmän tietojärjestelmäpalvelun tuottajan on kuvattava tietojärjestelmän tai osajärjestelmän käyttötarkoitus sekä se, miten järjestelmä täyttää sitä koskevat olennaiset vaatimukset (asiakastietolaki 29 §). Tämä selvitys tietojärjestelmän tai osajärjestelmän käyttötarkoituksesta ja sitä koskevien olennaisten vaatimusten täyttämisestä annetaan määräyksen 5/2021 mukaisella järjestelmälomakkeella.

Järjestelmälomakkeeseen on:

- kuvattava tiiviisti vapaamuotoisena tekstinä se, mihin tarkoitukseen tietojärjestelmä on tarkoitettu (käyttötarkoitus);
    - käyttötarkoituksen kuvauksesta tulisi ilmetä tiiviisti, millaiselle käyttäjäkunnalle (esim. mihin sosiaali- ja terveydenhuollonpalveluihin tai mille ammattiryhmille) ja mihin käyttöön (minkä tietojen käsittelyyn, minkä palvelujen tuottamiseen tai minkä toiminnan tukemiseen) järjestelmä on tarkoitettu;

- merkittävä ne olennaisiin vaatimuksiin kuuluvat toiminnot ja tietosisällöt, jotka kuuluvat järjestelmän käyttötarkoitukseen ja jotka toteutetaan järjestelmän kautta;

- merkittävä ne olennaiset tietoturvavaatimukset, jotka toteutetaan tai täytetään järjestelmän kautta järjestelmän käyttötarkoitus huomioiden;

- ilmaistava lomakkeen tiedoissa, mikäli jokin toiminto tai tietosisältö toteutuu vain osittain, mikäli toiminto tai tietosisältö toteutuu tietyin edellytyksin (edellytykset kuvattava) tai mikäli se toteutuu toisen tietojärjestelmän tai osajärjestelmän kautta;

- merkittävä kaikki ne olennaisten vaatimusten profiilit, jotka vastaavat järjestelmän käyttötarkoitusta.

Nämä tiedot muodostavat asiakastietolain mukaisen olennaisten vaatimusten täyttämistä koskevan selvityksen. Lisätietoja ja yksityiskohtia kuvataan THL:n määräyksessä 5/2021.

Järjestelmälomake on:

VANHENTUNUT

- toimitettava Kelalle yhteistestaukseen hakeutumisen yhteydessä yhteistestattavasta luokan A2 tai A3 tietojärjestelmästä;

- toimitettava tietoturvallisuuden arviointilaitokselle luokan A1, A2 tai A3 tietojärjestelmästä, jolle suoritetaan tietoturvallisuuden arviointi;

- toimitettava Valviralle järjestelmästä rekisteriin tehtävän ilmoituksen yhteydessä luokan A1, A2, A3 ja luokan B järjestelmissä;

- toimitettava osana tietojärjestelmästä tai osajärjestelmästä jätettävää tarjousta sote-palvelunantajalle, joka tarjouspyynnössä tai muussa hankintaprosessiin kuuluvassa menettelyssä edellyttää olennaisten vaatimusten tai niistä muodostettujen profiilien täyttämistä tarjouspyynnössä esitettyihin vaatimuksiin vastaavassa tietojärjestelmässä tai osajärjestelmässä.

Tietojärjestelmäpalvelun tuottaja vastaa siitä, että lomakkeella esitetyt ominaisuudet on toteutettu järjestelmään ja huomioitu järjestelmän suunnittelussa ja kehittämisessä, kun lomaketta käytetään yllä olevissa tilanteissa.

Tietojärjestelmäpalvelun tuottajan on tehtävä tarvittavat korjaukset tai täsmennykset lomakkeessa esitettyihin tietoihin lomakkeen selkeyden tai oikeellisuuden varmistamiseksi, mikäli Kela, tietoturvallisuuden arviointilaitos, THL tai Valvira niitä perustellusti edellyttää.

Tietojärjestelmäpalvelun tuottajan tai valmistajan on suunniteltava, toteutettava ja testattava itse järjestelmälomakkeessa ilmaistujen olennaisten vaatimusten toteutuminen ennen luokan A järjestelmän sertifiointiprosessiin hakeutumista tai ennen luokan B järjestelmän rekisteröintiä.

7 Sertifiointiprosessi

Luokkaan A kuuluva tietojärjestelmä tai osajärjestelmä on sertifioitava. Sertifioinnin käynnistämisestä ja läpiviennistä vastaa tietojärjestelmäpalvelun tuottajana toimiva taho, joka voi olla myös järjestelmän valmistaja (asiakastietolaki 33 §, 34 § ja 35 §).

7.1 Sertifiointiprosessiin liittyvät velvoitteet

Tietojärjestelmäpalvelun tuottajan tai valmistajan on toteutettava ja testattava tietojärjestelmän sertifioitavat ominaisuudet ennen yhteistestaukseen tai tietoturvallisuuden arviointiin hakeutumista. Olennaisten vaatimusten täyttäminen on dokumentoitava siten, että järjestelmään toteutetuista olennaisista vaatimuksista ei ole epäselvyyttä ja siten, että dokumentaation perusteella todennettavista vaatimuksista on saatavilla todentamiseen tarvittava dokumentaatio (ks. luku 6).

Sertifiointiin kuuluu:

- luokkaan A2 tai A3 kuuluvalle, erityisesti Kanta-palveluihin liittyvälle tietojärjestelmälle, tietojärjestelmäkokonaisuudelle tai osajärjestelmälle suoritettava *yhteistestaus*, jonka tuloksena Kela antaa puoltavan lausunnon yhteentoimivuudesta järjestelmille tai osajärjestelmille, jotka hyväksyttävästi täyttävät testatut yhteentoimivuuden vaatimukset;

- *tietoturvallisuuden arviointi*, jonka hyväksytysti läpäisseelle luokkaan A1, A2 tai A3 kuuluvalle tietojärjestelmälle tietoturvallisuuden arviointilaitos myöntää tietoturvallisuustodistuksen.

VANHENTUNUT

Tietojärjestelmäpalvelun tuottajan on ilmoitettava sertifioidun järjestelmän tai osajärjestelmän tiedot Valviralle luvun 8 mukaisesti.

Tietojärjestelmäpalvelun tuottaja ja tietojärjestelmää käyttävä palvelunantaja vastaavat siitä, että sertifiointia edellyttävä järjestelmä otetaan tuotantokäyttöön luvun 9 mukaisesti.

Sertifiointiprosessissa järjestelmästä testataan tai arvioidaan kaikki järjestelmän käyttötarkoitusta ja ominaisuuksia vastaavat olennaiset vaatimukset, joihin on määritelty yhteistestauksen tai tietoturvallisuuden arvioinnin toimenpiteitä määräyksen 5/2021 mukaisesti. Kanta-palveluihin liittyvät olennaiset vaatimukset on toteutettava Kanta-palveluihin liittyvien määrittelyjen mukaisesti.

Mikäli yhteistestauksessa tai tietoturvallisuuden arvioinnissa jokin järjestelmään kohdistuva olennainen vaatimus täytetään hyväksyttävällä tavalla osittain tai kompensoiden, tästä on oltava maininta yhteistestauslausunnossa tai tietoturvallisuustodistuksessa.

Mikäli luokkaan A kuuluvaan tietojärjestelmään tehdään merkittäviä muutoksia, on tietojärjestelmäpalvelun tuottajan ilmoitettava muutoksista Kelalle ja tietoturvallisuuden arviointilaitokselle sekä Valviralle tämän määräyksen liitteen 2 mukaisesti. Merkittävät muutokset ovat muutoksia, jotka muuttavat tietojärjestelmän toimintaa suhteessa määräyksen 5/2021 liitteissä 2–3 olevien olennaisten vaatimusten toteutumiseen. Muutoksista ja niiden vaikutusten laajuudesta riippuen on mahdollista suorittaa uusi yhteistestaus ja uusi tietoturvallisuuden arviointi tai vain toinen niistä. Muutokset voivat olla myös sellaisia, jotka eivät edellytä uutta yhteistestausta tai tietoturvallisuuden arviointia.

Luokan A järjestelmissä vaatimusten täyttyminen on todennettava määräyksessä 5/2021 kuvatulla tavalla osana sertifiointia myös silloin, kun vaatimuksia täytetään muiden tietojärjestelmien tai osajärjestelmien kuin sertifioitavana olevan tietojärjestelmän kautta.

Yhteistestauksen ja sertifioinnin kohteena voi olla useita eri osajärjestelmiä sisältävä järjestelmäkokonaisuus. Tietojärjestelmäkokonaisuudella tai kaikilla siihen kuuluvilla osajärjestelmillä on oltava tietojärjestelmäpalvelun tuottaja. Osajärjestelmillä voi olla tietojärjestelmäpalvelun tuottaja myös tilanteissa, joissa tietojärjestelmäkokonaisuudella on osajärjestelmien integroinnista vastaava tietojärjestelmäpalvelun tuottaja. Kunkin osajärjestelmän tietojärjestelmäpalvelun tuottaja vastaa osaltaan kyseisen osajärjestelmän nimeämisestä, käyttötarkoituksen kuvaamisesta, luokittelusta, kyseiseen osajärjestelmään kohdistuvien olennaisten vaatimusten ilmoittamisesta järjestelmälomakkeella sekä rekisteröinnistä. Tietojärjestelmäpalvelun tuottajan on ilmoitettava laajemman järjestelmäkokonaisuuden yhteistestaukseen tai tietoturvallisuuden arviointiin hakeutumisen yhteydessä, mikäli sen osajärjestelmälle tuotetaan erillinen lausunto niistä yhteistestauksen osioista ja erillinen todistus niistä tietoturvavaatimuksista, jotka kyseisen osajärjestelmän kautta todennetaan. Yhteistestauslausunnossa tai -raportissa ja tietoturvallisuustodistuksessa tai siihen liittyvässä raportissa on eriteltävä, minkä muiden tietojärjestelmien tai osajärjestelmien kanssa osajärjestelmän vaatimukset on todennettu. Jos tietojärjestelmäkokonaisuuden sertifiointiin osallistuu useita tietojärjestelmäpalvelujen tuottajia tai muita osapuolia, nämä sopivat keskenään sertifiointiin osallistumisesta ja osajärjestelmien vastuista.

Mikäli järjestelmäkokonaisuuden osana sertifioitu tietojärjestelmä tai osajärjestelmä on saanut erillisen hyväksytyn lausunnon niistä yhteistestauksen osioista tai erillisen todistuksen niistä tietoturvavaatimuksista, jotka kyseisen osajärjestelmän kautta on todennettu, sitä voidaan käyttää vastaavassa laajuudessa yhdessä myös muiden kuin niiden tietojärjestelmien tai osajärjestelmien kanssa, jotka ovat olleet sertifioitavana samassa järjestelmäkokonaisuudessa. Osajärjestelmän sertifioinnissa voidaan nojautua muiden aiemmin todennettujen tietojärjestelmien tai osajärjestelmien kautta täytettäviin vaatimuksiin. Tällöin aiemmin sertifioidut muut tietojärjestelmät tai osajärjestelmät eivät saa uutta yhteistestauslausuntoa tai tietoturvallisuustodistusta.

VANHENTUNUT

Järjestelmäkokonaisuuteen kuuluvat ohjelmistot voivat olla tuotantokäytössä asennettuna yhden tai useamman palvelunantajan tai tietojärjestelmäpalvelun tuottajan hallitsemaan käyttöympäristöön.

Sertifioinnissa tai siihen kuuluvissa todentamisissa ei edellytetä tietojärjestelmäpalvelun tuottajan asiakkaana toimivan palvelunantajan osallistumista, elleivät palvelunantaja ja tietojärjestelmäpalvelun tuottaja ole toisin sopineet.

Osana sertifiointia käydään läpi ne tietojärjestelmän käyttöympäristöön kohdistuvat vaatimukset, joista tietojärjestelmäpalvelun tuottaja tai tietojärjestelmän valmistaja vastaa tietojärjestelmää käytettäessä. Järjestelmän ja siihen liittyvän palvelun luonteesta ja sopimuksista riippuen osa käyttöympäristöön kohdistuvista vaatimuksista voi kohdistua järjestelmää käyttäviin palvelunantajiin.

Esimerkiksi järjestelmän loppukäyttäjien fyysisen käyttöympäristön suojaaminen on tyypillisesti palvelunantajan vastuulla, mutta tietojärjestelmäpalvelun tuottaja voi tukea suojaamista ohjeistusten ja tukipalvelujen kautta. Käyttöympäristöön kuuluvat palvelin- tai verkkoympäristöt voivat sopimusjärjestelyistä riippuen kuulua tietojärjestelmäpalvelun tuottajan, palvelunantajan tai näille palveluja tuottavan kolmannen tahon vastuulle. Tietojärjestelmäpalvelun tuottajan ja palvelunantajan on tarvittaessa sovittava keskenään siitä, mitkä käyttöympäristöön kohdistuvista olennaisista vaatimuksista ovat tietojärjestelmäpalvelun tuottajan, mitkä palvelunantajan vastuulla. Tällöin on huomioitava luvun 5 mukaiset tietojärjestelmäpalvelun tuottajan vastuut.

Sertifiointiprosessissa syntyvien ja käytettävien dokumenttien on oltava oikeellisia ja ristiriidattomia. Kunkin dokumentin laatija vastaa oikeellisuudesta. Keskeisiä dokumentteja ovat tietojärjestelmäpalvelun tuottajan laatima järjestelmälomake ja rekisteri-ilmoitus Valviran tietojärjestelmärekisteriin, Kelan yhteistestauksen laatima yhteistestauslausunto ja yhteistestausraportti ja tietoturvallisuuden arviointilaitoksen laatima tietoturvallisuustodistus sekä Valviran tietojärjestelmärekisteriin merkittävät tiedot.

Olennaisten vaatimusten todentamista ja vaatimustenmukaisuutta suhteessa erityyppisiin vaatimuksiin käsitellään yksityiskohtaisemmin määräyksessä 5/2021. Määräys 5/2021 ja sen liite 1 sisältävät lisätietoja sertifiointiprosessin soveltamisesta, olennaisten vaatimusten täyttämisestä ja olennaisten vaatimusten toteutumisen arvioinnista.

7.2 Yhteistestauksen sisältö ja tulokset

Yhteistestauksessa testataan järjestelmän käyttötarkoituksen kuuluviin profiileihin sisältyvät yhteistestattavat vaatimukset ja muut sellaiset toiminnot ja tietosisällöt, joita järjestelmää toteuttaa Kanta-palveluihin liittyen ja joihin kohdistuu yhteistestauksen testitapauksia. Kela voi antaa yhdelle tietojärjestelmälle useita yhteistestauslausuntoja eri toimintojen tai sisältöjen yhteistestauksesta tai yhdistää useita testauskokonaisuuksia samaan yhteistestauslausuntoon.

Yhteistestauslausunnosta on käytävä ilmi vähintään järjestelmän nimi- ja versiotiedot, luokka (esim. A2 tai A3), lausunnon ajankohta, järjestelmälle suoritettujen yhteistestausten sisältö (esimerkiksi testattujen kokonaisuuksien otsikot), yhteistestatussa järjestelmässä toteutetuksi ilmoitetut profiilit sekä havainnot, jotka on huomioitava järjestelmän käyttöönotoissa tai säädösten mukaisessa toiminnassa. Kelan tulee toimittaa yhteistestauslausunto liitteineen vähintään tietojärjestelmäpalvelun tuottajalle ja Valviralle. Jos tietojärjestelmälle ollaan suorittamassa tietoturvallisuuden arviointia, Kelan tulee toimittaa yhteistestauslausunto myös arviointia suorittavalle tietoturvallisuuden arviointilaitokselle.

Yhteistestauksessa läpikäytävien vaatimusten tulee perustua julkaistuissa määrittelyissä ja materiaaleissa asetettuihin vaatimuksiin sekä järjestelmän käyttötarkoituksen mukaisten ominaisuuksien testaamiseen suhteessa Kanta-palveluihin tai kansallisiin määrityksiin.

VANHENTUNUT

Yhteistestaukseen hakeutuvassa järjestelmässä on toteutettava yhteistestauksessa läpikäytävät olennaiset vaatimukset perustuen uusimpiin julkaistuihin tai muuten voimassa oleviin määrittelyversioihin. Määrittelyversioiden voimaantuloa ja eri versioiden tukemista kuvataan myös määräyksen 5/2021 luvussa 10.3.

Jos yhteistestauksen kohteena olevassa järjestelmässä osa järjestelmään kohdistuvista vaatimuksista toteutuu toisen järjestelmän tai osajärjestelmän kautta, on yhteistestauslausunnosta käytävä ilmi, minkä muiden järjestelmien tai osajärjestelmien kanssa yhteistestaus on mahdollisesti suoritettu. Lisäksi yhteistestauslausuntoon merkitään, mikäli tietojärjestelmäpalvelun tuottaja ilmoittaa *yhteistestauksessa läpikäytyjen vaatimusten osalta*, mitkä tai millaiset muut tietojärjestelmät tai muut osajärjestelmät toimivat yhdessä testatun järjestelmän kanssa muiden kuin Kanta-rajapintojen kautta.

7.3 Tietoturvallisuuden arvioinnin sisältö ja tulokset

Tämän määräyksen mukaisen tietoturvallisuuden arvioinnin kriteeristönä on käytettävä THL:n määräyksen 5/2021 mukaisia tietoturvavaatimuksia. Samaan tietoturvallisuustodistukseen ei tule sisällyttää muita kriteeristöjä, vaikka saman arvioinnin yhteydessä arvioitaisiin myös muiden kriteeristöjen mukaisia vaatimuksia.

Tietoturvallisuustodistuksesta on käytävä ilmi vähintään järjestelmän nimi- ja versiotiedot, luokka (A1, A2 tai A3), sekä arvioinnin kohteena olleessa järjestelmässä toteutetuksi ilmoitetut profiilit. Todistuksessa on ilmaistava mahdolliset tarkentavat havainnot ja edellytykset, jotka on huomioitava erityisesti järjestelmien käyttäjäorganisaatioissa vaatimusten täyttämiseksi järjestelmän käyttöönotoissa, säädösten mukaisessa toiminnassa tai tietoturvallisessa käytössä. Luokan A3 järjestelmästä on todistuksessa mainittava, mikäli kyseessä on kriittinen luokan A3 järjestelmä luvun 5 mukaisesti. Todistuksessa on oltava myös muut Liikenne- ja viestintäviraston (jäljempänä Traficom) arviointilaitosohjeiden mukaiset tiedot.

Tietoturvallisuuden arvioinnissa todennetaan kaikki sellaiset olennaiset tietoturvavaatimukset, jotka ovat järjestelmän käyttötarkoitus, luokka, laajuus, kriittisyys ja käsiteltävien tietojen luonne huomioiden todennettavia. Todennettavat vaatimukset sisältävät järjestelmän käyttötarkoitusta vastaavien profiilien mukaiset tietoturvavaatimukset ja muut järjestelmän kautta toteutetut tai täytettävät vaatimukset. Läpikäytäviä ja todennettavia vaatimuksia ovat myös muut kuin Kanta-palvelujen käyttöön ja hyödyntämiseen liittyvät tietoturvavaatimukset, jotka on ilmaistu THL:n määräyksen 5/2021 olennaisissa tietoturvavaatimuksissa. Tietoturvavaatimusten todentamisessa käytetään määräyksen 5/2021 sekä Traficomin ohjeiden mukaisia hallinnollisia ja soveltuvin osin myös teknisiä todentamistapoja.

Todentaminen tehdään THL:n määräyksen 5/2021 kunkin vaatimuksen edellyttämällä tasolla järjestelmän luokka, riskitaso, kriittisyys ja käsiteltävien tietojen luonne huomioiden. Tietoturvavaatimusten todentaminen on suoritettava laajuudessa, joka vastaa järjestelmän käyttötarkoitusta, riskitasoa ja asiakastietojen käsittelyn laajuutta ja vain siltä osin kuin vaatimusten täyttymistä ei ole todennettu mahdollisten järjestelmään liitettyjen muiden järjestelmien kautta.

Mikäli tietojärjestelmä on tuotantokäytössä, sille on suoritettava uuteen todistukseen tähtäävä tietoturvallisuuden arviointi ja kirjoitettava tietoturvallisuustodistus ennen aiemman todistuksen voimassaolon päättymistä luvun 10 mukaisesti.

Mikäli tietojärjestelmämuutoksista tehtävä ilmoitus johtaa muutosten johdosta tehtävään tietoturvallisuuden arviointiin, tässä arvioinnissa on käytävä läpi vaatimukset, joiden toteutumiseen muutoksilla on vaikutuksia. Mikäli muut vaatimukset täyttyvät tietojärjestelmäpalvelun tuottajan mukaan aiemmin todennetun tasoisesti, voidaan olemassa oleva tietoturvallisuustodistus päivittää siten, että aiemman todistuksen voimassaoloaika ei muutu. Tietojärjestelmäpalvelun tuottaja voi myös päättää, että mikäli muutosten johdosta tarvitaan tietoturvallisuuden arviointi, arviointi suoritetaan uuteen tietoturvallisuustodistukseen tähdäten. Tällöin tietoturvallisuuden

VANHENTUNUT

arvioinnissa käydään läpi luvun 10 mukaisesti kaikki järjestelmän kautta toteutetut tai täytetyt tietoturvavaatimukset ja kirjoitetaan uusi todistus, jolla on uusi voimassaoloaika.

Tietojärjestelmälle mahdollisesti suoritettavat tietoturvallisuuden seuranta-auditoinnit on erotettava todistuksen uusimiseen tähtäävistä tietoturvallisuuden arvioinneista. Seuranta-auditoinneista ei kirjoiteta uutta tietoturvallisuustodistusta ja vanhan todistuksen voimassaoloaikaa ei jatketa seuranta-auditoinnin tuloksena. Jos seuranta-auditointi ei johda uuteen tietoturvallisuustodistukseen tai aiheuta päivitystarpeita Valviran tietojärjestelmärekisterissä oleviin tietojärjestelmän tietoihin, seuranta-auditoinnista ei tarvitse tehdä merkintää Valviran tietojärjestelmärekisteriin.

Päivitettyyn tai uuteen tietoturvallisuustodistukseen sisällytetään tarvittaessa myös aiemmassa todistuksessa huomioitaviksi seikoiksi merkityt havainnot.

Viimeisin voimassa oleva tai päivitetty todistus korvaa samalle tietojärjestelmälle myönnetyt aiemmat todistukset.

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.

Luokkaan A2 tai 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.

Yhteistestauksen tuloksia ei ilmaista tai kerrata tietoturvallisuustodistuksessa.

Tietotuvallisuuden arvioinnin menettelyjä kuvataan tarkemmin myös määräyksen 5/2021 liitteen 1 luvuissa 5 ja 6.

8 Tietojärjestelmän rekisteröinti

Tietojärjestelmäpalvelun tuottajan on rekisteröitävä luokan A tai B tietojärjestelmä Valviran ylläpitämään tietojärjestelmien rekisteriin. Rekisteröinnin yhteydessä tulee toimittaa määräyksen 5/2021 mukainen järjestelmälomake. Tietojärjestelmäpalvelun tuottaja vastaa siitä, että järjestelmälomakkeella toimitettavat tiedot ovat oikeellisia ja täsmällisiä ja vastaavat järjestelmään toteutettuja tai sen kautta täytettyjä olennaisia vaatimuksia.

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.

VANHENTUNUT

Luokkaan A2 tai A3 kuuluvasta tietojärjestelmästä tai osajärjestelmästä vastaavan tietojärjestelmäpalvelun tuottajan on yksilöitävä Valviralle tehtävien rekisteri-ilmoitusten yhteydessä kaikki Kelan antamat yhteistestauslausunnot, jotka kohdistuvat järjestelmässä toteutettuna oleviin ja yhteistestattuihin testauskokonaisuuksiin. Vain viimeisin kuhunkin testattuun kokonaisuuteen liittyvä yhteistestauslausunto ilmoitetaan siten, että yhteistestatuista ominaisuuksista muodostuu kokonaiskuva.

Luokkaan A kuuluvan tietojärjestelmästä vastaavan tietojärjestelmäpalvelun tuottajan on yksilöitävä Valviralle tehtävien ilmoitusten yhteydessä tunniste voimassa olevasta tietoturvallisuustodistuksesta. Vain viimeisin ja voimassa oleva tietoturvallisuustodistus hyväksytystä tietoturvallisuuden arvioinnista ilmoitetaan.

Rekisterissä julkaistavat tietojärjestelmän tiedot perustuvat:

a) järjestelmälomakkeella ilmoitettuihin tietoihin: käyttötarkoituksen kuvaukseen, järjestelmässä toteutettuihin profiileihin, riskitasoon sekä järjestelmälomakkeella ilmoitettuihin olennaisiin vaatimuksiin,

b) yhteistestausraportteihin,

c) uusimpaan voimassa olevaan tietoturvallisuustodistukseen ja

d) muihin Valviran tarpeelliseksi katsomiin selvityksiin ja viranomaispäätöksiin.

Valvira voi antaa tarkempia ohjeita tehtävistä rekisteri-ilmoituksista ja pyytää tietojärjestelmäpalvelun tuottajalta, Kelalta tai arviointilaitokselta lisätietoja tietojärjestelmien rekisterissä olevien tietojen oikeellisuuden varmistamiseksi.

9 Tietojärjestelmän käyttöönotto

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.

Luokkaan B kuuluvan tietojärjestelmän tai osajärjestelmän saa ottaa tuotantokäyttöön sen jälkeen, kun tietojärjestelmäpalvelun tuottaja on antanut laissa ja tässä määräyksessä tarkoitetun kirjallisen selvityksen olennaisten toiminnallisten ja tietoturvavaatimusten täyttämisestä ja järjestelmän tiedot löytyvät Valviran tietojärjestelmien rekisteristä.

Luokkaan A kuuluvalta järjestelmältä edellytetään hyväksyttyä sertifiointia ja voimassa olevaa tietoturvallisuustodistusta (ks. tämän määräyksen luku 7), ennen kuin tietojärjestelmän saa ottaa tuotantokäyttöön. Tuotantokäytön edellytyksenä on myös, että tietojärjestelmäpalvelun tuottaja on antanut asiakastietolaissa ja tässä määräyksessä tarkoitetun kirjallisen selvityksen olennaisten vaatimusten täyttämisestä ja järjestelmän voimassa olevat tiedot löytyvät Valviran tietojärjestelmienrekisteristä.

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. Kela ja THL julkaisevat

VANHENTUNUT

tiedot siitä, mitä määrittelyjä ja määrittelyversioita Kanta-palveluihin liittyviltä järjestelmiltä edellytetään ja mitkä määrittelyversiot ovat voimassa. Kanta-palveluissa on mahdollista tukea useita määrittelyjen versioita eri toiminnoista ja tietosisällöistä. Määrittelyjen versionhallintaa suhteessa testattaviin kokonaisuuksiin kuvataan määräyksen 5/2021 luvussa 10.3.

Poikkeamia olennaisista vaatimuksista käsitellään määräyksen 5/2021 luvussa 10.4. Tietojärjestelmäpalvelun tuottaja tai palvelunantaja eivät saa ottaa käyttöön järjestelmää, johon Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella kohdistuu merkittävä poikkeama, joka estää tuotantokäyttöönoton.

Sosiaali- ja terveydenhuollon palvelunantajan tai apteekin tulee varmistaa, että sen toiminnassa tuotantokäyttöön otettavan asiakas- tai potilastietojen käsittelyyn tarkoitetun tietojärjestelmän tiedot löytyvät Valviran ylläpitämästä rekisteristä. Lisäksi palvelunantajan tai apteekin on varmistettava, että käytössä olevat tietojärjestelmät kokonaisuutena vastaavat palvelunantajan toimintaa ja että niillä pystytään täyttämään asiakastietolain 7 §:n ja 34 §:n ja määräyksen 5/2021 mukaiset yleiset ja mahdolliset palvelukohtaiset vähimmäisvaatimukset palvelunantajan tai apteekin toiminnassa.

10 Vaatimustenmukaisuuden uudistaminen

Kun tietojärjestelmälle tai osajärjestelmälle annetun tietoturvallisuustodistuksen tai aiemman lain nojalla saadun vaatimustenmukaisuustodistuksen voimassaolo on vanhentumassa, tulee tietojärjestelmäpalvelun tuottajan ottaa yhteyttä tietoturvallisuuden arviointilaitokseen tietoturvallisuustodistuksen uusimiseksi. Tietojärjestelmäpalvelun tuottajan tulee ottaa yhteyttä myös Kelaan, jotta järjestelmän yhteistestaustarve voidaan arvioida uudelleen.

Yhteydenotto tietoturvallisuuden arviointilaitokseen ja Kelaan tulee tehdä viimeistään kuusi kuukautta ennen aiemman todistuksen vanhenemista.

Tietojärjestelmä on tarvittaessa yhteistestattava suhteessa voimassa oleviin tai yhteistestauksessa edellytettäviin määrittelyihin ennen tietoturvallisuuden arvioinnista annettavan uusitun todistusten myöntämistä. Kela antaa hyväksytysti suoritetusta yhteistestauksesta puoltavan yhteistestauslausunnon.

Yllä kuvattua arviointia varten on tietojärjestelmäpalvelun tuottajan toimitettava Kelalle ajantasainen tieto siitä, mitkä Kanta-palveluihin liittyvistä yhteistestattavista vaatimuksista on toteutettu ja mihin määrittelyversioihin toteutukset perustuvat. Toteutus on muutettava perustumaan ajantasaiseen tai vaadittuun määrittelyversioon ennen yhteistestaukseen hakeutumista, mikäli:

- toteutus perustuu vanhentuneeseen määrittelyyn, jonka korvaavan uuden määrittelyn yhteydessä tai säädöksissä annettu määräaika uuden määrittelyversioon mukaiselle käyttöönotolle tai toteutukselle on menneisyydessä; tai
- toteutus ei vastaa Kanta-palvelujen tuotantoympäristössä edellytettävää julkaistua määrittelyä tai määrittelyversiota; tai
- toteutus ei vastaa Kanta-palvelujen yhteistestauksessa edellytettävää julkaistua määrittelyversiota, vaikka myös poistuvia vanhemman version mukaisia toteutuksia tuettaisiin edelleen Kanta-palvelujen tuotantoympäristössä.

Tietoturvallisuuden arviointilaitos suorittaa tietoturvallisuustodistuksen uusimiseen tähtäävän tietoturvallisuuden arvioinnin todentamalla kaikki järjestelmän kannalta relevantit olennaiset tietoturvavaatimukset. Kunkin vaatimuksen todentamisessa voidaan nojautua samoihin menettelyihin ja dokumentaatioihin kuin aiemmin

VANHENTUNUT

myönnetyssä tietoturvallisuustodistuksessa, mikäli vaatimuksen toteuttamis- tai täyttämistavat eivät ole muuttuneet järjestelmässä tai järjestelmän käyttöympäristössä ei ole tapahtunut vaatimusten toteutumiseen vaikuttavia muutoksia. Tietoturvallisuuden arviointilaitos antaa tietoturvallisuustodistuksen hyväksytystä tietoturvallisuuden arvioinnista tämän määräyksen luvun 7.3 mukaisesti.

Vaatimustenmukaisuuden uudistamisen johdosta tietojärjestelmäpalvelun tuottaja päivittää järjestelmän tiedot Valviran tietojärjestelmien rekisteriin. Myös uuden voimassa olevan tietoturvallisuustodistuksen ja mahdollisten uusien yhteistestauslausuntojen keskeiset tiedot tulevat saataville Valviran ylläpitämään tietojärjestelmärekisteriin tämän määräyksen luvun 8 mukaisesti.

Olennaisten vaatimusten suhdetta määrittelyihin ja määrittelyversioihin kuvataan myös THL:n määräyksen 5/2021 luvussa 10.3.

Sosiaalihuollon asiakasasiakirjojen rakenteiden ja tietojen eri versioiden tukemiseen liittyviä vaatimuksia kuvataan THL:n määräyksessä 1/2021.

Mikäli tietojärjestelmäpalvelun tuottajana on muu taho kuin tietojärjestelmän alkuperäinen valmistaja, on valmistajan ja tietojärjestelmäpalvelun tuottajan keskenään sovittava siitä, kuka vastaa vaatimusten seurannasta ja vaatimustenmukaisuuden uudistamisesta.

11 Ohjaus ja neuvonta

Lisätietoja tämän määräyksen soveltamisesta ja sertifiointiprosessista suhteessa tietojärjestelmille asetettaviin olennaisiin vaatimuksiin on määräyksessä 5/2021 ja sen Liitteessä 1.

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.

12 Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 9. päivänä joulukuuta 2021 ja on voimassa toistaiseksi.

Aiemman asiakastietolain 159/2007 sekä THL:n määräysten 1/2015 ja 2/2016 nojalla hyväksytysti sertifioitu järjestelmä voi toimia nykyisen laajuisessa tuotantokäytössä ja voidaan ottaa aiemmin hyväksyttyjen vaatimusten mukaisena tuotantokäyttöön uusilla palvelunantajilla aiemman vaatimustenmukaisuustodistuksen voimassaoloaikana.

Määräys ei edellytä luokan A järjestelmän voimassa olevan vaatimustenmukaisuustodistuksen välitöntä uudistamista, elleivät muut uusimisen edellytykset täyty. Järjestelmästä on toimitettava määräyksen 5/2021 mukainen järjestelmälomake Kelalle yhteistestauksen uudelleentestaustarpeen arviointia varten ja tietoturvallisuuden arviointilaitokselle tietoturvallisuuden uudelleenarviointitarpeen arviointia varten viimeistään 6kk ennen aiemman (lain 159/2007 mukaisen) vaatimustenmukaisuustodistuksen tai tietoturvallisuustodistuksen voimassaolon päättymistä.

Määräyksen 5/2021 mukaista järjestelmälomaketta edellytetään tämän määräyksen voimaantulon jälkeen, kun luokan A tietojärjestelmä hakeutuu Kelan yhteistestaukseen tai tietoturvallisuuden arviointilaitoksen arviointiin.

VANHENTUNUT

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. Tietojärjestelmäpalvelun tuottajan pyynnöstä myös näissä tapauksissa voidaan kuitenkin soveltaa myös THL:n määräysten 4/2021 ja 5/2021 mukaisia menettelyjä ja vaatimuksia. 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.

Aiemmin sertifioidun luokkaan A kuuluvan järjestelmän luokittelu on tarvittaessa tarkennettava tämän määräyksen voimaantuloa seuraavan yhteistestaukseen hakeutumisen, tietoturvallisuuden arviointiin hakeutumisen ja Valviralle tehtävän ilmoituksen yhteydessä.

Jos THL:n määräyksen 4/2021 tai 5/2021 mukaiset vaatimukset edellyttävät luokkaan B tai luokkaan A kuuluvan järjestelmän tietojen tarkentamista tai päivittämistä Valviran tietojärjestelmienrekisterissä, mutta eivät edellytä uutta sertifiointia, on järjestelmästä toimitettava päivitetty ilmoitus Valviran rekisteriin viimeistään *1 vuoden kuluessa* asiakastietolain voimaantulosta, ellei Valvira asiasta toisin määrää.

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.

Mikäli tietojärjestelmä siirtyy luokasta B luokkaan A tässä määräyksessä ja sen liitteissä kuvattujen kriteerien mukaisesti, järjestelmälle on suoritettava sertifiointi voimassa olevien olennaisten vaatimusten mukaisesti *viimeistään kolmen vuoden kuluessa asiakastietolain voimaantulosta*. Jos aiemmin Kanta-palveluihin liittymätön tietojärjestelmä liittyy Kanta-palveluihin suoraan tai nojautuen toiseen järjestelmään tai asiakastietojen välityspalveluun, järjestelmä on luokiteltava ja tarvittaessa sertifioitava ennen liittymistä.

Tietojärjestelmäpalvelun tuottajan on ilmoitettava tuotannossa käytettävän järjestelmän luokan muuttumisesta tai tarkentumisesta järjestelmää käyttäville palvelunantajille tai apteekeille.

Olennaisten vaatimusten vähimmäisvaatimusten profiilien voimaantulosta ja vaikutuksesta mm. sosiaalihuollon asiakastietojärjestelmiin on lisätietoja määräyksessä 5/2021.

Pekka Rissanen
vt. Tiedonhallintajohtaja

Jarmo Kärki
Yksikönpäällikkö

VANHENTUNUT

Liitteet

Liite 1 Esimerkkejä järjestelmien luokittelusta
Liite 2 Luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien muutosten ilmoittaminen

Jakelu

Sosiaali- ja terveydenhuollon palvelunantajat
Välittäjät
Kansaneläkelaitos
Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat
Sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat
Sosiaalialan osaamiskeskukset
Sosiaali- ja terveysministeriö
Suomen Kuntaliitto ry
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
Liikenne- ja viestintävirasto Traficom
Lääkealan turvallisuus- ja kehittämiskeskus FIMEA
Valtiovarainministeriö
Työ- ja elinkeinoministeriö
Digi- ja väestötietovirasto
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

VANHENTUNUT