Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

3.5.2024

MÄÄRÄYS SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN JA HYVINVOINTISOVELLUSTEN LUOKITTELUSTA JA SERTIFIOINNISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) 79 § 4 momentti, 82 § 4 momentti, 84 § 4 momentti ja 85 § 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat ja tietojärjestelmien valmistajat

Hyvinvointisovellusten valmistajat

Asiakastietojen välityspalvelujen tuottajat

Sosiaali- ja terveydenhuollon palvelunantajat

Apteekit

Kansaneläkelaitos

Tietoturvallisuuden arviointilaitokset

Välittäjät

Voimaantulo

Määräys tulee voimaan 10. toukokuuta 2024 ja se on voimassa toistaiseksi.

Tämä määräys korvaa aiemmat THL:n määräykset 4/2021 (määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista) ja 6/2021 (määräys omatietovarantoon liitettävien hyvinvointisovellusten olennaisista vaatimuksista ja sertifioinnista). Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) kumoaa aiemman määräyksen antamiseen valtuuttaneen lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), jonka nojalla annetut alemman asteiset säädökset kumoutuvat.

Sisällys

1 Määräyksen tarkoitus

Tämä määräys kuvaa menettelyt ja vastuut, joita toteutetaan sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelussa sekä niihin kohdistuvien olennaisten vaatimusten todentamisessa ja sertifioinnissa. Määräys ohjaa:

- vaatimustenmukaisuudessa edellytettävien selvitysten antamista,
- sertifiointiin kuuluvaa yhteistestausta,
- sertifiointiin kuuluvaa tietoturvallisuuden arviointia ja
- tietojärjestelmien ja hyvinvointisovellusten rekisteröintiä sekä käyttöönottoa.

2 Määritelmät

Tässä määräyksessä ja THL:n määräyksessä 5/2024 käytetään seuraavia käsitteitä:

- **Tietojärjestelmän valmistaja** (laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023, jäljempänä asiakastietolaki), 3 § 1 mom. 21 kohta)
    - taho, joka on vastuussa sosiaali- ja terveydenhuollon tietojärjestelmän suunnittelusta ja valmistuksesta
- **Tietojärjestelmäpalvelun tuottaja** (asiakastietolaki 3 § 1 mom. 20 kohta)
    - taho, joka tarjoaa tai toteuttaa palvelunantajalle tarkoitettua tietojärjestelmää. Tietojärjestelmäpalvelun tuottaja vastaa tietojärjestelmän valmistajana, valmistajan lukuun tai yhden tai useamman valmistajan puolesta tietojärjestelmälle asetetuista vaatimuksista.
    - Tietojärjestelmäpalvelun tuottaja vastaa myös asiakastietolain, tämän määräyksen ja määräyksen 5/2024 mukaisesti tietojärjestelmän luokittelusta, luokkaan A kuuluvan tietojärjestelmän sertifioinnista ja luokkaan A tai B kuuluvan tietojärjestelmän rekisteröinnistä Valviran tietojärjestelmärekisteriin.
- **Palvelunantaja** (asiakastietolaki 3 § 1 mom. 11 kohta)
    - viranomainen, julkisoikeudellinen yhteisö ja yksityinen elinkeinonharjoittaja, joka järjestää tai toteuttaa sosiaalipalveluja tai terveyspalveluja sekä työterveyshuoltolain (1383/2001) 7 §:n 1 momentin 2 kohdassa tarkoitettu työnantaja[1]:
        - itsenäisenä ammatinharjoittajana toimiva terveydenhuollon ammattihenkilö (laki sosiaali- ja terveydenhuollon valvonnasta (741/2023) ja laki terveydenhuollon ammattihenkilöistä (554/1994))
        - asiakastietolain mukaisen määritelmän lisäksi tässä määräyksessä palvelunantajaan kohdistuvat velvoitteet koskevat vastaavalla tavalla ja lain sähköisestä lääkemääräyksestä (61/2007) sekä asiakastietolain 82, 84 ja 90 §:n mukaisessa laajuudessa myös lääkelain (395/1987) 38 §:n mukaista apteekkia[2].

[1] Asiakastietolain 3 §:n 1 mom. 11 kohdan mukaista palvelunantajan määritelmää ollaan todennäköisesti muuttamassa STM:n valmisteltavana olevassa hallituksen esityksessä laiksi asiakastietolain muuttamisesta. Mahdollinen muutos on huomioitava myös määräysten 4/2024 ja 5/2024 soveltamisessa.
[2] Lisätietoja määräysten 4/2024 ja 5/2024 soveltamisesta apteekkien tietojärjestelmissä ja verkkopalveluissa on määräyksen 5/2024 liitteen 1 luvussa 6.6.

- **Tietojärjestelmä** (asiakastietolaki 3 § 1 mom. 19 kohta)
    - Ohjelmisto, järjestelmä tai osajärjestelmä, jota käytetään valmistajan suunnittelemien ominaisuuksien mukaisesti asiakasasiakirjojen sähköiseen käsittelyyn, niiden tallentamiseen tai liittämiseen valtakunnallisiin tietojärjestelmäpalveluihin tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja. Tässä määräyksessä sekä määräyksessä 5/2024 sekä niiden liitteissä käytetään myös lyhyempää ”järjestelmä” termiä, tarkoittaen tietojärjestelmää.
- **Osajärjestelmä** (asiakastietolaki 3 § 1 mom. 19 kohta)
    - tietojärjestelmä tai sitä vastaavaan käyttöön suunniteltu ja toteutettu ohjelmisto, 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 modulaarista tietojärjestelmäkokonaisuutta ja rekisteröidä erikseen, jos a) osajärjestelmän käyttötarkoitus ja siihen kohdistuvat olennaiset vaatimukset kuvataan ja todennetaan vastaavasti kuin yleisesti tietojärjestelmillä, ja b) osajärjestelmän liittyminen muihin tietojärjestelmiin tai osajärjestelmiin kuvataan määräysten mukaisesti3.
- **Hyvinvointitieto** (asiakastietolaki 3 § 1 mom. 9 ja 18 kohdat)
    - henkilön itsensä tuottama ja hallinnoima ja hänen terveyttään ja hyvinvointiaan koskeva tieto, jonka henkilö on tallentanut omatietovarantoon
    - voimassa olevan asiakastietolain perustelumuistion (HE 246/2022 vp) mukaan kyseessä voi olla myös henkilön käyttämän laitteen tuottama tieto
    - ”Hyvinvointitieto” termiä käytetään myös laajemmassa merkityksessä, joka on kuvattu sote-sanastot palvelussa; määräykset 4/2024 ja 5/2024 nojautuvat kuitenkin asiakastietolaissa kuvattuihin määritelmiin ja rajauksiin.
- **Omatietovaranto** (asiakastietolaki 3 § 1 mom. 17 kohta)
    - hyvinvointitietojen säilyttämistä ja käsittelemistä varten valtakunnallisiin tietojärjestelmäpalveluihin muodostettu keskitetty tietovaranto
- **Hyvinvointisovellus** (asiakastietolaki 3 § 1 mom. 18 kohta)
    - sovellus, joka liittyy omatietovarantoon ja jolla käsitellään hyvinvointitietoa sekä sovellus, johon henkilö (kansalainen) voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta
    - Hyvinvointisovellus voi liittyä sosiaali- ja terveydenhuollon palvelunantajan toimintaan tai olla siitä riippumaton[4].
    - ”Hyvinvointisovellus” termiä käytetään myös laajemmassa merkityksessä, joka on kuvattu sote-sanastot palvelussa; määräykset 4/2024 ja 5/2024 nojautuvat kuitenkin asiakastietolaissa kuvattuihin määritelmiin ja rajauksiin.
    - Ohjelmisto tai tietojärjestelmä voi olla käyttötarkoitukseltaan sekä asiakastietolain 3 §:n 19 kohdan määritelmän mukainen tietojärjestelmä että 18 kohdan mukainen hyvinvointisovellus.
- **Digitaalinen palvelu, digipalvelu**
    - Yleistermiä digipalvelu käytetään määräyksissä 4/2024 ja 5/2024 viitaten sekä hyvinvointisovelluksiin että digitaalisiin asiointipalveluihin. Termi kattaa sekä tietojärjestelmät että hyvinvointisovellukset, joissa on suoraan kansalaisen käytettäväksi tarkoitettuja ominaisuuksia. Digipalveluihin voi kuulua sekä digitaalisia asiointipalveluja että Kanta-palveluihin kuten omatietovarantoon liittyviä hyvinvointisovelluksia. On mahdollista myös, että yksi

[3] lisätietoja: määräys 5/2024 liite 1, luku 6.3
[4] lisätietoja: määräys 5/2024 liite 1, luku 6.5

tietojärjestelmä tai digipalvelu täyttää sekä hyvinvointisovelluksen että tietojärjestelmän määritelmän asiakastietolaissa.

- **Digitaalinen asiointipalvelu**
  - palvelunantajan asiakkailleen tarjoama asiakas- tai henkilötietojen käsittelyyn tarkoitettu tietojärjestelmä tai osajärjestelmä, jonka käyttäjänä on kansalainen ja jonka käyttäjinä voi olla myös ammattihenkilöitä. Digitaalinen asiointipalvelu voi täyttää esimerkiksi vaatimukset profiilista ”Palvelunantajan digitaalinen asiointipalvelu” (määräys 5/2024 liite 3h), joka kuvaa palvelun vaatimukset siltä osin kuin kyseessä ei ole hyvinvointisovellus. Ks. myös *hyvinvointisovellus*, *digipalvelu*[5].
- **Kanta-palvelut** (asiakastietolaki 65 §)
  - Kansaneläkelaitoksen (jäljempänä Kela) järjestämät ja ylläpitämät sosiaali- ja terveydenhuollon valtakunnalliset tietojärjestelmäpalvelut
- **Asiakastietojen välityspalvelu**
  - tietojärjestelmä tai osajärjestelmä, jota hyödyntää sosiaali- ja terveydenhuollon organisaatio tai apteekki Kanta-palveluihin liittymisessä ja jonka kautta siirretään toisen järjestelmän tuottamia asiakastietoja Kanta-palveluihin tai hyödynnetään Kanta-palveluissa olevia asiakastietoja. Asiakastietojen välityspalvelussa ei ole Kanta-palveluihin liittyvän tietojärjestelmän loppukäyttäjille suunnattuja ominaisuuksia. Lisätietoja ks. liite 1: Esimerkkejä järjestelmien luokittelusta.
- **Olennaiset vaatimukset** (asiakastietolaki 84 §)
  - tietojärjestelmän ja hyvinvointisovelluksen toiminnallisuuteen, yhteentoimivuuteen, tietoturvallisuuteen tai saavutettavuuteen kohdistuvia kansallisesti asetettuja vaatimuksia. Olennainen vaatimus nojautuu siinä viitattuihin lähdedokumentteihin, kuten eri säädöksiin tai määrityksiin.
- **Toiminnallinen vaatimus** (asiakastietolaki 80 §, 84–86 §, toiminnallisuutta koskevat vaatimukset)
  - toiminnallisuus tai kyky käsitellä tietosisältöä, jonka toteuttamisesta tietojärjestelmään tai hyvinvointisovellukseen säädetään tai määrätään asiakastietolain 84 §:n ja THL:n määräyksen 5/2024 mukaisesti. Olennaisiin vaatimuksiin kuuluvat toiminnalliset vaatimukset on kuvattu THL määräyksessä 5/2024 liitteessä 2 Olennaisten vaatimusten luettelo osioissa ”Toiminnot” ja ”Tietosisällöt”.
- **Profiili**
  - dokumentti, jossa kuvataan tietojärjestelmässä tai hyvinvointisovelluksessa toteutettavien toimintojen, tietosisältöjen ja tietoturvavaatimusten kansalliset vähimmäisvaatimukset järjestelmän tai hyvinvointisovelluksen käyttötarkoituksen mukaisesti
- **Sertifiointi** (asiakastietolaki 3 § 1 mom. 23 kohta)
  - menettely, jolla todennetaan, että tietojärjestelmä tai hyvinvointisovellus täyttää tuotantokäyttöä varten vaadittavat olennaiset vaatimukset
- **Todentaminen**
  - menettely, jolla osoitetaan, että järjestelmä tai hyvinvointisovellus täyttää sille asetettuja vaatimuksia. Todentamistapoja ovat mm. ohjelmiston testaus, tietojärjestelmän tai hyvinvointisovelluksen dokumentaation tai ohjeiden läpikäynti tai ohjelmiston tuottamien sanomien, lokien tai muiden tuotosten läpikäynti. Todentamiseen voi liittyä myös ohjelmiston valmistajan, tietojärjestelmäpalvelujen tuottajan tai hyvinvointisovelluksen valmistajan

[5] Yleistermiä ”asiointipalvelu” käytetään usein tarkoittamaan digitaalisia palveluita, joissa on myös hyvinvointisovellusten tai asiakasviestinnän ominaisuuksia.

dokumentoitu haastattelu. Todentamista käsitellään tarkemmin THL:n määräyksen 5/2024 luvussa 10.

- **Yhteistestaus** (asiakastietolaki 86 §)
  - yhteentoimivuuden testaus, jossa todennetaan tietojärjestelmän tai hyvinvointisovelluksen yhteentoimivuus Kanta-palvelujen ja muiden niihin liitettyjen tietojärjestelmien tai hyvinvointisovellusten kanssa. Kela järjestää yhteistestauksen ja antaa asiakastietolain 86 §:n mukaisen todistuksen yhteentoimivuutta koskevien vaatimusten täyttymisestä (puoltava yhteistestauslausunto), kun testattavat vaatimukset on hyväksytysti todennettu. Yhteistestauslausunnon liitteenä on yksityiskohtaisempi yhteistestausraportti.
- **Tietoturvallisuuden arviointi** (asiakastietolaki 87 §)
  - sertifiointiprosessin osa, jossa hyväksytty tietoturvallisuuden arviointilaitos todentaa asiakastietolain 87 §:n perusteella tietoturvavaatimukset ja tuottaa todistuksen tietoturvallisuuden arvioinnista
- **Todistus tietoturvallisuuden arvioinnista** tai **tietoturvallisuustodistus** (asiakastietolaki 87 §)
  - todistus, jonka hyväksytty arviointilaitos antaa, jos järjestelmä, osajärjestelmä tai hyvinvointisovellus on hyväksytysti läpäissyt tietoturvallisuuden arvioinnin

Monet käytettävistä käsitteistä perustuvat asiakastietolain määritelmiin ja aiempiin määräyksiin. Keskeisiä käsitteitä on myös THL:n julkaisemassa Sote-sanastot-palvelussa, joiden yhtenä lähteenä tämä määräys toimii. Määräyksissä 4/2024 ja 5/2024 termillä ”määräys” viitataan THL:n määräyksiin, ja muiden viranomaisten määräyksiin viitattaessa täsmennetään, minkä viranomaisen määräyksestä on kyse.

3 Määräyksen soveltamisala

Terveyden ja hyvinvoinnin laitoksella (jäljempänä THL) on asiakastietolain 84 §:n 4 momentin perusteella valtuus antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä järjestelmissä ja hyvinvointisovelluksissa. Asiakastietolain 85 §:n perusteella THL:lla on valtuus antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä. Asiakastietolain 79 §:n perusteella THL voi antaa määräyksiä järjestelmien luokkien määräytymisestä.

Tämä määräys koskee sosiaali- ja terveydenhuollon asiakas- tai potilastietoja käsittelevien tietojärjestelmien sekä hyvinvointisovellusten luokittelussa ja vaatimustenmukaisuuden osoittamisessa noudatettavia menettelyjä ja annettavaa selvitystä.[6] Määräys koskee:

- valtakunnallisiin tietojärjestelmäpalveluihin (Kanta-palvelut) liitettäviksi tarkoitettuja asiakas- ja potilastietoja käsitteleviä järjestelmiä (luokka A),
- muita käyttötarkoituksensa perusteella sertifioitavia järjestelmiä ja välittäjien palveluja (luokka A),
- muita sosiaali- ja terveydenhuollon järjestelmiä, joiden käyttötarkoituksena on asiakas- ja potilastietojen käsittely (luokka B),
- hyvinvointisovelluksia, jotka liittyvät omatietovarantoon ja joilla käsitellään hyvinvointitietoa (luokka A),
- hyvinvointisovelluksia, joihin henkilö voi saada asiakastietonsa valtakunnallisesta asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta; (luokka A).

Pääosa sertifioinnin, luokittelun ja olennaisten vaatimusten todentamisen velvoitteista kohdistuu tietojärjestelmäpalvelun tuottajaan tai hyvinvointisovelluksen valmistajaan. Joitakin aihepiirin velvoitteita kohdistuu kuitenkin myös sosiaali- ja terveydenhuollon palvelunantajiin ja apteekkeihin, ks. mm. määräys 4/2024

[6] Asiakastietolaki, 12 luku ”Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset”

luku 9 ”Tietojärjestelmän ja hyvinvointisovelluksen käyttöönoton edellytykset” ja määräys 5/2024 luku 9 ”Olennaisten vaatimusten täyttäminen / palvelunantaja”. Jos tietojärjestelmäpalvelun tuottaja on eri taho kuin tietojärjestelmän valmistaja, on tärkeää sopia toimijoiden välisistä vastuista (lisätietoja määräys 5/2024 liite 1 luku 2 ”Yleiskuva olennaisten vaatimusten käytöstä”).

Tämä määräys ei kohdistu vaatimustenmukaisuuden seurantaan eikä valvontaan. Tietojärjestelmäpalvelun tuottaja ja palvelunantaja vastaavat kuitenkin siitä, että vaatimustenmukaisuus toteutuu tuotantokäytössä toimivissa järjestelmissä.

4 Määräyksen rajaukset ja suhde muihin säädöksiin ja dokumentteihin

THL on antanut asiakas- ja potilastietojen käsittelyyn tarkoitettujen järjestelmien ja hyvinvointisovellusten olennaisista toiminnallisista ja tietoturvavaatimuksista erillisen määräyksen (THL:n määräys 5/2024: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista).

THL on antanut erillisen määräyksen Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (määräys 3/2024).

Tällä määräyksellä korvataan THL:n aiemmin antamat määräykset 4/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista sekä 6/2021: Omatietovarantoon liittyvien hyvinvointisovellusten sertifioinnista ja olennaisista vaatimuksista. Tämä määräys korvaa kyseisissä määräyksissä aiempien säädösten mukaiset luokitteluun ja sertifiointiin sekä olennaisten vaatimusten todentamiseen liittyneet sisällöt.

Tämä määräys tai sen voimaantuloaika ja siirtymäsäännökset eivät vaikuta asiakastietolain 67 ja 102 §:ssä säädettyihin palvelunantajien velvoitteiden määräaikoihin liittyä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi.

Tätä määräystä ei sovelleta järjestelmiin, joiden käyttötarkoituksena ovat pelkästään Sosiaali- ja terveysalan tietolupaviranomaisen (Findata) antaman määräyksen 1/2022 (Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista) mukaiset käyttökohteet. Findatan määräystä sovelletaan kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin toisiolain mukaan tarvitaan tietolupa: tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä.

Tämän määräyksen kohdealueena eivät ole lääkinnällisten laitteiden säädökset. Tämä määräys koskee sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitettuja järjestelmiä sekä luvun 2 määritelmän mukaisia hyvinvointisovelluksia. 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. Jos tietojärjestelmä tai hyvinvointisovellus täyttää lääkinnällisen laitteen määritelmän, on otettava huomioon sekä asiakastietolaki että lääkinnällisiä laitteita koskevat säädökset, kuten Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita koskeva asetus (EU) 2017/746 sekä laki lääkinnällisistä laitteista 719/2021. Laitteet tulee ilmoittaa Lääkealan turvallisuus- ja kehittämiskeskus Fimean rekisteriin tai EUDAMED-tietokantaan edellä olevien säädösten mukaisesti. Tämä määräys ja määräys 5/2024 ovat riippumattomia siitä, millä tavoin ohjelmistoja tai laitteita luokitellaan lääkinnällisten laitteiden säädösten perusteella. Järjestelmän ja hyvinvointisovelluksen valmistajan on otettava erikseen kantaa siihen, onko järjestelmä tai osa siitä tai hyvinvointisovellus lääkinnälliseksi laitteeksi luokiteltava.

Tämän määräyksen ja määräyksen 5/2024 tarkoittamalla sertifioinnilla ei tarkoiteta vapaaehtoista rekisterinpitäjään tai henkilötietojen käsittelijään kohdistuvaa sertifiointia ((EU) 2016/679 (*yleinen tietosuoja-asetus*)[7] 42-44 artikla). Tämän määräyksen mukaista sertifiointia ei siten pidetä selvityksenä tietosuoja-asetuksen noudattamisesta tai

[7] 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).

tietosuoja-asetuksessa säädetyn osoitusvelvollisuuden toteuttamisesta. Asiakastietolaissa säädetty sertifiointi ei vaikuta tietosuojavaltuutetun toimiston toimivaltuuksiin tietosuojalainsäädännön perusteella.

5 Tietojärjestelmien ja hyvinvointisovellusten luokittelu ja yleiset vastuut

Sosiaali- ja terveydenhuollon tietojärjestelmät luokitellaan luokkiin A (sertifioitavat) ja B (ei-sertifioitavat). Hyvinvointisovellukset kuuluvat luokkaan A. Luokkaan A kuuluvat tietojärjestelmät ja hyvinvointisovellukset luokitellaan tarkemmin luokkiin A1, A2 ja A3 tämän määräyksen mukaisesti. Luokittelun perusteet kuvataan tässä luvussa, ja esimerkkejä erityyppisten järjestelmien luokittelusta on liitteessä 1.

Luokittelusta vastaa tietojärjestelmäpalvelun tuottaja. Luokittelu vaikuttaa siihen, millaisia sertifioinnin ja rekisteröinnin toimenpiteitä (ks. luku 7) järjestelmille ja hyvinvointisovelluksille on suoritettava.

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on arvioitava luokiteltuun järjestelmään tai hyvinvointisovellukseen ja sen kautta tehtävään asiakastietojen käsittelyyn liittyvät riskit. Järjestelmän tietoturvallisuus on suunniteltava ja mitoitettava riskiarvion mukaisesti. Järjestelmien riskitason ja asiakastietojen käsittelyn laajamittaisuuden arviointi on tehtävä tämän määräyksen liitteessä 1 Esimerkkejä järjestelmien ja hyvinvointisovellusten luokittelusta kuvatuilla perusteilla.

Luokkaan A kuuluvat järjestelmät ja hyvinvointisovellukset, 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.

Järjestelmien ja hyvinvointisovellusten osalta luokka A jaetaan edelleen A1, A2 ja A3-luokkiin, jotka erotellaan toisistaan järjestelmän ja hyvinvointisovelluksen käyttötarkoituksen, käsiteltyjen tietojen luonteen ja laajuuden sekä riskitason ja kriittisyyden perusteella seuraavasti:

- A1: Ulkoista tietoturvallisuuden arviointia vaativat järjestelmät, joilta ei edellytetä yhteistestausta. Luokkaan A1 kuuluvat asiakastietojen välityspalvelut sekä järjestelmät tai osajärjestelmät, joiden yhteentoimivuuden vaatimukset on todennettu toiselle järjestelmällä suoritetun yhteistestauksen kautta, mutta joihin kohdistuu todennettavia tietoturvavaatimuksia. Luokkaan A1 kuuluvat myös sellaiset järjestelmät tai osajärjestelmät, joihin sisältyy asiakastietojen laajamittaista säilyttämistä tai käsittelyä, vaikka ne eivät liittyisi Kanta-palveluihin tai kuuluisi luokkiin A2 tai A3. Luokan A1 järjestelmän riskitaso voi olla perustaso tai korkea riskitaso. Myös digitaalinen asiointipalvelu tai hyvinvointisovellus, jonka Kanta-liittyminen tapahtuu toisen järjestelmän tai hyvinvointisovelluksen kautta voi kuulua luokkaan A1.
- A2: Yhteistestausta ja tietoturvallisuuden arviointia vaativat, rajattua tietosisältöä tai käyttötarkoitusta palvelevat järjestelmät tai hyvinvointisovellukset. Järjestelmät tai sovellukset ovat Kanta-palvelujen rajapintoihin suoraan liittyviä tai Kanta-palveluihin toimitettavia asiakirjoja tuottavia tai käyttäviä. Luokan A2 järjestelmän avulla ei voida yksin täyttää kaikkia sote-palvelunantajaan kohdistuvia vaatimuksia esimerkiksi kaikkien toiminnassa tarvittavien tietosisältöjen tai kaikkien Kanta-palveluihin liittyvien velvoitteiden osalta. Luokan A2 järjestelmän tai hyvinvointisovelluksen riskitaso voi olla korkea tai perustaso.
- A3: Yhteistestausta ja tietoturvallisuuden arviointia vaativat, Kanta-palveluihin liittyvät, sosiaali- ja terveydenhuollon palvelunantajaan kohdistuvat vaatimukset kattavasti tai Kanta-liittymisvelvoitteiden osalta täysin täyttävät pääjärjestelmät, joissa käsitellään laajasti hoidollisia tai palvelujen sisältöön liittyviä asiakastietoja. Luokan A3 järjestelmän riskitaso on oletusarvoisesti korkea.
    - *Kriittisiä luokan A3 järjestelmiä* ovat ne luokan A3 järjestelmät, 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 ja hyvinvointisovelluksiin kohdistuvat vaatimukset on todennettava sertifiointiin kuuluvassa yhteistestauksessa tai tietoturvallisuuden arvioinnissa tämän määräyksen luvun 7 Sertifiointiprosessi mukaisesti.

Kanta-palveluilta edellytetään aina ulkoista tietoturvallisuuden arviointia. Kanta-palveluilta, jotka sisältävät sosiaali- ja terveydenhuollon palvelunantajille tai asiakkaille tarkoitettuja käyttöliittymiä edellytetään soveltuvin osin luokan 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. Luokan B järjestelmät eivät muodosta laajamittaista henkilötietojen keskittymää tai sijoitu korkealle riskitasolle. 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 järjestelmiin voivat kuulua lääkinnällisten laitteiden säädösten mukaisesti lääkinnällisiksi laitteiksi [8] 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. Luokkaan B kuuluva tietojärjestelmä voi olla digitaalinen asiointipalvelu, jossa käsitellään palvelunantajan henkilörekisteriin tallennettavia ja palvelunantajan palveluksessa toimiville ammattihenkilöille näkyviä tai välitettäviä asiakastietoja.

Esimerkkejä erityyppisten järjestelmien ja hyvinvointisovellusten luokittelusta on tämän määräyksen liitteessä 1.

Mikäli tietojärjestelmäpalvelun tuottajana tai hyvinvointisovelluksen valmistajana on muu taho kuin järjestelmän, osajärjestelmän tai sovelluksen alkuperäinen valmistaja, on valmistajan ja tietojärjestelmäpalvelun tuottajan keskenään sovittava siitä, kuka vastaa järjestelmän tai sovelluksen käyttötarkoituksen kuvaamisesta, luokittelusta, rekisteröinnistä ja olennaisten vaatimusten seurannasta. Luokkaan A kuuluvissa tietojärjestelmissä ja hyvinvointisovelluksissa on sovittava myös olennaisten vaatimusten sertifioinnista ja todentamisesta ja vaatimustenmukaisuuden uudistamisesta. Myös järjestelmää käyttävä palvelunantaja voi toimia tietojärjestelmäpalvelun valmistajana tai tietojärjestelmäpalvelun tuottajan roolissa (ks. määräys 5/2024 luku 9).

Järjestelmä tai hyvinvointisovellus voi a) täyttää kaikki käyttötarkoituksensa mukaiset olennaiset vaatimukset itsenäisesti, b) nojautua olennaisten vaatimusten täyttämisessä toisen valmistajan tai tietojärjestelmäpalvelun tuottajan järjestelmään tai sovellukseen tai c) kolmannen osapuolen alustaan tai palveluun. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on huolehdittava siitä, että järjestelmän tai hyvinvointisovelluksen vaatimustenmukaisuus voidaan todentaa ja kuvata myös tapauksissa b ja c. Tällöin on joko suoritettava todentaminen kunkin relevantin vaatimuksen osalta tai viitattava aiemmin suoritettuun voimassa olevien vaatimusten mukaiseen sertifiointiin tai rekisteröintiin.

6 Käyttötarkoituksen kuvaaminen ja selvitys olennaisten vaatimusten täyttämisestä

Luokkaan A ja luokkaan B kuuluvan järjestelmän tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on kuvattava järjestelmän tai osajärjestelmän käyttötarkoitus (asiakastietolaki 79 §) sekä se, miten

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

järjestelmä tai hyvinvointisovellus täyttää sitä koskevat olennaiset vaatimukset (asiakastietolaki 84 §). Selvitys järjestelmän tai osajärjestelmän ja hyvinvointisovelluksen käyttötarkoituksesta ja sitä koskevien olennaisten vaatimusten täyttämisestä annetaan määräyksen 5/2024 liitteen 4 mukaisella järjestelmälomakkeella.

Järjestelmälomakkeeseen on:

- kuvattava tiiviisti vapaamuotoisena tekstinä se, mihin tarkoitukseen tietojärjestelmä tai hyvinvointisovellus on tarkoitettu (käyttötarkoitus);
    - käyttötarkoituksen kuvauksesta tulisi ilmetä tiiviisti, millaiselle käyttäjäkunnalle (esim. mihin sosiaali- ja terveydenhuollonpalveluihin tai mille ammatti- tai asiakasryhmille) ja mihin käyttöön (minkä tietojen käsittelyyn, minkä palvelujen tuottamiseen tai minkä toiminnan tukemiseen) järjestelmä tai hyvinvointisovellus on tarkoitettu;
- merkittävä ne olennaisiin vaatimuksiin kuuluvat toiminnot ja tietosisällöt, jotka kuuluvat järjestelmän tai hyvinvointisovelluksen käyttötarkoitukseen ja jotka toteutetaan tai täytetään järjestelmän tai hyvinvointisovelluksen kautta;
- merkittävä ne olennaiset tietoturvavaatimukset, jotka toteutetaan tai täytetään järjestelmän tai hyvinvointisovelluksen kautta järjestelmän tai hyvinvointisovelluksen käyttötarkoitus huomioiden;
- ilmaistava lomakkeen tiedoissa lisätietoineen, mikäli jokin olennainen vaatimus toteutuu vain osittain, mikäli vaatimus toteutuu tietyin edellytyksin tai ei ole sovellettavissa, tai mikäli se toteutuu toisen järjestelmän, osajärjestelmän tai hyvinvointisovelluksen kautta;
- merkittävä kaikki ne olennaisten vaatimusten profiilit, jotka vastaavat järjestelmän tai hyvinvointisovelluksen käyttötarkoitusta;
- kuvattava hyvinvointisovelluksesta se, kuinka sovellus täyttää asiakastietolain vaatimuksen terveyden ja hyvinvoinnin edistämisen käyttötarkoituksesta (asiakastietolaki 84 §).

Nämä tiedot muodostavat asiakastietolain mukaisen olennaisten vaatimusten täyttämistä koskevan selvityksen. Lisätietoja ja yksityiskohtia kuvataan THL:n määräyksessä 5/2024.

Järjestelmälomake on:

- toimitettava Kelalle yhteistestaukseen hakeutumisen yhteydessä yhteistestattavasta luokan A2 tai A3 järjestelmästä tai hyvinvointisovelluksista;
- toimitettava tietoturvallisuuden arviointilaitokselle luokan A1, A2 tai A3 järjestelmästä tai hyvinvointisovelluksesta, jolle suoritetaan tietoturvallisuuden arviointi;
- toimitettava Valviralle tietojärjestelmärekisteriin tehtävän rekisteri-ilmoituksen yhteydessä luokan A ja luokan B järjestelmästä sekä luokan A hyvinvointisovelluksesta (rekisteröinti tai rekisterin tietojen muutoksen ilmoittaminen);
- toimitettava osana järjestelmästä, osajärjestelmästä tai palvelunantajan toiminnassa käytettävästä hyvinvointisovelluksesta jätettävää tarjousta sote-palvelunantajalle, joka tarjouspyynnössä tai muussa hankintaprosessiin kuuluvassa menettelyssä a) edellyttää olennaisten vaatimusten tai niistä muodostettujen profiilien täyttämistä tarjouspyynnössä esitettyihin vaatimuksiin vastaavassa järjestelmässä tai osajärjestelmässä tai b) edellyttää järjestelmälomakkeen toimittamista.

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa siitä, että lomakkeella kirjatut ominaisuudet on toteutettu järjestelmään tai hyvinvointisovellukseen ja ne on huomioitu järjestelmän tai hyvinvointisovelluksen suunnittelussa ja kehittämisessä, kun lomaketta käytetään yllä olevissa tilanteissa.

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

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

7 Sertifiointiprosessi

Luokkaan A kuuluva järjestelmä, osajärjestelmä tai hyvinvointisovellus on sertifioitava. Tietojärjestelmän sertifioinnin käynnistämisestä ja läpiviennistä vastaa tietojärjestelmäpalvelun tuottajana toimiva taho, joka voi olla myös järjestelmän valmistaja (asiakastietolaki 85 §). Hyvinvointisovelluksen sertifioinnin käynnistämisestä ja läpiviennistä vastaa hyvinvointisovelluksen valmistaja.

7.1 Sertifiointiprosessiin liittyvät velvoitteet

Tietojärjestelmäpalvelun tuottajan tai valmistajan ja hyvinvointisovelluksen valmistajan on toteutettava ja testattava järjestelmän tai hyvinvointisovelluksen sertifioitavat olennaiset vaatimukset ennen yhteistestaukseen tai tietoturvallisuuden arviointiin hakeutumista. Kanta-palveluihin liittyvät olennaiset vaatimukset on toteutettava Kanta-palveluihin liittyvien tarkempien määritysten mukaisesti.

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on dokumentoitava olennaisten vaatimusten täyttäminen siten, että järjestelmään tai hyvinvointisovellukseen toteutetuista olennaisista vaatimuksista ei ole epäselvyyttä. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on koottava ja esitettävä tarvittava dokumentaatio sertifiointia varten niistä vaatimuksista, joissa vaatimuksen todentamistapana on dokumentaatio (ks. luku 6 ja määräys 5/2024 luku 10.2).

Sertifiointiin kuuluu (asiakastietolaki 85 §):

- tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antama *selvitys olennaisten vaatimusten täyttämisestä*, joka annetaan määräyksen 5/2024 mukaisella järjestelmälomakkeella;
- luokkaan A2 tai A3 kuuluvalle järjestelmälle, hyvinvointisovellukselle, järjestelmäkokonaisuudelle tai osajärjestelmälle suoritettava *yhteistestaus*, jonka tuloksena Kela antaa puoltavan yhteistestauslausunnon yhteentoimivuuden vaatimusten hyväksyttävästä täyttämisestä;
- *tietoturvallisuuden arviointi*, jonka hyväksytysti läpäisseelle luokkaan A1, A2 tai A3 kuuluvalle järjestelmälle tai hyvinvointisovellukselle tietoturvallisuuden arviointilaitos myöntää tietoturvallisuustodistuksen.

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

Sertifiointiprosessissa järjestelmästä tai hyvinvointisovelluksesta testataan tai arvioidaan kaikki sen käyttötarkoitusta ja ominaisuuksia vastaavat määräyksen 5/2024 mukaiset olennaiset vaatimukset, jotka on määritelty yhteistestauksessa tai tietoturvallisuuden arvioinnissa todennettaviksi.

Yhteistestauslausunnossa tai tietoturvallisuustodistuksessa on oltava maininta, jos jokin järjestelmään tai digipalveluun kohdistuva olennainen vaatimus täyttyy hyväksyttävällä tavalla osittain tai kompensoiden[9].

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on ilmoitettava luokkaan A kuuluvan järjestelmän tai hyvinvointisovelluksen merkittävistä muutoksista Kelalle ja tietoturvallisuuden arviointilaitokselle sekä Valviralle tämän määräyksen liitteen 2 mukaisesti. Merkittävät muutokset ovat sellaisia, jotka muuttavat järjestelmän tai sovelluksen toimintaa suhteessa määräyksen 5/2024 liitteissä 2–3 olevien olennaisten vaatimusten toteutumiseen. Muutoksista ja niiden vaikutusten laajuudesta riippuen Kela tai arviointilaitos arvioivat, tarvitaanko

[9] lisätietoja: määräys 5/2024 luku 10.2

uusi yhteistestaus ja uusi tietoturvallisuuden arviointi tai vain toinen niistä. Tehdyt muutokset eivät aina edellytä uutta yhteistestausta tai tietoturvallisuuden arviointia.

Luokan A järjestelmissä ja hyvinvointisovelluksissa vaatimusten täyttyminen on todennettava määräyksessä 5/2024 liitteessä 1 luvussa 6 kuvatulla tavalla osana sertifiointia myös silloin, kun vaatimuksia täytetään muiden järjestelmien, osajärjestelmien tai sovellusten kuin sertifioitavana olevan kautta.

Laki ei edellytä tietojärjestelmäpalvelun tuottajan asiakkaana olevan palvelunantajan osallistumista sertifiointiin tai siihen kuuluviin todentamisiin. Palvelunantaja ja tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja voivat kuitenkin sopia yhteistyöstä sertifiointiin liittyen. Kelan suorittamaan yhteistestaukseen tai asiakastestaukseen voi kuulua myös tietojärjestelmätoimittajan ja tämän asiakkaana olevan palvelunantajan kanssa suoritettava testaus, ja Kela voi asiakastietolain 85 §:n mukaan antaa määräyksiä yhteentoimivuuden todentamisessa noudatettavista menettelyistä.

Osana sertifiointia käydään läpi ne järjestelmän ja hyvinvointisovelluksen käyttöympäristöön kohdistuvat olennaiset tietoturvavaatimukset, joista tietojärjestelmäpalvelun tuottaja, tietojärjestelmän valmistaja tai hyvinvointisovelluksen valmistaja vastaa järjestelmää tai sovellusta käytettäessä. Tietojärjestelmän ja siihen liittyvän palvelun luonteesta ja sopimuksista riippuen osa käyttöympäristöön kohdistuvista vaatimuksista voi kohdistua tietojärjestelmää käyttäviin palvelunantajiin. Tietojärjestelmän käyttäjinä toimivien ammattihenkilöiden fyysisen käyttöympäristön suojaaminen on tyypillisesti palvelunantajan vastuulla, mutta tietojärjestelmäpalvelun tuottaja voi tukea suojaamista ohjeistusten ja tukipalvelujen kautta. Käyttöympäristöön kuuluvat palvelin- tai verkkoympäristöt voivat sopimuksista riippuen kuulua tietojärjestelmäpalvelun tuottajan, hyvinvointisovelluksen valmistajan, 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 ja palvelunantajan vastuulla. Tämä koskee myös niitä hyvinvointisovelluksia, joita hyödynnetään palvelunantajan toiminnassa. Tällöin on huomioitava tämän määräyksen luvun 5 mukaiset tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan vastuut.

Sertifiointiprosessissa syntyvien ja käytettävien dokumenttien on oltava oikeellisia ja ristiriidattomia. Kunkin dokumentin laatija vastaa oikeellisuudesta. Keskeisiä dokumentteja ovat tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan täyttämä 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 5/2024. Määräys 5/2024 ja sen liite 1 sisältävät lisätietoja ja havainnollistavia kuvauksia sertifiointiprosessin soveltamisesta sekä olennaisten vaatimusten täyttämisestä ja todentamisesta.

Tietojärjestelmäpalvelun tuottaja, järjestelmää käyttävä palvelunantaja ja hyvinvointisovelluksen valmistaja vastaavat siitä, että sertifiointia edellyttävä järjestelmä tai hyvinvointisovellus otetaan tuotantokäyttöön asiakastietolain 81 §:ssä ja tämän määräyksen luvussa 9 kuvattujen edellytysten mukaisesti.

Yhteistestauksen ja sertifioinnin kohteena voi olla useita eri osajärjestelmiä ja digipalveluja sisältävä järjestelmäkokonaisuus. Järjestelmäkokonaisuudella tai kaikilla siihen kuuluvilla osajärjestelmillä ja sovelluksilla on oltava tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja. Näin on myös tilanteissa, joissa järjestelmäkokonaisuudella on osajärjestelmien integroinnista vastaava tietojärjestelmäpalvelun tuottaja. Kunkin osajärjestelmän tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa osaltaan kyseisen osajärjestelmän nimeämisestä, käyttötarkoituksen kuvaamisesta, luokittelusta, kyseiseen osajärjestelmään kohdistuvien olennaisten vaatimusten ilmoittamisesta järjestelmälomakkeella sekä rekisteröinnistä[10].

[10] lisätietoja vaatimusten kohdistamisesta modulaarisissa järjestelmäkokonaisuuksissa: määräys 5/2024 liite 1, luku 6.3

7.2 Yhteistestauksen sisältö ja tulokset

Yhteistestauksessa testataan järjestelmän tai hyvinvointisovelluksen käyttötarkoituksen kuuluviin profiileihin sisältyvät yhteistestattavat vaatimukset ja muut sellaiset toiminnot ja tietosisällöt, joita järjestelmä tai hyvinvointisovellus toteuttaa Kanta-palveluihin liittyen ja joihin kohdistuu yhteistestauksen testitapauksia.

Niistä toiminnoista ja tietosisällöistä, jotka liittyvät järjestelmässä Kanta-palvelujen kautta toteutettaviin ominaisuuksiin ja jotka sisältyvät Kanta-palvelujen yhteistestauksen testauskokonaisuuksiin, on oltava asiakastietolain 86 §:n mukainen todistus (jäljempänä yhteistestauslausunto) yhteistestauksen hyväksymisestä Kelalta. Kela voi antaa yhdelle järjestelmälle tai hyvinvointisovellukselle useita yhteistestauslausuntoja eri toimintojen tai sisältöjen yhteistestauksesta tai yhdistää useita testauskokonaisuuksia samaan yhteistestauslausuntoon. Yhteistestaus suoritetaan järjestelmän käyttötarkoituksen mukaisessa laajuudessa.

Yhteistestauslausunnosta on käytävä ilmi vähintään järjestelmän tai hyvinvointisovelluksen:

- nimi- ja versiotiedot sekä luokka (esimerkiksi A2 tai A3);
- yhteistestauslausunnon antamisen ajankohta (yhteistestauslausunnon päiväys);
- suoritettujen yhteistestausten sisältö (esimerkiksi testattujen yhteistestauskokonaisuuksien otsikot);
    - jos suoritettu yhteistestaus korvaa aiemman yhteistestauksen, tieto siitä mikä aiempi lausunto tai mitkä lausunnot korvautuvat uudella yhteistestauslausunnolla;
- tieto niistä määräyksen 5/2024 mukaisista profiileista, jotka tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja on ilmoittanut toteutetuksi järjestelmässä tai sovelluksessa;
- mahdolliset havainnot, jotka on huomioitava järjestelmän tai hyvinvointisovelluksen käyttöönotoissa tai säädösten mukaisessa toiminnassa tuotantoympäristössä.

Yhteistestauslausunnon liitteenä on yksityiskohtaisempi yhteistestausraportti, jossa voi olla myös muita tietoja. Kelan tulee toimittaa yhteistestauslausunto liitteineen tietojärjestelmäpalvelun tuottajalle tai hyvinvointisovelluksen valmistajalle. Yhteistestauslausunto on toimitettava myös Valviralle. Jos järjestelmälle tai hyvinvointisovellukselle ollaan suorittamassa myös sertifiointiin tai tietoturvallisuustodistuksen uusimiseen tähtäävää tietoturvallisuuden arviointia, Kelan tulee toimittaa yhteistestauslausunto myös arviointia suorittavalle tietoturvallisuuden arviointilaitokselle.

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

Yhteistestaukseen hakeutuvassa järjestelmässä tai hyvinvointisovelluksessa on toteutettava yhteistestauksessa läpikäytävät olennaiset vaatimukset perustuen uusimpiin julkaistuihin tai muuten voimassa oleviin määritysversioihin. Järjestelmätoteutuksen, yhteistestauksen ja puoltavan lausunnon on perustuttava sellaisiin määrityksiin ja määritysversioihin, joita kulloinkin edellytetään Kanta-palveluihin liittyvältä järjestelmältä. Kela ja THL julkaisevat tiedot siitä, mitä määrityksiä ja määritysversioita Kanta-palveluihin liittyviltä järjestelmiltä edellytetään ja mitkä määritysversiot ovat voimassa tuotantokäytössä ja sertifioinnissa. Kanta-palveluissa on mahdollista tukea useita määritysten versioita eri toiminnoista ja tietosisällöistä. Määritysten versionhallintaa suhteessa testattaviin kokonaisuuksiin kuvataan määräyksen 5/2024 luvussa 10.3.

Yhteistestauslausunnosta on käytävä ilmi, minkä muiden järjestelmien, osajärjestelmien tai sovellusten kanssa yhteistestaus on mahdollisesti suoritettu, jos yhteistestauksen kohteena olevassa järjestelmässä tai sovelluksessa osa olennaisista vaatimuksista toteutuu toisen järjestelmän, osajärjestelmän tai sovelluksen kautta. Jos yhteistestauksessa läpikäytyjen vaatimusten toteutus perustuu muihin rajapintoihin kuin Kanta-rajapintoihin, yhteistestauslausuntoon merkitään, mitkä tai millaisia rajapintoja toteuttavat muut järjestelmät toimivat yhdessä testatun järjestelmän kanssa. Toisiinsa liitettyjen järjestelmien tai osajärjestelmien vaatimusten kohdistamista käsitellään tarkemmin määräyksen 5/2024 liitteen 1 luvussa 6.3.

7.3 Tietoturvallisuuden arvioinnin sisältö ja tulokset

Tämän määräyksen mukaisen tietoturvallisuuden arvioinnin kriteeristönä on käytettävä THL:n määräyksen 5/2024 mukaisia tietoturvavaatimuksia ja digitaalisten palvelujen vaatimuksia. Samaan tietoturvallisuustodistukseen ei tule sisällyttää muita kriteeristöjä, vaikka saman arvioinnin yhteydessä arvioitaisiin myös muiden kriteeristöjen mukaisia vaatimuksia.

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

Tietoturvallisuuden arvioinnissa todennetaan kaikki sellaiset olennaiset tietoturvavaatimukset, jotka ovat tietojärjestelmän tai hyvinvointisovelluksen käyttötarkoitus, luokka, laajuus, kriittisyys ja käsiteltävien tietojen luonne huomioiden todennettavia. Todennettavat vaatimukset sisältävät järjestelmän tai sovelluksen käyttötarkoitusta vastaavien profiilien mukaiset tietoturvavaatimukset ja muut järjestelmän tai sovelluksen kautta toteutetut tai täytettävät vaatimukset. Läpikäytäviä ja todennettavia vaatimuksia ovat myös muut kuin Kanta-palvelujen käyttöön ja hyödyntämiseen liittyvät tietoturvavaatimukset. Vaatimusten todentamisessa käytetään määräyksen 5/2024 sekä Traficomin ohjeiden mukaisia hallinnollisia ja soveltuvin osin myös teknisiä todentamistapoja.

Todentaminen tehdään THL:n määräyksen 5/2024 kunkin vaatimuksen edellyttämällä todentamistavalla järjestelmän tai hyvinvointisovelluksen luokka, riskitaso, kriittisyys ja käsiteltävien tietojen luonne huomioiden. Tietoturvavaatimusten todentaminen on suoritettava todentamistavoilla, jotka vastaavat järjestelmän tai sovelluksen käyttötarkoitusta, riskitasoa ja asiakastietojen käsittelyn laajuutta. Jos vaatimuksia täytetään järjestelmään tai sovellukseen liitettyjen muiden sertifioitujen järjestelmien tai sovellusten kautta, todentaminen tehdään vain siltä osin kuin vaatimusten täyttymisen toteaminen myös sertifioinnin kohteena olevassa järjestelmässä tai sovelluksessa edellyttää.

Asiakastietolain 84 § edellyttää sitä, että hyvinvointisovellukset täyttävät saavutettavuusvaatimukset. Osana hyvinvointisovellusten tietoturvallisuuden arviointia läpikäydään raportti saavutettavuustestauksen tuloksista. Hyvinvointisovelluksen saavutettavuus tulee testata valmistajan itse tai ulkopuolisen toimijan toteuttaman saavutettavuuden arvioinnin avulla. Saavutettavuuteen liittyviä olennaisia vaatimuksia on hyödynnettävä soveltuvin osin myös digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) soveltamisalaan kuuluvien digitaalisten palvelujen saavutettavuuden varmistamiseen sosiaali- ja terveyspalveluissa, jos ne täyttävät tietojärjestelmän tai hyvinvointisovelluksen määritelmän.

Mikäli järjestelmä tai hyvinvointisovellus on tuotantokäytössä, sille on suoritettava tietoturvallisuuden arviointi ja kirjoitettava uudistettu tietoturvallisuustodistus ennen aiemman todistuksen voimassaolon päättymistä tämän määräyksen luvun 10 (Vaatimustenmukaisuuden uudistaminen) mukaisesti.

Tietoturvallisuuden arviointia koskeva todistus tai yhteentoimivuuden testaus on uudistettava, jos järjestelmään tai hyvinvointisovellukseen tehdään merkittäviä muutoksia, tai olennaisia vaatimuksia on muutettu tavalla, joka edellyttää uutta sertifiointia (asiakastietolaki 82 §). Ilmoitus tietojärjestelmään tai hyvinvointisovellukseen tehdyistä muutoksista on tehtävä tämän määräyksen liitteen 2 mukaisissa tilanteissa. Jos järjestelmän tai sovelluksen merkittävistä muutoksista tehtävä ilmoitus johtaa tietoturvallisuuden arviointiin, tässä arvioinnissa on käytävä läpi vaatimukset, joiden toteutumiseen muutoksilla on vaikutuksia. Mikäli muut vaatimukset täyttyvät tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan mukaan aiemmin todennetun tasoisesti, voidaan olemassa oleva tietoturvallisuustodistus päivittää siten, että aiemman todistuksen voimassaoloaika ei muutu. Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja voi myös päättää, että mikäli

muutosten johdosta tarvitaan tietoturvallisuuden arviointi, arviointi suoritetaan uuteen tietoturvallisuustodistukseen tähdäten. Tällöin tietoturvallisuuden arvioinnissa käydään läpi tämän määräyksen luvun 10 mukaisesti kaikki järjestelmän kautta toteutetut tai täytetyt tietoturvallisuusvaatimukset ja kirjoitetaan uusi todistus, jolla on uusi voimassaoloaika.

Asiakastietolaki ei edellytä tietoturvallisuuden säännöllisiä seuranta-auditointeja, mutta tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja voi sopia arviointilaitoksen kanssa seuranta-auditoinneista. Järjestelmälle tai hyvinvointisovellukselle 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. Seuranta-auditoinnista ei tehdä merkintää Valviran tietojärjestelmärekisteriin. Jos seuranta-auditoinnissa havaitaan muutoksia, joiden perusteella tietoturvallisuustodistus on uusittava tai päivitettävä, käynnistetään käynnistettävä todistuksen uusimiseen tai päivittämiseen tähtäävä tietoturvallisuuden arviointi, jonka pohjalta myös Valviran tietojärjestelmärekisterin tiedot päivitetään.

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

Uusi tai päivitetty todistus tietoturvallisuuden arvioinnista korvaa samalle järjestelmälle tai hyvinvointisovellukselle aiemmin myönnetyn todistuksen.

Tietoturvallisuustodistus tulee 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 tai hyvinvointisovellukselle voidaan kirjoittaa tietoturvallisuustodistus vasta sen jälkeen, kun järjestelmä on hyväksytysti läpäissyt ainakin yhden yhteistestauksen.

Jos luokan A2 tai A3 järjestelmä tai hyvinvointisovellus on sertifioitavana ensimmäistä kertaa siten, että sille suoritetaan sekä yhteistestaus että tietoturvallisuuden arviointi, tulisi pyrkiä siihen, että tietoturvallisuustodistus ja yhteistestauslausunto kohdistuvat samaan järjestelmäversioon. Tietoturvallisuuden arviointi on mahdollista käynnistää ennen yhteistestauslausunnon valmistumista. Näissä tilanteissa tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tulee huolehtia, että yhteistestauksen ja tietoturvallisuuden arvioinnin kohteena on sama järjestelmä- tai sovellusversio tai sellainen versio, jossa yhteistestattaviin olennaisiin vaatimuksiin liittyvät mahdolliset järjestelmämuutokset eivät vaikuta arvioitaviin tietoturvavaatimuksiin. Tällöin myös tietoturvallisuuden arviointilaitos varmistaa ennen tietoturvallisuustodistuksen myöntämistä tietojärjestelmäpalvelun tuottajalta tai hyvinvointisovelluksen valmistajalta, että yhteistestauksen kohteena olevaan järjestelmään tai sovellukseen ei ole tulossa muutoksia, jotka voisivat vaikuttaa tietoturvallisuusvaatimusten toteuttamiseen. Arviointilaitoksen on varmistettava asia myös Kelalta. Myöhemmissä samalle järjestelmällä suoritettavissa sertifioinneissa ja vaatimustenmukaisuuden uudistamisessa toimitaan luvun 10 ” Vaatimustenmukaisuuden uudistaminen” mukaisesti.

Yhteistestauksen tuloksia ei kirjata tietoturvallisuustodistukseen.

Tietotuvallisuuden arvioinnin menettelyjä kuvataan tarkemmin määräyksen 5/2024 liitteen 1 luvuissa 5 ja 6.

8 Tietojärjestelmän ja hyvinvointisovelluksen rekisteröinti ja valvonta

Tietojärjestelmäpalvelun tuottajan on ilmoitettava järjestelmästä ja hyvinvointisovelluksen valmistajan on ilmoitettava hyvinvointisovelluksesta Valviralle rekisteri-ilmoituksella ennen järjestelmän tai hyvinvointisovelluksen ottamista tuotantokäyttöön. Asiakastietolain 80 § kuvaa, mitä tietoja ilmoituksessa on oltava.

Valvira ylläpitää julkista rekisteriä sille ilmoitetuista, vaatimukset täyttävistä sosiaali- ja terveydenhuollon järjestelmistä ja hyvinvointisovelluksista.

Ilmoituksessa ja rekisterissä on asiakastietolain 80 §:n mukaiset tiedot. Tietojen ilmoittamisessa hyödynnetään tässä määräyksessä ja määräyksessä 5/2024 täsmennettyjä menettelyjä. Määräyksen 5/2024 mukainen järjestelmälomake sisältää monia rekisteriin ilmoitettavia tietoja. Rekisteri-ilmoituksen mukana lähetettävä järjestelmälomake on asiakastietolain 80 ja 85 §:n mukainen selvitys järjestelmässä toteutetuista olennaisista vaatimuksista.

Rekisterissä julkaistavat tietojärjestelmän tai hyvinvointisovelluksen tiedot perustuvat:

a) Valviran rekisteri-ilmoituksen yhteydessä edellyttämiin tietoihin,

b) määräyksen 5/2024 mukaisella järjestelmälomakkeella ilmoitettuihin tietoihin: tietojärjestelmän perustietoihin, käyttötarkoituksen kuvaukseen, järjestelmässä toteutettuihin profiileihin, riskitasoon sekä järjestelmälomakkeella ilmoitettuihin olennaisiin vaatimuksiin (luokka A ja B),

c) yhteistestauksen lausuntoihin ja/tai raportteihin (luokka A2 ja A3),

d) uusimpaan voimassa olevaan tietoturvallisuustodistukseen (luokka A),

e) valvontaprosessista tulevaan tietoon luokkaan A kuuluvan järjestelmän ja sovelluksen merkittävästä poikkeamasta poikkeaman keston ajan, ja

f) muihin Valviran tarpeelliseksi katsomiin ja selvityksiin ja viranomaispäätöksiin.

Rekisteröinnin yhteydessä tulee toimittaa määräyksen 5/2024 mukainen järjestelmälomake. Järjestelmälomakkeeseen sisältyvät keskeisimmät käyttötarkoituksen kuvaamiseen, sertifiointiin, rekisteröintiin ja olennaisten vaatimusten täyttämiseen liittyvät tiedot. Tietojärjestelmäpalvelun tuottaja ja hyvinvointisovelluksen valmistaja vastaavat siitä, että järjestelmälomakkeella toimitettavat tiedot ovat oikeellisia, ajantasaisia ja täsmällisiä ja vastaavat järjestelmään toteutettuja tai sen kautta täytettyjä olennaisia vaatimuksia.

Valviran tietojärjestelmärekisteriin rekisteröinti edellyttää sitä, että tietojärjestelmä tai digitaalinen asiointipalvelu on sertifioitu, jos se kuuluu luokkaan A. Hyvinvointisovellukset kuuluvat lain mukaan luokkaan A ja ne on sertifioitava ennen rekisteröintiä Valviran tietojärjestelmärekisteriin.

Luokkaan A2 tai A3 kuuluvasta tietojärjestelmästä, hyvinvointisovelluksesta tai osajärjestelmästä vastaavan tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on esitettävä Valviralle tehtävän rekisteri-ilmoituksen yhteydessä ne Kelan antamat yhteistestauslausunnot, jotka kohdistuvat järjestelmässä tai hyvinvointisovelluksessa toteutettuna oleviin ja testattuihin yhteistestauskokonaisuuksiin. Ainakin viimeisin kuhunkin järjestelmässä tai hyvinvointisovelluksessa testattuun yhteistestauskokonaisuuteen liittyvä yhteistestauslausunto ilmoitetaan. Yhteistestatuista ominaisuuksista on muodostuttava kokonaiskuva (ks. myös luku 7.2).

Luokkaan A kuuluvasta järjestelmästä tai hyvinvointisovelluksesta vastaavan tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on esitettävä Valviralle tehtävien ilmoitusten yhteydessä voimassa oleva tietoturvallisuustodistus. Vain viimeisin ja voimassa oleva tietoturvallisuustodistus hyväksytystä tietoturvallisuuden arvioinnista ilmoitetaan.

Sertifiointiin liittyvä rekisteri-ilmoitus ja järjestelmälomake toimitetaan Valviraan viimeistään, kun tietojärjestelmään tai hyvinvointisovellukseen kohdistuva sertifiointi on suoritettu loppuun hyväksytysti. Valvira voi ohjeistaa ilmoituksen ja lomakkeen toimittamisesta myös ennen kuin tietoturvallisuuden arviointilaitos on myöntänyt tietoturvallisuustodistuksen.

Valvira voi antaa määräyksiä asiakastietolain 80 §:n mukaisesti ilmoituksen sisällöstä, voimassaolosta, ilmoituksen uudistamisesta ja rekisteriin merkittävistä tiedoista. Valvira päivittää rekisterin tietoja rekisteröintiprosessin lisäksi valvontaprosessin ja asiakastietolain 91 §:n mukaisten sekä muiden tietopyyntöjen kautta.

9 Tietojärjestelmän tai hyvinvointisovelluksen käyttöönoton edellytykset

Tietojärjestelmän ja hyvinvointisovelluksen tuotantokäyttöönoton edellytykset on kuvattu asiakastietolain 81 §:ssä. Tässä luvussa täsmennetään näitä edellytyksiä suhteessa määräyksissä 4/2024 ja 5/2024 määrättäviin seikkoihin olennaisista vaatimuksista ja sertifioinnista.

Luokkaan B kuuluvan tietojärjestelmän on täytettävä seuraavat edellytykset ennen kuin järjestelmä voidaan ottaa tuotantokäyttöön:

- järjestelmä täyttää sen käyttötarkoitusta vastaavat olennaiset vaatimukset (ks. luku 6);
- tietojärjestelmäpalvelun tuottaja on antanut määräyksen 5/2024 mukainen kirjallisen selvityksen olennaisten vaatimusten täyttämisestä Valviralle tehtävän rekisteröinnin yhteydessä;
- järjestelmästä on ajantasaiset tiedot Valviran tietojärjestelmärekisterissä;
- järjestelmään ei kohdistu Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella merkittävää poikkeamaa (ks. määräys 5/2024 luku 10.4), joka estää tuotantokäyttöönoton.

Luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen on täytettävä seuraavat edellytykset ennen kuin järjestelmä voidaan ottaa tuotantokäyttöön:

- järjestelmä tai hyvinvointisovellus täyttää sen käyttötarkoitusta vastaavat olennaiset vaatimukset (ks. luku 6);
- järjestelmä tai hyvinvointisovellus on hyväksytysti sertifioitu (ks. luku 7):
    - luokkaan A2 tai A3 kuuluvalla järjestelmällä tai hyvinvointisovelluksella on hyväksytyt yhteistestauslausunnot Kanta-palveluihin liittyvistä yhteistestattavista ominaisuuksista voimassa oleviin määrityksiin perustuen;
    - luokkaan A1, A2 tai A3 kuuluvalla järjestelmällä on tietoturvallisuustodistus, joka ei saa olla vanhentunut;
- hyvinvointisovellus edistää asiakastietolain 84 §:ssä tarkoitetulla tavalla toiminnallisten vaatimusten täyttymisen edellytyksenä olevaa kansalaisten terveyttä ja hyvinvointia;
- tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja on antanut määräyksen 5/2024 mukaisen kirjallisen selvityksen olennaisten vaatimusten täyttämisestä Valviralle tehtävän rekisteröinnin yhteydessä;
- järjestelmästä tai hyvinvointisovelluksesta on ajantasaiset tiedot Valviran tietojärjestelmärekisterissä;
- järjestelmään ei kohdistu Valviran tietojärjestelmärekisteristä löytyvien tietojen perusteella merkittävää poikkeamaa (ks. määräys 5/2024 luku 10.4), joka estää tuotantokäyttöönoton.

Kanta-palveluihin liitettävän luokan A järjestelmän tai hyvinvointisovelluksen on oltava hyväksytysti yhteistestattu voimassa olevien määritysten mukaisesti, jotta se voidaan liittää Kanta-palveluihin. Tällainen järjestelmä tai hyvinvointisovellus voidaan ottaa tuotantokäyttöön niiden määräyksen 5/2024 liitteen 3 profiilien mukaisiin käyttötarkoituksiin, joiden pakollisia vaatimuksia vastaavat yhteistestauksiin kuuluvat olennaiset vaatimukset on hyväksytysti yhteistestattu.

Sosiaali- ja terveydenhuollon palvelunantajan tai apteekin tulee varmistaa, että sen toiminnassa tuotantokäyttöön otettavan asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän tiedot löytyvät Valviran ylläpitämästä rekisteristä. Lisäksi palvelunantajan tai apteekin on varmistettava, että käytössä olevat järjestelmät kokonaisuutena vastaavat palvelunantajan tai apteekin toimintaa ja että niillä pystytään täyttämään asiakastietolain 67 §:n ja 84 §:n

ja määräyksen 5/2024 mukaiset yleiset ja mahdolliset palvelukohtaiset vähimmäisvaatimukset palvelunantajan tai apteekin toiminnassa[11].

10 Vaatimustenmukaisuuden uudistaminen

Tuotantokäytössä olevan luokkaan B kuuluvan tietojärjestelmän vaatimustenmukaisuuden uudistaminen tapahtuu siten, että tietojärjestelmäpalvelun tuottaja varmistaa lukujen 6 ja 8 mukaisesti, että:

1. tietojärjestelmä täyttää sen käyttötarkoitusta ja toteutettuja ominaisuuksia vastaavat voimassa olevat olennaiset vaatimukset;
2. tietojärjestelmästä on oikeelliset ja ajantasaiset tiedot Valviran tietojärjestelmärekisterissä.

Loppuosa tästä luvusta käsittelee luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen vaatimustenmukaisuuden uudistamista.

Tuotantokäytössä olevan luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovelluksen vaatimustenmukaisuuden uudistamisen osana on:

1. uudistettava tietoturvallisuustodistus ennen kuin tuotannossa toimivan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuustodistus vanhenee;
2. varmistettava, että Kanta-palveluihin liittyvällä tietojärjestelmällä tai hyvinvointisovelluksella on hyväksytyt yhteistestauslausunnot sen käyttötarkoitukseen kuuluvista yhteistestattavista olennaisista vaatimuksista perustuen tuotantokäytössä edellytettyihin vaatimuksiin ja määritysversioihin.

Vaatimustenmukaisuus on uudistettava ennen aiemman voimassa olevan tietoturvallisuustodistuksen voimassaolon päättymistä.

Vaatimustenmukaisuuden ylläpito voi edellyttää myös uusien järjestelmään kohdistuvien vaatimusten toteuttamista ja sertifiointia säädöksissä olevien määräaikojen mukaisesti tai järjestelmämuutosten takia tehtäviä toimenpiteitä (ks. luku 7.1 ja liite 2).

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tulee ottaa yhteyttä tietoturvallisuuden arviointilaitokseen tietoturvallisuustodistuksen uusimiseksi silloin, kun luokkaan A kuuluvalle järjestelmälle, osajärjestelmälle tai hyvinvointisovellukselle annetun tietoturvallisuustodistuksen voimassaolo on vanhentumassa. Yhteydenotto tietoturvallisuuden arviointilaitokseen ja tarvittaessa Kelaan tulee tehdä viimeistään kuusi kuukautta ennen aiemman todistuksen vanhenemista.

Tietoturvallisuuden arviointilaitos uusii tietoturvallisuustodistuksen todentamalla kaikki järjestelmän tai hyvinvointisovelluksen kannalta relevantit olennaiset tietoturvavaatimukset. Näitä ovat ne vaatimukset olennaisten vaatimusten luettelossa (määräys 5/2024 liite 2), joiden todentamistapana on tietoturvallisuuden arviointi ja jotka liittyvät arvioinnin kohteena olevaan järjestelmään tai hyvinvointisovellukseen. Kunkin vaatimuksen todentamisessa voidaan nojautua samoihin menettelyihin ja dokumentaatioihin kuin aiemmin myönnetyssä tietoturvallisuustodistuksessa, jos:

- vaatimus tai sen perusteena oleva määritys ei ole muuttunut ja on edelleen voimassa sertifioinnissa, ja
- vaatimuksen toteuttamis- tai täyttämistavat eivät ole muuttuneet järjestelmässä tai hyvinvointisovelluksessa, ja
- niiden käyttöympäristöissä ei ole tapahtunut vaatimusten toteutumiseen vaikuttavia muutoksia, ja
- käytetyissä menettelyissä tai ohjelmistoissa ei ole havaittu ajan kuluessa uusia haavoittuvuuksia tai hyväksikäyttömenettelyitä.

[11] lisätietoja määräys 5/2024 luku 9

Tietoturvallisuuden arviointilaitos antaa tietoturvallisuustodistuksen hyväksytystä tietoturvallisuuden arvioinnista tämän määräyksen luvun 7.3 mukaisesti. Tietoturvallisuustodistus voidaan antaa riippumatta siitä, onko tietojärjestelmällä tai hyvinvointisovelluksella meneillään olevia yhteistestauksia vai ei.

Jos kyseessä on luokkaan A2 tai A3 kuuluva tietojärjestelmä tai hyvinvointisovellus, tulee tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan ottaa yhteyttä myös Kelaan yhteistestaustarpeen uudelleen arvioimiseksi, kun tietoturvallisuustodistuksen uudistaminen käynnistetään. Mikäli arvioinnissa päädytään uuteen yhteistestaukseen, tulee testaus tehdä voimassa olevien tai yhteistestauksessa edellytettävien määritysten mukaisesti. Kela antaa hyväksytystä yhteistestauksesta puoltavan yhteistestauslausunnon.

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

- toteutus perustuu vanhentuneeseen määritykseen, jonka korvaavan uuden määrityksen yhteydessä tai säädöksissä annettu määräaika uuden määritysversioon mukaiselle käyttöönotolle tai toteutukselle on menneisyydessä; tai
- toteutus ei vastaa Kanta-palvelujen yhteistestauksessa edellytettävää julkaistua määritysversiota[12], vaikka myös poistuvia vanhemman version mukaisia toteutuksia tuettaisiin edelleen Kanta-palvelujen tuotantoympäristössä.

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tulee ilmoittaa vaatimustenmukaisuuden uudistamiseen liittyvät päivitetyt tiedot Valviran tietojärjestelmärekisteriin viimeistään kuukauden kuluessa uudistetun tietoturvallisuustodistuksen myöntämisestä. Valviran rekisteriin tehtävässä ilmoituksessa ei tule ilmoittaa sellaisia olennaisia vaatimuksia eikä sellaisia määräyksen 5/2024 mukaisia profiileja, joihin liittyviä sertifioitavia vaatimuksia ei ole hyväksytysti sertifioitu voimassa olevien vaatimusten ja määritysten mukaisesti[13].

Uuden voimassa olevan tietoturvallisuustodistuksen ja mahdollisten uusien yhteistestauslausuntojen keskeiset tiedot tulevat saataville Valviran ylläpitämään tietojärjestelmärekisteriin tämän määräyksen luvussa 8 kuvatulla tavalla.

Uudistetun tietoturvallisuustodistuksen saanut sovellus- tai järjestelmäversio voidaan päivittää käytössä oleviin tuotantoympäristöihin yhteistestauksista riippumatta, kun sen ajantasaiset tiedot ovat Valviran rekisterissä. Tällöin on kuitenkin huomioitava, että:

- Kanta-palvelujen kanssa suoritettua hyväksyttyä yhteistestausta edellyttäviä ominaisuuksia saa ottaa tuotantokäyttöön vasta, kun niiden toteuttamista koskeva yhteistestauslausunto on annettu;
- Valviran tietojärjestelmärekisteriin ei tule ilmoittaa järjestelmässä tai hyvinvointisovelluksissa toteutetuiksi sellaisia olennaisia vaatimuksia tai profiileja, joiden vaatimuksia järjestelmä tai sovellus ei täytä; sertifioitavien vaatimusten osalta käyttötarkoituksen mukaisten profiilien ja vaatimusten ilmoittaminen Valviran tietojärjestelmärekisteriin edellyttää sitä, että niihin liittyvät yhteistestaukset on suoritettu ja tietoturvallisuustodistus voimassa.

Olennaisten vaatimusten suhdetta määrityksiin ja määritysversioihin, joiden perusteella vaatimustenmukaisuus uudistetaan, kuvataan myös THL:n määräyksen 5/2024 luvussa 10.3.

---

[12] Kela ja THL ilmaisevat sertifioinnissa käytettävien määritysversioiden voimassaolotiedot fraasilla ”voimassa sertifioinnissa” ja tuotantokäytössä käytettävien määritysversioiden voimassaolotiedot fraasilla ”voimassa tuotannossa”.

[13] Valviralla on mahdollisuus verrata järjestelmästä tai hyvinvointisovelluksesta aiemmin toimitettuja tietoja vaatimustenmukaisuuden uudistamisen yhteydessä toimitettuihin tietoihin ja eri testauskokonaisuuksista saatuihin yhteistestauslausuntoihin.

Sosiaalihuollon asiakasasiakirjojen rakenteiden ja tietojen eri versioiden tukemiseen liittyviä vaatimuksia kuvataan THL:n määräyksessä 1/2024. Vaatimustenmukaisuuden uudistamisessa on huomioitava määräyksen 1/2024 mukaisesti asiakirjarakenteiden tila.

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

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa siitä, että järjestelmä tai sovellus täyttää olennaiset vaatimukset koko tuotantokäytön ajan asiakastietolain 94 §:n mukaisesti.

11 Ohjaus ja neuvonta

Lisätietoja tämän määräyksen soveltamisesta ja sertifiointiprosessista suhteessa tietojärjestelmille ja hyvinvointisovelluksille asetettaviin olennaisiin vaatimuksiin on määräyksessä 5/2024 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 10. päivänä toukokuuta 2024 ja on voimassa toistaiseksi.

Määräys ei edellytä luokan A tietojärjestelmän tai hyvinvointisovelluksen voimassa olevan vaatimustenmukaisuustodistuksen välitöntä uudistamista, elleivät muut uusimisen edellytykset täyty. Viimeistään kuusi kuukautta ennen aiemman asiakastietolain (784/2021) mukaisen tietoturvallisuustodistuksen voimassaolon päättymistä järjestelmästä tai sovelluksesta on toimitettava määräyksen 5/2024 mukainen järjestelmälomake Kelalle yhteistestauksen uudelleentestaustarpeen arviointia varten ja tietoturvallisuuden arviointilaitokselle tietoturvallisuuden uudelleenarviointitarpeen arviointia varten.

Aiemman asiakastietolain (784/2021) sekä THL:n määräysten 4/2021 ja 5/2021 tai 1/2022 nojalla hyväksytysti sertifioitu tietojärjestelmä voidaan ottaa aiemmin hyväksyttyjen vaatimusten mukaisena tuotantokäyttöön uusilla palvelunantajilla, jos sillä on voimassa oleva tietoturvallisuustodistus ja sen yhteistestauksessa todennetut vaatimukset vastaavat tuotantokäytön voimassa olevia vaatimuksia.

Määräyksen 5/2024 mukaista järjestelmälomaketta edellytetään tämän määräyksen voimaantulon jälkeen, kun luokan A tietojärjestelmä tai hyvinvointisovellus hakeutuu Kelan yhteistestaukseen tai tietoturvallisuuden arviointilaitoksen arviointiin.

Määräyksessä kuvattuja luokittelu- ja sertifiointimenettelyjä sovelletaan kaikkiin sertifioitaviin järjestelmiin ja hyvinvointisovelluksiin *viimeistään 1.11.2024 alkaen*. Sertifioinnissa olennaisia vaatimuksia sovelletaan määräyksessä 5/2024 kuvattujen profiili- ja vaatimuskohtaisten voimassaoloaikojen mukaisesti. Jos kuitenkin tietojärjestelmän yhteistestaus tai tietoturvallisuuden arviointi on käynnistetty ennen määräyksen voimaantuloa, voidaan sertifiointiprosessi suorittaa loppuun *31.12.2024 mennessä* niiden vaatimusten, säädösten ja menettelyjen mukaisesti, jotka olivat voimassa prosessin käynnistyessä. Tietoturvallisuustodistuksessa tai yhteistestauslausunnossa on tällöin oltava selvä merkintä siitä, että arviointi on suoritettu asiakastietolain 784/2021 vaatimusten ja THL:n määräysten 4/2021 ja 5/2021 mukaisesti. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan pyynnöstä myös näissä tapauksissa voidaan kuitenkin soveltaa myös THL:n määräysten 4/2024 ja 5/2024 mukaisia menettelyjä ja vaatimuksia.

Aiemman asiakastietolain 784/2021 sekä THL:n määräysten 4/2021 ja 5/2021 tai 6/2021 tai 1/2022 nojalla sertifioitujen järjestelmien tai sovellusten tietoturvallisuustodistus on uudistettava ennen aiemman lain mukaisen tietoturvallisuustodistuksen voimassaolon päättymistä. Uudistamisen yhteydessä tietojärjestelmäpalvelun

tuottajan on varmistettava luvun 10 mukaisesti, että järjestelmään on toteutettu ja sertifioitu kaikki sen käyttötarkoitusta vastaavat olennaiset vaatimukset, joihin kohdistuu todentaminen yhteistestauksessa tai tietoturvallisuuden arvioinnissa.

Jos luokkaan B kuuluvan järjestelmän tiedot Valviran tietojärjestelmärekisterissä perustuvat vanhentuneisiin säädöksiin, vaatimustenmukaisuus on uudistettava ja tietojärjestelmärekisterin tiedot päivitettävä luvun 10 ja Valviran ohjeiden tai määräysten mukaisesti.

Jos järjestelmä siirtyy luokasta B luokkaan A1 tässä määräyksessä ja sen liitteissä kuvattujen kriteerien mukaisesti, järjestelmälle on suoritettava sertifiointi voimassa olevien olennaisten vaatimusten mukaisesti tai ennen määräyksen voimaantuloa käynnistetty sertifiointi on vietävä loppuun *1.11.2024* mennessä[14].

Jos THL:n määräyksen 4/2024 tai 5/2024 mukaiset vaatimukset edellyttävät luokkaan B tai luokkaan A kuuluvan tietojärjestelmän tietojen päivittämistä[15] Valviran tietojärjestelmärekisterissä, mutta eivät edellytä uutta sertifiointia, on järjestelmästä toimitettava päivitetty ilmoitus Valviran tietojärjestelmärekisteriin *1.11.2024 mennessä*, ellei Valvira asiasta toisin määrää.

Jos aiemmin Kanta-palveluihin liittymätön järjestelmä tai hyvinvointisovellus liittyy Kanta-palveluihin suoraan tai nojautuen toiseen järjestelmään, sovellukseen tai asiakastietojen välityspalveluun, järjestelmä tai hyvinvointisovellus on luokiteltava ja sertifioitava luokan A2 tai A3 vaatimusten mukaisesti ennen liittymistä.

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

Ennen vuotta 2021 voimassa olleen asiakastietolain 159/2007 ja määräyksen 1/2015 mukaisen vaatimustenmukaisuustodistusten saaneelle järjestelmälle on suoritettava tämän määräyksen tai sen siirtymäsäännösten mukainen olennaisten vaatimusten todentaminen ja tietoturvallisuuden arviointi 1.11.2024[16] mennessä. Tässä yhteydessä tietojärjestelmäpalvelun tuottajan on varmistettava, että järjestelmään on toteutettu ja sertifioitu kaikki sen käyttötarkoitusta vastaavat olennaiset vaatimukset.

Olennaisten vaatimusten profiilien ja niissä ilmaistujen vaatimusten voimaantulosta ja vaikutuksesta mm. sosiaalihuollon asiakastietojärjestelmiin on lisätietoja määräyksessä 5/2024.

Sirpa Soini

Johtaja

Jarmo Kärki

Yksikönpäällikkö

[14] Luokkiin B ja A kuulumisen kriteerit ja luokan A1 vaatimukset vastaavat määräyksessä 4/2024 pääosin aiemman asiakastietolain (784/2021) mukaista määräystä 4/2021, joten määräaika on sama kuin määräyksessä 4/2021.

[15] Päivitystarve voi koskea esimerkiksi järjestelmän luokittelua, järjestelmässä toteutettuja profiileja tai sellaisia luokan B järjestelmään toteutettuja määräyksen 5/2024 mukaisia olennaisia vaatimuksia, joita ei ole ollut mukana aiemmassa Valviralle toimitetussa rekisteröinnissä tai ilmoituksessa. Asiakastietolain 81 §:n mukaisesti Valvira voi antaa yksityiskohtaisempia määräyksiä ilmoituksen uudistamisesta.

[16] Määräaika on sama kuin määräyksessä 4/2021: kolmen vuoden kuluessa aiemman asiakastietolain 784/2021 voimaan tulosta. Laki 784/2021 määritteli todistuksen enintään kolme vuotta voimassa olevaksi. Kumotun lain 159/2007 mukaisesti todistus oli ennen vuotta 2021 mahdollista kirjoittaa enintään viisi vuotta voimassa olevaksi.

Liitteet

Liite 1. Esimerkkejä järjestelmien ja hyvinvointisovellusten luokittelusta

Liite 2. Luokkaan A kuuluvien tietojärjestelmien ja hyvinvointisovellusten muutosten ilmoittaminen

Tiedoksi

sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien sekä apteekkien järjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat

sosiaali- ja terveydenhuollon julkiset ja yksityiset palvelunantajat

apteekit

välittäjät

hyvinvointisovellusten valmistajat

sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat

Kansaneläkelaitos

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

sosiaalialan osaamiskeskukset

tietoturvallisuuden arviointilaitokset

Kyberturvallisuuskeskus

Tietosuojavaltuutetun toimisto

sosiaali- ja terveysministeriö

valtiovarainministeriö

liikenne- ja viestintäministeriö

Lääkealan turvallisuus- ja kehittämiskeskus FIMEA

aluehallintovirastot

Digi- ja väestötietovirasto

Huoltovarmuuskeskus

Suomen Kuntaliitto ry

Tämä määräys julkaistaan viranomaisten määräyskokoelmissa

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

ja on saatavissa:

- Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä
- Internet-osoitteesta https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-jamaarittelyt/maaraykset