Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

3.5.2024

MÄÄRÄYS 5/2024 LIITE 1: OLENNAISTEN VAATIMUSTEN SOVELTAMISOHJEET

Sisällys

1 Tavoitteet

Asiakastietolain 84 §:n mukaisesti sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää toiminnallisuutta, yhteentoimivuutta sekä tietoturvaa ja tietosuojaa koskevat olennaiset vaatimukset.

THL:n määräyksillä 4/2024 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista ja 5/2024 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista kootaan yhteen menettelyt ja kansallisesti asetetut vaatimukset sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetuille tietojärjestelmille ja hyvinvointisovelluksille. Tarkempia tavoitteita ja käyttökohteita on kuvattu määräyksen 5/2024 luvussa 2.

Tietojärjestelmien ja hyvinvointisovellusten olennaisten vaatimusten kuvaaminen on osa sosiaali- ja terveydenhuollon tietojärjestelmiin ja hyvinvointisovelluksiin kohdistuvia lakisääteisiä velvoitteita. Velvoitteiden avulla pyritään varmistamaan tietojärjestelmien ja hyvinvointisovellusten toimivuus ja varmistamaan sekä kansalaisten että sote-ammattilaisten oikeusturvan toteutuminen. Olennaiset vaatimukset ovat yksi keino tietojärjestelmien ja hyvinvointisovellusten kehittämisen valtakunnalliseen ohjaamiseen sekä niiden tietoturvallisuuden varmistamiseen. Toiminnallisuutta koskevat olennaiset vaatimukset luovat pohjan myös yhteentoimivuuteen ja tietoturvallisuuteen liittyville olennaisille vaatimuksille. Järjestelmien ja hyvinvointisovellusten käyttötarkoituksen kuvaaminen ja rajaaminen yhdenmukaisesti olennaisten vaatimusten kautta selkeyttää viestintää eri järjestelmien ja hyvinvointisovellusten käyttötarkoituksista ja siitä, mitä kansallisia vaatimuksia ratkaisut täyttävät. Tietoturvallisuuden perustavoitteiden kuten luottamuksellisuuden, eheyden, saatavuuden ja kiistämättömyyden varmistamiseksi järjestelmiin, hyvinvointisovelluksiin, tietojärjestelmäpalvelujen tuottajiin ja valmistajiin kohdistuu sekä yleisiä että yksityiskohtaisia vaatimuksia.

Sote-tietojärjestelmille asetettavien vaatimusten kautta yhtenäistetään asiakastietojen käsittelyssä sellaisia seikkoja, joita säädösten nojalla on tarpeen yhdenmukaistaa, asettaen mm. järjestelmien toiminnallisuudelle, tietosisällöille sekä tietoturvallisuuteen ja tietosuojaan liittyville ratkaisuille kansallinen vähimmäistaso. Vastaavat tavoitteet kohdistuvat myös hyvinvointisovelluksiin. Tämä mahdollistaa sen, että voidaan luottaa siihen, että järjestelmissä ja sovelluksissa on riittävät ja tarvittavat ominaisuudet esimerkiksi Kanta-palveluihin liittämisen ja tietoturvallisuuden näkökulmasta, kun niitä hankitaan, kehitetään ja tarjotaan eri palveluihin ja eri asiakasryhmille. Järjestelmien, hyvinvointisovellusten ja tuotteiden välinen kilpailu voi kohdistua muun muassa käytettävyyteen sekä erityistä lisäarvoa käyttäjille tuoviin ominaisuuksiin. Olennaisten vaatimusten kokoaminen yhtenäiseen luetteloon yhtenäistää säädöksiin ja valtakunnallisiin määrityksiin perustuvissa vaatimuksissa käytettävää käsitteistöä ja yhdenmukaistaa järjestelmien ja hyvinvointisovelluksien valmistajiin ja niiden käyttäjiin kohdistuvia perusvaatimuksia.

Säädösten kautta asetettavien vaatimusten lisäksi tietojärjestelmiä ja hyvinvointisovelluksia on mahdollista arvioida esimerkiksi käytettävyyden, prosessimuutosten, kustannusten, vaikuttavuuden ja useiden muiden näkökulmien kautta. Näitä muita seikkoja ja näkökulmia sisältyy tyypillisesti terveysteknologian arviointimalleihin (health technology assessment, HTA). Säädösten kautta asetetaan ja arvioidaan vähimmäisvaatimuksia, joita voidaan täydentää terveysteknologian laajempien arviointien kautta.

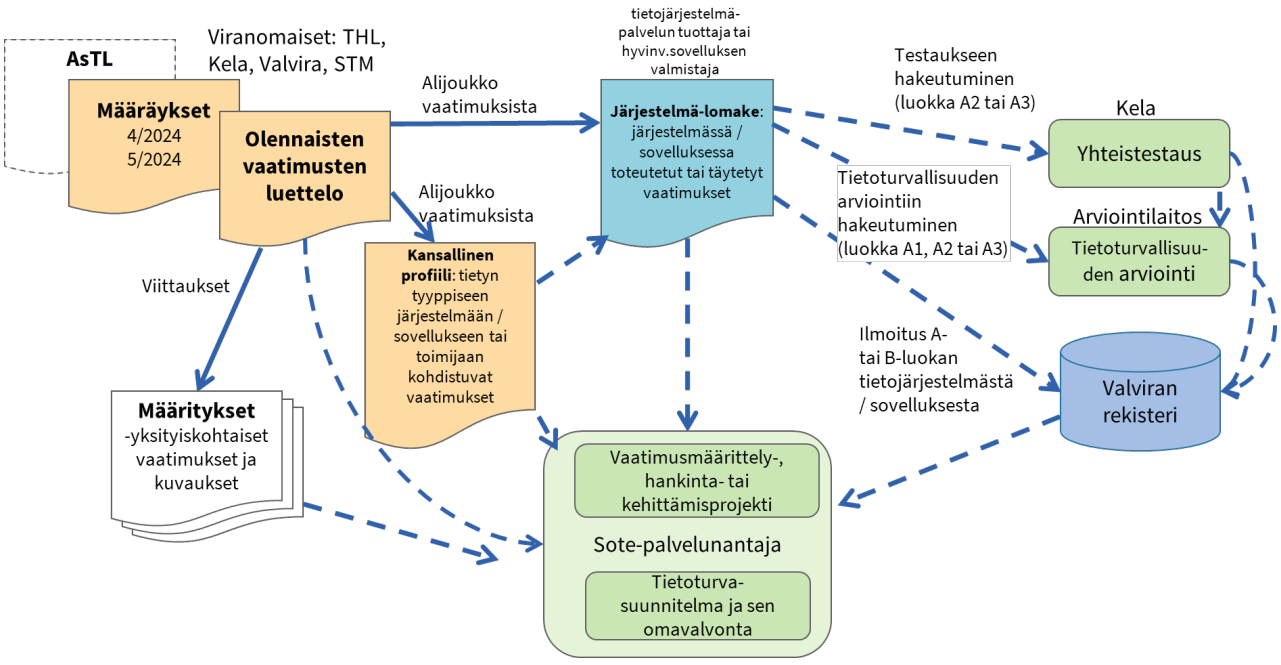
2 Yleiskuva olennaisten vaatimusten käytöstä

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoituksen kuvaamisesta, tietojärjestelmän tai hyvinvointisovelluksen luokittelusta, olennaisten vaatimusten huomioimisesta ratkaisun suunnittelussa ja toteutuksessa, sekä tietojärjestelmän tai hyvinvointisovelluksen sertifioinnista ja rekisteröinnistä. Tietojärjestelmäpalvelun tuottaja voi olla järjestelmän valmistaja tai muu taho, joka voi vastata kansallisten vaatimusten todentamisen lisäksi esimerkiksi järjestelmän tuesta käyttäjäorganisaatioille.

On yleistä, että tietojärjestelmän valmistaja vastaa järjestelmän luokittelusta, sertifioinnista ja rekisteröinnistä Valviran tietojärjestelmärekisteriin, vaikka käyttäjäorganisaatiolla olisi kolmas taho, jonka kanssa on sovittu esimerkiksi integraatio-, ylläpito-, sovellustuki-, käyttötuki-, koulutus- tai muista toimenpiteistä. Tietojärjestelmän valmistaja on oletusarvoisesti tietojärjestelmäpalvelun tuottaja, ellei jokin muu taho vastaa järjestelmän rekisteröinnistä ja sertifioinnista. Kolmas taho toimii tietojärjestelmäpalvelun tuottajana, jos se vastaa järjestelmän rekisteröinnistä ja olennaisten vaatimusten täyttämisestä / sertifioinnista. On tärkeää, että eri osapuolten välisissä sopimuksissa vastuut on selkeästi määritelty. Myös tietojärjestelmän valtuutettu edustaja, maahantuoja tai jakelija voi toimia tietojärjestelmäpalvelun tuottajan roolissa, jos asiasta on sovittu tietojärjestelmän valmistajan kanssa. Poikkeustilanteissa myös palvelunantaja voi vastata tietojärjestelmäpalvelun tuottajaan tai tietojärjestelmän valmistajaan kohdistuvista velvoitteista (ks. määräys 5/2024 luku 9).

Tietojärjestelmää käyttävä palvelunantaja vastaa siitä, että käyttää tuottamiaan sote-palveluita vastaavien vaatimusten mukaisia tietojärjestelmiä. Järjestelmiä on käytettävä tietojärjestelmäpalvelun tuottajalta saatujen ohjeiden mukaisesti. Palvelunantajan tehtävänä on osaltaan varmistaa, että käytettävä tietojärjestelmä on vaatimusten mukainen. Tämä tapahtuu muun muassa nojautumalla Valviran tietojärjestelmärekisteristä löytyviin tietoihin järjestelmän vaatimustenmukaisuudesta sekä varmistamalla järjestelmien hankintaan ja ylläpitoon liittyvissä sopimuksissa kansallisten vähimmäisvaatimusten profiilien mukaisten järjestelmien mukaisten vaatimusten täyttyminen. Järjestelmiä käyttävien palvelunantajien ei tarvitse tuntea kaikkia olennaisia vaatimuksia tai niiden täyttämisen tai todentamisen yksityiskohtia.

Kuvassa 1 on yleiskuva olennaisten vaatimusten määräyksen ja luettelon hyödyntämisestä. Keskeisiä kokonaisuuteen liittyviä materiaaleja ovat määräykset, olennaisten vaatimusten luettelo, järjestelmälomake sekä profiilit.



Kuva 1. Olennaisten vaatimusten kokonaisuus.

2.1 Olennaisten vaatimusten luettelo

Olennaisten vaatimusten luettelo (määräys 5/2024 liite 2) on taulukko, joka kokoaa asiakas- ja potilastietoja käsitteleville järjestelmille ja hyvinvointisovelluksille kansallisesti määritellyt:

- toiminnallisuudet / toiminnot (Toiminnot-välilehti)
- tietosisällöt (eri tietosisältöjen käsittelyn kyvykkyydet) (Tietosisällöt-välilehti)
- tietoturvavaatimukset (Tietoturvavaatimukset-välilehti).

Hyvinvointisovelluksiin, hyvinvointitietoihin ja kansalaisten käyttämiin digipalveluihin liittyviä toiminnallisuuksia ka tietoturvallisuuden arvioinnissa läpikäytäviä vaatimuksia on lisäksi koottu Digitaalisten palvelujen vaatimukset -välilehdelle.

Toiminnot ja tietosisällöt muodostavat *olennaiset toiminnalliset vaatimukset*.

Pääosa vaatimuksista on peräisin eri kehittämiskokonaisuuksiin liittyvistä määritysdokumenteista. Toiminnot, tietosisällöt ja tietoturvavaatimukset kuvataan yleisellä tasolla siten, että niihin liittyvät tarkemmat määritykset löytyvät olennaisten vaatimusten luettelon kautta. Kullakin vaatimusrivillä on yksi tai useampia lähdeviitteitä, ja Lähdeviittaukset -välilehdellä olevien linkkien kautta pääsee tarkastelemaan yksityiskohtaisempia määritysdokumentteja ja säännöksiä, joihin olennaiset vaatimukset perustuvat. Ajantasaisimmat voimassa olevat määritykset erityisesti Kanta-palveluihin liittyville järjestelmille on kuvattu Kelan ja THL:n sivustoilla [1] sekä eri tietosisältöjen julkaisukanavissa kuten THL:n ja Kelan koodistopalvelussa sekä Sosmeta- ja Termeta-palveluissa. Viitatut määritysdokumentit sisältävät tarkemmat tiedot siitä, mitkä ominaisuudet tai yksityiskohtaiset tiedot toteutuksissa ovat vapaaehtoisia tai pakollisia. Tietyn toiminnon tai tietosisällön pakollisuus ei muodostu siis yksinomaan profiilissa ja luettelossa kuvattujen tietojen pohjalta, vaan vaatimusten toteutuksissa on huomioitava tarkemmat määritykset. Uusissa toteutuksissa tulee käyttää määritysten uusimpia voimassa olevia versioita ja tuotantokäyttöön voidaan hyväksyä tiettyjen määritysversioiden mukaisia toteutuksia.

Eri toimintojen ja tietosisältöjen kohdalla luettelossa kerrotaan myös niihin liittyvät Kanta-palveluihin liittyvien järjestelmien ja sovellusten yhteistestauksen testauskokonaisuudet sekä tietoturvallisuuden arvioinnissa todennettavat tietoturvavaatimukset (mikäli toiminto liittyy johonkin tietoturvavaatimuksista). Eri toimintoihin, tietosisältöihin ja tietoturvavaatimuksiin liittyvät keskeisimmät määritykset mainitaan kunkin olennaisen vaatimuksen kohdalla, ja ne löytyvät olennaisten vaatimusten luettelo -taulukosta ”Viittaukset lähdedokumentteihin” -välilehdeltä. Luettelossa kuvataan myös eri tietosisällöistä saatavilla olevien kansallisten määritysten rakenteisuuden taso. Olennaisten vaatimusten välisiä suhteita kuvataan osana luetteloa, esimerkiksi kun tiettyyn toimintoon liittyy joukko erikseen kuvattuun tietosisältöön tai toiseen toimintoon liittyviä vaatimuksia.

Olennaisiin vaatimuksiin sisältyvät toiminnot, tietosisällöt ja tietoturvavaatimukset on ryhmitelty siten, että samassa vaatimusryhmässä on samaan aihepiiriin liittyviä vaatimuksia. Ryhmittely on pelkästään samaan aihepiiriin liittyvien vaatimusten kokoamiseen tarkoitettu - varsinaiset järjestelmien vaatimukset sekä profiilit kohdistuvat aina yksilöityihin vaatimuksiin eikä vaatimusryhmiin.

Järjestelmän tai hyvinvointisovelluksen käyttötarkoitus ja kansallisesti asetetut vaatimukset ohjaavat osaltaan sitä, millaisia sisältöjä ja toiminnallisuuksia sekä tietoturvaominaisuuksia järjestelmässä tai sovelluksessa vähintään on oltava. Kanta-palveluihin liittyvissä järjestelmissä tai hyvinvointisovelluksissa (luokka A2 tai A3) toiminnalliset vaatimukset toteutetaan yksityiskohtaisten viitattujen määritysten mukaisesti. Muissa järjestelmissä (luokassa B ja A1) monet olennaiset vaatimukset perustuvat ylemmän tason säädöksiin ja vain joihinkin järjestelmien sisältöihin tai toimintoihin on yksityiskohtaisia kansallisia määritysdokumentteja.

2.2 Vähimmäisvaatimusten profiilit

Olennaisten vaatimusten luettelo toimii pohjana myös *profiileille*. Yksi profiili kokoaa tiettyyn käyttötarkoitukseen tarkoitetuille järjestelmille tai sovelluksille asetetut kansalliset vähimmäisvaatimukset. Yksi profiili sisältää siis osajoukon olennaisten vaatimusten luettelossa kuvatuista toiminnoista, tietosisällöistä ja tietoturvavaatimuksista.

[1] Esimerkiksi Kanta-määritysten uusimmat versiot löytyvät Kanta-sivustolta (Järjestelmäkehittäjät-osio) ja THL:n sivuilta (Määrittelyt-osio).

Profiileja julkaistaan sellaisiin käyttötarkoituksiin, joissa on tärkeää yhtenäistää vähimmäistason vaatimukset joukolle tietojärjestelmiä tai hyvinvointisovelluksia.

Profiileja on mahdollista julkaista erillään olennaisten vaatimusten luettelon päivittämisestä, ja eri käyttötarkoituksiin tarkoitetuille tietojärjestelmille tai hyvinvointisovelluksille voidaan julkaista uusia vähimmäisvaatimusten profiileja. Profiilit eivät kata kaikkia mahdollisia luokkien A tai B järjestelmien tai hyvinvointisovellusten käyttötarkoituksia. Esimerkiksi kaikille eri terveydenhuollon erikoisalojen tai eri sosiaalipalveluissa käytettäville järjestelmille ei ole julkaistu spesifejä profiileja.

Olennaiset vaatimukset ja profiilit toimivat terveydenhuollon potilastietojen tai sosiaalihuollon asiakasitietojen käsittelyyn tarkoitettujen järjestelmien tai hyvinvointisovellusten suunnittelun ja toteuttamisen yhtenä keskeisenä lähtökohtana. Määräyksen liitteenä olevan profiilin mukaisten vähimmäisvaatimusten toteuttaminen on edellytyksenä profiilin mukaiseen käyttötarkoitukseen käytettävän tietojärjestelmän tai tietojärjestelmäkokonaisuuden tai hyvinvointisovelluksen ottamiselle tuotantokäyttöön. Tietojärjestelmässä tai tietojärjestelmäkokonaisuudessa, jolla on profiilia vastaava käyttötarkoitus, on toteutettava tai täytettävä viitattujen määritysten mukaisesti vähintään profiilissa pakolliseksi määritellyt ominaisuudet. Vastaava vaatimus koskee hyvinvointisovelluksia.

Profiilit ovat määräyksen 5/2024 liitteessä 3. Liitteessä on useita taulukoita, joista jokaisessa on yksi tai useampia profiileja. Esimerkiksi Liite 3a sisältää kaksi profiilia: Lääkemääräyksiä käsittelevä potilastietojärjestelmä ja Apteekkijärjestelmä.

Kukin profiili sisältää sellaiset toiminnot, tietosisällöt ja tietoturvavaatimukset, joiden toteuttamista määritysten mukaisesti edellytetään profiilin mukaiseen tarkoitukseen käytettävässä tietojärjestelmässä tai hyvinvointisovelluksessa. Esimerkiksi Apteekkijärjestelmä-profiili (määräys 5/2024 liite 3a, profiili 3a2) sisältää apteekkien lääkemääräysten ja lääketoimitusten käsittelyyn käyttämiltä tietojärjestelmiltä vähintään edellytettävät toiminnallisuudet ja tiedot. Profiili sisältää muun muassa lääkemääräystietojen hakemista ja lääkkeen toimittamista varten tarvittavat toiminnot ja tiedot sekä sellaiset tietoturvavaatimukset, joiden täyttäminen on vähintään tarpeen apteekkitoiminnassa lääkemääräysten ja lääketoimitusten käsittelyyn käytettävässä tietojärjestelmässä (ks. myös luku 6.6).

Profiileja on koottu erityisesti eri Kanta-palveluihin kuten potilastiedon arkistoon, sosiaalihuollon asiakastiedon arkistoon, omatietovarantoon ja reseptikeskukseen liittyville tietojärjestelmille tai hyvinvointisovelluksille. Osa profiileista kuten määräyksen 5/2024 liitteen 3g profiili kokoaa kuitenkin laajemmin kaikkiin luokkaan B tai A kohdistuviin järjestelmiin kohdistuvia vaatimuksia eri säädöksistä. Luokkaan A (myös A1) kuuluvissa järjestelmissä ja hyvinvointisovelluksissa tietoturvavaatimukset käydään läpi tietoturvallisuuden arvioinnissa, mutta useat tietoturvavaatimukset koskevat myös luokkaan B kuuluvia tietojärjestelmiä.

Yksi järjestelmä tai hyvinvointisovellus voi täyttää usean eri profiilin mukaiset vaatimukset. Esimerkiksi laaja asiakas- ja potilastietojärjestelmä voi täyttää kaikki liitteen 3b profiilit, potilaskertomusjärjestelmän perusvaatimukset (liitteestä 3c), sosiaalihuollon asiakastiedon arkiston profiileja (liitteestä 3d), lääkemääräyksiä käsittelevän potilastietojärjestelmän profiilin (liitteestä 3a), Kanta-arkistoon todistuksia tai lausuntoja tuottavan palvelun profiilin (liitteestä 3f) sekä hyvinvointitietoja ammattihenkilöille hakevan järjestelmän profiilin (liitteestä 3h). Samassa järjestelmässä voi olla myös osio kansalaisasiointiin (liitteestä 3h) tai hyvinvointisovelluksen määritelmän mukainen osajärjestelmä kansalaiskäyttöön (liitteestä 3h), ks. luku 6.5. Järjestelmissä toteutetaan profiilien sisältämien vaatimusten lisäksi aina myös muita vaatimuksia. Nämä voivat olla sekä sellaisia, joille on oma olennainen vaatimus (profiilin ulkopuolella) tai projekti- tai käyttäjäorganisaatiokohtaisia vaatimuksia.

Profiileissa kuvataan myös sitä, minä ajankohtana eri vaatimuksia on täytettävä. Profiileilla ja niihin kuuluvilla vaatimuksilla on voimaantuloaikoja, jotka heijastavat esimerkiksi säädösten edellyttämiä määräaikoja sen suhteen, koska tietyn tyyppiset tiedot on arkistoitava Kanta-palveluihin tai koska tiettyä määrittelyversiota on tuettava Kanta-palveluihin liittyvissä tuotantokäytössä toimivissa järjestelmissä. Profiilien voimassaolo- ja siirtymäajat nojautuvat valtakunnallisiin säädöksiin ja määräyksiin, kuten asiakastietolain siirtymäsäännöksiin. Jos profiilin voimaantulopäivämäärä ja vaatimuksen kohdalla ilmaistu päivämäärä ovat menneisyydessä, ”voimassa”

tai ”liittymisen yhteydessä”, tarkoittaa se sitä, että vaatimus on jo voimassa. Tällöin profiilin mukaisen käyttöön otettavan, käytössä olevan tai Kanta-palveluihin liitettävän järjestelmän (ja sen uusien versioiden) tulee toteuttaa vaatimus.

Järjestelmän luokkaa ei suoraan päätellä siitä, mitä profiileja tai toimintoja järjestelmässä toteutetaan. Esimerkiksi luokassa A1 voi olla järjestelmä, jossa Kanta-palveluihin liittyvät rajapinnat ja vaatimukset täytetään ja todennetaan luokkaan A3 kuuluvan tietojärjestelmän tai osajärjestelmän kautta.

2.3 Järjestelmälomake tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan työkaluna

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja kuvaa oman järjestelmänsä tai hyvinvointisovelluksen käyttötarkoituksen, järjestelmässä tai hyvinvointisovelluksessa toteutetut olennaiset vaatimukset sekä järjestelmän tai hyvinvointisovelluksen noudattamat vähimmäisvaatimusten profiilit järjestelmälomakkeella. Järjestelmälomake perustuu olennaisten vaatimusten luetteloon. Lomakkeella kuvataan yksittäisen tietojärjestelmän, hyvinvointisovelluksen, osajärjestelmän tai tietojärjestelmäkokonaisuuden sisältämät toiminnot, tietosisällöt ja tietoturvavaatimukset. Järjestelmälomake ei sisällä kaikkia olennaisten vaatimusten luetteloon sisältyviä lisätietoja. Luettelon ja siinä viitattujen lähdedokumenttien kautta löytyy lisätietoja järjestelmälomakkeella olevista vaatimuksista.

Täytetty järjestelmälomake toimii asiakastietolain mukaisena selvityksenä olennaisten vaatimusten täyttämisestä järjestelmässä tai hyvinvointisovelluksessa. Järjestelmälomake on täytettävä ja selvitys annettava kaikista asiakastietolain määritelmän mukaisista tietojärjestelmistä (luokka A tai B) tai hyvinvointisovelluksista. Järjestelmälomake dokumentoi sen, kuinka järjestelmän tai hyvinvointisovelluksen suunnittelussa, toteuttamisessa, dokumentoinnissa sekä käytön suunnittelussa ja ohjeistamisessa on huomioitu siihen kohdistuvat olennaiset vaatimukset. Järjestelmän tai hyvinvointisovelluksen käyttötarkoitus, luokittelu, riskitaso, olennaiset vaatimukset ja profiilit on tärkeää huomioida jo järjestelmän tai hyvinvointisovelluksen tai niiden päivitysten suunnitteluvaiheessa.

Järjestelmälomaketta käytetään, kun tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja hakeutuu Kelan yhteistestaukseen Kanta-palveluihin liittyvän luokan A2 tai A3 tietojärjestelmän tai hyvinvointisovelluksen testaamista varten. Monet olennaisista vaatimuksista liittyvät tietosisältöihin ja toimintoihin, joita testataan osana yhteistestausta. Tällaiset olennaiset vaatimukset on linkitetty Kelan yhteistestauskokonaisuuksiin, joissa eri vaatimuksissa viitattujen määritysten pohjalta testataan Kanta-palveluihin liittyvien järjestelmien tai hyvinvointisovellusten yhteentoimivuus Kanta-palvelujen ja muihin Kanta-palveluihin liitettyjen järjestelmien tai sovellusten kanssa.

Järjestelmälomaketta käytetään myös, kun luokkaan A1, A2 tai A3 kuuluvan tietojärjestelmän tai hyvinvointisovelluksen tietoturvallisuuden arviointi käynnistetään. Olennaisia tietoturvavaatimuksia käytetään tietoturvallisuuden arvioinnin kriteereinä ja pohjana luokan A järjestelmille tai hyvinvointisovelluksille annettavaan tietoturvallisuustodistukseen.

Lomake on liitteenä myös ilmoituksessa, joka on lakisääteisesti tehtävä jokaisesta sosiaali- ja terveydenhuollossa käyttöönotettavasta luokkaan B, A1, A2 tai A3 kuuluvasta asiakas- tai potilastietoja käsittelevästä tietojärjestelmästä Valviralle. Myös hyvinvointisovelluksista on tehtävä ilmoitus, jonka liitteenä lomake on. Valvira ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon tietojärjestelmistä tai hyvinvointisovelluksista. Valviran tietojärjestelmärekisteri sisältää tiedot tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antamasta ilmoituksesta, tietoja järjestelmälle tai sovellukselle suoritetuista yhteistestauksista ja tietoturvallisuuden arvioinnista sekä esimerkiksi Valviran valvontaprosessin kautta syntyneitä tietoja. Rekisterin tietojen tarkastelu onnistuu Valviran sivujen kautta.

Valviralle tehtävä lakisääteinen ilmoitus koskee kaikkia luokkiin A ja B kuuluvia sosiaali- ja terveydenhuollon tietojärjestelmiä, joiden käyttötarkoituksena on asiakas- tai potilastietojen käsittely, vaikka järjestelmä ei olisikaan Kanta-palveluihin liittyvä. Valviralle tehtävä lakisääteinen ilmoitus koskee kaikkia luokkaan A kuuluvia hyvinvointisovelluksia, joiden käyttötarkoituksena on oltava hyvinvoinnin ja terveyden edistäminen.

Tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa myös siitä, että rekisteriin ilmoitetut tiedot ovat ajantasaisia.

Järjestelmälomakkeella tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja täyttää siis joukon lakisääteisiä velvoitteita. Lomakkeella ilmoitetaan järjestelmää tai hyvinvointisovellusta koskevat perustiedot, kuvataan järjestelmän tai hyvinvointisovelluksen käyttötarkoitus, otetaan kantaa siihen mitä kansallisia profiileja ja vaatimuksia on toteutettu sekä ilmaistaan tarvittaessa aiempiin versioihin verrattuna muutettuja ominaisuuksia tai suhde muihin järjestelmiin tai sovelluksiin.

Vain järjestelmään tai hyvinvointisovellukseen toteutetut tai sen kautta täytettävät vaatimukset merkitään järjestelmälomakkeeseen. Vaatimusten täyttyminen on pystyttävä tarvittaessa todentamaan osana sertifiointia tai valvontaviranomaisen pyynnöstä.

Järjestelmälomakkeen täyttämisessä on seuraavat vaiheet, kun tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja käyttää lomaketta sertifioinnissa tai Valviralle tehtävän ilmoituksen tekemisessä:

1. Täytä järjestelmän tai hyvinvointisovelluksen perustiedot: järjestelmän tai hyvinvointisovelluksen nimi, tietojärjestelmäpalvelun tuottaja, valmistaja (voi olla myös sama kuin tietojärjestelmäpalvelun tuottaja) tai hyvinvointisovelluksen valmistaja, versio[2].
2. Kuvaa lyhyesti järjestelmän tai hyvinvointisovelluksen käyttötarkoitus: mihin tarkoitukseen, millaisiin palveluihin ja millaisilla rajauksilla järjestelmää tai hyvinvointisovellusta on tarkoitus käyttää. Nämä tiedot merkitään lomakkeen kohtiin Käyttötarkoituksen kuvaus ja Käyttökonteksti (valittavana esim. julkiset tai yksityiset sosiaali- tai terveyspalvelut, digipalvelut kansalaiselle).
3. Kuvaa järjestelmälle tehdyn riskiarvion pohjalta järjestelmän riskitaso ja se, kuinka laajamittaiseen asiakas- tai hyvinvointitietojen käyttöön järjestelmä on suunniteltu määräyksessä 4/2024 ja sen liitteessä 1 kuvatuilla perusteilla. Hyödynnä tarvittaessa tukimateriaalia kuten THL:n julkaisemaa riskiarviointityökalua.
4. Merkitse lomakkeen kohtaan *Järjestelmän / hyvinvointisovelluksen luokka* määräyksen 4/2024 ja sen Liitteen 1 mukaisesti se, mihin luokkaan järjestelmä kuuluu (A3, A2, A1 tai B).
5. Merkitse järjestelmälomakkeen Profiilit-kohtaan ne määräyksen 5/2024 liitteissä 3 olevat profiilit, joissa profiilissa ilmaistu käyttötarkoitus on osa järjestelmän tai hyvinvointisovelluksen käyttötarkoitusta. Kunkin profiilin nimi ja kuvaus sekä lisätiedot antavat tietoa profiilin soveltamisesta. Järjestelmään tai hyvinvointisovelluksen on toteutettava ja lomakkeeseen merkittävä ne profiilit, joiden mukaisiin käyttötarkoituksiin järjestelmä tai hyvinvointisovellus on tarkoitettu. Järjestelmälomakkeelle riittää profiilien tunnusten merkitseminen (esim. ”3a1, 3c1”), profiilin koko nimeä ei tarvitse kirjoittaa lomakkeelle. Erityisesti luokkaan A2 tai A3 kuuluvissa sertifioitavissa järjestelmissä on tärkeää tunnistaa ja merkitä järjestelmän käyttötarkoitusta vastaavat profiilit ja niiden kautta muodostuvat vaatimukset oikein jo siinä vaiheessa, kun hakeudutaan yhteistestaukseen.
6. Merkitse lomakkeen Toiminnot-välilehdelle ne olennaisia vaatimuksia vastaavat toiminnallisuudet, jotka järjestelmään tai hyvinvointisovellukseen on toteutettu.
7. Merkitse lomakkeen Tietosisällöt-välilehdelle ne olennaisia vaatimuksia vastaavat tietosisällöt, jotka järjestelmään tai hyvinvointisovellukseen on toteutettu.

[2] Vaikka versionumero voi muuttua usein, on tärkeää erottaa uudemmat ja vanhemmat järjestelmän tai hyvinvointisovelluksen versiot toisistaan sertifioinnissa, jotta todennettujen vaatimusten toteutus on jäljitettävissä, sertifioinnin tuloksia voidaan verrata eri käyttöympäristöissä tuotannossa toimiviin järjestelmiin, ja jotta yhteistestaus ja tietoturvallisuuden arviointi kohdistuvat oikeisiin järjestelmäversioihin. Ks. myös määräys 4/2024 luku 7.3 ja tämän liitteen luku 2.2.

8. Merkitse lomakkeen Tietoturvavaatimukset-välilehdelle ne tietoturvallisuusvaatimukset, jotka järjestelmään on toteutettu tai jotka täytetään järjestelmän tai hyvinvointisovelluksen kautta.
9. Jos kyseessä on hyvinvointisovellus, hyvinvointitietoja käyttävä järjestelmä tai kansalaisille suunnattu digitaalinen asiointipalvelu (tai järjestelmässä on näitä ominaisuuksia), merkitse lomakkeen Digit. palvelujen vaatimukset -välilehdelle ne olennaiset vaatimukset, jotka koskevat näitä ominaisuuksia, vastaavasti kuin kohdissa 6-8.
10. Varmista, että järjestelmälomakkeelle täyttämäsi Toiminnot, Tietosisällöt ja Tietoturvavaatimukset vastaavat niitä vaatimuksia, jotka on merkitty pakollisiksi kohdassa 3 valitsemiisi profiileihin. Profiileja voi myös käyttää pohjana kohtien 6-9 täyttämiseen siten, että kaikkien järjestelmää tai sovellusta koskevien profiilien vaatimukset täytetään ensin, ja sitten lomakkeelle täydennetään muut järjestelmässä tai sovelluksessa relevantit olennaiset vaatimukset.
11. Varmista vaatimustenmukainen toteutus, testaa ja dokumentoi järjestelmään tai hyvinvointisovellukseen toteutetut olennaiset vaatimukset ennen järjestelmän tai hyvinvointisovelluksen sertifiointia tai rekisteröintiä sekä profiileihin kuuluvien että muiden järjestelmään tai hyvinvointisovellukseen toteutettujen olennaisten vaatimusten osalta.
12. Tarkista lomakkeen tiedot ja käytä lomaketta kuvan 1 mukaisissa tilanteissa järjestelmän tai hyvinvointisovelluksen sertifioinnissa ja rekisteröinnissä.
13. Päivitä lomake, kun järjestelmään tai hyvinvointisovellukseen tehdään muutoksia - lomakkeen uusiin versioihin merkitään muuttuneina ne vaatimukset, jotka ovat muuttuneet aiempaan lomakkeesta toimitettuun versioon verrattuna.
14. Seuraa olennaisten vaatimusten ja niiden viittaamien määritysten muutoksia sekä versiopäivityksiä ja huomioi ne järjestelmään toteutetuissa ominaisuuksissa, muutosilmoituksissa ja vaatimustenmukaisuuden uudistamisessa.

Lomakkeen käytön merkitys täytettyjen olennaisten vaatimusten ilmoittamisessa ja tarkennuksia esimerkiksi toteutettujen profiilien ilmoittamiseen on kuvattu määräyksen 5/2024 luvussa 8. Järjestelmälomakkeen eri kohdissa sekä ”Yleistiedot ja täyttöohjeet” sivulla on tarkempia ohjeita eri kohtiin. Jokaisesta järjestelmälomakkeen vaatimusrivistä löytyy tarvittaessa tarkempaa tietoa määräyksen 5/2024 liitteestä 2 Olennaisten vaatimusten luettelo. Tarkempia tietoja ovat muun muassa eri vaatimusten väliset suhteet, tarkemmat kuhunkin vaatimukseen liittyvät määritykset ja säädökset, ja vaatimusten vastaavuudet aiempien määräysten mukaisiin vaatimuksiin.

Kohdissa 6-9 lomakkeelle merkitään sekä järjestelmän tai hyvinvointisovelluksen käyttötarkoitusta vastaavien profiilien perusteella että muutenkin järjestelmään tai hyvinvointisovellukseen toteutetut ominaisuudet. Esimerkiksi jos järjestelmään on toteutettu potilaskertomusjärjestelmän perusvaatimusten profiilin (profiili 3c1) mukaiset vaatimukset mutta lisäksi ravitsemustietojen kirjaamisen ja hallinnan ominaisuudet (tietosisältövaatimus TPOT25, jota profiilissa ei ole pakollisena vaadittu), myös ravitsemustietojen toteutus merkitään järjestelmälomakkeelle.

Lomakkeeseen merkitään kohdissa 6-9 myös sellaiset vaatimukset, joita täytetään järjestelmää käytettäessä muiden järjestelmään liittyvien tietojärjestelmien tai erikseen kuvattujen osajärjestelmien kautta. Samassa järjestelmäkokonaisuudessa tai asiakasympäristössä on mahdollista olla eri tahojen valmistamia tai eri tietojärjestelmäpalvelujen tuottajien vastuulla olevia järjestelmiä tai osajärjestelmiä. Eri järjestelmistä koostuvissa tietojärjestelmäkokonaisuuksissa ja modulaarisissa tietojärjestelmissä lomaketta käytetään osajärjestelmäkohtaisesti, jos eri osajärjestelmiä sertifioidaan tai rekisteröidään osajärjestelmäkohtaisesti. Lomaketta on mahdollista käyttää myös kuvaamaan useista osajärjestelmistä koostuvaa järjestelmäkokonaisuutta, esimerkiksi jos yhteistestauksen kohteena on kuvantamisen tietojärjestelmäkokonaisuudessa useiden eri osajärjestelmien kautta täytettävä kokonaisuus. Sertifioinnissa ja järjestelmien rekisteröinnissä on kuitenkin huolehdittava siitä, että lomake on täytetty kustakin osajärjestelmästä, jolle tulee oma yhteistestauslausunto, tietoturvallisuustodistus tai rekisteröinti. Lisätietoja on tämän liitteen luvussa 6.3.

Järjestelmälomake on toimitettava pyynnöstä myös sote-palvelunantajalle tai apteekille, joka pyytää tarjouksia potilastietojen tai sosiaalihuollon asiakastietojen käsittelyyn tarkoitetusta järjestelmästä.

3 Valviran tietojärjestelmärekisterin merkitys ja hyödyntäminen

Valviran rekisteri sosiaali- ja terveydenhuollon tietojärjestelmistä kokoaa tiedot ilmoitetuista tietojärjestelmistä ja hyvinvointisovelluksista sekä tietojärjestelmien ja hyvinvointisovellusten yhteistestauksen ja tietoturvallisuuden arvioinnin tulokset. Valvira julkaisee rekisterissä olevat keskeiset tiedot tietojärjestelmistä ja hyvinvointisovelluksista.

Tietojärjestelmärekisterin kautta on julkisesti saatavilla tiedot hyvinvointisovelluksista sekä sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetuista tietojärjestelmistä. Rekisterin julkiset tiedot ovat keskeinen pohja muun muassa tietojärjestelmien ja hyvinvointisovellusten ja niiden vaatimustenmukaisuuden valvonnassa. Sote-palvelunantajat voivat hyödyntää Valviran tietojärjestelmärekisterin tietoja esimerkiksi hankintojen tukena. Tietojärjestelmien ja hyvinvointisovellusten ilmoittaminen rekisteriin olennaisia vaatimuksia ja profiileja hyödyntäen mahdollistaa sen, että esimerkiksi eri profiileja täyttävien hyväksyttyjen ja sertifioitujen järjestelmien ja hyvinvointisovellusten tiedot saadaan vertailtavasti näkyviin tai haettavaksi. Tietojärjestelmärekisterin tiedot sekä lisätietoja rekisteristä on julkaistu Valviran sivuilla.

Valviralle tehdyn ilmoituksen ja siihen liittyvien kuvausten kautta tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vakuuttaa, että järjestelmä tai hyvinvointisovellus asianmukaisesti asennettuna, ylläpidettynä ja käyttötarkoituksen mukaisesti käytettynä täyttää asiakastietolain 84 § kautta säädetyt olennaiset vaatimukset. Ilmoittaja vastaa siitä, että ilmoitetut toiminnot ja tietosisällöt ovat järjestelmään tai hyvinvointisovellukseen toteutettuja. Luokkaan A kuuluvissa tietojärjestelmissä ja hyvinvointisovelluksissa on lomakkeen tietojen vastattava myös tietoturvallisuuden arvioinnin ja mahdollisen yhteistestauksen tuloksia.

Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa on noudatettava mahdollisia Valviran antamia ohjeita ja määräyksiä. Kaikkia tietojärjestelmän tai hyvinvointisovellusten uusia versioita ei ole välttämätöntä ilmoittaa Valviran tietojärjestelmärekisteriin. Ilmoituksesta riippumatta tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja vastaa siitä, että uusi versio täyttää olennaiset vaatimukset vähintään samalla tasolla kuin aiempi versio.

Valvontaviranomaiset kuten Valvira, Tietosuojavaltuutetun toimisto ja aluehallintovirastot valvovat asiakastietolain mukaisten vaatimusten toteutumista rekisteriä hyödyntäen. Rekisteriin toimitettavien tietojen on oltava oikeellisia ja ajantasaisia.

4 Olennaisten vaatimusten ja profiilien hyödyntäminen sote-organisaatioissa

Asiakastietolain 84 § mukaisesti palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Määräys 5/2024 (erityisesti luku 9) tarkentaa sitä, kuinka nämä seikat varmistetaan. Palvelunantajan toimintaan liittyvät olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.

Sote-palvelujen järjestäjän tai tuottajan tulee varmistaa, että:

1. sen käyttämät tietojärjestelmät tai osajärjestelmät kokonaisuutena vastaavat käyttötarkoitukseltaan organisaation toimintaa;
2. sen käyttämistä luokan A ja luokan B tietojärjestelmistä löytyy tiedot Valviran rekisteristä;
3. sen käyttämillä luokkaan A1, A2 ja A3 kuuluvilla järjestelmillä on asianmukainen ja voimassa oleva tietoturvallisuustodistus;
4. sen käyttämät luokkaan A2 tai A3 kuuluvat Kanta-palveluihin liittyvät järjestelmät on yhteistestattu suhteessa niihin toimintoihin ja tietosisältöihin, joissa on Kanta-palveluihin liittyviä yhteistestauksessa todennettavia vaatimuksia;
5. siltä osin kuin toiminnassa tarvitaan kansallisten vähimmäisvaatimusten profiileissa kuvattuihin käyttötarkoituksiin käytettäviä tietojärjestelmiä, käytetyt tietojärjestelmät tai osajärjestelmät kokonaisuutena toteuttavat kyseisten profiilien mukaiset vaatimukset;
6. tietojärjestelmien käytössä huomioidaan sellaiset olennaisiin vaatimuksiin liittyvät sertifioinnissa esiin nousseet havainnot ja edellytykset, jotka vaikuttavat olennaisten vaatimusten toteutumiseen käytetyissä järjestelmissä;
7. jos sen toiminnassa käytetään myös hyvinvointisovelluksia tai järjestelmissä on hyvinvointisovelluksen määritelmän täyttäviä osajärjestelmiä, kohdat 2, 3, 4 ja 6 toteutuvat myös käytettyjen hyvinvointisovellusten osalta.

Käytännön välineenä näiden seikkojen varmistamisessa tulisi käyttää määräyksen 3/2024 mukaista tietoturvasuunnitelmaa, jossa on kuvattava ne tietojärjestelmät, joita palvelunantaja käyttää potilastietojen tai sosiaalihuollon asiakastietojen käsittelyyn. Käytettävien tietojärjestelmien ja niiden vaatimustenmukaisuuden tiedot päivitetään tarvittaessa osana tietoturvasuunnitelman säännöllistä päivitystä ja omavalvontaa hyödyntäen esimerkiksi Valviran tietojärjestelmärekisteriä ja tietojärjestelmäpalvelujen tuottajilta saatavia tietoja. Suunnitelmaan on sisällytettävä myös ne palvelunantajan käytössä olevat tietojärjestelmät, joissa on kansalaisille tarjottavia asiakastietoja käsitteleviä digipalveluita, ja siihen tulisi sisällyttää myös toiminnassa mahdollisesti käytettävät tai asiakkaille tarjottavat hyvinvointisovellukset.

Sosiaali- ja terveydenhuollon palvelunantaja voi hyödyntää ja soveltaa olennaisten vaatimusten luetteloa ja profiileja, Valviran rekisteriä sekä järjestelmälomaketta tietojärjestelmien vaatimusmäärittelyissä, hankinnoissa ja kehittämistyössä. Tietojärjestelmäkohtaisten riskiarvioiden tekemisessä on mahdollista hyödyntää tietojärjestelmien luokitteluun ja sertifiointiin käytettävää riskiarviointityökalua, vaikka se onkin ensisijaisesti tarkoitettu tukemaan tietojärjestelmäpalvelun tuottajia ja hyvinvointisovellusten valmistajia riskitason määrittelyssä.

Tietojärjestelmähankintojen yhteydessä on varmistettava, että hankittavat järjestelmät toteuttavat kansallisesti asetetut vähimmäisvaatimukset. Jos hankinnan kohteena on asiakas- tai potilastietoja käsittelevä järjestelmä, osa hankinnan vaatimuksista tulisi määritellä olennaisten vaatimusten ja niitä kokoavien profiilien kautta. Valviran tietojärjestelmärekisteristä on mahdollista tarkistaa, mitä eri luokkiin kuuluvia ja eri profiileja täyttäviä järjestelmiä on saatavilla. Rekisterissä on myös keskeisimmät tiedot Kanta-palveluihin liittyville järjestelmille Kelan kanssa hyväksytysti suoritetuista yhteistestauksista sekä tiedot luokan A sertifioitujen järjestelmien tietoturvallisuuden arvioinnista ja tietoturvallisuustodistuksen voimassaolosta. Vastaavat tiedot ovat rekisterissä myös hyvinvointisovelluksista.

Sote-palvelun järjestäjä tai tuottaja voi myös pyytää hankintoihin liittyvissä tarjouspyynnöissä tietojärjestelmäpalvelujen tuottajalta järjestelmälomakkeen ja verrata sen tietoja hankinnassa määrittelemiinsä vaatimuksiin ja Valviran tietojärjestelmärekisteristä löytyviin tietoihin. Näin voidaan varmistaa, että hankittava järjestelmä täyttää kansallisesti asiakastietolain nojalla asetetut vaatimukset.

Järjestelmälomaketta on mahdollista soveltaa myös muulla tavoin palvelunantajan toiminnassa. Esimerkiksi lomakkeeseen olisi mahdollista merkitä eri järjestelmät, joiden kautta palvelunantajan omassa toiminnassa eri vaatimukset täytetään tai voidaan täyttää.

5 Sertifiointiprosessin soveltaminen

Sertifiointi koskee luokkaan A1, A2 tai A3 kuuluvia tietojärjestelmiä sekä kaikkia asiakastietolain tarkoittamia hyvinvointisovelluksia. Tietojärjestelmän luokittelu tehdään määräyksen 4/2024 ja sen liitteen 1 mukaisesti. Hyväksytty sertifiointi on edellytys luokan A tietojärjestelmän tai hyvinvointisovelluksen rekisteröinnille ja käyttöönotolle. Sertifioitavana voi olla myös osajärjestelmä, joka on tarkoitettu käytettäväksi yhdessä muiden tietojärjestelmien tai osajärjestelmien kanssa.

Määräyksen 4/2024 mukaista sertifiointiprosessia edeltäviä luokan A tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan toimenpiteitä ovat muun muassa:

- järjestelmän tai hyvinvointisovelluksen käyttötarkoituksen määrittely
    - mukaan lukien luokittelu sekä kannanotto siihen, mitkä olennaisten vaatimusten profiileista sekä muista olennaisista vaatimuksista sisältyvät käyttötarkoitukseen;
- järjestelmän tai hyvinvointisovelluksen suunnittelu ja toteutus;
- tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan oma testaus;
- tarvittava dokumentointi
    - mukaan lukien järjestelmälomake ja dokumentaation kautta todennettavien olennaisten vaatimusten täyttämisen dokumentointi.

Kuva 2. Sertifiointiprosessi sekä sitä edeltävät ja seuraavat toimenpiteet.

Kuvassa 2 on esitetty yleiskuva sertifiointiprosessista, sitä edeltävistä ja seuraavista vaiheista sekä prosessiin osallistuvista toimijoista. Myös muutoksiin liittyvissä ilmoituksissa noudatetaan samoja menettelyjä, seuraten määräyksen 4/2024 liitteen 2 ohjeita.

Jos järjestelmä kuuluu luokkaan A2 tai A3, tietojärjestelmäpalvelun tuottaja käynnistää sertifiointiprosessin ottamalla yhteyttä Kelan yhteistestaukseen ja sopimalla yhteistestauksesta. Kela ohjeistaa tarkemmin yhteistestaukseen hakeutumisesta ja siitä, missä vaiheessa sertifiointiprosessia voidaan käynnistää myös tietoturvallisuuden arviointi, jos järjestelmälle ollaan suorittamassa sekä yhteistestausta että tietoturvallisuuden arviointia. Määräyksen 5/2024 mukainen järjestelmälomake on toimitettava Kelalle yhteistestaukseen hakeutumisen yhteydessä. Hyväksytysti suoritetun yhteistestauksen jälkeen Kela antaa yhteistestauslausunnon.

Jos järjestelmä kuuluu luokkaan A1, tietojärjestelmäpalvelun tuottaja käynnistää sertifiointiprosessin ottamalla yhteyttä tietoturvallisuuden arviointilaitokseen ja sopimalla tietoturvallisuuden arvioinnin toteuttamisesta. Myös luokkaan A2 ja A3 kuuluville järjestelmille suoritetaan tietoturvallisuuden arviointi.

Vastaavat menettelyt koskevat myös Kanta-palveluihin liittyviä hyvinvointisovelluksia.

Tietoturvallisuuden arviointeja voivat tehdä sellaiset tietoturvallisuuden arviointilaitokset, jotka Traficom on hyväksynyt suorittamaan asiakastietolakiin pohjautuvia tietoturvallisuuden arviointeja. Hyväksytyt arviointilaitokset ilmoitetaan Traficomin verkkosivuilla. Määräyksen 5/2024 mukainen järjestelmälomake on toimitettava arviointilaitokselle tietoturvallisuuden arviointiin hakeutumisen yhteydessä.

Jos tietojärjestelmälle tai hyvinvointisovellukselle ollaan suorittamassa sekä yhteistestaus että tietoturvallisuuden arviointi, tulisi pyrkiä siihen, että tietoturvallisuustodistus kirjoitetaan samalle järjestelmäversiolle kuin yhteistestauslausunto. Tietoturvallisuuden arvioinnin hyväksytysti läpäissyt luokkaan A kuuluva tietojärjestelmä, osajärjestelmä tai hyvinvointisovellus saa tietoturvallisuustodistuksen. Kesken olevan yhteistestauksen valmistuminen ei ole tietoturvallisuustodistuksen kirjoittamisen este, mutta Valviran tietojärjestelmärekisteriin tulee ilmoittaa vain sellaiset vaatimukset ja profiilit, joiden vaatimukset on hyväksytysti yhteistestattu.

Asiakastietolaki ei edellytä tietoturvallisuuden säännöllisiä seuranta-auditointeja, mutta tietojärjestelmäpalvelun tuottaja ja arviointilaitos voivat sopia seuranta-auditoinneista. THL suosittelee luokan A3 järjestelmille ja korkean riskitason järjestelmille seuranta-auditointeja, joissa vuosittain käydään läpi keskeiset tietoturvavaatimusten toteutumiseen mahdollisesti vaikuttavat tietojärjestelmän ja sen teknisen käyttöympäristön (mukaan lukien alustapalvelut ja käyttöjärjestelmät) muutokset ja riskit, olennaisten vaatimusten mahdolliset muutokset ja päivitykset sekä mahdollinen tarve muutosilmoitukselle. Mahdolliset seuranta-auditoinnit eivät ole asiakastietolain tai tämän määräyksen edellyttämä osa sertifiointia. Mahdollisissa seuranta-auditoinneissa on kuitenkin huomioitava määräyksen 4/2024 mukaiset rajaukset ja sen liitteen 2 mukaiset muutosilmoituskäytännöt. Seuranta-auditoinnista ei tehdä merkintöjä Valviran tietojärjestelmärekisteriin. Jos kuitenkin seuranta-auditointi johtaa arviointiin, josta syntyy uusi tietoturvallisuustodistus, tiedot on päivitettävä myös Valviran tietojärjestelmärekisteriin.

Muiden kuin kansallisesti määriteltyjen vaatimusten ulkoista testausta, todentamista tai tietoturvallisuuden arviointia ei edellytetä THL määräysten perusteella. Jos esimerkiksi tietoturvallisuuden arvioinnissa todennetaan myös muita kuin Määräyksen 5/2024 mukaisten tietoturvavaatimusten mukaisia vaatimuksia, näiden todentamisten tulokset on selkeästi erotettava määräyksen mukaisen arvioinnin tuloksista.

Hyväksyttyä sertifiointia seuraa aina järjestelmän ilmoittaminen tai järjestelmän tietojen päivittäminen Valviran tietojärjestelmärekisteriin.

Tietojärjestelmän käyttöönottavat ja Kanta-palveluihin liittyvät organisaatiot tekevät tarvittavat sopimukset Kanta-palvelujen käyttämiseksi ja suorittavat käyttöönottokokeen sekä muut järjestelmän käyttöönottoon tarvittavat toimenpiteet yhdessä tietojärjestelmäpalvelun tuottajan kanssa. Käyttöönotto ei ole osa sertifiointia, mutta sertifiointi on käyttöönoton edellytys.

Tietojärjestelmäpalvelun tuottajan ja hyvinvointisovelluksen valmistajan on ilmoitettava tuotantokäyttöön tarkoitetun järjestelmän version tuen päättymisestä Valviralle AsTL 80 § mukaisesti. Tämä koskee myös tilanteita, joissa järjestelmä tai sovellus poistetaan tuotantokäytöstä. Nämä toimenpiteet eivät ole osa sertifiointia.

6 Tarkennuksia olennaisten vaatimusten soveltamiseen ja voimaantuloon

6.1 Vaatimusten voimaantulossa huomioitavat ajankohdat

Määräysten sisältämien vaatimusten voimaantulon ja todentamisen kannalta keskeisiä päivämääriä ovat:

1. *Määräyksen voimaantulopäivämäärä*, josta lähtien määräystä ja sen liitteitä sovelletaan;
2. *Määräyksen 4/2024 siirtymäsäännöksissä ilmaistut päivämäärät*, joiden kautta ilmaistaan ennen määräysten voimaantuloa tehtyjen toimenpiteiden ja vaatimusten voimassaoloa ja jatkuvuutta, kuten aiemmin sertifioitujen järjestelmien vaatimustenmukaisuuden voimassaoloa tai määräyksen voimaan tullessa käynnissä olevien sertifiointiprosessien menettelyjä;

3. Määräyksen liitteessä olevan *profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa*, joka ohjaa muun muassa sertifioinnissa eri ajankohtina todennettavia vaatimuksia – ks. määräys 5/2024 luku 12;
4. *Profiilissa yksittäisen vaatimuksen kohdalla näkyvä päivämäärä*, joka koskee säädösten mukaisen vaatimuksen voimaantuloa tuotantokäytössä toimivissa järjestelmissä – ks. määräys 5/2024 luku 12.

Edellä mainituilla päivämäärillä on yhtymäkohtia eri säännösten ja määritysdokumenttien voimaantuloajankohtiin. Esimerkiksi asiakastietolain siirtymäsäännöksissä ilmaistut päivämäärät ohjaavat eri tietosisältöihin ja toimintoihin liittyvien vaatimusten määräaikoja sen suhteen, milloin eri vaatimuksia on oltava toteutettuna tuotantokäytössä toimiviin tietojärjestelmiin. Nämä määräajat vastaavat vaatimuskohtaisia olennaisten vaatimusten voimaantuloaikoja (kohta 4 yllä).

Tietyn vaatimuksen voimaantuloajoissa voi olla eroja eri profiilien välillä johtuen siitä, että eri käyttötarkoituksiin tarkoitettujen järjestelmien kansalliset vaatimukset voivat osin muuttua riippumatta muihin käyttötarkoituksiin tarkoitettujen järjestelmien vaatimuksista. Esimerkiksi ”perusjärjestelmiltä” aiemmin edellytettyjä vaatimuksia voidaan myöhemmin edellyttää myös erikoistuneemmilta järjestelmiltä tai kuvantamisen vaatimuksia voidaan myöhempinä ajankohtina edellyttää erikoisalakohtaisten profiilien vaatimukset täyttävissä järjestelmissä. Vaatimukset, joiden ilmaistaan olevan voimassa, ovat mukana profiilin mukaiselle järjestelmälle suoritettavassa tietoturvallisuuden arvioinnissa tai yhteistestauksessa.

6.2 Riskipohjainen vaatimusten ja todentamistapojen kohdistaminen

Erityisesti tietoturvavaatimuksissa ja tietosuojavaatimuksissa on keskeistä huomioida järjestelmään kohdistuvien riskien luonne ja laajuus. Sekä tietojärjestelmäpalvelun tuottajan että tietojärjestelmää käyttävän organisaation on tunnistettava keskeisimmät järjestelmien käyttöön liittyvät riskit ja pyrittävä varautumaan niihin. Sama koskee hyvinvointisovellusten valmistajia riippumatta siitä, onko sovellus suoraan kansalaisille tarjottava vai käytetäänkö sitä osana palvelunantajien toimintaa.

Järjestelmään tai sovellukseen kohdistuva *riskitaso* vaikuttaa järjestelmän luokitteluun, järjestelmään kohdistuviin vaatimuksiin sekä vaatimusten todentamiseen. Järjestelmän käyttötarkoitus on keskeisin riskitasoa määrittävä tekijä. Vaatimukset toteutetaan ja arvioidaan suhteessa järjestelmän kautta käsiteltäviin tietoihin ja järjestelmän tarjoamiin toiminnallisuuksiin. Tämän lisäksi riskitasoon vaikuttavat järjestelmän toteutustapa, tiedossa oleva tai aiottu käytön laajuus, asiakastietojen käsittelyn laajamittaisuus, käsiteltävien tietojen sensitiivisyys ja sisällöllinen laajuus sekä arkkitehtuuriin ja sopimuksiin liittyvät riippuvuudet eri osajärjestelmien tai järjestelmän ja sen käyttämien alustojen välillä.

Määräysten 4/2024 ja 5/2024 osana ja järjestelmien luokittelun ja todentamisen pohjaksi esitetään yhtenäiset perusteet järjestelmien ja sovellusten luokkien (A1, A2, A3, B) sekä vaatimusten ja todentamisen kohdistamisessa käytettävän riskitason määräytymiseen. Luokittelun perusteet kuvataan määräyksessä 4/2024 ja sen liitteessä 1. Riskitason määrittelyssä kyseessä *ei ole* yksityiskohtainen palvelunantajan omassa toiminnassa tilannekohtaisesti tehtävä riskiarvio, joka riippuu järjestelmän lisäksi aina myös järjestelmää käyttävän organisaation toiminnasta ja käyttöympäristössä huomioitavista seikoista sekä siitä, kuinka todennäköiseksi erilaisten riskien toteutuminen arviointihetkellä arvioidaan.

Keskeisimpiin kriittisimmissä sosiaali- ja terveydenhuollon palveluissa käytettäviin järjestelmiin (*kriittiset luokan A3 järjestelmät*) kohdistetaan erityisiä poikkeustilanteiden varautumisvaatimuksia.

Luokkaan A3 kuuluvat järjestelmät ja osa luokkien A2 tai A1 järjestelmistä kuuluvat *korkean riskitason* järjestelmiin, joihin kohdistetaan enemmän vaatimuksia ja yksityiskohtaisempia todentamistapoja kuin riskitasoltaan *perustason* järjestelmiin. Riskitaso (korkea / perustaso) on mahdollista arvioida yllä kuvattujen riskiin vaikuttavien seikkojen perusteella. Erityisesti luokissa A1 ja A2 voi olla järjestelmän riskitasosta riippuen eri vaatimuksia tai eritasoisia vaatimusten todentamisia. Jos järjestelmä ei liity Kanta-palveluihin, järjestelmän kautta tapahtuvan asiakastietojen käytön laajamittaisuus ja riskitaso voivat olla määrittelevä tekijä sen suhteen, kuuluuko järjestelmä luokkaan B vai luokkaan A1.

Järjestelmän riskitason ja käytön laajamittaisuuden määrittelyn tueksi on saatavilla määräyksen 4 materiaalien lisäksi tukimateriaalia kuten riskiarviotyökalu, jota tietojärjestelmäpalvelun tuottaja tai tietojärjestelmän arviointia tekevä asiantuntija voi käyttää tietojen käytön laajamittaisuuden ja riskitason arviointiin.

Riskiarvioiden ohjeiden ja työkalun pohjana ovat toimineet muun muassa Tietosuojavaltuutetun toimiston ohjeet tietosuojan riskiarvioinneista, ISO-standardeissa olevat riskien arvioinnin mallit, aiemmat VAHTI-ohjeet ja -työkalut sekä määräysluonnoksiin saadut kommentit ja kehittämisehdotukset.

6.3 Vaatimusten kohdistaminen ja sertifioinnin velvoitteet modulaarisissa järjestelmäkokonaisuuksissa

Koska eri palvelujen tuottamisessa on erilaisia tarpeita, on olennaiset vaatimukset kohdistettava tarkoituksenmukaisesti tietojärjestelmien käyttötarkoituksen näkökulmasta. Myös tietojärjestelmien erityyppisiä hankinta- ja kehittämistapoja on pystyttävä hyödyntämään. Vaatimusten täyttäminen on mahdollista eri tavoin koostettujen tietojärjestelmäkokonaisuuksien kautta. Esimerkiksi modulaarisissa järjestelmäkokonaisuuksissa kokonaisuuden eri osiin kohdistuvat erilaiset vaatimukset. Toiminto- ja profiilipohjainen lähestymistapa tukee vaatimusten kohdistamista siten, että vaatimukset ovat sovitettavissa eri palveluihin ja niiden eri tuottamistapoihin. Lisäksi se tukee vaatimusten kohdistamista eri tavoin koostettaviin järjestelmäkokonaisuuksiin ja niiden osajärjestelmiin.

Sertifioinnin toimenpiteitä voidaan kohdistaa useista osajärjestelmistä koostuviin järjestelmiin tai järjestelmäkokonaisuuksiin. Yhteistestaukseen ja tietoturvallisuuden arviointiin hakeuduttaessa on näissä tapauksissa toimitettava selkeä kuvaus kokonaisuuteen kuuluvista osajärjestelmistä ja niiden vastuutahoista. Lisäksi kustakin erikseen rekisteröitävästä osajärjestelmästä on kuvattava osajärjestelmän käyttötarkoitus sekä osajärjestelmässä täytetyt olennaiset vaatimukset. Näiden seikkojen ilmaisemiseen kullekin osajärjestelmälle käytetään määräyksen 5/2024 mukaista järjestelmälomaketta, johon merkitään määräyksen mukaisesti myös olennaisten vaatimusten täyttäminen muiden osajärjestelmien kautta.

Järjestelmiä on mahdollista integroida toisiinsa eri tavoin, esimerkiksi siirtämällä tietoa järjestelmien välisten rajapintojen kautta tai käynnistämällä toinen järjestelmä. Toisiinsa liitetyt tietojärjestelmät tai tietojärjestelmäpalvelut voivat kuulua eri luokkiin ja eri riskitasoille. Kukin tietojärjestelmä on luokiteltava ja tarvittaessa sertifioitava järjestelmän nimenomainen käyttötarkoitus huomioiden. Jos järjestelmän kautta käynnistetään toinen järjestelmä, käynnistettävässä järjestelmässä olevat ominaisuudet eivät lähtökohtaisesti ole käynnistävän järjestelmän vastuulla. Toisiinsa liittyvien järjestelmien ja osajärjestelmien luokittelua ja sertifiointia käsitellään tarkemmin myös määräyksen 4/2024 luvuissa 7.1 ja määräyksen 4/2024 liitteessä 1.

Määräyksen 5/2024 olennaisten vaatimusten lisätiedoissa ja profiileissa on useiden vaatimusten kohdalla mainittu erikseen, jos vaatimus on sellainen, jonka toteuttaminen on tarpeen *jollakin järjestelmällä* palvelunantajan toiminnassa, mutta sitä ei ole pakko toteuttaa esimerkiksi kaikkiin tietyn palvelunantajan käyttämiin järjestelmiin.

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on ilmoitettava laajemman järjestelmäkokonaisuuden yhteistestaukseen hakeutumisen yhteydessä Kelalle, jos sen osajärjestelmälle tuotetaan erillinen lausunto niistä yhteistestauksen osioista, jotka kyseisen osajärjestelmän kautta todennetaan. Vastaavasti on ilmoitettava arviointilaitokselle tietoturvallisuuden arviointiin hakeutumisen yhteydessä, jos osajärjestelmälle tuotetaan erillinen tietoturvallisuustodistus niistä tietoturvavaatimuksista, jotka kyseisen osajärjestelmän kautta todennetaan. Yhteistestauslausunnossa tai -raportissa ja tietoturvallisuustodistuksessa tai siihen liittyvässä raportissa on eriteltävä, minkä muiden järjestelmien, osajärjestelmien tai sovellusten kanssa vaatimukset on todennettu. Jos järjestelmäkokonaisuuden sertifiointiin osallistuu useita tietojärjestelmäpalvelujen tuottajia, hyvinvointisovelluksen valmistajia tai muita osapuolia, kukin vastaa lähtökohtaisesti tietojärjestelmäpalvelun tuottajana oman osajärjestelmänsä sertifioinnista. Käytännön todentamismenettelyistä, sertifiointiin osallistumisesta ja osajärjestelmien vastuista on kuitenkin mahdollista sopia järjestelmäkokonaisuuteen kuuluvien tietojärjestelmäpalvelun tuottajien välillä.

Jos osana järjestelmäkokonaisuutta sertifioitu järjestelmä, osajärjestelmä tai hyvinvointisovellus 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 järjestelmien, osajärjestelmien tai sovellusten kanssa, jotka ovat olleet sertifioitavana samassa järjestelmäkokonaisuudessa.

Osajärjestelmän sertifioinnissa voidaan nojautua muiden aiemmin sertifioitujen järjestelmien, osajärjestelmien tai hyvinvointisovellusten kautta täytettäviin vaatimuksiin. Näin toimittaessa aiemmin sertifioidut muut järjestelmät, osajärjestelmät tai hyvinvointisovellukset eivät saa uutta yhteistestauslausuntoa tai tietoturvallisuustodistusta osajärjestelmän sertifioinnin yhteydessä.

Jos järjestelmäkokonaisuuden hyväksyntä on joltain osaltaan riippuvainen toisessa yhteydessä hyväksytystä osajärjestelmästä, järjestelmäkokonaisuus voidaan hyväksyä vain, jos kyseisen osajärjestelmän hyväksyntä on voimassa, jos kyseistä ominaisuutta ei todenneta osana järjestelmäkokonaisuuden sertifiointia.

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

Tietojärjestelmän määritelmä ei estä sitä, että osajärjestelmä olisi tarkoitettu asiakastietojen käsittelyyn ilman, että tietoja tuottaa tai käsittelee ammattihenkilö. Myös näissä tilanteissa tietojärjestelmäpalvelun tuottaja vastaa järjestelmän luokittelusta ja olennaisista vaatimuksista. Järjestelmää käyttävä palvelunantaja vastaa myös tällaisten järjestelmien toiminnasta ja omassa toiminnassaan asiakastietojen käsittelystä.

Järjestelmäkokonaisuuteen on mahdollista kuulua myös hyvinvointisovelluksia tai hyvinvointisovellus voi olla laajemman järjestelmän osajärjestelmä. Myös hyvinvointisovellusten välillä on mahdollista olla integraatioita ja nojautumista toisen sovelluksen kautta täytettyihin vaatimuksiin. Tietojärjestelmässä voi olla ominaisuuksia, joiden kautta se täyttää myös hyvinvointisovelluksen määritelmän, eli tietojärjestelmä voi olla myös hyvinvointisovellus asiakastietolain määritelmien perusteella.

6.4 Kolmansien osapuolten palveluihin liittyvät tietosuoja- ja varautumisvaatimukset

Tietosuoja- ja tietoturvallisuusriskien sekä varautumistarpeiden huomiointi on osa sekä palvelunantajien että tietojärjestelmäpalvelun tuottajien toimintaa. Tietojärjestelmäpalvelun tuottaja vastaa tietojärjestelmään liittyvistä olennaisista vaatimuksista myös siltä osin kuin tietojärjestelmä nojautuu kolmannen osapuolen tuottamiin välineisiin tai alustoihin tai jaettuja resursseja tarjoaviin ICT-palveluihin, ellei ole asiasta toisin sopinut asiakkaanaan toimivan palvelunantajan kanssa. Samoja perusvaatimuksia sovelletaan myös tilanteissa, joissa käytetään kolmannen osapuolen tuottamia kapasiteettipalveluita kuten palvelinvuokrausta, palvelinhallintaa, varmistuspalveluja, konesalipalveluja ja pilvipalveluja. Näiden ratkaisujen käyttö on mahdollista myös hyvinvointisovelluksissa.

Alustapalveluja, mukaan lukien jaettuja resursseja tarjoavat pilvipalvelut, voivat tuottaa muut osapuolet kuin palvelunantaja tai tietojärjestelmäpalvelun tuottaja. Julkisen hallinnon pilvipalvelulinjausten mukaisesti ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu. Myös varsinainen tietojärjestelmä tai osajärjestelmä voidaan toteuttaa esimerkiksi pilvipohjaisena SaaS-palveluna, mikäli olennaiset vaatimukset voidaan täyttää ja todentaa, ja mikäli riski- ja varautumisnäkökulmat on riittävällä tasolla huomioitu. Tietojärjestelmäpalvelun tuottaja tai palvelunantaja voi käyttää pilvipohjaisia PaaS- tai IaaS-ratkaisuja järjestelmän toteuttamisessa skaalautuvasti sen lisäksi tai vaihtoehtoisesti sille, että järjestelmän tekninen suoritusympäristö olisi kokonaisuudessaan tietojärjestelmäpalvelun tuottajan tai palvelunantajan hallinnoima. Jaetuissa ympäristöissä voi olla mahdollista myös varautua ja reagoida nopeasti uusiin uhkatilanteisiin ja riskeihin. Näissä ratkaisuissa on kuitenkin erityisesti huolehdittava verkkopalvelujen saatavuuteen liittyvien riskien hallinnasta ja siitä, että teknisillä, organisatorisilla ja sopimuksellisilla suojatoimilla varmistutaan tiedon arkaluonteisuus huomioiden, että sivulliset eivät pääse käsiksi siirrettäviin tai säilytettäviin selkokielisiin asiakastietoihin. Näistä seikoista on huolehdittava myös hyvinvointisovelluksissa, jotka nojautuvat ulkoisiin alustapalveluihin.

Monet teknisistä suojatoimenpiteistä toteutetaan tietojärjestelmille tai hyvinvointisovelluksille asetettavien tunnistus-, todennus- ja pääsynhallintavaatimusten kautta. Kolmansien osapuolten alustapalveluihin liittyviä teknisiä suojatoimenpiteitä ovat muun muassa tietoliikenteen ja tiedon säilytyksen salaaminen tai suljettujen verkkojen käyttö. Ulkoisissa palveluissa säilytettävä asiakastieto on salattava tiedon arkaluonteisuus huomioiden riittävän vahvasti siten, että vain palvelunantajalla tai tietojärjestelmäpalvelun tuottajalla on salatun tiedon purkamiseen tarvittavat avaimet.

Organisatorisia suojatoimenpiteitä ovat sertifiointimenettelyjen lisäksi mm. palvelunantajien ja välittäjien tietoturvasuunnitelmat ja käyttäjien koulutus tietosuoja- ja tietoturvallisuusasioihin. Sopimuksellisesti on huolehdittava siitä, että kaikki tietojen käsittelyyn ja järjestelmäpalvelujen tuottamiseen osallistuvat toimijat toimivat riittävän yhdenmukaisesti asiakastietojen suojaamiseksi.

Kansalaisten mahdollisuudet saada terveyttään koskevia tietoja tai palveluja myös ulkomailla ja toimijoiden mahdollisuus yli rajojen tapahtuvaan yhteistyöhön ovat esimerkkejä yli rajojen tapahtuvasta tietojen käsittelystä. EU- ja ETA-tasoinen tietojen liikkuvuusperiaate mahdollistaa sen, että myös EU:n yleisen tietosuoja-asetuksen mukaisiin erityisiin henkilötietoryhmiin kuuluvia tietoja voidaan käsitellä samantasoisilla suojatoimenpiteillä Suomessa sekä EU- ja ETA-maissa. Tietojen siirto myös kolmansiin maihin ja käsittely kolmansissa maissa on mahdollista, mikäli henkilötietojen käsittely on sallittu kyseisissä tilanteissa ja EU-tasoisesti säädettyjä siirtoperusteita, riittävän tarkkaa tapaus- ja maakohtaista tietosuojan tason arviointia sekä tarvittavia täydentäviä suojatoimenpiteitä pystytään noudattamaan. Esimerkiksi EU-komission hyväksymät vakiolausekkeet ja hyväksytyt käytännesäännöt voivat olla siirtoperusteena. Tapauskohtaiset olosuhteet, kolmannen maan lainsäädäntö ja käytössä oleva siirtoperuste huomioon ottaen täydentävinä suojatoimina voidaan edellyttää teknisiä, organisatorisia ja sopimuspohjaisia suojatoimia. Jos tietoja siirretään kolmanteen maahan sillä siirtoperusteella, että komissio on tehnyt kyseisen maan osalta päätöksen riittävästä tietosuojan tasosta (komission vastaavuuspäätökset), tietoja voidaan sen sijaan siirtää kyseiseen maahan sellaisenaan ilman muita lisävaatimuksia tai lupia. Käsiteltävien tietojen minimointi sekä tietojen anonymisointi tai pseudonymisointi laskentaa ja päättelyä tekevissä osajärjestelmissä vähentävät myös tietosuojaan liittyviä riskejä.

Osa olennaisista vaatimuksista linkittyy myös laajamittaisten kriisi- tai häiriötilanteiden varautumisen tarpeisiin, joiden kautta asetetaan olennaisia vaatimuksia esimerkiksi keskeisten tietoliikenneyhteyksien katkeamiseen varautumiseksi erityisen kriittisille järjestelmille. Varautumista toisen tyyppisiin riskeihin voidaan myös tehdä pilviratkaisujen kautta tapahtuvan järjestelmien maantieteellisen hajautuksen kautta. Kansallisesti kriittisimmiksi määriteltyjen järjestelmien lisäksi sote-toimijat ja tietojärjestelmäpalvelujen tuottajat voivat hyödyntää samoja tai vastaavia varautumis- ja tietoturvallisuusratkaisuja myös muissa järjestelmissä.

6.5 Hyvinvointisovellusten ja asiointipalvelujen vaatimukset ja suhde tietojärjestelmiin

Asiakastietolain mukaisesti tietojärjestelmä on asiakastietojen sähköiseen käsittelyyn tai asiakasasiakirjojen tallentamiseen ja ylläpitoon tarkoitettu järjestelmä. Jos järjestelmä on suunniteltu käsittelemään sote-palvelunantajan rekisterinpitoon kuuluvia asiakastietoja ja asiakasasiakirjoihin kuuluvia tietoja, se täyttää tietojärjestelmän määritelmän. Ratkaisevaa ei ole esimerkiksi se, tarjoaako tietojärjestelmä käyttöliittymiä sekä ammattihenkilöille että kansalaisille. Useissa tietojärjestelmissä on asiointiosioita, joiden kautta asiakkaat saavat itseään koskevia tietoja tai antavat tietoja palvelunantajan työntekijöille, palveluprosesseihin ja asiakirjoihin, tai niiden pohjaksi. Palvelunantajan henkilöasiakkailleen tarjoama sähköinen asiointipalvelu, jossa käsitellään palvelunantajan rekisterinpitoon kuuluvia asiakas- tai potilasasiakirjoihin meneviä tai niistä tulevia asiakastietoja, on asiakastietolain määritelmän mukainen tietojärjestelmä.

Hyvinvointisovellus on asiakastietolain mukaisesti omatietovarantoon liittyvä hyvinvointitietoja käsittelevä sovellus yksityishenkilöiden käyttöön tai sovellus, johon kansalainen voi saada asiakastietonsa Kanta-palvelujen asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta. Hyvinvointisovelluksia on mahdollista tuottaa ja käyttää sekä sote-palvelunantajan tuottamien palvelujen yhteydessä että irrallaan niistä. Hyvinvointisovelluksilla omatietovarantoon tallennettujen tietojen käyttäminen palvelunantajan toiminnassa on mahdollista asiakastietolain siirtymäsäännösten mukaisesti. Hyvinvointisovelluksessa (tai tietojärjestelmässä, jonka

osajärjestelmänä hyvinvointisovellus on), on mahdollista olla myös muuta kuin Kanta-palvelujen kautta tapahtuvaa henkilötietojen rekisterinpitoa. Näiden tietojen rekisterinpidosta voi vastata hyvinvointisovelluksen valmistaja tai tämän asiakasorganisaatio kuten sote-palvelunantaja. Toisaalta on mahdollista luoda erittäin rajattuja hyvinvointisovelluksia, jotka nojautuvat lähes täysin esimerkiksi omatietovarantoon.

Palvelunantajan asiakkailleen tarjoama digitaalinen palvelu voi siis asiakastietolain määritelmien mukaisesti olla joko tietojärjestelmä, hyvinvointisovellus, tai molempia. Määräyksissä 4/2024 ja 5/2024 käytetään termiä digitaalinen palvelu (tai digipalvelu) viitaten kansalaisen käyttämiin hyvinvointisovelluksiin ja niihin tietojärjestelmiin, joiden käyttäjänä ovat ammattihenkilöiden lisäksi kansalaiset.

Hyvinvointisovellusten sertifioinnin vaatimukset poikkeavat osin tietojärjestelmistä. Syynä tähän on se, että hyvinvointisovellusten säädöspohja, käyttäjäkunta, käsiteltävien tietojen luonne ja sisältö, riskit, Kanta-liittymisratkaisut sekä omavalvonnan ja valvonnan vastuut voivat poiketa merkittävästi tietojärjestelmistä. Aiemmin erillisissä määräyksissä tietojärjestelmille ja hyvinvointisovelluksille säädetyt olennaiset vaatimukset ja menettelyt on yhdistetty määräyksissä 4/2024 ja 5/2024. Syynä tähän on se, että a) monet vaatimuksista ja menettelyistä ovat samoja sekä tietojärjestelmissä että hyvinvointisovelluksissa, b) käytännön digipalveluratkaisuissa Kanta-palveluihin liittyvissä ja muilla tavoin toteutetuissa kansalaiselle suunnatuissa palveluissa on tärkeää täyttää samoja perusvaatimuksia, c) samojen tai lähes samojen vaatimusten kaksinkertainen todentaminen ei ole tarkoituksenmukaista tietojärjestelmäratkaisuissa, joiden osajärjestelmät voivat täyttää myös hyvinvointisovelluksen määritelmän, d) sekä ammattihenkilöiden että kansalaisten käyttämissä tietojärjestelmissä, asiointipalveluissa ja hyvinvointisovelluksissa hyödynnetään entistä enemmän samoja tietoja, e) kansalaiset tai heidän käyttämänsä laitteet tai sovellukset voivat tuottaa entistä enemmän tietoa myös ammattihenkilöiden ja palvelunantajien hyödynnettäväksi, f) tietosuoja- ja tietoturvallisuusriskien hallinta on suunniteltava kokonaisuutena, huomioiden sekä ammattihenkilöt että kansalaiset ja myös uudet käyttökanavat kuten mobiilisovellukset ja verkkopalvelut.

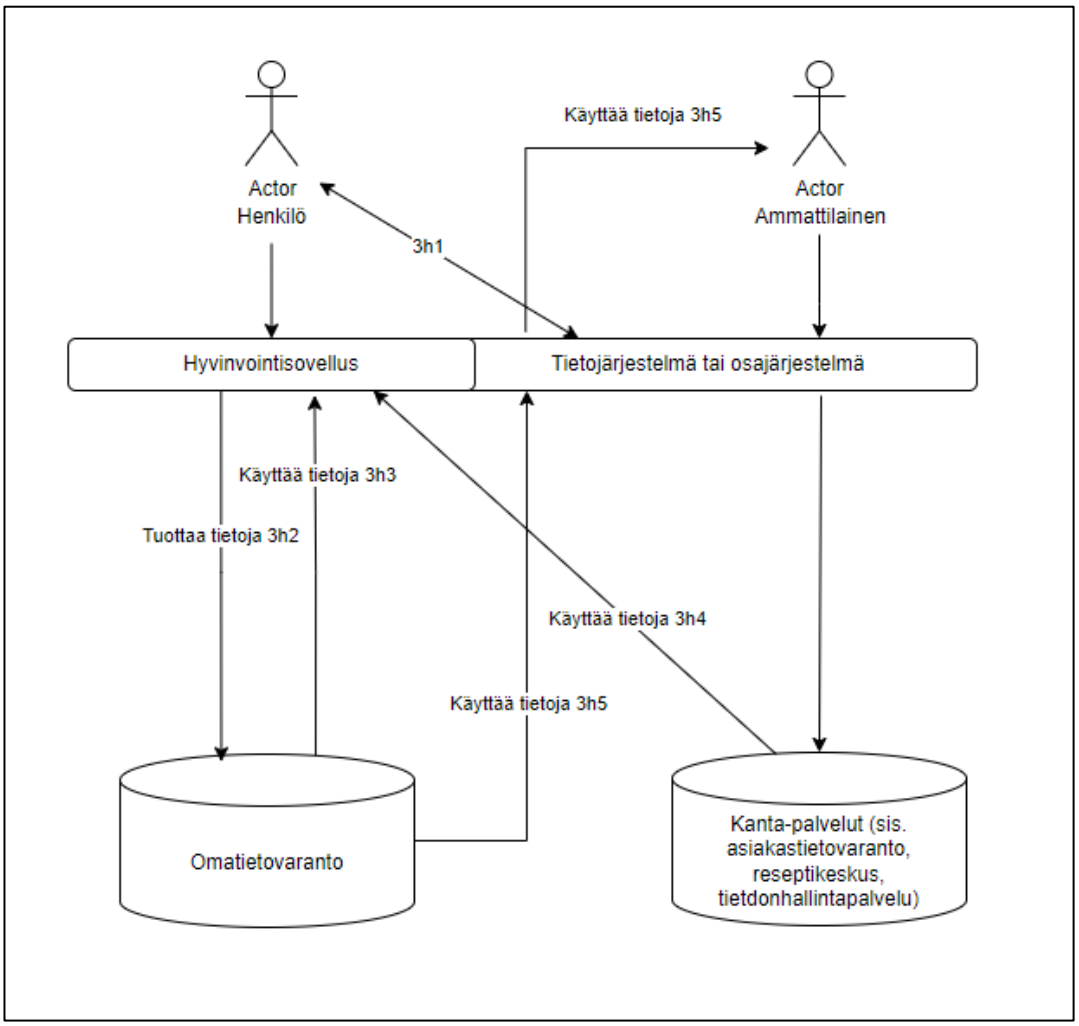
Aiemmin erillisessä määräyksessä 6/2021 esitetyt omatietovarantoon liittyvien hyvinvointisovellusten menettelyt ja vaatimukset on integroitu tietojärjestelmien vaatimuksiin ja menettelyihin määräyksissä 4/2024 ja 5/2024. Yhteistestaus ja tietoturvallisuuden arviointi suoritetaan sekä tietojärjestelmissä että hyvinvointisovelluksissa näiden määräysten mukaisesti. Hyvinvointisovellusten kautta tuotettujen hyvinvointitietojen hyödyntämiseen liittyviä määrityksiä palvelunantajien ja ammattilaisten käyttämille tietojärjestelmille on valmisteltavana, ja aiheeseen liittyviä olennaisia vaatimuksia on mukana määräyksissä.

Asiointiratkaisujen ja hyvinvointisovellusten suunnittelussa, toteuttamisessa ja arvioinnissa on huomioitava se, että ratkaisun käyttäjinä toimivat kansalaiset ja yksilöt ammattihenkilöiden sijaan. Ero on merkittävä esimerkiksi käyttöliittymien suunnittelussa, tunnistautumisratkaisuissa ja asiakastietojen tuottamiseen liittyvissä vaatimuksissa. Useita ammattihenkilöiden käyttämiin järjestelmiin määriteltyjä vaatimuksia ei voida suoraan soveltaa kansalaisille tarjottavia käyttöliittymiä sisältäviin asiointipalveluihin tai hyvinvointisovelluksiin. Hyvinvointisovelluksiin kohdistuvien vaatimusten lisäksi kansallisia vaatimuksia on määritelty koskien asiakkaille suunnattuja palvelunantajien asiointipalveluja. Hyvinvointisovelluksiin ja muihin digipalveluihin kohdistuvia vaatimuksia sekä omatietovarannon hyvinvointitietojen käyttöön liittyviä vaatimuksia on koottu määräyksen 5/2024 olennaisissa vaatimuksissa osioon ”Digit. palvelujen vaatimukset”. Osio sisältää toiminnallisia vaatimuksia, yhteistestauksessa läpikäytäviä vaatimuksia sekä tietoturvallisuuden arvioinnissa läpikäytäviä vaatimuksia. Myös omatietovarannon tietosisällöt ovat mukana määräyksen 5/2024 tietosisältövaatimuksissa.

Monet erityisesti hyvinvointisovelluksiin liittyvistä vaatimuksista käydään läpi hyvinvointisovellusten sertifioinnissa. Tietojärjestelmiin sisältyvien asiointipalvelujen vaatimukset ovat osa kyseisen tietojärjestelmän sertifiointia, koska asiointipalveluista syntyy myös uudenlaisia tietoturva- ja tietosuojariskejä asiakastietojen käsittelyyn.

Määräyksen 5/2024 liitteen 3h tietojärjestelmäprofiileissa on koottu yhteen monia hyvinvointitietojen käytön sekä digipalvelujen (sekä asiointipalvelut että hyvinvointisovellukset) vaatimuksia. Profiileihin on koottu vaatimuksia seuraaviin käyttötarkoituksiin (ks. myös kuva 3):

- palvelunantajan asiointipalvelu (tietojärjestelmä, joka sisältää myös asiakkaille tarkoitettuja käyttöliittymiä / käyttökanavia) (3h1) siltä osin, kuin kyseessä ei ole hyvinvointisovellus,
- hyvinvointisovellus, joka tuottaa tietoja omatietovarantoon (3h2),
- hyvinvointisovellus, joka käyttää tietoja omatietovarannosta (3h3),
- hyvinvointisovellus, joilla asiakas voi saada itseään koskevia asiakastietoja Kanta-palvelujen asiakastietovarannosta, reseptikeskuksesta tai tiedonhallintapalvelusta (3h4),
- tietojärjestelmä, jonka avulla palvelunantaja ja ammattihenkilöt voivat käyttää omatietovarannon hyvinvointitietoja (3h5).



Kuva 3. Määräyksen 5/2024 liitteen 3h profiilien suhde käyttäjiin, tietojärjestelmiin, hyvinvointisovelluksiin ja Kanta-tietovarantoihin.

Yksi tietojärjestelmä tai hyvinvointisovellus voi täyttää useiden profiilien mukaisia vaatimuksia myös liitteessä 3h kuvattujen vaatimusten näkökulmasta. Esimerkiksi laaja asiakas- ja potilastietojärjestelmä (joka täyttää esimerkiksi profiileja 3a1 lääkemääräysten tekemiseen, 3c1 potilaskertomustietojen käsittelyyn ja 3d1 sosiaalihuollon asiakastietojen käsittelyyn) voi sisältää myös asiointipalveluja (3h1) ja ammattihenkilöiden käyttöön haettavia hyvinvointitietoja (3h5), tai sen osajärjestelmäksi voi olla integroituna esimerkiksi profiilien 3h2 ja 3h3 mukainen hyvinvointisovellus osana asiakkaille tarjottavaa portaalia tai pienempinä mobiilisovelluksina.

6.6 Lääkemääräysten käsittely sekä apteekkien tietojärjestelmät ja verkkopalvelut

Lääkkeen toimittamista varten laaditut asiakirjat eli lääkemääräykset ovat asiakastietolain 703/2023 mukaisesti asiakasasiakirjoja. Asiakastietolain tietojärjestelmiä, organisaation tietojenkäsittelyn periaatteita ja tietoturvasuunnitelmaa koskevat säännökset ovat koskeneet apteekkeja ja niiden tietojärjestelmiä jo aiemman asiakastietolain voimassa ollessa. Apteekkijärjestelmät ovat olleet sertifioitavia luokkaan A3 kuuluvia tietojärjestelmiä jo aiemmissa määräyksissä. Lääkemääräyksen määritelmän muuttaminen potilasasiakirjaksi ei ole muuttanut oleellisesti apteekeissa jo aiemmin tapahtunutta lääkemääräysten käsittelyä tai sen laajuutta. Apteekkien oikeudet käsitellä lääkemääräyksiä sekä apteekkijärjestelmiä koskevat vaatimukset ovat säilyneet laissa 703/2023 entisellään.

Asiakastietolakiin 703/2023 liittyvässä hallituksen esityksessä on rajattu, että lääkkeen toimittamisessa käytettävät tietojärjestelmät kuuluvat tietojärjestelmän määritelmän piiriin, mutta eivät muut apteekin käyttämät tietojärjestelmät. Lääkemääräysten toimittamiseen apteekeissa tarkoitettujen apteekkijärjestelmien vaatimukset on koottu määräyksen 5/2024 liitteen 3 profiiliin 3a2. Määräykset 4/2024 ja 5/2024 koskevat apteekkeja ja apteekkijärjestelmiä tarjoavia tietojärjestelmäpalvelujen tuottajia vain näiden tietojärjestelmien osalta.

Apteekkien verkkopalveluja säädellään lääkelaissa (395/1987), lääkeasetuksessa (693/1987) ja Fimean määräyksessä 2/2011 apteekin verkkopalveluista. Hyvinvointisovelluksia koskeva sääntely asiakastietolaissa ei sisällä esimerkiksi apteekkien verkkopalveluiden edellyttämää muuta sääntelyä. Nykyinen lainsäädäntö ei mahdollista lääkemääräyksiin ja lääkekorvauksiin liittyvien tietojen tiedonsiirtoa ja koostamista asiakkaan nähtäville apteekin verkkopalveluun. Asiakastietolakiin liittyvässä hallituksen esityksessä (HE 246/2022 vp) on todettu, että verkkoapteekkeja ei voi toteuttaa pelkästään asiakastietolain nojalla. Apteekkien verkkopalveluissa käsitellään apteekin henkilö- ja asiakasrekistereihin kuuluvia tietoja. Näiden tietojen käsittely ei ole sosiaali- ja terveydenhuollon asiakastietojen käsittelyä. Apteekkien verkkopalvelut eivät näin ollen ole asiakastietolain tarkoittamia tietojärjestelmiä eivätkä hyvinvointisovelluksia. Asiakastietolain ja määräysten 4/2024 ja 5/2024 velvoitteet tietojärjestelmien ja hyvinvointisovellusten luokittelusta, sertifioinnista, olennaisista vaatimuksista tai rekisteröinnistä eivät koske apteekkien verkkopalveluita. On kuitenkin suositeltavaa, että apteekkien verkkopalvelujen kehittämisessä huomioidaan soveltuvin osin vaatimuksia, joita asetetaan sosiaali- ja terveyspalveluissa käytettäville digipalveluille (esimerkiksi määräyksen 5/2024 profiilin 3h1 mukaisia vaatimuksia).

Lääkemääräystiedot ovat Kansaneläkelaitoksen, apteekkien ja lääkemääräyksiä laativien palvelunantajien ja itsenäisten lääkkeen määrääjien yhteisrekisterinpitoon kuuluvia (laki sähköisestä lääkemääräyksestä 18 §). Yhteisrekisterin rekisterinpitäjien välinen tietojen käyttö näiden toimijoiden välillä ei ole asiakastietojen luovuttamista, joten lääkemääräystietoja eivät koske esimerkiksi luovutusilmoituksiin liittyvät asiakastietoihin kohdistuvat säännökset.

7 Lisätietoja määräysten 4/2024 ja 5/2024 valmistelusta

Määräysten 4/2024 ja 5/2024 sisällöt perustuvat pääosin vuosina 2015, 2016 ja 2021 annettuihin aiempiin määräyksiin, joiden pohjalta Valviran tietojärjestelmärekisteriin on rekisteröity yli 60 sertifioitua luokkaan A kuuluvaa järjestelmää tai hyvinvointisovellusta ja yli 320 luokkaan B kuuluvaa järjestelmää. Pääosa vaatimuksista on samoja kuin aiemmissa määräyksissä. Uusien vaatimusten voimaantulossa (esimerkiksi määräyksen 5/2024 profiileissa) on huomioitu lainsäädännössä asetetut aikataulut, järjestelmien kehitys- ja sertifiointisyklit sekä määräysten lausuntokierroksella saatu palaute.

Määräysten 4/2024 ja 5/2024 sekä niiden liitteiden valmistelussa on laista lähtevien muutos- ja täydennystarpeiden lisäksi huomioitu vuonna 2021 voimaan tulleen asiakastietolain nojalla annetuista määräyksistä saadut kokemukset ja tarkennustarpeet sekä joukko valtakunnallisiin määrityksiin ja Kanta-palveluihin kohdistuvia tarpeita sosiaali- ja terveydenhuollon palvelunantajilta, tietojärjestelmäpalvelujen tuottajilta sekä kansallisilta viranomaisilta. Määräyksen, luettelon ja profiilien valmistelussa on järjestetty laaja kuulemiskierros sekä esitelty aihetta useissa eri yhteistyöryhmissä ja tilaisuuksissa. Kuulemiskierroksella saatujen yli 300 kommentin pohjalta määräyksiin 4/2024 ja 5/2024 liitteineen sekä niiden sisältämiin vaatimuksiin on tehty tarkennuksia, täydennyksiä ja korjauksia.

Olennaisten vaatimusten määräysten ensimmäisissä versioissa vuosina 2015-2016 painotettiin erityisesti Kanta-palvelujen kautta muodostuvia vaatimuksia. Asiakastietolaissa 784/2021 ja sen mukaisissa määräyksissä vaatimuksia laajennettiin mm. eduskunnan sekä ohjaavien viranomaisten kannanottojen pohjalta koskemaan aiempaa enemmän myös luokkaan B kuuluvia sekä muita kuin Kanta-palveluihin liittyviä tietojärjestelmiä, ja vaatimusten todentamiseen käytettyjä menettelyjä ja todentamistapoja tiukennettiin.

Merkittävimpiä muutoksia ja täydennyksiä vuoden 2024 määräyksissä ovat seuraavat:

- erillinen hyvinvointisovellusten määräys on integroitu osaksi laajempaa olennaisten vaatimusten ja sertifioinnin kokonaisuutta;
- kansalaiselle suunnattujen digipalvelujen ja asiointipalvelujen vaatimuksia on otettu aiempaa selkeämmin omaksi osiokseen olennaisten vaatimusten kokonaisuudessa;
- Kelan yhteistestauskokonaisuuksien linkityksiä olennaisiin vaatimuksiin on täsmennetty;
- lokimerkintöjen ja käyttölokien hallinnan yhtenäistämiseen liittyvien kansallisten vaatimusten toimeenpano aikatauluineen on sisällytetty olennaisiin vaatimuksiin (ei erillistä määräystä);
- määräysten suhdetta apteekkien tietojärjestelmiin ja verkkopalveluihin on selkeytetty;
- tietoturvavaatimusten suorat ja toteutusta tukevat lähteet on sisällytetty olennaisten vaatimusten luetteloon;
- tietoturvallisuuden arvioinnin ja yhteistestausten tulosten suhdetta tietojärjestelmien rekisteröintiin on täsmennetty;
- tietoturva- ja tietosuojavaatimusten lähteitä ja linkityksiä kansainvälisiin standardeihin on selkeytetty.

Vuoden 2024 määräyksiin on yhdistetty ja tiivistetty useiden aiemmin erillään olleiden ohjeiden sisältöä ja vaatimuksista on poistettu vanhentuneita lähteitä sekä lisätty päivitettyjä lähteitä (säädökset, määritykset, standardit ja eri vaatimuksia taustoittavat lähteet).

THL päivittää määräysten 4/2024 ja 5/2024 sisältöjä sekä olennaisia vaatimuksia ja profiileja tarvittaessa uusien määräysten kautta, perustuen uusiin määritysdokumentteihin, sertifiointiprosessista nouseviin kokemuksiin ja eri sidosryhmien kehitysehdotuksiin.