Tietopalvelut
Sote-tieto ja -tiedonhallinta

9.12.2021

OLENNAISTEN VAATIMUSTEN SOVELTAMISOHJEET

Sisällys

1 Tavoitteet

Asiakastietolain 34 §:n mukaisesti sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää

- toiminnallisuutta,
- yhteentoimivuutta,
- sekä tietoturvaa ja tietosuojaa

koskevat olennaiset vaatimukset.

THL:n määräyksillä 4/2021 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista ja 5/2021 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista kootaan yhteen menettelyt ja kansallisesti asetetut vaatimukset sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetuille tietojärjestelmille. Tarkempia tavoitteita ja käyttökohteita on kuvattu määräyksen 5/2021 luvussa 2.

Tietojärjestelmien olennaisten vaatimusten kuvaaminen on osa sosiaali- ja terveydenhuollon tietojärjestelmiin kohdistuvia lakisääteisiä velvoitteita. Velvoitteiden avulla pyritään varmistamaan tietojärjestelmien toimivuus ja varmistamaan sekä asiakkaiden että sote-ammattilaisten oikeusturvan toteutuminen. Olennaiset vaatimukset ovat yksi keino tietojärjestelmien kehittämisen valtakunnalliseen ohjaamiseen sekä niiden tietoturvallisuuden varmistamiseen. Toiminnalliset vaatimukset luovat pohjan myös yhteentoimivuuteen ja tietoturvallisuuteen liittyville olennaisille vaatimuksille. Järjestelmien käyttötarkoituksen kuvaaminen ja rajaaminen yhdenmukaisesti olennaisten vaatimusten kautta selkeyttää viestintää eri järjestelmien käyttötarkoituksista ja siitä, mitä kansallisia vaatimuksia järjestelmät täyttävät. Tietoturvallisuuden perustavoitteiden kuten luottamuksellisuuden, eheyden, saatavuuden ja kiistämättömyyden varmistamiseksi järjestelmiin ja tietojärjestelmäpalvelujen tuottajiin kohdistuu sekä yksityiskohtaisia että yleisiä 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. Tämä mahdollistaa sen, että voidaan luottaa siihen, että järjestelmissä on riittävät ja tarvittavat ominaisuudet esimerkiksi Kanta-palveluihin liittämisen ja tietoturvallisuuden näkökulmasta, kun niitä hankitaan ja kehitetään eri palveluihin. Järjestelmien ja tuotteiden välinen kilpailu voi kohdistua muun muassa käytettävyyteen sekä erityistä lisäarvoa käyttäjille tuoviin ominaisuuksiin. Olennaisten vaatimusten kokoaminen yhtenäiseen luokitukseen yhtenäistää säädöksiin ja valtakunnallisiin määrityksiin perustuvissa vaatimuksissa käytettävää käsitteistöä ja yhdenmukaistaa järjestelmien valmistajiin ja niiden käyttäjiin kohdistuvia vaatimuksia.

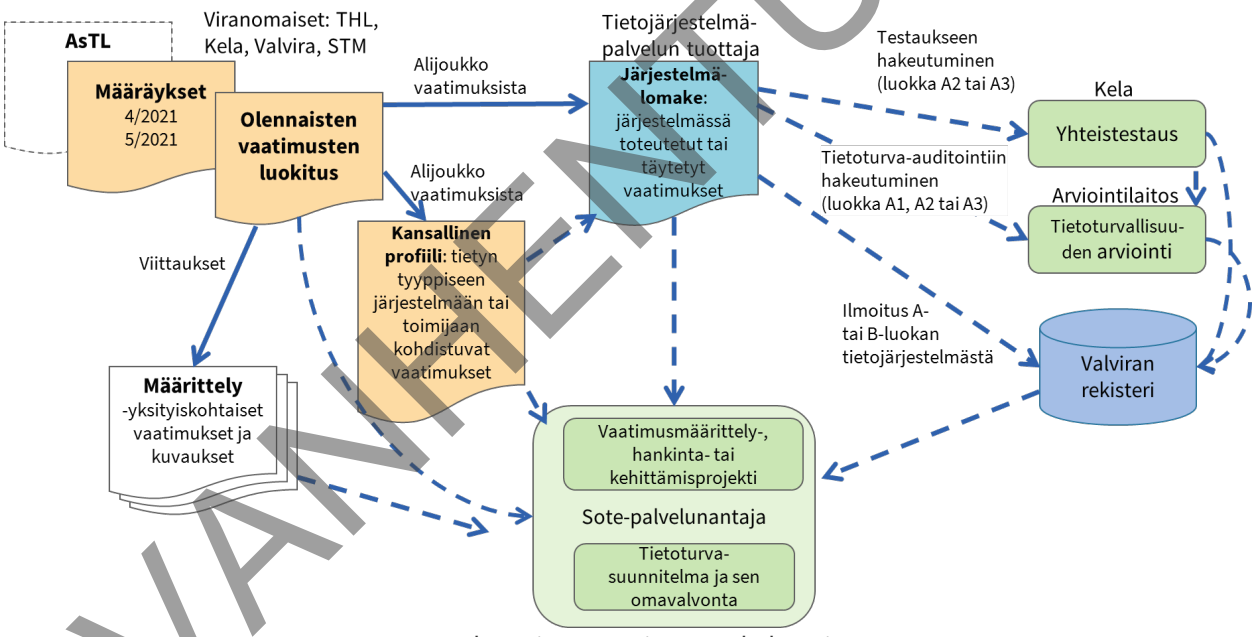
2 Yleiskuva olennaisten vaatimusten käytöstä

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

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 luokituksen hyödyntämisestä. Keskeisiä kokonaisuuteen liittyviä materiaaleja ovat määräykset, olennaisten vaatimusten luokitus, järjestelmälomake sekä profiilit.

Määräysten 4/2021 ja 5/2021 kautta annetaan ohjeet siitä, kuinka olennaiset vaatimukset on kuvattava ja todennettava sekä kuinka niihin liittyvät lakisääteiset selvitykset ja ilmoitukset annetaan. Määräykset perustuvat asiakastietolakiin.



Kuva 1. Olennaisten vaatimusten kokonaisuus.

2.1 Olennaisten vaatimusten luokitus

Olennaisten vaatimusten luokitus (määräys 5/2021 liite 2) on taulukko, joka kokoaa asiakas- ja potilastietoja käsitteleville järjestelmille kansallisesti määritellyt:

- toiminnallisuudet / toiminnot (Toiminnot-välilehti)
- tietosisällöt (Tietosisällöt-välilehti)
- tietoturvavaatimukset (Tietoturvavaatimukset-välilehti).

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 luokituksen 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 tarkasti kuvattu Kelan ja THL:n sivustoilla[1] sekä eri tietosisältöjen julkaisukanavissa kuten THL:n ja Kelan koodistopalvelussa sekä Sosmeta-palvelussa. Viitatut määritysdokumentit sisältävät tarkemmat tiedot siitä, mitkä ominaisuudet tai yksityiskohtaiset tiedot toteutuksissa ovat pakollisia, vapaaehtoisia tai pakollisia. Tietyn toiminnon tai tietosisällön pakollisuus ei muodostu siis yksinomaan profiilissa ja luokituksessa kuvattujen tietojen pohjalta, vaan vaatimusten toteutuksissa on huomioitava tarkemmat määritykset. Uusissa toteutuksissa tulee käyttää määritysten uusimpia voimassa olevia versioita ja tuotantokäyttöön voidaan hyväksyä tiettyjen versioiden mukaisia toteutuksia.

Eri toimintojen ja tietosisältöjen kohdalla luokituksessa kerrotaan myös niihin liittyvät Kanta-palveluihin liittyvien järjestelmien yhteistestauksen testauspaketit sekä tietoturvallisuuden arvioinnissa todennettavat tietoturvavaatimukset (mikäli toiminto liittyy johonkin arvioitavista tietoturvavaatimuksista). Eri toimintoihin, tietosisältöihin ja tietoturvavaatimuksiin liittyvät keskeisimmät määritykset mainitaan kunkin toiminnon ja sisällön kohdalla, ja ne löytyvät luokituksen ”Viittaukset lähdedokumentteihin” -välilehden kautta. Luokituksessa kuvataan myös eri tietosisällöistä saatavilla olevien määritysten rakenteisuuden taso. Toimintojen ja tietosisältöjen välisiä suhteita kuvataan tarvittaessa osana luokitusta, esimerkiksi tilanteessa, jossa 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, ja varsinaiset järjestelmien vaatimukset sekä profiilit kohdistuvat aina yksilöityihin vaatimuksiin.

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

2.2 Vähimmäisvaatimusten profiilit

Olennaisten vaatimusten luokitus toimii pohjana myös *profiileille*. Yksi profiili kokoaa tiettyyn käyttötarkoitukseen tarkoitetuille tietojärjestelmille asiakas- tai potilastietojen käsittelyssä asetetut kansalliset vähimmäisvaatimukset. Yksi profiili sisältää siis osajoukon olennaisten vaatimusten luokituksessa kuvatuista toiminnoista, tietosisällöistä ja tietoturvavaatimuksista. Profiileja julkaistaan sellaisiin käyttötarkoituksiin, joissa on tärkeää yhtenäistää vähimmäistason vaatimukset joukolle tietojärjestelmiä.

Profiileja on mahdollista julkaista erillään olennaisten vaatimusten luokituksen päivittämisestä, ja eri käyttötarkoituksiin tarkoitetuille tietojärjestelmille voidaan julkaista uusia vähimmäisvaatimusten profiileja.

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

Profiilit eivät kata kaikkia mahdollisia luokkien A tai B järjestelmien käyttötarkoituksia. Esimerkiksi kaikille eri erikoisalojen järjestelmille ei ole julkaistu spesifejä profiileja.

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

Profiilit löytyvät määräyksen 5/2021 liitteestä 3. Liitteessä on useita taulukoita, joista jokaisessa on yksi tai useampia profiileja. Esimerkiksi Liite 3a sisältää kaksi profiilia: Lääkemääräyksiä käsittelevä potilastietojärjestelmä ja Apteekkijärjestelmä.

Profiili sisältää sellaiset toiminnot, tietosisällöt ja tietoturvavaatimukset, joiden toteuttamista määritysten mukaisesti edellytetään profiilin mukaiseen tarkoitukseen käytettävässä tietojärjestelmässä. Esimerkiksi Apteekkijärjestelmä-profiili (määräys 5/2021 liite 3a, profiili 3a2) sisältää apteekkien käyttämiltä tietojärjestelmiltä vähintään edellytettävät toiminnallisuudet ja tiedot muun muassa lääkemääräystietojen hakemista ja lääkkeen toimittamista varten sekä sellaiset tietoturvavaatimukset, joiden täyttäminen on vähintään tarpeen apteekkitoiminnassa.

Profiileja on koottu erityisesti eri Kanta-palveluihin kuten potilastiedon arkistoon, sosiaalihuollon asiakastiedon arkistoon ja reseptikeskukseen liittyville tietojärjestelmille. Osa profiileista kuten määräyksen 5/2021 liitteen 3g profiili kokoaa kuitenkin laajemmin kaikkiin luokkaan B tai A kohdistuviin järjestelmiin kohdistuvia vaatimuksia eri säädöksistä. Luokkaan A (myös A1) kuuluvissa järjestelmissä tietoturvavaatimukset käydään läpi tietoturvallisuuden arvioinnissa, mutta vaatimukset koskevat myös luokkaan B kuuluvia tietojärjestelmiä.

Yksi järjestelmä voi täyttää usean eri profiilin mukaiset vaatimukset. Esimerkiksi laaja asiakas- ja potilastietojärjestelmä voi täyttää kaikki liitteen 3b profiilit, potilaskertomusjärjestelmän perusvaatimukset (liitteestä 3c), useita sosiaalihuollon asiakastiedon arkiston profiileja (liitteestä 3d), lääkemääräyksiä käsittelevän potilastietojärjestelmän profiilin (liitteestä 3a) sekä Kanta-arkistoon todistuksia tai lausuntoja tuottavan palvelun profiilin (liitteestä 3f). Järjestelmissä toteutetaan profiilien lisäksi aina myös muita vaatimuksia, joista osa voi sisältyä olennaisiin vaatimuksiin.

Profiileissa kuvataan myös sitä, milloin 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 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 ole tarkoitus 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 työkaluna

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

Täytetty järjestelmälomake toimii asiakastietolain mukaisena selvityksenä olennaisten vaatimusten täyttämisestä järjestelmässä sekä luokkaan B että A kuuluvissa tietojärjestelmissä. Järjestelmälomake dokumentoi sen, kuinka järjestelmän suunnittelussa, toteuttamisessa, dokumentoinnissa sekä käytön suunnittelussa ja ohjeistamisessa on huomioitu järjestelmään kohdistuvat olennaiset vaatimukset. Järjestelmän käyttötarkoitus, luokittelu, riskitaso, olennaiset vaatimukset ja profiilit on tärkeää huomioida jo järjestelmän tai sen päivitysten suunnitteluvaiheessa.

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

Järjestelmälomaketta käytetään myös, kun luokkaan A1, A2 tai A3 kuuluvan tietojärjestelmän tietoturvallisuuden arviointi käynnistetään. Olennaisia tietoturvavaatimuksia käytetään tietoturvallisuuden arvioinnin kriteereinä ja pohjana luokan A järjestelmille 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. Valvira ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon tietojärjestelmistä ja voi tuoda ilmoitusten tietoja saataville esimerkiksi omien web-sivujensa kautta. Valviran tietojärjestelmärekisteri sisältää tiedot tietojärjestelmäpalvelun tuottajan antamasta ilmoituksesta sekä tietoja järjestelmälle suoritetuista yhteistestauksista sekä tietoturvallisuuden arvioinnista.

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.

Järjestelmälomakkeella tietojärjestelmäpalvelun tuottaja täyttää siis joukon lakisääteisiä velvoitteita. Lomakkeella ilmoitetaan järjestelmää koskevat perustiedot, kuvataan järjestelmän käyttötarkoitus, otetaan kantaa siihen mitä kansallisia profiileja ja vaatimuksia järjestelmässä on toteutettu sekä ilmaistaan tarvittaessa aiempiin versioihin verrattuna muutettuja ominaisuuksia tai suhteita muihin järjestelmiin, joiden kanssa järjestelmä toimii.

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

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

1. Täytä järjestelmän perustiedot: järjestelmän nimi, tietojärjestelmäpalvelun tuottaja, valmistaja (voi olla myös sama kuin tietojärjestelmäpalvelun tuottaja), versio.

2. Kuvaa lyhyesti järjestelmän käyttötarkoitus: mihin tarkoitukseen, millaisiin palveluihin ja millaisilla rajauksilla järjestelmää on tarkoitus käyttää. Nämä tiedot merkitään lomakkeen kohtiin Käyttötarkoituksen kuvaus, ja Käyttökonteksti (valittavana esim. julkiset tai yksityiset sosiaali- tai terveyspalvelut).

3. Kuvaa järjestelmälle tehdyn riskiarvion pohjalta järjestelmän riskitaso ja se, kuinka laajamittaiseen asiakastietojen käyttöön järjestelmä on suunniteltu määräyksessä 4/2021 ja sen liitteessä 1 kuvatuilla perusteilla. Hyödynnä tarvittaessa tukimateriaalia kuten THL:n julkaisemaa riskiarviointityökalua.

4. Merkitse lomakkeen kohtaan *Järjestelmän luokka* määräyksen 4/2021 ja sen Liitteen 1 mukaisesti se, mihin luokkaan järjestelmä kuuluu (A3, A2, A1 tai B).

5. Merkitse järjestelmälomakkeen Profiilit-kohtaan ne määräyksen 5/2021 liitteissä 3 olevat profiilit, joissa profiilissa ilmaistu käyttötarkoitus on osa järjestelmän käyttötarkoitusta. Kunkin profiilin nimi ja kuvaus sekä lisätiedot antavat tietoa profiilin soveltamisesta. Järjestelmään on toteutettava ja lomakkeeseen merkittävä ne profiilit, joiden mukaisia käyttötarkoituksia järjestelmällä tuetaan. Järjestelmälomakkeelle riittää profiilien tunnusten merkitseminen (esim. ”3a1, 3c1”), profiilin koko nimeä ei tarvitse kirjoittaa lomakkeelle.

6. Merkitse lomakkeen Toiminnot-välilehdelle ne olennaisia vaatimuksia vastaavat toiminnallisuudet, jotka järjestelmään on toteutettu.

7. Merkitse lomakkeen Tietosisällöt-välilehdelle ne olennaisia vaatimuksia vastaavat tietosisällöt, jotka järjestelmään on toteutettu.

8. Merkitse lomakkeeseen ne Tietoturvavaatimukset, jotka järjestelmään on toteutettu tai jotka täytetään järjestelmän kautta.

9. Varmista, että järjestelmälomakkeelle täyttämäsi Toiminnot, Tietosisällöt ja Tietoturvavaatimukset vastaavat niitä vaatimuksia, jotka on merkitty pakollisiksi kohdassa 3 valitsemiisi profiileihin.

10. Varmista itse, testaa ja dokumentoi järjestelmään toteutetut olennaiset vaatimukset ennen järjestelmän sertifiointia tai rekisteröintiä sekä profiileihin kuuluvien että muiden järjestelmään toteutettujen olennaisten vaatimusten osalta.

11. Tarkista lomakkeen tiedot ja käytä lomaketta kuvan 1 mukaisissa tilanteissa järjestelmän sertifioinnissa ja rekisteröinnissä.

12. Päivitä lomake, kun järjestelmään tehdään muutoksia - lomakkeen uusiin versioihin merkitään muuttuneina ne vaatimukset, jotka ovat muuttuneet aiempaan lomakkeesta toimitettuun versioon verrattuna.

Lomakkeen käytön merkitys täytettyjen olennaisten vaatimusten ilmoittamisessa ja tarkennuksia esimerkiksi toteutettujen profiilien ilmoittamiseen on kuvattu määräyksen 5/2021 luvussa 8. Järjestelmälomakkeen eri kohdissa sekä ”Yleistiedot ja täyttöohjeet” sivulla on tarkempia ohjeita eri kohtiin. Jokaisesta järjestelmälomakkeen vaatimusrivistä löytyy tarvittaessa tarkempaa tietoa määräyksen 5/2021 liitteestä 2 Olennaisten vaatimusten luokitus. Tarkempia tietoja ovat muun muassa eri vaatimusten väliset suhteet, tarkemmat vaatimukseen liittyvät määritykset ja tietoturvavaatimusten vastaavuudet aiempien määräysten mukaisiin vaatimuksiin.

Kohdissa 6-8 lomakkeelle merkitään sekä järjestelmän käyttötarkoitusta vastaavien profiilien perusteella että muutenkin järjestelmään 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 6-8 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 eri osajärjestelmien kautta täytettävä kokonaisuus. Järjestelmämuutoksiin liittyvissä ilmoituksissa järjestelmälomakkeeseen merkitään lomakkeessa olevien ohjeiden mukaisesti ne vaatimukset, joiden toteutus tai täyttäminen on muuttunut aiempaan järjestelmäversioon ja lomakkeeseen verrattuna.

Järjestelmälomake on toimitettava pyynnöstä myös sote-palvelunantajalle, 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 luokan A ja B tietojärjestelmistä sekä luokan A tietojärjestelmien yhteistestauksen ja tietoturvallisuuden arvioinnin tulokset. Valvira julkaisee rekisterissä olevat keskeiset tiedot tietojärjestelmistä.

Tietojärjestelmärekisterin kautta on julkisesti saatavilla tiedot sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitetuista tietojärjestelmistä. Rekisterin julkiset tiedot ovat keskeinen pohja muun muassa tietojärjestelmien ja niiden vaatimustenmukaisuuden valvonnassa. Sote-palvelunantajat voivat hyödyntää Valviran tietojärjestelmärekisterin tietoja esimerkiksi hankintojen tukena. Tietojärjestelmien ilmoittaminen rekisteriin luokitusta ja profiileja hyödyntäen mahdollistaa sen, että esimerkiksi eri profiileja täyttävien hyväksyttyjen ja sertifioitujen järjestelmien 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 vakuuttaa, että järjestelmä asianmukaisesti asennettuna, ylläpidettynä ja käyttötarkoituksen mukaisesti käytettynä täyttää asiakastietolain 34 § kautta säädetyt olennaiset vaatimukset. Ilmoittaja vastaa siitä, että ilmoitetut toiminnot ja tietosisällöt vastaavat järjestelmään toteutettuja. Mikäli järjestelmä kuuluu luokkaan A, on lomakkeen tietojen vastattava myös tietoturvallisuuden arvioinnin ja mahdollisen yhteistestauksen tuloksia.

Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa on noudatettava mahdollisia Valviran antamia ohjeita ja määräyksiä. Kaikista tietojärjestelmän uusista versioista ei ole välttämätöntä ilmoittaa Valviran tietojärjestelmärekisteriin. Ilmoituksesta riippumatta tietojärjestelmäpalvelun tuottaja 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.

4 Olennaisten vaatimusten ja profiilien hyödyntäminen sote-organisaatioissa

Asiakastietolain 34 § mukaisesti palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Määräys 5/2021 (erityisesti luku 9) tarkentaa sitä, kuinka nämä seikat varmistetaan. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta.

Sote-palvelujen järjestäjän tai tuottajan tulee varmistaa, että:

- sen käyttämät tietojärjestelmät tai osajärjestelmät kokonaisuutena vastaavat käyttötarkoitukseltaan organisaation toimintaa;
- sen käyttämistä luokan A ja luokan B tietojärjestelmistä löytyy tiedot Valviran rekisteristä;
- sen käyttämillä luokkaan A1, A2 ja A3 kuuluvilla järjestelmillä on asianmukainen ja voimassa oleva tietoturvallisuustodistus;
- 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;
- siltä osin kuin toiminnassa tarvitaan kansallisten vähimmäisvaatimusten profiileissa kuvattuihin käyttötarkoituksiin käytettäviä tietojärjestelmiä, käytetyt tietojärjestelmät tai osajärjestelmät kokonaisuutena toteuttavat kyseisten profiilien mukaiset vaatimukset;
- tietojärjestelmien käytössä huomioidaan sellaiset olennaisiin vaatimuksiin liittyvät sertifioinnissa esiin nousseet havainnot ja edellytykset, jotka vaikuttavat olennaisten vaatimusten toteutumiseen käytetyissä järjestelmissä.

Käytännön välineenä näiden seikkojen varmistamisessa tulisi käyttää määräyksen 3/2021 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 omavalvontaa hyödyntäen esimerkiksi Valviran tietojärjestelmärekisteriä ja tietojärjestelmäpalvelujen tuottajilta saatavia tietoja.

Sosiaali- ja terveydenhuollon palvelunantaja voi myös hyödyntää olennaisten vaatimusten luokitusta ja profiileja, Valviran rekisteriä sekä järjestelmälomaketta tietojärjestelmien vaatimusmäärittelyissä, hankinnoissa ja kehittämistyössä. Tietojärjestelmäkohtaisten riskiarvioiden tekemisessä on mahdollista hyödyntää tietojärjestelmien luokitteluun ja sertifiointiin käytettävää riskiarviointimallia ja riskiarviointityökalua, vaikka se onkin ensisijaisesti tarkoitettu tukemaan tietojärjestelmäpalvelun tuottajia oman järjestelmänsä 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 voidaan määritellä olennaisten vaatimusten tai profiilien kautta. Valviran tietojärjestelmärekisteristä on mahdollista tarkistaa, mitä eri luokkiin kuuluvia ja eri profiileja täyttäviä järjestelmiä on saatavilla. Valviran tietojärjestelmärekisterissä on myös keskeisimmät tiedot Kanta-palveluihin liittyville järjestelmille Kelan kanssa hyväksytysti suoritetuista yhteistestauksista sekä tiedot luokan A sertifioitujen järjestelmien tietoturvallisuuden arvioinnista ja tietoturvallisuustodistuksen voimassaolosta.

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 asetetut vähimmäisvaatimukset.

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

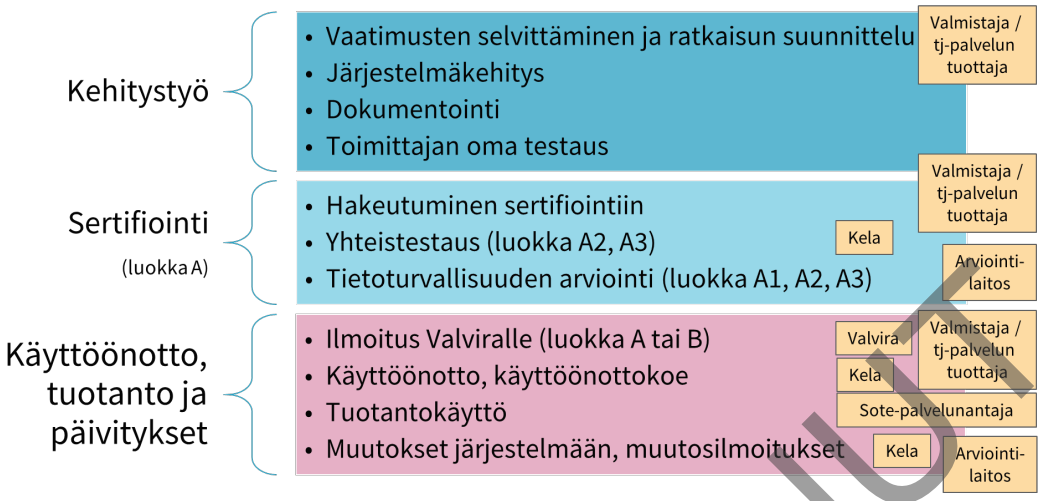
5 Sertifiointiprosessin soveltaminen

Sertifiointi koskee luokkaan A1, A2 tai A3 kuuluvia tietojärjestelmiä. Tietojärjestelmän luokittelu tehdään määräyksen 4/2021 ja sen liitteen 1 mukaisesti. Hyväksytty sertifiointi on edellytys luokan A tietojärjestelmän rekisteröinnille ja käyttöönotolle. Sertifioitavana voi olla myös osajärjestelmä, joka on tarkoitettu käytettäväksi yhdessä muiden tietojärjestelmien tai osajärjestelmien kanssa.

Määräyksen 4/2021 mukaista sertifiointiprosessia edeltäviä luokan A tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan toimenpiteitä ovat muun muassa:

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

Kuvassa 2 on esitetty yleiskuva sertifiointiprosessista, sitä edeltävistä ja seuraavista vaiheista sekä prosessiin osallistuvista toimijoista. Myös järjestelmämuutoksiin liittyvissä ilmoituksissa noudatetaan samoja menettelyjä, seuraten määräyksen 4/2021 liitteen 2 ohjeita.



Kuva 2. Sertifiointiprosessi sekä sitä edeltävät ja seuraavat toimenpiteet.

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 5/2021 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 järjestelmissä suoritetaan tietoturvallisuuden arviointi, mutta uuden järjestelmän sertifiointi käynnistetään yhteistestauksen kautta.

Tietoturvallisuuden arviointeja voivat tehdä sellaiset tietoturvallisuuden arviointilaitokset, jotka Traficom on hyväksynyt suorittamaan asiakastietolakiin pohjautuvia tietoturvallisuuden arviointeja. Hyväksytyt arviointilaitokset ilmoitetaan Traficomin verkkosivuilla. Määräyksen 5/2021 mukainen järjestelmälomake on toimitettava arviointilaitokselle tietoturvallisuuden arviointiin hakeutumisen yhteydessä.

Jos tietojärjestelmälle ollaan suorittamassa sekä yhteistestaus että tietoturvallisuuden arviointi, tietoturvallisuustodistus voidaan kirjoittaa vasta sen jälkeen, kun yhteistestaus on suoritettu loppuun. Tietoturvallisuuden arvioinnin hyväksytysti läpäissyt luokkaan A kuuluva tietojärjestelmä tai osajärjestelmä saa tietoturvallisuustodistuksen.

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. Mahdollisissa seuranta-auditoinneissa on huomioitava määräyksen 4/2021 mukaiset rajaukset ja sen liitteen 2 mukaiset muutosilmoituskäytännöt. Mikäli seuranta-auditointi ei johda uuteen tietoturvallisuustodistukseen tai aiheuta muutoksia tietojärjestelmästä ilmoitettuihin tietoihin, seuranta-auditoinnista ei tehdä merkintöjä Valviran tietojärjestelmärekisteriin.

Muiden kuin kansallisesti määriteltyjen vaatimusten ulkoista testausta, todentamista tai tietoturvallisuuden arviointia ei edellytetä. Jos esimerkiksi tietoturvallisuuden arvioinnissa todennetaan myös muiden kuin Määräyksen 5/2021 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 organisaatiot tekevät tarvittavat sopimukset Kanta-palvelujen käyttämiseksi ja suorittavat käyttöönottokokeen sekä muut järjestelmän käyttöönottoon tarvittavat toimenpiteet yhdessä tietojärjestelmäpalvelun tuottajan kanssa.

Tietojärjestelmäpalvelun tuottajan on ilmoitettava tuotantokäyttöön tarkoitetun järjestelmän version tuen päättymisestä Valviralle AsTL 30 § mukaisesti. Tämä koskee myös tilanteita, joissa tietojärjestelmäpalvelun tuottaja poistaa järjestelmän tuotantokäytöstä. Nämä vaiheet 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 4/2021 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 5/2021 luku 12;

4. *Profiilissa yksittäisen vaatimuksen kohdalla näkyvä päivämäärä*, joka koskee säädösten mukaisen vaatimuksen voimaantuloa tuotantokäytössä toimivissa järjestelmissä - ks. määräys 5/2021 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, koska eri vaatimuksia on oltava toteutettuna tuotantokäytössä toimiviin tietojärjestelmiin. Nämä määräajat vastaavat vaatimuskohtaisia voimaantuloaikoja (kohta 4).

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 seuraavassa 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.

Järjestelmään 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 4/2021 ja 5/2021 osana ja järjestelmien luokittelun ja todentamisen pohjaksi esitetään yhtenäiset perusteet järjestelmien luokkien (A1, A2, A3, B) sekä vaatimusten ja todentamisen kohdistamisessa käytettävän riskitason määräytymiseen. Luokittelun perusteet kuvataan määräyksessä 4/2021 ja sen liitteessä 1. Riskitason määrittelyssä kyseessä *ei ole* yksityiskohtainen palvelunantajien omassa toiminnassa tilannekohtaisesti tehtävä riskiarvio, joka riippuu itse järjestelmän lisäksi aina myös järjestelmää käyttävien organisaatioiden 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, VAHTI-ohjeet ja -työkalut sekä määräysluonnoksiin saadut kommentit ja kehittämisehdotukset.

6.3 Vaatimusten kohdistaminen 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 tietoturva-auditointiin 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 5/2021 mukaista järjestelmälomaketta, johon merkitään määräyksen mukaisesti myös olennaisten vaatimusten täyttäminen muiden osajärjestelmien kautta. Toisiinsa liitetyt tietojärjestelmät tai tietojärjestelmäpalvelut voivat kuulua eri luokkiin ja eri riskitasoille. Kukin tietojärjestelmä on luokiteltava ja tarvittaessa sertifioitava järjestelmän nimenomainen käyttötarkoitus huomioiden.

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.

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.

Monet teknisistä suojatoimenpiteistä toteutetaan tietojärjestelmille 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 ja 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 siirtoperustetta 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 ja laskentaa ja päättelyä tekevissä osajärjestelmissä tietojen anonymisointi tai pseudonymisointi vähentävät myös tietosuojaan liittyviä riskejä.

Osa olennaisista vaatimuksista linkittyy myös laajamittaisten kriisi- tai häiriötilanteiden varautumisen tarpeisiin, joiden kautta asetetaan joitakin 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 Tietojärjestelmien vaatimusten suhde asiointipalveluihin ja hyvinvointisovelluksiin

Asiakastietolain mukaisesti tietojärjestelmä on asiakastietojen sähköiseen käsittelyyn tai asiakasasiakirjojen tallentamiseen ja ylläpitoon tarkoitettu järjestelmä. Mikäli 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 esimerkiksi asiointiosioita, joiden kautta asiakkaat saavat itseään koskevia tietoja tai antavat tietoja palvelunantajien prosesseihin ja asiakirjoihin tai niiden pohjaksi.

Hyvinvointisovellus on asiakastietolain mukaisesti omatietovarantoon liittyvä hyvinvointitietoja käsittelevä sovellus yksityishenkilöiden käyttöön. Asiakastietolaissa säännöksissä olevien siirtymäaikojen mukaisesti yksityishenkilö voi saada myös asiakastietojaan hyvinvointisovellukseen. Hyvinvointisovellusten sertifioinnin vaatimukset poikkeavat tietojärjestelmistä. Syynä tähän on se, että hyvinvointisovellusten säädöspohja, käyttäjäkunta, käsiteltävien tietojen luonne ja sisältö, riskit, Kanta-liittymisratkaisut sekä omavalvonnan ja valvonnan vastuut poikkeavat merkittävästi tietojärjestelmistä. Tietojärjestelmäratkaisussa, joka on sekä tietojärjestelmä että hyvinvointisovellus, noudatetaan ensisijaisesti Määräyksiä 4/2021 ja 5/2021, toissijaisesti määräystä 6/2021. Näissä tilanteissa on mahdollista testata yhteistestauksessa ja todentaa tietoturvallisuuden arvioinnissa sekä määräyksen 5/2021 että määräyksen 6/2021 mukaisia vaatimuksia osana yhtä sertifiointiprosessia. Näissä tapauksissa määräysten 4/2021 ja 5/2021 mukaisen tietoturvallisuuden arvioinnin kautta todennettuja tai niitä vastaavia vaatimuksia ei todenneta erikseen hyvinvointisovellusten tietoturvallisuuden arvioinnissa. Hyvinvointisovellusten kautta tuotettujen tietojen hyödyntämiseen liittyviä vaatimuksia palvelunantajien ja ammattilaisten käyttämille tietojärjestelmille voidaan tulevaisuudessa julkaista mahdollisten aiheeseen liittyvien kansallisten määritysten pohjalta.

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.

7 Lisätietoja määräysten 4/2021 ja 5/2021 valmistelusta

Määräysten 4/2021 ja 5/2021 sekä niiden liitteiden valmistelussa on laista lähtevien tarpeiden lisäksi huomioitu vuonna 2014 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 ja vaatimusten valmistelussa on kuultu keskeisiä sidosryhmiä. Olennaisten vaatimusten määräysten ensimmäisissä versioissa vuosina 2015-2016 painotettiin erityisesti Kanta-palvelujen kautta muodostuvia vaatimuksia. Asiakastietolaissa 784/2021 ja sen mukaisissa määräyksissä vaatimuksia laajennetaan mm. eduskunnan sekä ohjaavien viranomaisten kannanottojen pohjalta koskemaan aiempaa enemmän myös luokkaan B kuuluvia sekä muita kuin Kanta-palveluihin liittyviä tietojärjestelmiä. Myös vaatimusten todentamiseen käytettyjä menettelyjä ja todentamistapoja tiukennetaan.

Vuonna 2021 julkaistaviin määräyksiin on yhdistetty ja tiivistetty useiden aiemmin erillään olleiden ohjeiden sisältöä. Useista aiemmista erillisistä ohje- ja yleiskuvadokumenteista luovutaan määräysten voimaantulon yhteydessä.

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

Määräyksen, luokituksen ja profiilien valmistelussa on järjestetty myös laaja kuulemiskierros sekä esitelty aihetta useissa eri yhteistyöryhmissä ja tilaisuuksissa. Kuulemiskierroksella saadun palautteen pohjalta määräyksiin 4/2021 ja 5/2021 sekä niiden sisältämiin vaatimuksiin on tehty useita tarkennuksia, täydennyksiä ja korjauksia muun muassa käytettyjen käsitteiden, järjestelmien luokittelun, todentamistapojen, järjestelmiin liittyvän riskin huomioinnin, muiden aihepiiriin liittyvien säädösten sekä joidenkin vaatimusten sisältöjen osalta. Luonnosversioon verrattuna lopullisen määräyksen sisältöjä on selkeytetty muun muassa suhteessa EU:n yleiseen tietosuoja-asetukseen ja sen EU-tasoisiin tulkintoihin (mm. Tietosuojavaltuutetun toimiston ja Euroopan tietosuojaneuvoston materiaalien pohjalta), STM:n asetusluonnokseen käyttöoikeudesta asiakastietoon, lääkinnällisten laitteiden MDR-asetukseen ja lakiin lääkinnällisistä laitteista, ISO-standardeihin, tiedonhallintalakiin, valtioneuvoston päätökseen huoltovarmuuden tavoitteista, julkisen hallinnon pilvipalvelulinjauksiin sekä VAHTI-, Pitukri- ja Katakri -suosituksiin.