Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

3.5.2024

MÄÄRÄYS 4/2024 LIITE 2: LUOKKAAN A KUULUVIEN TIETOJÄRJESTELMIEN JA HYVINVOINTISOVELLUSTEN MUUTOSTEN ILMOITTAMINEN

Tässä liitteessä kuvataan, mitkä ovat sellaisia muutoksia aikaisemmin yhteistestatussa tai tietoturvallisuuden arvioinnin hyväksytysti läpäisseessä tietojärjestelmässä ja hyvinvointisovelluksessa, joista tulee ilmoittaa Kelalle ja tietoturvallisuuden arviointilaitokselle. Liite kokoaa ja tarkentaa asiakastietolain ja määräyksen 4/2024 mukaisia menettelyjä järjestelmien ja sovellusten muutostilanteissa.

Asiakastietolain 82 § perusteella tietojärjestelmän ja hyvinvointisovelluksen olennaisista muutoksista on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontaviranomaiselle. Tässä liitteessä ei kuvata Valviralle ilmoitettavia olennaisia muutoksia, pelkästään vaatimustenmukaisuuden osoittamiseen ja säilyttämiseen liittyvät muutosilmoitukset Kelalle ja tietoturvallisuuden arviointilaitokselle. Valvira voi ohjeistaa olennaisten muutosten ilmoittamisen erikseen, joko pohjautuen tähän liitteeseen tai muulla tavoin. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan on kuitenkin noudatettava määräyksessä 4/2024 kuvattuja käytäntöjä silloin, kun Valviralle tehtävä rekisteröinti ja muutosten ilmoittaminen liittyy sertifiointiprosessiin.

Tausta ja perusteet

Asiakastietolaissa säädetään, että luokkaan A kuuluvien tietojärjestelmien ja hyvinvointisovellusten merkittävistä muutoksista on ilmoitettava *tietoturvallisuuden arviointilaitokselle*. Todistus tietoturvallisuuden arvioinnista on uudistettava, jos tietojärjestelmään tai hyvinvointisovellukseen tehdään merkittäviä muutoksia tai siihen kohdistuvia olennaisia tietoturvavaatimuksia muutetaan tavalla, joka edellyttää tietoturvatodistuksen uudistamista.

Tietojärjestelmien ja hyvinvointisovellusten Kanta-palveluihin talletettavien tietojen yhteentoimivuus Kanta-palvelujen ja muiden asiakas- ja potilastietojärjestelmien kanssa on osoitettava Kelan kanssa suoritettavassa yhteistestauksessa. Yhteentoimivuusvaatimus koskee myös tilanteita, joissa tietojärjestelmiin tai hyvinvointisovelluksiin tehdään merkittäviä muutoksia. Tämän vuoksi asiakastietolaissa säädetään, että merkittävät Kanta-palveluihin liittyvien tietojärjestelmien ja hyvinvointisovellusten muutokset ilmoitetaan myös *Kelalle*.

Kelalle tehtävä muutosilmoitus on eri asia kuin yhteistestaukseen ilmoittautuminen. Muutosilmoitus johtaa Kelan arviointiin siitä, tarvitaanko yhteistestausta. Yhteistestauksiin ilmoittautuminen on mahdollista myös muissa tilanteissa kuin järjestelmämuutosten yhteydessä. Tietojärjestelmäpalvelun tuottaja voi esimerkiksi ilmoittautua suoraan yhteistestaukseen, jos järjestelmä tai hyvinvointisovellus liittyy Kanta-palveluun, johon se ei ole aiemmin liittynyt, esimerkiksi reseptikeskuksen lisäksi potilastiedon arkistoon, potilastiedon arkiston lisäksi sosiaalihuollon asiakastiedon arkistoon tai omatietovarantoon, tai sosiaalihuollon asiakastiedon arkiston lisäksi potilastiedon arkistoon. Lisätietoja yhteistestauksiin ilmoittautumisista on Kelan Kanta-sivuilla.

Yhteistestauksen ja tietoturvallisuuden arvioinnin edellytyksenä on valmistajan selvitys siitä, kuinka tietojärjestelmän ja hyvinvointisovelluksen toiminnallisuutta koskevat vaatimukset on toteutettu ja testattu. Selvityksessä käytetään THL:n määräyksen 5/2024 liitteen 4 mukaista järjestelmälomaketta.

Tietojärjestelmiin, hyvinvointisovelluksiin tai määrittelyihin kohdistuvissa muutostilanteissa muutosten rajaamisella tiettyihin toimintoihin tai sisältöihin voidaan suoraviivaistaa uudelleentestaus- tai uudelleenarviointimenettelyjä. Esimerkiksi uuden asiakirjatyypin tai rakenteisen sisällön toteuttaminen järjestelmässä ei välttämättä edellytä kaikkien viestinvälitykseen liittyvien toiminnallisuuksien uutta testausta.

Tämä liite korvaa aiemman määräyksen 4/2021 liitteen 2. Liitteen sisältö on valmisteltu viranomaisyhteistyössä (THL, Kela, Valvira, Viestintävirasto, STM, tietoturvallisuuden arviointilaitokset), pohjautuen näille tahoille tulleisiin kyselyihin sekä sertifiointiprosessista saatuihin kokemuksiin. Liitteessä käytetyt termit vastaavat asiakastietolaissa ja määräyksessä 4/2024 noudatettuja termejä.

Muutosten ilmoittamisen menettely

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan tulee ilmoittaa luokkaan A kuuluvan tietojärjestelmän tai hyvinvointisovellusten olennaisista muutoksista Kelalle ja tietoturvallisuuden arviointilaitokselle asiakastietolain 82 §:n, THL:n määräyksen 4/2024 ja tämän liitteen mukaisesti. Ilmoituksen perusteella Kela tai tietoturvallisuuden arviointilaitos arvioivat, edellyttävätkö muutokset uutta yhteistestausta tai sellaista uutta tietoturvallisuuden arviointia, jonka johdosta tietojärjestelmälle, hyvinvointisovellukselle tai osajärjestelmälle on kirjoitettava uusi tietoturvallisuustodistus.

Jos tietojärjestelmäpalvelun tuottajana on muu taho kuin järjestelmän alkuperäinen valmistaja, on valmistajan ja tietojärjestelmäpalvelun tuottajan keskenään sovittava siitä, kuka vastaa muutosilmoituksen laatimisesta ja ilmoittamisesta. Sama koskee tilannetta, jossa hyvinvointisovelluksen sertifioinnista tai rekisteröinnistä vastaa joku muu taho kuin hyvinvointisovelluksen alkuperäinen valmistaja.

Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan vaihtuessa tulee huolehtia siitä, että järjestelmää ja sen päivityksiä koskevat vaatimukset täyttyvät edelleen, ja että niiden täyttyminen on dokumentoitu.

Muutosilmoituksen mukana on toimitettava THL:n määräysten 4/2024 ja 5/2024 mukaisesti täytetty järjestelmälomake (määräys 5/2024 liite 4). Lomake toimitetaan Kelalle, kun Kelalle tehdään muutosilmoitus yhteistestaustarpeen arviointia varten. Lomake toimitetaan myös tietoturvallisuuden arviointilaitokselle tehtävän muutosilmoituksen mukana, jotta se voi arvioida, onko tarpeen suorittaa uusi tietoturvallisuuden arviointi. *Järjestelmälomakkeeseen on merkittävä määräyksen 5/2024 mukaisilla merkinnöillä uudet ja merkittäviä muutoksia sisältävät järjestelmään tai hyvinvointisovellukseen toteutetut tai järjestelmän kautta täytettävät toiminnot, tietosisällöt ja tietoturvavaatimukset. Uusien ja muuttuneiden järjestelmään tai hyvinvointisovellukseen toteutettujen olennaisten vaatimusten on erotuttava lomakkeessa selkeästi aiemmin todennetuista olennaisista vaatimuksista. Kelalle tai arviointilaitokselle toimitettavan järjestelmälomakkeen on sisällettävä ajantasaiset tiedot tietojärjestelmän tai hyvinvointisovelluksen versiosta. Lomakkeessa on kuvattava ajantasaisesti kyseisessä järjestelmäversiossa toteutetut määräyksen 5/2024 mukaiset olennaiset vaatimukset ja profiilit.*

Kela ja tietoturvallisuuden arviointilaitos voivat ohjeistaa tarkemmin muutosilmoituksissa käytettävistä lomakkeista ja yhteydenottokanavista sekä siitä, voiko jo muutosilmoituksen yhteydessä toimittaa myös muita tietoja tai materiaaleja esimerkiksi tilanteissa, joissa on todennäköistä, että uusi yhteistestaus tai tietoturvallisuuden arviointi tarvitaan.

Mikäli tämä liite ei sisällä vastausta siihen, tarvitaanko uuden yhteistestauksen tarpeen arviointia, asiaa voi tiedustella Kelan Kanta-palvelujen tai THL:n kautta. Tietoturvallisuuden uudelleenarvioinnin tarvetta voi tiedustella arviointilaitokselta tai THL:n kautta, jos liitteessä kuvatut säännöt eivät ole sovellettavissa.

Merkittävät muutokset

Luokkaan A2 tai A3 kuuluvaan tietojärjestelmään ja hyvinvointisovellukseen tehtävistä merkittävistä muutoksista tulee ilmoittaa Kelaan, joka arvioi tietojärjestelmän tai hyvinvointisovelluksen yhteistestauksen uusimistarpeen tai tarpeen suorittaa täydentävä yhteistestaus. Luokkaan A1 kuuluvan tietojärjestelmän merkittävistä muutoksista ei tehdä muutosilmoitusta Kelaan.

Jos tietojärjestelmä tai hyvinvointisovellus siirtyy luokasta A1 tai luokasta B luokkaan A2 tai A3, Kelan kanssa käynnistetään yhteistestaus vastaavasti kuin uuden järjestelmän hakeutuessa yhteistestaukseen.

Luokkaan A1, A2 tai A3 kuuluvaan tietojärjestelmään tai hyvinvointisovellukseen tehtävistä merkittävistä muutoksista tulee ilmoittaa tietoturvallisuuden arviointilaitokselle, joka arvioi, onko tietojärjestelmälle tai hyvinvointisovellukselle tarpeen suorittaa uusi tietoturvallisuuden arviointi.

Jos tietojärjestelmä siirtyy luokasta B luokkaan A1, A2 tai A3, tietoturvallisuuden arviointilaitoksen kanssa käynnistetään tietoturvallisuuden arviointi vastaavasti kuin uuden järjestelmän hakeutuessa tietoturvallisuuden arviointiin.

Alla kuvatut muutokset ovat sellaisia, jotka edellyttävät ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten *sekä* ilmoitusta tietoturvallisuuden arviointilaitokselle, jotta arviointilaitos voi päättää tarvitaanko uusi tietoturvallisuuden arviointi.

1. Järjestelmään tai hyvinvointisovellukseen toteutetaan toiminnallisuuksia kansallisten määrittelyjen perusteella, ja näissä määrittelyissä tai niihin liittyvässä julkaisusuunnitelmassa mainitaan, että määrittelyn käyttöönotto edellyttää uudelleentestaustarpeen ja tietoturvallisuustodistuksen uudistamistarpeen arviointia.
2. Järjestelmän tai hyvinvointisovelluksen käyttäjäkunta tai liittymismalli muuttuu olennaisesti uuden version yhteydessä, esimerkiksi ammattilaiskäyttäjien lisäksi järjestelmän käyttäjiksi tulee sote-palvelujen asiakkaita tai potilaita, tai järjestelmän käyttäjäksi tulee yksityisten palveluntuottajien lisäksi julkisia palveluntuottajia tai päinvastoin.
3. Järjestelmän tai hyvinvointisovelluksen käyttöliittymä tai toiminnallisuus uusitaan merkittävin osin tai niihin tehdään merkittäviä muutoksia. Tällaisista muutoksista on ilmoitettava, jos muutokset voivat vaikuttaa myös Kanta-palveluihin lähetettävien tai sieltä haettavien tietojen tai asiakirjojen oikeellisuuteen, Kanta-rajapintojen tai sanomarakenteiden toimivuuteen, tai tietoturvavaatimusten toteuttamistapaan.
4. Järjestelmä tai hyvinvointisovellus liitetään suoraan Kanta-palveluihin, kun se on aiemmin ollut liittyneenä Kanta-palveluihin asiakastietojen välityspalvelun tai Kanta-palveluista tietoja välittävän toisen järjestelmän kautta.
5. Valvontaviranomainen, kuten Valvira, edellyttää järjestelmän tai sen uuden version uudelleentestaustarpeen arviointia tai arviointia siitä, tarvitaanko järjestelmälle tai hyvinvointisovellukselle uusi tietoturvallisuuden arviointi.
6. Tietojärjestelmän tai hyvinvointisovelluksen valmistaja tai tietojärjestelmäpalvelun tuottaja tekee tietoturvallisuuden arviointivaatimuksiin liittyvissä dokumentaatiojärjestelyissä tai järjestelmän tai hyvinvointisovelluksen kehitystyön organisoinnissa merkittäviä muutoksia (esimerkiksi merkittävä liiketoimintamuutos kuten yritysfuusio tai yrityskauppa, järjestelmän tai hyvinvointisovelluksen tuottaneen kehittäjätiimin vaihtuminen).
7. Järjestelmään tai hyvinvointisovellukseen X kohdistuvia olennaisia vaatimuksia on yhteistestattu tai todennettu tietoturvallisuuden arvioinnissa hyväksytysti järjestelmän tai tuotteen Y kautta, ja järjestelmä Y muuttuu siten, että muutos voi vaikuttaa olennaisten vaatimusten toteutumiseen järjestelmässä tai hyvinvointisovelluksessa X.
8. Järjestelmästä tai hyvinvointisovelluksesta löydetään merkittäviä potilas- tai asiakasturvallisuuteen liittyviä puutteita tai virheitä. Merkittävien virheiden osalta on erityisesti huolehdittava myös ilmoituksista valvontaviranomaisille (Valvira) sekä järjestelmän tai sovelluksen käyttäjille.

Merkittäviä muutoksia, jotka edellyttävät ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten, mutta eivät edellytä ilmoitusta tietoturvallisuuden arviointilaitokselle ovat seuraavan tyyppiset muutokset:

9. Järjestelmään tai hyvinvointisovellukseen tehdään muutoksia, jotka vaikuttavat Kanta-rajapintaan, järjestelmän käyttämiin Kanta-palvelupyyntöihin tai näissä käytettyihin sanoma- tai dokumenttirakenteisiin.

Merkittäviä muutoksia, jotka edellyttävät ilmoitusta tietoturvallisuuden arviointilaitokselle, mutta eivät edellytä ilmoitusta Kelan Kanta-palveluihin yhteistestaustarpeen arviointia varten ovat seuraavan tyyppiset muutokset:

10. Tietojärjestelmän tai hyvinvointisovelluksen käyttötarkoituksen laajuus kasvaa merkittävästi esimerkiksi yksittäisestä palveluntuottajasta laajaksi alueeksi, tai tietojärjestelmän tai sovelluksen riskitaso nousee perustasolta korkean riskin tasolle järjestelmään tehtyjen muutosten tai muiden riskitasoon vaikuttavien seikkojen muuttumisen johdosta. Riskitason määrittely tehdään määräyksen 4/2024 mukaisesti.

11. Tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan vastuulla olevaan järjestelmän käyttö- tai suoritusympäristöön tehdään sellaisia merkittäviä muutoksia, jotka vaikuttavat käyttöympäristön tietoturvallisuuden olennaisten vaatimusten toteuttamiseen. Muutos voi olla esimerkiksi sellainen, jossa järjestelmä tai sen merkittävä osakomponentti siirtyy sote-palveluntuottajan tai tietojärjestelmäpalvelun tuottajan ympäristöstä ulkoiselle alusta- tai ohjelmistopalvelun tuottajalle. Ilmoitustarve ei koske hyväksytyn ja tietoturvallisuuden arvioinnin hyväksytysti läpäisseen järjestelmän asennusta uuteen asiakasympäristöön, jossa vaatimukset täytetään vastaavalla tasolla ja vastaavilla menettelyillä kuin aiemmissa käyttöympäristöissä. Uusittavissa tietoturvallisuuden arvioinneissa on kuitenkin syytä käydä läpi, onko järjestelmää asennettu sellaisiin uusiin käyttöympäristöihin, joiden riskit poikkeavat aiemmista.
12. Järjestelmästä tai hyvinvointisovelluksesta löydetään merkittäviä tietoturvallisuuteen liittyviä puutteita tai virheitä, joiden korjaaminen on varmistettava tietoturvallisuuden arvioinnilla. Merkittävien virheiden osalta on erityisesti huolehdittava myös ilmoituksista valvontaviranomaisille (erityisesti Valvira) sekä järjestelmän tai hyvinvointisovelluksen käyttäjille.

Järjestelmää tai hyvinvointisovellusta ei tarvitse ilmoittaa uuden tietoturvallisuuden arvioinnin tarpeen tai uuden yhteistestaustaustarpeen arviointiin seuraavissa tilanteissa. Näissäkin tilanteissa on kuitenkin huolehdittava siitä, että Valviran tietojärjestelmärekisterissä sekä Kelan Kanta-palveluissa ja tietoturvallisuuden arviointilaitoksella on ajantasaiset tiedot tuotannossa käytettävien järjestelmien tuotenimistä ja niiden valmistajista:

13. Aiemmin hyväksytysti testattuun tai tietoturvallisuuden arvioinnin hyväksytysti suorittaneeseen järjestelmään tai sovellukseen toteutetaan uusi sisältö tai toiminnallisuus, joka ei vaikuta Kanta-rajapintoihin tai tietoturvavaatimusten toteutumiseen, esimerkiksi sairaalajärjestelmään toteutetaan uusi osaston vuodepaikkojen statusnäkymä tai sosiaalihuollon asiakastietojärjestelmään toteutetaan uusi toiminnallisuus muistutteiden esittämiseen käyttäjille.
14. Järjestelmän tai hyvinvointisovelluksen myyntinimi tai tuotenimi muuttuu, mutta järjestelmään tai hyvinvointisovellukseen ei tehdä Kanta-rajapintoihin, tietoturvavaatimuksiin, tai merkittäviä toiminnallisuuteen liittyviä muutoksia. Todistus tietoturvallisuuden arvioinnista on sallittua päivittää järjestelmän tai hyvinvointisovelluksen uudelle tuotenimelle siten, että tuotannossa olevien versioiden nimet käyvät ilmi todistuksessa ja todistuksen voimassaoloaika säilyy ennallaan.
15. Yrityksen nimi tai y-tunnus muuttuu, mutta muutoksella ei ole vaikutuksia yrityksen toteuttamiin tuotteisiin, hyvinvointisovelluksiin tai tietojärjestelmiin.
16. Tietojärjestelmän tai hyvinvointisovelluksen valmistajan tai tietojärjestelmäpalvelun tuottajan yhteyshenkilö tai yhteystiedot tietoturvallisuuden arvioinnissa tai yhteistestauksessa muuttuvat.