Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus 16.2.2022

MÄÄRÄYS OMATIETOVARANTOON LIITETTÄVIEN HYVINVOINTITIETOJA KÄSITTELEVIEN HYVINVOINTISOVELLUSTEN OLENNAISISTA VAATIMUKSISTA JA SERTIFIOINNISTA

Valtuutussäännökset

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

Kohderyhmät

Hyvinvointisovellusten valmistajat
Kansaneläkelaitos
Tietoturvallisuuden arviointilaitokset
Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat ja valmistajat

Voimassaoloaika

Määräys tulee voimaan 16. päivänä helmikuuta 2022 ja se on voimassa toistaiseksi.

Sisällys

Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus

16.2.2022

1. Määräyksen tarkoitus

Tämän määräyksen tarkoitus on täsmentää sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (784/2021), jäljempänä *asiakastietolaki*, tarkoitettuihin hyvinvointisovelluksiin kohdistuvat olennaiset vaatimukset ja niiden sertifioinnissa käytettävät menettelyt ja vastuut. Määräys ohjaa hyvinvointisovellusten vaatimustenmukaista toteuttamista, hyvinvointisovelluksilta edellytettävien selvitysten antamista, sertifiointiin kuuluvaa yhteistestausta ja tietoturvallisuuden arviointia sekä hyvinvointisovelluksen rekisteröintiä ja käyttöönottoa.

2. Määräyksen soveltamisala

Tämä määräys koskee yksityishenkilön hyvinvointitietoja käsittelevien omatietovarantoon liitettävien hyvinvointisovellusten vaatimustenmukaisuuden osoittamisessa noudatettavia menettelyjä sekä annettavan selvityksen sisältöä (asiakastietolaki, 7 luku ”Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset”). Terveyden ja hyvinvoinnin laitoksella (jäljempänä THL) on asiakastietolain 34 §:n 4 momentin perusteella valtuus antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä hyvinvointisovelluksissa. Asiakastietolain 35 §:n 3 momentin perusteella THL voi antaa määräyksiä myös vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

Tämä määräys koskee hyvinvointitietoja käsitteleviä hyvinvointisovelluksia, jotka ovat liittymässä tai liittyneet sosiaali- ja terveydenhuollon valtakunnallisiin tietojärjestelmäpalveluihin (jäljempänä Kanta-palvelut) kuuluvaan omatietovarantoon. Kaikki omatietovarantoon liittyneet hyvinvointisovellukset kuuluvat asiakastietolain 29 §:n mukaisesti luokkaan A. Hyvinvointisovelluksia ei koske sosiaali- ja terveydenhuollon tietojärjestelmien luokittelu luokkiin A ja B, eikä A-luokan jaottelu edelleen A1, A2 ja A3 -luokkiin.

3. Määritelmät

Tässä määräyksessä tarkoitetaan:

Asiakastiedolla tarkoitetaan sosiaali- tai terveydenhuollon asiakasta tai potilasta koskevaa henkilötietoa, joka on asiakastietolain 3 § mukaisesti sosiaalihuollon asiakastietoa tai potilastietoa, sisältyy palvelunantajan asiakastietorekisteriin ja on yleensä sosiaali- tai terveydenhuollon ammattihenkilön kirjaama ja hallinnoima.

Hyvinvointitiedolla henkilön itsensä tuottamia terveyttään ja hyvinvointiaan koskevia tietoja, jotka henkilö on tallentanut omatietovarantoon (asiakastietolaki 3 §).

Hyvinvointisovelluksella yksityishenkilön käyttämää omatietovarantoon liittyvää hyvinvointisovellusta, jolla käsitellään hyvinvointitietoja (asiakastietolaki 3 §).

Integraatiopalvelulla eri laitteista ja/tai hyvinvointisovelluksista omatietovarantoon tietoja kokoavaa palvelua. Integraatiopalvelu voi olla esimerkiksi useista omamittauslaitteista tietoja kokoava palvelu tai terveysseuranta-alustan tietoja välittävä palvelu. Integraatiopalvelua koskevat myös muut siihen soveltuvat kriteerit kuin ne, joissa integraatiopalvelu mainitaan erikseen. Kyseessä ei ole THL:n määräyksessä 4/2021 tai asiakastietolain 29 §:n perusteluissa (HE 212/2020) tarkoitettu asiakastietojen välityspalvelu.

Omatietovarannolla hyvinvointitietojen säilyttämistä ja käsittelemistä varten valtakunnallisiin tietojärjestelmäpalveluihin muodostettua keskitettyä sähköistä tietovarantoa (asiakastietolaki 3 §).

Sertifioinnilla menettelyä, jolla todennetaan hyvinvointisovelluksen täyttävän sitä koskevat tuotantokäyttöä varten vaadittavat olennaiset vaatimukset (asiakastietolaki 3 §). Luokkaan A kuuluvien hyvinvointisovellusten vaatimusten todentaminen tehdään tietoturvallisuuden arvioinnin ja yhteistestauksen kautta. Hyvinvointisovellukselle hyväksytysti suoritetun yhteistestauksen tuloksista ja tietoturvallisuuden arviointia koskevan todistuksen voimassaolosta tehdään merkinnät valvontaviranomaisen rekisteriin.

Tietoja eteenpäin välittävällä hyvinvointisovelluksella eri laitteisiin ja/tai hyvinvointisovelluksiin omatietovarannosta tietoja välittävää palvelua. Tietoja eteenpäin välittävää hyvinvointisovellusta koskevat myös muut tämän määräyksen liitteen 1 kriteerit kuin ne, joissa tietoja eteenpäin välittävä hyvinvointisovellus mainitaan erikseen.

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

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

Tietoturvallisuuden arviointilaitoksella sellaista yritystä, yhteisöä ja viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella suorittamaan tietoturvallisuuden arviointeja.

Todentamisella menettelyä, jolla osoitetaan, että hyvinvointisovellus täyttää sille asetettuja vaatimuksia. Todentamistapoja ovat mm. dokumentaation läpikäynti, hyvinvointisovelluksen testaus, hyvinvointisovelluksen tuottamien sanomien, lokien tai muiden tuotosten läpikäynti ja tarvittaessa täydentävänä todentamistapana hyvinvointisovelluksen valmistajan dokumentoitu haastattelu. Todentamista käsitellään tarkemmin luvussa 9.2.

Todistuksella tietoturvallisuuden arvioinnista tai tietoturvallisuustodistuksella hyväksytyn arviointilaitoksen antamaa todistusta siitä, että hyvinvointisovellus on hyväksytysti läpäissyt tietoturvallisuuden arvioinnin.

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

4. Määräyksen keskeinen sisältö ja rajaukset

Hyvinvointitietojen käsittelyssä käytettävän hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset sekä saavutettavuusvaatimukset. Lain mukaan hyvinvointisovelluksen valmistajan on osoitettava hyvinvointisovelluksen vaatimustenmukaisuus. Osoittamiseen kuuluu selvitys siitä, että hyvinvointisovellus täyttää ne olennaiset vaatimukset, jotka vastaavat sen käyttötarkoitusta.

Tämä määräys sisältää hyvinvointisovellusten olennaiset vaatimukset, jotka on kuvattu liitteessä 1 *omatietovarantoon liittyneiden hyvinvointisovellusten olennaiset vaatimukset*. Lisäksi tässä määräyksessä tarkennetaan olennaisten vaatimusten ilmoittamisessa, sertifioinnissa ja todentamisessa käytettäviä menettelyjä.

Määräyksen mukaisten olennaisten vaatimusten todentaminen voi olla osa tai liittyä laajempaan hyvinvointisovelluksen tai hyvinvointiteknologioiden arviointiin, jossa arvioidaan myös muita kuin määräyksen sisältämiin kriteereihin liittyviä asioita, kuten erilaisia digipalveluiden laatuun laajemmin liittyviä tekijöitä tai ominaisuuksia. Määräyksen mukaisen sertifioinnin painopisteenä on hyvinvointisovelluksen toimivuus yhdessä omatietovaranto-palvelun ja muiden omatietovarantoon liittyneiden hyvinvointisovellusten kanssa, kansalaiselle annettavien kuvausten ja informoinnin riittävyys sekä tietosuojaan ja tietoturvallisuuteen liittyvien riskien hallinta. Mahdollisen laajemman arvioinnin tulostiedot on selkeästi erotettava määräyksen mukaisten vaatimusten arvioinnista ja yhteistestauksesta siten, että määräyksen mukaisiin vaatimuksiin kohdistuvasta arvioinnista syntyy vain vaatimuksiin kohdistuva tietoturvallisuustodistus ja yhteistestaustulokset.

Tässä määräyksessä ei kuvata asiakastietolain tarkoittamien tietojärjestelmien olennaisia vaatimuksia tai niihin liittyviä sertifiointimenettelyjä, joita on kuvattu THL:n määräyksissä 4/2021 ja 5/2021. Asiakastietolain mukaisesti *tietojärjestelmä* on asiakastietojen sähköiseen käsittelyyn tai asiakasasiakirjojen tallentamiseen ja ylläpitoon tarkoitettu järjestelmä. Mikäli järjestelmä on suunniteltu käsittelemään sosiaali- ja terveydenhuollon 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 palvelunantajan henkilörekisterissä olevia tietoja tai antavat tietoja palvelunantajien prosesseihin ja palvelunantajan henkilörekisterissä oleviin asiakirjoihin tai niiden pohjaksi.

Hyvinvointisovellusten sertifioinnin vaatimukset poikkeavat tietojärjestelmistä. Syynä tähän on se, että hyvinvointisovellusten säädökset, käyttäjäkunta, käsiteltävien tietojen luonne ja sisältö, riskit, Kanta-liittymisratkaisut sekä omavalvonnan ja viranomaisvalvonnan vastuut poikkeavat merkittävästi tietojärjestelmistä. Mikäli kyseessä on asiakastietolain tarkoittama tietojärjestelmä, joka täyttää myös hyvinvointisovelluksen määritelmän:

- Noudatetaan ensisijaisesti määräyksiä 4/2021 ja 5/2021, toissijaisesti määräystä 6/2021 (tämä määräys).
- Järjestelmän sertifiointi ja järjestelmää koskevien olennaisten vaatimusten todentaminen suoritetaan ensisijaisesti määräysten 4/2021 ja 5/2021 mukaisesti.
- 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.
- Järjestelmässä tapahtuva henkilötietojen ja mahdollinen asiakastietojen käsittely on huomioitava järjestelmää käyttävien sosiaali- ja terveydenhuollon palvelunantajien tietoturvasuunnitelmassa määräyksen 3/2021 mukaisesti.
- Hyvinvointisovelluksiin liittyvät vaatimukset ja ne tietoturvallisuusvaatimukset, jotka eivät vastaa määräyksen 5/2021 kautta todennettavia vaatimuksia todennetaan tämän määräyksen 6/2021 mukaisesti.

Hyvinvointisovellusten kautta tuotettujen tietojen hyödyntämiseen liittyviä vaatimuksia palvelunantajien ja ammattilaisten käyttämille tietojärjestelmille voidaan tulevaisuudessa julkaista. Vaatimusten pohjana ovat mahdolliset aiheeseen liittyvät tulevat kansalliset määritykset. Hyvinvointisovellus on asiakastietolain mukaisesti omatietovarantoon liittyvä hyvinvointitietoja käsittelevä hyvinvointisovellus yksityishenkilöiden käyttöön. Asiakastietolain siirtymäsäännöksissä mainittujen siirtymäaikojen mukaisesti yksityishenkilö voi saada myös asiakastietojaan hyvinvointisovellukseen.

Hyvinvointisovellus voi olla lääkinnällinen laite tai hyvinvointisovelluksessa voi olla osia, joilla on lääkinnällinen käyttötarkoitus[1]. Jos hyvinvointisovelluksella tai siihen liittyvä laitteella on lääkinnällisten laitteiden lainsäädännön mukainen käyttötarkoitus, kuten diagnostinen tai hoitoa ohjaava käyttötarkoitus, sitä ja sen valmistajaa koskevat lääkinnällisten laitteiden lainsäädännön vaatimukset ja velvoitteet (mm. MD-asetus (EU) 2017/745) ja laite tulee ilmoittaa Fimean rekisteriin. Tämä määräys on riippumaton siitä, millä tavoin hyvinvointisovelluksia luokitellaan lääkinnällisten laitteiden säädösten perusteella. Hyvinvointisovelluksen valmistajan on otettava erikseen kantaa siihen, onko hyvinvointisovellus tai osa siitä lääkinnälliseksi laitteeksi luokiteltava.

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

5. Sertifiointiprosessi

Sertifiointiprosessissa hyvinvointisovelluksilta edellytetään:

1. selvitystä olennaisten vaatimusten täyttämisestä;

2. Kansaneläkelaitoksen (jäljempänä Kela) yhteistestausta, jonka tuloksena Kela antaa puoltavan lausunnon yhteentoimivuudesta hyvinvointisovellukselle, joka hyväksyttävästi täyttää yhteentoimivuuden vaatimukset;

3. tietoturvallisuuden arviointia, jonka hyväksytysti läpäisseelle luokkaan A kuuluvalle hyvinvointisovellukselle tietoturvallisuuden arviointilaitos myöntää todistuksen tietoturvallisuuden arvioinnista.

Sertifioinnin käynnistämisestä ja läpiviennistä vastaa hyvinvointisovelluksen valmistaja.

Hyvinvointisovelluksen valmistajan on toteutettava ja testattava hyvinvointisovelluksen sertifioitavat ominaisuudet ennen yhteistestaukseen tai tietoturvallisuuden arviointiin hakeutumista. Olennaisten vaatimusten täyttäminen on dokumentoitava liitteen 1 mukaisesti siten, että hyvinvointisovellukseen toteutetuista olennaisista

[1] **Lääkinnällisellä laitteella** tarkoitetaan instrumenttia, laitteistoa, välinettä, ohjelmistoa, implanttia, reagenssia, materiaalia tai muuta tarviketta, jonka valmistaja on tarkoittanut käytettäväksi ihmisillä, joko yksinään tai yhdistelminä, seuraaviin lääketieteellisiin tarkoituksiin:

- sairauden diagnosointi, ehkäisy, ennakointi, ennusteen laatiminen, tarkkailu, hoito tai lievitys,
- vamman tai toimintarajoitteen diagnosointi, tarkkailu, hoito, lievitys tai kompensointi,
- anatomian taikka fysiologisen tai patologisen toiminnon tai tilan tutkiminen, korvaaminen tai muuntaminen,
- tietojen saaminen ihmiskehon ulkopuolella (in vitro) suoritettavien tutkimusten avulla ihmiskehosta otetuista näytteistä, mukaan lukien elinten, veren ja kudosten luovutukset,

ja jonka pääasiallista aiottua vaikutusta ihmiskehossa tai -kehoon ei saavuteta farmakologisin, immunologisin tai metabolisin keinoin mutta jonka toimintaa voidaan tällaisilla keinoilla edistää. Myös hedelmöitymisen säätelyyn tai tukemiseen tarkoitettuja tuotteita pidetään lääkinnällisinä laitteina (Euroopan parlamentin ja neuvoston asetus (EU) 2017/745 lääkinnällisistä laitteista 2 artikla).

vaatimuksista ei ole epäselvyyttä ja siten, että dokumentaation perusteella todennettavista vaatimuksista on saatavilla todentamiseen tarvittava dokumentaatio.

Sertifiointiprosessi toteutetaan alla esitellyssä järjestyksessä:

1) Yhteistestaus (asiakastietolaki 36 §). Ennen yhteistestausta hyvinvointisovelluksen valmistajan on annettava Kelalle selvitys siitä, miten hyvinvointisovelluksen toiminnallisuutta koskevat vaatimukset on toteutettu ja testattu ja mitä yhteentoimivuuteen liittyviä vaatimuksia hyvinvointisovellukseen on toteutettu. Hyvinvointisovelluksen valmistaja ilmoittaa hyvinvointisovelluksen Kelan Kanta-palvelujen kanssa suoritettavaan yhteistestaukseen Kelan ohjeistuksen mukaisesti tai hyvinvointisovellukseen tehtyjen olennaisten muutosten takia suoritettavaan yhteistestaustarpeen arviointiin. Yhteistestauksen ajankohdasta ja toteuttamisesta on sovittava Kelan kanssa. Olennaisten vaatimusten täyttämisen kuvaava selvitys (liite 1) on toimitettava Kelalle täytettynä yhteistestaukseen hakeutumisen yhteydessä. Hyvinvointisovelluksen valmistaja vastaa siitä, että liitteen 1 mukaisten olennaisten vaatimusten toteuttamista koskevat tiedot ovat oikein ja täsmällisiä. Kelan on tarkistettava perustietojen oikeellisuus ja suoritettava yhteistestaus yhteistyössä hyvinvointisovelluksen valmistajan kanssa hyvinvointisovellukseen toteutettujen omatietovarannon määrittelyihin perustuvien toiminnallisuuksien, rajapintojen ja sisältöjen osalta. Hyväksytysti suoritetun yhteistestauksen jälkeen Kela antaa yhteistestauslausunnon. Yhteistestauslausunto on edellytys tietoturvallisuuden arviointilaitoksen myöntämälle todistukselle tietoturvallisuuden arvioinnista. Kelan tulee toimittaa yhteistestauslausunto vähintään hyvinvointisovelluksen valmistajalle ja Sosiaali- ja terveysalan lupa- ja valvontavirastolle (jäljempänä Valvira). Jos hyvinvointisovellukselle ollaan suorittamassa tietoturvallisuuden arviointia, Kelan tulee toimittaa yhteistestauslausunto myös arviointia suorittavalle tietoturvallisuuden arviointilaitokselle.

2) Tietoturvallisuuden arviointi (asiakastietolaki 37 §). Hyvinvointisovelluksen valmistaja ilmoittaa hyvinvointisovelluksen tietoturvallisuuden arviointilaitoksen kanssa suoritettavaan tietoturvallisuuden arviointiin tai hyvinvointisovellukseen tehtyjen olennaisten muutosten takia suoritettavaan tietoturvallisuuden uudelleenarviointitarpeen arviointiin. Tietoturvallisuuden arvioinnin kriteeristönä on käytettävä liitteen 1 välilehtien mukaisia vaatimuksia, joissa todentamistavaksi on merkitty arvioinnissa läpikäytävä dokumentaatio, arvioinnissa suoritettava toiminnallinen testaus (tietoturvallisuus- tai oikeellisuusvaatimuksiin liittyvän toteutuksen tai käytännön kokeilemiseksi) tai tekninen tietoturvatestaus. Yhteistestauksessa läpikäytäviä vaatimuksia ei läpikäydä uudelleen tietoturvallisuuden arvioinnissa. Valmistajan on toimitettava arviointilaitokselle selvitys olennaisten vaatimusten täyttämisestä liitteen 1 mukaisella lomakkeella, tarvittaessa vaatimusten todentamiseen edellytettävä lisädokumentaatio ja yhteistestauslausunto. Eri kohtiin tarvittavia selvityksiä ja dokumentaatiota voi yhdistää samoihin dokumentteihin, jolloin on huolehdittava siitä, että kunkin vaatimuksen täyttymisen todentamiseen tarvittava dokumentaatio löytyy selvästi liitteen 1 lomakkeelle täytettyjen tietojen kautta. Osana tietoturvallisuuden arviointia läpikäydään raportti saavutettavuustestauksen tuloksista. Hyvinvointisovelluksen saavutettavuus tulee testata valmistajan itse tai ulkopuolisen toimijan toteuttaman saavutettavuuden arvioinnin avulla.

Jos hyvinvointisovellus on sertifioitavana siten, että sille suoritetaan sekä yhteistestaus että tietoturvallisuuden arviointi, on hyvinvointisovelluksen valmistajan huolehdittava siitä, että yhteistestauksen ja tietoturvallisuuden arvioinnin kohteena on sama hyvinvointisovellusversio tai sellainen versio, jossa yhteistestattaviin olennaisiin vaatimuksiin liittyvät mahdolliset hyvinvointisovellusmuutokset eivät vaikuta auditoitaviin tietoturvallisuusvaatimuksiin.

Arvioinnin hyväksytysti läpäissyt hyvinvointisovellus saa todistuksen tietoturvallisuuden arvioinnista sekä siihen liittyvän tarkastusraportin arviointilaitokselta. Arviointi on suoritettava hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai hyvinvointisovellukseen tehtyjen muutosten laajuuden mukaisesti. Todistus on voimassa enintään kolme vuotta. Todistuksen voimassaoloa voidaan jatkaa enintään kolmeksi vuodeksi kerrallaan. Vaatimustenmukaisuuden uudistaminen on kuvattu luvussa 8.

Vaatimuksissa, joissa todentamistavaksi on merkitty vaihtoehtoisesti tekninen tietoturvatestaus tai dokumentaatio, todentaminen voi perustua arviointilaitoksen suorittamaan tekniseen tietoturvatestaukseen tai hyvinvointisovelluksen valmistajan toimittaman testausraportin arviointiin. Jos kaikki teknistä tietoturvatestausta sisältävät hyvinvointisovellukseen sovellettavissa olevat vaatimukset todennetaan arviointilaitoksen suorittaman teknisen tietoturvatestauksen kautta osana sertifiointia, todistukseen tietoturvallisuuden arvioinnista merkitään "Tietoturvavaatimusten todentamisessa suoritettu ulkoinen tekninen tietoturvatestaus" ja hyvinvointisovelluksen rekisteröinnissä sekä markkinointi- tai tiedotusmateriaalissa voidaan käyttää ilmaisua "Ulkoisesti tietoturvatestattu".

Asiakastietolaki ei edellytä tietoturvallisuuden säännöllisiä seuranta-auditointeja, mutta hyvinvointisovelluksen valmistaja ja arviointilaitos voivat sopia seuranta-auditoinneista. Hyvinvointisovellukselle mahdollisesti suoritettavat tietoturvallisuuden seuranta-auditoinnit on erotettava todistuksen uusimiseen tähtäävistä arvioinneista. Seuranta-auditoinneista ei kirjoiteta uutta todistusta tietoturvallisuuden arvioinnista ja vanhan todistuksen voimassaoloaikaa ei jatketa seuranta-auditoinnin tuloksena. Jos seuranta-auditointi ei johda uuteen tietoturvallisuustodistukseen tai aiheuta päivitystarpeita Valviran tietojärjestelmärekisterissä oleviin tietoihin, seuranta-auditoinnista ei tarvitse tehdä merkintää Valviran tietojärjestelmärekisteriin.

6. Hyvinvointisovelluksen rekisteröinti

Hyvinvointisovelluksen valmistajan on ilmoitettava hyvinvointisovelluksesta Sosiaali- ja terveysalan lupa- ja valvontavirastolle ennen hyvinvointisovelluksen ottamista tuotantokäyttöön (asiakastietolaki 30 §). Ilmoittamisessa on noudatettava Valviran antamia ohjeita tai määräyksiä hyvinvointisovelluksen ilmoittamisesta. Ilmoituksen mukana on toimitettava yhteistestauslausunto, todistus tietoturvallisuuden arvioinnista ja liitteen 1 mukainen selvitys, joka vastaa yhteistestauksessa ja arvioinnissa läpikäytyjä olennaisia vaatimuksia. Hyvinvointisovelluksen valmistaja vastaa siitä, että liitteen 1 mukaisten olennaisten vaatimusten toteuttamista koskevat tiedot ovat oikein ja täsmällisiä. Ilmoitettavien tietojen on vastattava hyvinvointisovellukseen toteutettuja tai sen kautta täytettäviä olennaisia vaatimuksia. Hyvinvointisovelluksen tietojen tulee olla julkaistuna Valviran tietojärjestelmärekisterissä ennen kuin hyvinvointisovelluksen saa ottaa tuotantokäyttöön. Valviralle tehdyn ilmoituksen ja siihen liittyvien kuvausten kautta hyvinvointisovelluksen valmistaja vakuuttaa, että hyvinvointisovellus asianmukaisesti asennettuna ja käyttötarkoituksen ja ohjeiden mukaisesti käytettynä täyttää asiakastietolain 34 §:ssä säädetyt ja tässä määräyksessä määrätyt olennaiset vaatimukset.

Valvira voi antaa tarkempia ohjeita tehtävistä rekisteri-ilmoituksista ja pyytää hyvinvointisovelluksen valmistajalta, Kelalta tai arviointilaitokselta lisätietoja tietojen oikeellisuuden varmistamiseksi.

7. Hyvinvointisovelluksen käyttöönotto ja käyttöönoton jälkeinen seuranta

Hyvinvointisovelluksen saa ottaa tuotantokäyttöön ja liittää Kanta-palveluihin sen jälkeen, kun hyvinvointisovellus on sertifioitu asiakastietolain 35 §:n mukaisesti ja kun sen tiedot löytyvät Valviran tietojärjestelmärekisteristä.

Hyvinvointisovelluksen on täytettävä hyvinvointisovelluksen käyttötarkoitusta vastaavat olennaiset vaatimukset ennen kuin hyvinvointisovellus voidaan ottaa tuotantokäyttöön. Hyvinvointisovelluksen valmistajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tuotantokäytön aikana hyvinvointisovelluksesta saatavia kokemuksia asiakastietolain 32 § mukaisesti. Hyvinvointisovelluksen merkittävistä poikkeamista (ks. luku 9.4) on ilmoitettava kaikille hyvinvointisovelluksen käyttäjille, Kelalle ja Valviralle.

Hyvinvointisovelluksen valmistajan on seurattava hyvinvointisovellusten olennaisten vaatimusten muutoksia ja tehtävä muutosten edellyttämät korjaukset. Hyvinvointisovelluksen olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle ja Kelalle. Todistus tietoturvallisuuden arvioinnista tai yhteistestaus on

uusittava, jos hyvinvointisovellukseen tehdään merkittäviä muutoksia, tai olennaisia vaatimuksia on muutettu tavalla, joka edellyttää uutta sertifiointia. Liitteen 1 vaatimuksissa on kuvattu joitakin muutoksia, jotka katsotaan olennaisiksi ja ilmoitettaviksi muutoksiksi. THL voi ohjeistaa mitkä ovat sellaisia muutoksia aikaisemmin yhteistestatussa tai tietoturvallisuuden arvioinnin hyväksytysti läpäisseessä hyvinvointisovelluksessa, joista tulee ilmoittaa Kelalle ja tietoturvallisuuden arviointilaitokselle.

8. Vaatimustenmukaisuuden uudistaminen

Kun hyvinvointisovellukselle annettu todistus tietoturvallisuuden arvioinnista on vanhentumassa, tulee hyvinvointisovelluksen valmistajan ottaa yhteyttä tietoturvallisuuden arviointilaitokseen tietoturvallisuustodistuksen uusimiseksi. Hyvinvointisovelluksen valmistajan tulee ottaa yhteyttä myös Kelaan, jotta hyvinvointisovelluksen yhteistestaustarve voidaan arvioida uudelleen.

Yhteydenotto tietoturvallisuuden arviointilaitokseen ja Kelaan tulee tehdä viimeistään 6 kuukautta ennen tietoturvallisuustodistuksen vanhenemista.

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

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

- toteutus perustuu vanhentuneeseen määrittelyyn, jonka korvaavan uuden määrittelyn yhteydessä tai säädöksissä annettu määräaika uuden määrittelyversioon mukaiselle käyttöönotolle tai toteutukselle on menneisyydessä; tai

- toteutus ei vastaa omatietovarannon tuotantoympäristössä edellytettävää julkaistua määrittelyä tai määrittelyversiota; tai

- toteutus ei vastaa omatietovarannon yhteistestauksessa edellytettävää julkaistua määrittelyversiota, vaikka myös poistuvia vanhemman version mukaisia toteutuksia tuettaisiin edelleen omatietovarannon tuotantoympäristössä.

Tietoturvallisuuden arviointilaitos suorittaa tietoturvallisuustodistuksen uusimiseen tähtäävän tietoturvallisuuden arvioinnin todentamalla kaikki hyvinvointisovelluksen kannalta relevantit tietoturvavaatimukset. Kunkin vaatimuksen todentamisessa voidaan nojautua samoihin menettelyihin ja dokumentaatioihin kuin aiemmin myönnetyssä tietoturvallisuustodistuksessa, mikäli vaatimuksen toteuttamis- tai täyttymistavat eivät ole muuttuneet hyvinvointisovelluksessa tai hyvinvointisovelluksen käyttöympäristössä ei ole tapahtunut vaatimusten toteutumiseen vaikuttavia muutoksia. Tietoturvallisuuden arviointilaitos antaa tietoturvallisuustodistuksen hyväksytystä tietoturvallisuuden arvioinnista tämän määräyksen luvun 5. mukaisesti.

Vaatimustenmukaisuuden uudistamisen johdosta hyvinvointisovelluksen valmistaja toimittaa hyvinvointisovelluksen päivitetyt tiedot Valviralle, jotta tiedot voidaan päivittää Valviran tietojärjestelmärekisteriin.

9. Olennaiset vaatimukset

Hyvinvointisovelluksen valmistaja on vastuussa hyvinvointisovelluksen suunnittelusta ja valmistuksesta. Hyvinvointitietojen käsittelyssä käytettävän hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Asiakastietolain mukaan hyvinvointisovelluksen tulee täyttää myös saavutettavuusvaatimukset. Hyvinvointisovelluksen valmistaja vastaa hyvinvointisovelluksen käyttötarkoituksen määrittelystä ja vaatimustenmukaisuudesta annettavasta selvityksestä sekä hyvinvointisovelluksen sertifioinnista ja rekisteröinnistä. Vaatimustenmukaisuudesta annettava selvitys tehdään liitteen 1 lomakkeen avulla. Selvityksen kautta hyvinvointisovelluksen valmistaja vakuuttaa, että hyvinvointisovellus täyttää sitä koskevat olennaiset vaatimukset ja kuvaa sen, kuinka olennaiset vaatimukset täytetään. Liitteen 1 mukainen selvitys on edellytyksenä hyvinvointisovelluksen sertifioinnille ja rekisteröinnille.

Vaatimukset on tarkoitettu varmistamaan hyvinvointisovellusten vaatimustenmukaisuus sekä selkeyttämään ja tukemaan hyvinvointisovellusten kehittämistä, testausta, sertifiointia, arviointia, hankintaa ja eri osapuolten välistä viestintää. Hyvinvointisovelluksen valmistajan tulee lähtökohtaisesti täyttää sellaiset liitteen 1 vaatimukset, jotka ovat hyvinvointisovellukseen sovellettavissa, ellei niiden kohdalla ole muuta mainintaa siitä, millaisia hyvinvointisovelluksia vaatimus koskee.

Hyvinvointisovelluksen tulee täyttää asiakastietolaissa ja tässä määräyksessä määrättyjen vaatimusten lisäksi muiden sitä koskevien säädösten mukaiset vaatimukset. Esimerkiksi mikäli hyvinvointisovellus tallentaa henkilötietoja muualle kuin omatietovarantoon, on hyvinvointisovellukseen liittyvät rekisterinpitovastuut ja tähän liittyvät hallinta-, suojaus- ja valvontavastuut määriteltävä ja kuvattava säädösten mukaisesti. Mikäli osana sertifiointia havaitaan, että hyvinvointisovellus ei täytä muiden sitä koskevien säädöksien mukaisia vaatimuksia, sertifiointia ei voida hyväksyä.

9.1 Olennaisten vaatimusten osa-alueet

Vaatimuksiin kuuluvat seuraavat osa-alueet, joiden täyttämisestä ja kuvaamisesta määräyksen liitteenä 1 olevalle lomakkeelle vastaa hyvinvointisovelluksen valmistaja:

Perustiedot

Hyvinvointisovellusta koskevat perustiedot on täytettävä liitteen 1 Perustiedot-välilehdelle. Perustietoihin kuuluu myös hyvinvointisovelluksen käyttötarkoituksen kuvaaminen, josta vastaa hyvinvointisovelluksen valmistaja. Hyvinvointisovelluksesta on myös annettava käyttäjille tarpeelliset tiedot ja tarvittaessa ohjeet hyvinvointisovelluksen käyttöönotosta ja käytöstä.

Säädökset ja ohjeistukset

Liitteen 1 Säädökset ja ohjeistukset-välilehdelle kuvataan se, kuinka hyvinvointisovelluksessa täytetään keskeisiä eri säädösten velvoitteita. Myös hyvinvointisovelluksen käyttötarkoitus, luonne ja rajaukset vaikuttavat siihen, mitkä eri säädöksistä tulevat vaatimukset koskevat hyvinvointisovellusta.

Perusvaatimukset

Liitteen 1 Perusvaatimukset-välilehdelle hyvinvointisovelluksen valmistaja raportoi hyvinvointisovelluksen perusvaatimuksia sekä muun muassa hyvinvointisovelluksen tyyppiin ja mahdolliseen hyvinvointisovellukseen liittyvään mainontaan liittyviä seikkoja.

Kuvaukset kansalaiselle

Liitteen 1 Kuvaukset kansalaiselle -välilehdellä kuvataan keskeisimpiä seikkoja, joiden informointi ja selkeä viestintä hyvinvointisovellusta käyttäville kansalaisille on suoritettava vaatimusten mukaisesti.

Tietoturvavaatimukset ja tietosuojavaatimukset

Tietoturvallisuuteen ja tietosuojaan liittyvät vaatimukset hyvinvointisovelluksille on koottu tämän määräyksen liitteeseen 1 Tietoturvavaatimukset- ja Tietosuoja-välilehdille.

Toiminnalliset vaatimukset

Keskeisiä toiminnallisia vaatimuksia on kuvattu liitteen 1 Toiminnalliset vaatimukset-välilehdellä. Toiminnallisia vaatimuksia hyvinvointisovelluksessa toteutettuihin toimintoihin ja tietosisältöihin liittyen on myös muilla välilehdillä, ja niitä käydään läpi yhteistestauksessa tai tietoturvallisuuden arvioinnissa.

Saavutettavuusvaatimukset

Hyvinvointisovellusten tulee täyttää saavutettavuusvaatimukset. Saavutettavuusvaatimukset löytyvät tämän määräyksen liitteen 1 Saavutettavuusvaatimukset-välilehdeltä.

Yhteistestausvaatimukset

Yhteentoimivuus on osoitettava Kelan järjestämässä yhteistestauksessa. Yhteistestausvaatimukset löytyvät liitteen 1 välilehdeltä Yhteistestausvaatimukset.

9.2 Vaatimusten todentamistavat

Liitteessä 1 kuvatut vaatimukset ovat sitovia vaatimuksia. Kaikkien hyvinvointisovellukseen sovellettavissa olevien vaatimusten toteutuminen on kuvattava. Yhteistestaukseen ja arviointiin sisältyvät vaatimukset on todennettava. Hyvinvointisovelluksen on täytettävä kaikki ne vaatimukset, jotka ovat sovellettavissa kyseisessä hyvinvointisovelluksessa. Mikäli jokin vaatimus ei ole sovellettavissa hyvinvointisovelluksessa, on hyvinvointisovelluksen valmistajan merkittävä tämä selvästi liitteen 1 avulla annettavaan selvitykseen. Hyvinvointisovelluksen yhteentoimivuuden testauksesta vastaava Kela tai tietoturvallisuuden arvioinnista vastaava arviointilaitos voi kuitenkin tehdä päätöksen siitä, sovelletaanko vaatimusta hyvinvointisovellukseen. Jos pakollinen olennainen vaatimus ei täyty, arvioija voi asettaa vaatimuksen täyttymiselle määräajan ennen testauksen tai tietoturvallisuuden arvioinnin hyväksymistä osana käynnissä olevaa sertifiointiprosessia.

Osana todentamista arvioija (ja soveltuvin osin / tarvittaessa yhteentoimivuuden testaaja) raportoi kaikkien arviointiin (tai testaukseen) kuuluvien vaatimusten osalta seuraavat asiat:

- vaatimuksen täyttyminen, jokin seuraavista vaihtoehdoista
    - vaatimus täyttyy täysin
    - vaatimus täyttyy osittain ja täyttymättä jäävä osa kompensoidaan; kompensointitapa kuvattava
    - vaatimus ei täyty
- mikäli vaatimus ei ole sovellettavissa tai on vain osin sovellettavissa arvioitavan hyvinvointisovelluksen osalta, maininta tästä perusteluineen

- todentamistapa ja tieto siitä, kuinka vaatimuksen täyttyminen on todettu, esimerkiksi viite dokumentaatioon, testausraporttiin tai ohjelmiston tuotokseen.

Sovellettavissa olevien olennaisten vaatimusten täyttyminen on osoitettava osana sertifiointia, jotta hyvinvointisovelluksen sertifiointi voidaan hyväksyä.

Vaatimusten todentamisessa käytetään seuraavia todentamistapoja:

- V: validointi tai tekninen tarkastus, esimerkiksi hyvinvointisovelluksen tuottaman lokin, sanomainstanssin tai järjestelmän tuottaman raportin läpikäynti

- T: testaus, jossa soveltuvin osin

    - YT: käydään läpi osana Kelan yhteistestausta
    - TT: tarkistetaan hyvinvointisovellusta käyttämällä (toiminnallisella testauksella) ominaisuuden olemassaolo ja asianmukaisuus, osana tietoturva-arviointia (myös loppukäyttäjälle näytettävät kuvaukset)
    - HT: tekninen tietoturva- ja haavoittuvuustestaus ja turvallisuustason arviointi, osana tietoturva-arviointia
    - ST: saavutettavuusvaatimusten testaus osana hyvinvointisovelluksen valmistajan omaa tai ulkoisen toimijan toteuttamaa saavutettavuusvaatimusten arviointia. Osana tietoturvallisuuden arviointia läpikäydään raportti saavutettavuustestauksen tuloksista.

- D: hyvinvointisovelluksen dokumentaation (myös muu kuin loppukäyttäjälle näytettävä) läpikäynti:

- (täydentävä) H: haastattelu ja haastattelun dokumentointi osana tietoturvallisuuden arviointia, jolla voidaan syventää ja täydentää arviointia; haastattelu ei ole hyväksyttävä ensisijaiseksi vaatimuksen todentamistavaksi luokan A hyvinvointisovelluksissa

YT-merkityt todentamiset suoritetaan osana Kelan kanssa tehtävää yhteistestausta. D-, HT-, TT- ja V-merkityt todentamiset suoritetaan osana tietoturvallisuuden arviointia.

Vaatimusten todentamisessa on käytettävä todentamistapaa, joka on riittävä kunkin vaatimuksen tai vaatimuskohdan todentamiseen. Riittävä todentamistapa on ilmoitettu kunkin vaatimuksen kohdalla erikseen. Liikenne- ja viestintävirasto Traficomin ohjeiden mukaiset hallinnolliset ja soveltuvin osin myös tekniset todentamistavat ovat arvioinnissa tehtävän soveltamisen tärkeä lähtökohta.

Erityisesti teknisessä tietoturva- ja haavoittuvuustestauksessa (todentamistapa HT) tulisi soveltaa sopivaa yleistä tietoturvatestauksen kehikkoa, kuten OWASP ASVS tai MASVS, sikäli kuin vaatimukset ovat vastaavia tai yhteensopivia liitteessä 1 esitettyjen tietoturvavaatimusten kanssa.

9.3 Vaatimusten ja määritysten versionhallinta

Kela tai THL julkaisevat tiedot siitä, mitkä ovat voimassa olevia määrityksiä ja määritysversioita, ja minkä versioiden nojalla vaatimustenmukaisuus todennetaan. Kela julkaisee ajantasaiset tiedot siitä, mitä määrityksiä ja määritysversioita edellytetään Kanta-palvelujen tuotantoympäristössä ja Kanta-rajapintoihin liittyvässä yhteistestauksessa.

Jos uusien Kelan tai THL:n tuottamien määritysten tai määritysversioiden voimaantulon yhteydessä edellytetään aiemman hyvinvointisovellustoteutuksen muuttamista uutta sertifiointia vaativalla tavalla, Kela tai THL ilmaisee tämän määritysten julkaisun yhteydessä. Mikäli uudelleensertifiointia tai sertifiointitarpeen uutta arviointia edellytetään, on nämä toimenpiteet toteutettava määräyksessä tai määrityksen yhteydessä ilmaistun määräajan puitteissa. Mikäli näitä toimenpiteitä tai määräaikoja ei edellytetä, ovat myös aiempien määritysversioiden mukaiset toteutukset hyväksyttäviä testauksessa ja tuotantokäytössä.

9.4 Merkittävät poikkeamat

Merkittäviä poikkeamia ovat:

- poikkeamat, jotka aiheuttavat merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai sosiaali- ja terveyspalvelujen toiminnalle tai potilas- tai asiakasturvallisuudelle,
- sellaiset poikkeamat olennaisista vaatimuksista tuotantokäytössä olevassa hyvinvointisovelluksessa, jotka aiheuttavat merkittäviä tai pitkäaikaisia heijastusvaikutuksia tai lisäpoikkeamia useille toimijoille tai useille muille hyvinvointisovelluksille,
- tuotantokäytössä toimivan hyvinvointisovelluksen tietoturvallisuustodistuksen vanheneminen,
- tuotantokäytössä toimivassa hyvinvointisovelluksessa toteutettujen ominaisuuksien perustuminen vanhentuneeseen määrittelyversioon, jonka voimassaolo on päättynyt tai tuki omatietovarannossa on poistunut tai poistumassa,
- sertifiointiprosessissa havaituille korjaustarpeille asetettuja määräaikoja ei ole noudatettu, tai
- muut valvontaviranomaisen (kuten Valvira, Etelä-Suomen aluehallintovirasto tai Tietosuojavaltuutetun toimisto) merkittäväksi poikkeamaksi toteamat poikkeamat

Merkittävistä poikkeamista on ilmoitettava asiakastietolain 32 §:n mukaisesti. Hyvinvointisovelluksen valmistajan ja tarvittaessa palvelunantajan, jota merkittävä poikkeama koskee, on ryhdyttävä toimenpiteisiin poikkeaman korjaamiseksi. Valvira julkaisee tietoa hyvinvointisovelluksia koskevista poikkeamista osana tietojärjestelmärekisteriä.

Jos osana sertifiointiprosessia havaitaan sellainen poikkeama olennaisista vaatimuksista, joka johtaisi merkittävään poikkeamaan tuotantokäytössä, ei sertifiointia voida hyväksytysti suorittaa loppuun ennen kuin poikkeama on korjattu. Vaatimukset, jotka eivät täyty tai täyttyvät puutteellisesti voivat aiheuttaa korjaustarpeen ennen yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä, kuten luvussa 9.2 on kuvattu.

Mikäli tuotannossa toimiva hyvinvointisovellus ei täytä voimassa olevia siihen kohdistuvia olennaisia vaatimuksia tai sen vaatimustenmukaisuus on vanhentunut, hyvinvointisovelluksen valmistajan on ilmoitettava asiasta Valviralle ja Kelalle. Merkittävistä poikkeamista on ilmoitettava asiakastietolain 32 §:n mukaisesti Valviralle ja hyvinvointisovelluksen käyttäjille. Jos poikkeama johtuu hyvinvointisovelluksesta tai hyvinvointisovelluksen valmistajan toiminnasta, on hyvinvointisovelluksen valmistajan arvioitava poikkeamista koituva riski ja suunniteltava tarvittavat korjaus- tai jatkotoimenpiteet riskiarvion perusteella. Tämä toimenpide on suoritettava sen lisäksi, mitä asiakastietolain 32 §:ssä säädetään hyvinvointisovelluksen käyttöönoton jälkeisestä seurannasta.

9.5 Kolmansien osapuolten palveluihin liittyvät tietosuoja- ja varautumisvaatimukset

Tietosuoja- ja tietoturvallisuusriskien sekä varautumistarpeiden huomiointi on osa hyvinvointisovelluksen valmistajan toimintaa. Hyvinvointisovelluksen valmistaja vastaa hyvinvointisovellukseen liittyvistä olennaisista vaatimuksista myös siltä osin kuin hyvinvointisovellus nojautuu kolmannen osapuolen tuottamiin välineisiin tai alustoihin tai jaettuja resursseja tarjoaviin ICT-palveluihin. Samoja perusvaatimuksia sovelletaan myös tilanteissa, joissa käytetään kolmannen osapuolen tuottamia kapasiteettipalveluita kuten palvelinvuokrausta, palvelinhallintaa, varmistuspalveluja, konesalipalveluja tai pilvipalveluja.

Alustapalveluja, mukaan lukien jaettuja resursseja tarjoavat pilvipalvelut, voivat tuottaa muut osapuolet kuin hyvinvointisovelluksen valmistaja. Kuten julkisen hallinnon pilvipalvelulinjauksissa, myös hyvinvointisovelluksissa käsiteltävää ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu. Myös varsinainen hyvinvointisovellus voidaan toteuttaa esimerkiksi pilvipohjaisena SaaS-palveluna, mikäli olennaiset vaatimukset voidaan täyttää ja todentaa, ja mikäli riskien hallinta on riittävällä tasolla liitteen 1 tietoturva- ja tietosuojavaatimusten mukaisesti huomioitu. Hyvinvointisovelluksen valmistaja voi käyttää pilvipohjaisia PaaS- tai IaaS-ratkaisuja hyvinvointisovelluksen toteuttamisessa skaalautuvasti sen lisäksi tai vaihtoehtoisesti sille, että hyvinvointisovelluksen tekninen suoritusympäristö olisi kokonaisuudessaan hyvinvointisovelluksen valmistajan 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 hyvinvointisovellukselle 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 hyvinvointitieto on salattava tiedon arkaluonteisuus huomioiden riittävän vahvasti siten, että vain hyvinvointisovelluksen valmistajalla on salatun tiedon purkamiseen tarvittavat avaimet. Sopimuksellisesti on huolehdittava siitä, että kaikki tietojen käsittelyyn ja hyvinvointisovelluksen tuottamiseen osallistuvat toimijat toimivat riittävän yhdenmukaisesti hyvinvointitietojen suojaamiseksi.

10. Ohjaus ja neuvonta

Terveyden ja hyvinvoinnin laitos ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa. Lisätietoja olennaisista vaatimuksista, sertifiointiprosessista ja hyvinvointisovelluksiin kohdistuvista määrittelyistä löytyy Kanta.fi-verkkosivustolta ja THL:n verkkosivustolta.

11. Voimaantulo

Tämä määräys tulee voimaan 16. päivänä helmikuuta 2022 ja on voimassa toistaiseksi.

Tämän määräyksen mukaisia menettelyjä ja vaatimuksia noudatetaan hyvinvointisovellusten sertifioinnissa ja rekisteröinnissä heti määräyksen voimaantulon jälkeen. Määräyksen mukaiset vaatimukset tulevat voimaan kaikissa tuotantokäyttöön tarkoitetuissa hyvinvointisovelluksissa 1.1.2023, johon mennessä kaikkien tuotantokäytössä toimivien hyvinvointisovellusten on suoritettava hyväksytty sertifiointi ja rekisteröinti. Aiemmat hyväksymiskriteerit hyväksytysti täyttänyt hyvinvointisovellus voi olla liittyneenä omatietovarantoon siihen asti, kun vaatimukset tuotantokäytössä tulevat voimaan (1.1.2023), johon mennessä sille on suoritettava tämän määräyksen mukainen sertifiointi ja rekisteröinti.

Tätä määräystä voidaan muuttaa päivittämällä tai antaa uusi määräys (sekä kumota aiempi) viimeistään silloin, kun aletaan soveltaa hyvinvointisovellukseen vaikuttavia asiakastietolain 52 §:n siirtymäsäännöksiä, joita ovat mm. asiakastietolain 13 §:n 2 momentti, 20 §:n 4 momentti ja 21 §:n 4 momentti.

Allekirjoitukset

Sirpa Soini
Osastonjohtaja

Jarmo Kärki
Yksikönpäällikkö

Jakelu

Kansaneläkelaitos
Sosiaali- ja terveysministeriö
Valtiovarainministeriö
Sosiaali- ja terveydenhuollon lupa- ja valvontavirasto Valvira
Lääkealan turvallisuus- ja kehittämiskeskus Fimea
Liikenne- ja viestintäviestintävirasto Traficom
Tietoturvallisuuden arviointilaitokset
Aluehallintovirastot
Healthtech Finland
Suomen Kuntaliitto ry
HL7 Finland Personal Health SIG
Tietosuojavaltuutetun toimisto

Tämä määräys on julkaistu viranomaisten määräyskokoelmissa

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

Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä

Internet-osoitteesta https://thl.fi/fi/web/tiedonhallinta-sosiaalija-terveysalalla/maaraykset-ja-maarittelyt/maaraykset