Määräyksen antopäivä	19.1.2022
Määräyksen voimaantulopäivä	19.1.2022
Voimassa	Toistaiseksi
Kumottava normi	Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2020
Säädösperusta	Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) 22 § 3 momentti sekä 24 § 2 momentti (määräyksessä nimellä ”toisiolaki”)

Sosiaali- ja terveysalan tietolupaviranomaisen määräys: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset

1 Tausta

Sosiaali- ja terveysalan tietolupaviranomainen Findata (myöhemmin ”Tietolupaviranomainen”) ylläpitää toisiolain 20 §:n 1 momentin mukaisesti tietoturvallista käyttöympäristöä. Ne tietoaineistot, joiden käyttöön Tietolupaviranomainen on myöntänyt luvan, luovutetaan pääsääntöisesti luvansaajan käsittelyä varten kyseiseen käyttöympäristöön.

Mikäli tietolupahakemuksessa pyydetään luovuttamaan tietoaineistoja käsiteltäviksi muussa kuin Tietolupaviranomaisen tietoturvallisessa käyttöympäristössä, hakemuksessa on toisiolain 20 §:n 3 momentin mukaan erikseen perusteltava syyt, joiden vuoksi tämä on välttämätöntä. Tietolupaviranomainen tai muu toisiolaissa tarkoitettu viranomainen saa tällöin luovuttaa tiedot hakijalle vain, jos käyttöympäristö täyttää 20 § 2 momentissa ja 21–29 §:ssä säädetyt edellytykset.

Jos toisiolain 44 §:n 3 momentissa tarkoitettu yksittäinen rekisterinpitäjä on tehnyt omiin rekistereihinsä sisältyviä tietoja koskevan tietolupapäätöksen, sen tulee luovuttaa tietoaineisto luvansaajan käsiteltäväksi aina toisiolain 20 §:ssä tarkoitettuun tietoturvalliseen käyttöympäristöön.

Toisiolain 24 §:n 2 momentin mukaan Tietolupaviranomainen antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Vaatimuksissa on edellytettävä vastaavaa tietoturvan tasoa kuin Tietolupaviranomaisen omassa käyttöympäristössä vaaditaan.

Määräyksestä järjestettiin ennen sen voimaantuloa lausuntokierros 26.11.2021 – 17.12.2021, jonka aikana lausuntoja annettiin yhteensä 23 kpl. Lausunnot on huomioitu määräyksen valmistelussa.

Tietoturvallisen käyttöympäristön vaatimukset ovat tämän määräyksen liitteenä 1.

2 Määräyksen soveltamisala

Tämä määräys on toisiolain 24 §:n 2 momentissa tarkoitettu Tietolupaviranomaisen määräys muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista.

Tämä määräys korvaa 5.10.2020 voimaan tulleen määräyksen THL/2492/4.00.00/2020.

Tätä määräystä sovelletaan kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin toisiolain mukaan tarvitaan tietolupa. Näitä käyttötarkoituksia ovat määräyksen antohetkellä tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä. Opetuksen osalta määräys koskee opetusaineiston valmistamista, ei varsinaista opetusta.

Tässä määräyksessä annettujen vaatimusten toteuttaminen on edellytyksenä sille, että Tietolupaviranomainen voi harkita ja luovuttaa tietoaineistoja luvansaajan käsiteltäväksi muussa kuin sen omassa käyttöympäristössä toisiolain 20 §:n 3 momentin mukaisesti. Määräystä sovelletaan viimeistään 1.5.2022 alkaen toisiolain 1.9.2021 voimaan tulleen uuden siirtymäsäännöksen (60 §:n 1 momentti) mukaisesti (laki sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta, 793/2021).

3 Todistuksen myöntämisen perusteet

Tämän määräyksen vaatimusten toteutuminen osoitetaan toisiolain 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Todistus myönnetään tarkastusraportin havaintojen perusteella. Jotta todistus voidaan myöntää, tulee tarkastusraportin täyttää kaikki seuraavat ehdot:

- Tarkastusraportti ei saa sisältää yhtään tämän määräyksen mukaan vakavaksi poikkeamaksi luokiteltavaa havaintoa.

- Mikäli tarkastusraportissa todetaan yksi tai useampi tämän määräyksen mukaan keskitason poikkeamaksi luokiteltava havainto, tulee tarkastusraportin sisältää myös arviointilaitoksen hyväksymä korjaussuunnitelma, jossa on asetettu myös määräaika korjaussuunnitelman mukaisen uudelleenarvioinnin valmistumiselle. Uudelleenarviointi on suoritettava hyväksytysti viimeistään 6 kuukauden kuluessa tarkastusraportin valmistumisesta.

- Muiden kuin vakavien poikkeamien ei arvioida yhdessä muodostavan vakavaksi luokiteltavaa poikkeamaa.

Poikkeamien luokittelu tapahtuu osana tietoturvallisuuden arviointilaitoksen suorittamaa arviointia seuraavia pääperiaatteita noudattaen:

- Vakava poikkeama: Kriteeri ei täyty, muut kontrollit eivät kompensoi puutetta ja tietoturva on poikkeaman takia selkeästi uhattuna.

- Keskitason poikkeama: Kriteeri ei täyty sellaisenaan, muut kontrollit kompensoivat puutetta ja tietoturva ei ole suoraan uhattuna.

- Lievä poikkeama: Kriteeri ei täyty, mutta tietoturva ei ole poikkeaman takia uhattuna.

Tietoturvallisen käyttöympäristön tietoturvallisuuden arvioinnista ja todistuksella tapahtuvasta tietoturvallisuuden osoitusvelvollisuudesta on säädetty toisiolain 25-29 §:ssä.

3 Määräyksen voimassaolo ja muutokset

Tämä määräys korvaa aiemman, 5.10.2020 annetun määräyksen THL/2492/4.00.00/2020. Mainitun aiemman määräyksen voimassaolo päättyy samalla hetkellä kuin tämä määräys tulee voimaan. Tämä määräys on voimassa toistaiseksi, ja se sisältää edellä mainittua aiempaa määräystä tarkempia ja yksityiskohtaisempia määräyksiä muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista.

4 Sovelletut oikeusohjeet

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) 18 - 34 §, 60 § 1 momentti sekä laki sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta, (793/2021) 60 §.

Seppänen Johanna 912110564
Digitaalinen allekirjoittaja: Seppänen Johanna 912110564
Päiväys: 2022.01.20 15:11:09 +02'00'

Johanna Seppänen
Johtaja

Lanu Heikki 91215375E
Digitaalinen allekirjoittaja: Lanu Heikki 91215375E
Päiväys: 2022.01.12 14:29:03 +02'00'

Heikki Lanu
ICT-päällikkö

Tämä määräys on sähköisesti allekirjoitettu.