

Laki

sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023) 2 §:n 3 momentti ja 90 § seuraavasti:

2 §

Soveltamisala ja suhde muuhun lainsäädäntöön

Tällä lailla annetaan toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2022/2555 (*NIS 2 -direktiivi*) ja kyberturvallisuuslakia (/) täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveystalvueluita järjestettäessä ja toteutettaessa.

90 §

Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä

Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän tai hyvinvointisovelluksen poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kansaneläkelaitoksen tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. Jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin apteekin toiminnalle, on apteekin ilmoitettava siitä lisäksi Lääkealan turvallisuus- ja kehittämiskeskukseen. Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.

Palvelunantajan, apteekin, Kansaneläkelaitoksen ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Sosiaali- ja terveysalan lupa- ja valvontavirastolle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveystalvueluiden toteuttaminen voi merkittävästi vaarantua. Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Apteekin on lisäksi ilmoitettava viipymättä Lääkealan turvallisuus- ja kehittämiskeskuselle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena apteekin toiminta voi merkittävästi vaarantua. Lääkealan turvallisuus- ja kehittämiskeskus voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Jos 1 ja 2 momentissa tarkoitetusta tietoturvallisuuteen liittyvästä poikkeamasta tai häiriöstä ilmoittaminen on yleisen edun mukaista, Sosiaali- ja terveysalan lupa- ja valvontavirasto voi velvoittaa palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Lisäksi Lääkealan turvallisuus- ja kehittämiskeskus voi velvoittaa apteekin tiedottamaan yleisölle 3 momentissa tarkoitetusta häiriöstä taikka kuultuaan ilmoitusvelvollista tiedottaa häiriöstä itse.

Tämä laki tulee voimaan 8 päivänä huhtikuuta 2025.

Helsingissä 4.4.2025

Tasavallan Presidentti

Alexander Stubb

Liikenne- ja viestintäministeri Lulu Ranne