

27.10.2020

LAKI SOSIAALI- JA TERVEYDENHUOLLON ASIAKASTIETOJEN SÄHKÖISESTÄ KÄSITTELYSTÄ (ASIAKASTIETOLAKI), TIETOSUOJAA JA TIETOTURVAA KOSKEVA SÄÄNTELY

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä säädetään asiakastietolaissa, jonka päivitystä sosiaali- ja terveysministeriö on valmistellut useamman vuoden ajan. HE on tavoitteena antaa Eduskunnalle heti, kun Kanta-palveluiden toimeenpanon edellyttämä määräraha on varmistunut. Määrärahatarve vuosille 2021-2023 on 15,6 milj. euroa.

Asiakastietolain HE:n keskeisenä tavoitteena on saattaa asiakastietojen sähköistä käsittelyä koskeva sääntely EU:n tietosuoja-asetuksen vaatimusten mukaiseksi ja luoda asetusta täydentävä sääntely. Tietoturvallisuuden osalta Asiakastietolaki sisältää säännökset myös mm. tietojärjestelmien luokittelusta, tietojärjestelmiä ja tietojärjestelmien valmistajia koskevista vaatimuksista, omavalvontasuunnitelmasta sekä valvonnasta. Laissa on määräyksenantovaltuudet Terveiden ja hyvinvoinnin laitokselle koskien mm. tietojärjestelmien olennaisia vaatimuksia (toiminnalliset ja tietoturva vaatimukset).

HE laajentaa yksityisten palvelunantajien liittymisvelvoitetta Kanta-palveluihin koskemaan kaikkien asiakas- tai potilastietojärjestelmiä käyttäviä palvelunantajia. Niiden käyttämien Kanta-palveluihin liitettävän tietojärjestelmän tulee kuulua asiakastietolain mukaiseen ns. A-luokkaan, eli järjestelmän on tullut läpäistä Kanta-palveluiden yhteentoimivuuden testaus sekä tietoturvallisuuden arviointilaitoksen suorittava tietoturvallisuuden arviointi.

Palvelunantajilta edellytettävän omavalvonta-/tietoturvasuunnitelman sisältö laajentuisi koskemaan tietojärjestelmien olennaisten vaatimusten täyttyminen varmistamista sekä suunnitelmaa omavalvonnan järjestämisestä ja toteuttamisesta palvelunantajan toiminnassa.

Terveiden ja hyvinvoinnin laitoksen määräyksenantovaltuuden kautta voidaan kehittää esim.

- tietojärjestelmien tietoturva vaatimuksia koskevan määräyksen ulottaminen Kanta-palveluihin liittymättömiin järjestelmiin (ns. B-luokan järjestelmät)
- tietoturvallisuutta koskevien vaatimusten ja vaatimustenmukaisuuden todentamisen menettelyjen kehittäminen, esim. teknisen (ulkoisen) tietoturvatestauksen tarve

Kansallisessa toimeenpanossa määräysten laatiminen, vaatimustenmukaisuuden todentaminen, ohjaus ja valvonta muodostavat kokonaisuuden, jonka resursointia on syytä vahvistaa niin, että esimerkiksi valvontaa voidaan toteuttaa ennakoivasti. Myös palvelunantajien tietoturvasuunnitelmia koskevaa ohjausta ja valvontaa on syytä vahvistaa.

Sanktiomahdollisuuksia arvioidaan olevan jo riittävästi sekä EU:n yleisen tietosuojasetuksen että asiakastietolain kautta, eikä niitä ole tarpeen lisätä.

Voimassa olevan asiakastietolain tietoturvallisuutta ja valvontaa koskevat keskeiset säädökset

Voimassa oleva asiakastietolaki sisältää useita tietoturvallisuutta koskevia säädöksiä.

Tietojärjestelmien luokittelu

Asiakastietojen käsittelyssä käytettävät tietojärjestelmät luokitellaan A- ja B-luokkiin. A-luokkaan kuuluvat kaikki Kanta-palveluihin liitettävät tietojärjestelmät ja välityspalvelut, muut kuuluvat luokkaan B. Esimerkiksi yksityisen palvelunantajan tietojärjestelmä, kun se ei ole liittynyt Kanta-palveluun, tai laboratoriojärjestelmä, jonka tiedot välitetään palvelunantajan potilastietojärjestelmään.

Kanta-palveluihin liitettäviltä A-luokan järjestelmiltä vaaditaan Kelan koordinoiman yhteentoimivuuden testauksen suorittaminen sekä tietoturvallisuuden arviointilaitoksen antama vaatimustenmukaisuustodistus.

B-luokan järjestelmissä on myös toteutettava tietoturvallisuutta ja tietosuojaa koskevat vaatimukset, mutta niiden todentamisen vaatimuksista ei säädetä laissa.

A-luokkaan kuuluvia tietojärjestelmiä ja välityspalveluita on Valviran rekisterissä 82, B-luokan järjestelmiä on 260.

Tietojärjestelmiä koskevat vaatimukset

Asiakastietolaki sisältää vaatimuksia sekä A- että B-luokan tietojärjestelmille. Kaikkien asiakastietojen käsittelyssä käytettävien tietojärjestelmien tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Tietojärjestelmä täyttää olennaiset vaatimukset silloin, kun se on suunniteltu, valmistettu ja toimii tietoturvaa ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määräysten mukaisesti. THL voi tarvittaessa antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä.

Vaatimustenmukaisuuden osoittaminen ja tietojärjestelmän käyttöönotto

Vaatimustenmukaisuuden osoittamisen menettelytavat ovat A- ja B-luokissa erilaiset. THL voi antaa tarkempia määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava tietojärjestelmän valmistajan antamalla selvityksellä siitä, että järjestelmä täyttää kaikki toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteistestauksella ja tietoturvallisuuden arviointilaitoksen antamalla vaatimustenmukaisuustodistuksella.

Luokkaan B kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava valmistajan antamalla kirjallisella selvityksellä siitä, että järjestelmä asianmukaisesti asennettuna, ylläpidettynä ja käyttötarkoituksensa mukaan käytettynä täyttää

olennaiset vaatimukset. Tietojärjestelmän saa ottaa tuotantokäyttöön sen jälkeen, kun järjestelmän valmistaja on antanut em. kirjallisen selvityksen.

Molempien luokkien osalta tuotantokäyttöön otettavasta tietojärjestelmästä on ilmoitettava Valviralle, joka ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon tietojärjestelmistä.

Palvelunantajia koskevat vaatimukset asiakastietolaissa

Palvelunantajan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä omaevalvontasuunnitelma, jossa on selvitettävä, miten palvelunantajan toiminnassa varmistetaan tietojärjestelmien käyttöön liittyvä turvallisuus. Esim. tietojärjestelmien käytön vaatimus koulutus ja kokemus, valmistajan ohjeistuksen mukainen tietojärjestelmien ylläpito ja päivitys sekä käyttöympäristön asianmukaisuus ja tietoturvallisuus

Jos palvelunantaja havaitsee olennaisten vaatimusten täyttymisessä merkittäviä poikkeamia, on sen ilmoitettava siitä tietojärjestelmän valmistajalle. Jos poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle, on siitä ilmoitettava myös Valviralle.

Tietojärjestelmien valvonta

Valviran tehtävänä on valvoa ja edistää tietojärjestelmien vaatimustenmukaisuutta. Se voi määrätä asiakastietolaissa säädetyn velvollisuuden toteutettavaksi määräajassa ja samalla määrätä tietojärjestelmän valmistajan korjaamaan tuotantokäytössä olevia tietojärjestelmiä koskevat puutteet.

Jos tietojärjestelmä voi vaarantaa tietosuojan taikka asiakas- tai potilasturvallisuuden, eikä puutteita ole korjattu määräajassa, voi Valvira kieltää tietojärjestelmän käytön, kunnes turvallisuuden vaarantava ominaisuus on korjattu.

THL:n määräykset

Asiakastietolain mukaisesti THL voi antaa määräyksiä tietojärjestelmien olennaisista vaatimuksista, vaatimusten todentamisen menettelyistä ja omaevalvontasuunnitelman selvityksistä ja vaatimuksista.

THL:n voimassa olevat tietoturvan kannalta relevantit määräykset:

- Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturva-vaatimukset
- Määräys 2/2015: Omaevalvontasuunnitelmaan sisällytettävät selvitykset ja vaatimukset

Toimenpide-ehdotukset

- Asiakastietolain HE:n etenemisen varmistaminen (rahoitus) siten, että HE voidaan esitellä viikolla 45

- Tietojärjestelmien vaatimuksia, todentamisen menettelyjä sekä palveluntarjoajien tietoturvaan koskevien määräysten laatimisen, ohjauksen ja valvonnan resurssien vahvistaminen (THL 1 hvt ja Valvira 2 htv)