



Asiakastietolaki: tietojärjestelmiä ja sertifiointia koskeva sääntely

Anna Kärkkäinen

26.10.2021





Asiakastietolain 784/2021 voimaantulo

- Asiakastietolaki ja siihen liittyvät lait voimaan 1.11.2021
- Seuraavilla sivuilla keskeiset sisällöt omavalvontaa, tietojärjestelmiä ja sertifiointia koskevasta sääntelystä (luvut 6 – 8), erityisesti muutokset suhteessa voimassa olevaan lakiin 159/2007
 - Luku 5: tietoturvallisuuden ja tietosuojan omavalvonta
 - Luku 6: Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja käyttöönotto
 - Luku 7: Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset



Tietoturvallisuuden ja tietosuojan omavalvonta

- 27 § Tietoturvasuunnitelma
 - Vastaa aiempaa omavalvontasuunnitelmaa
 - Sanamuotoja täsmennetty
 - Lisätty kohdat, joiden mukaan tietoturvasuunnitelmassa on oltava selvitykset siitä,
 - Miten tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset
 - Miten tietoturvan ja tietosuojan omavalvonta järjestetään ja toteutetaan toiminnassa
 - Palvelunantajien lisäksi myös välittäjien ja Kelan laadittava ko. suunnitelma
- 28 § Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu
 - Kelan ja välittäjän on seurattava tietoturvasuunnitelmansa toteuttamista

Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja käyttöönotto 1



29 § Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu

- A-luokkaan voivat kuulua Kantan ja Kantaan liitettävien asiakastietoja käsittelevien tietojärjestelmien ja hyvinvointisovellusten lisäksi myös muut käyttötarkoituksensa perusteella sertifioitavat tietojärjestelmät ja hyvinvointisovellukset ja välittäjien palvelut
 - Esim. vain hyvinvointitietoja käsittelevät hyvinvointisovellukset
- Muut tietojärjestelmät kuuluvat luokkaan B
 - Hyvinvointisovelluksia ei voi kuulua luokkaan B

Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja käyttöönotto 2



30 § Tietojärjestelmien ja hyvinvointisovellusten rekisteröinti

- Myös hyvinvointisovellukset rekisteröitävä
- Rekisterin tietosisältöjä täsmennetty
 - tietojärjestelmien ja hyvinvointisovellusten käyttötarkoituksista sekä niiden täyttämistä olennaisista vaatimuksista
 - yhteentoimivuuden testauksen tuloksista
 - tietoturvallisuuden arviointia koskevan todistuksen voimassa olosta
 - Tuotantokäytössä olevan tietojärjestelmän ja hyvinvointisovelluksen merkittävästä poikkeamasta (poikkeaman keston ajan)

Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja käyttöönotto 3



31 § Tietojärjestelmän ja hyvinvointisovelluksen ottaminen tuotantokäyttöön

- Saa ottaa tuotantokäyttöön ja liittää Kantaan kun sertifioitu
- Lisäksi tietojärjestelmän tai hyvinvointisovelluksen tietojen oltava Valviran rekisterissä, eikä tietoturvallisuuden arviointia koskeva todistus saa olla vanhentunut

32 § Tietojärjestelmän ja hyvinvointisovelluksen käyttöönoton jälkeinen seuranta

- Koskee myös hyvinvointisovelluksia
- Olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitoksen lisäksi Kelalle

Tietojärjestelmän ja hyvinvointisovelluksen olennaiset vaatimukset 1



33 § Tietojärjestelmäpalvelun tuottajan ja valmistajan sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet

- Koskee myös hyvinvointisovelluksia
- Eroteltu tietojärjestelmän valmistajan ja tietojärjestelmäpalvelun tuottajan vastuut

34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat olennaiset vaatimukset

- Koskee myös hyvinvointisovelluksia
- Hyvinvointisovellusten täytettävä muiden vaatimusten lisäksi saavutettavuusvaatimukset

Tietojärjestelmän ja hyvinvointisovelluksen olennaiset vaatimukset 2



35 § Vaatimustenmukaisuuden osoittaminen

- A-luokan tietojärjestelmän ja hyvinvointisovelluksen osoittaminen sertifiointilla
 - Selvitys, että tietojärjestelmä tai hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnalliset vaatimukset
 - Hyväksytty yhteentoimivuuden testaus
 - Todistus tietoturvallisuuden arvioinnista
- B-luokan tietojärjestelmän vaatimuksenmukaisuus osoitetta tietojärjestelmäpalvelun tuottajan antamalla kirjallisella selvityksellä

37 § Tietoturvallisuuden arviointi

- Todistus tietoturvallisuuden arvioinnista voimassa viiden vuoden sijaan enintään kolme vuotta (myös jatkaminen enintään kolme vuotta)

Huom! Todistus ainoastaan tietoturvallisuuden arvioinnista

stm.fi ›
@STM_Uutiset ›



Kiitos!

Lisätietoja

anna.karkkainen@stm.fi

