



# THL määräys 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

Asiakastietolain täytäntöönpanoa ohjaavat määräykset -infotilaisuus  
9.12.2021

Sote-tiedonhallinta

Terveyden ja hyvinvoinnin laitos

# Mikä tietoturvasuunnitelma 1/2?

Määräys 3/2021 on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uudistuvaa asiakastietolakia

- Uudessa **asiakastietolaissa** aiemman lain tietosuojan ja tietoturvallisuuden sekä tietojärjestelmien käytön omavalvontasuunnitelma **korvautuu tietoturvasuunnitelmalla**
- Sosiaali- ja terveydenhuollon toimijat **velvoitetaan laatimaan** tietoturvasuunnitelma  
- aiempi tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelma on pohja **uuden lain mukaiselle tietoturvasuunnitelmalle**  
- **sisältö pääosin vastaava** kuin aiemman lain edellyttämässä omavalvontasuunnitelmassa
- Suunnitelma edistää asiakas- ja potilastietojen **turvallista käsittelyä** ja **parantaa** sote-toimijoiden **tietosuojaa ja tietoturvaa – vahvistaa tietoturvallisuuden ja tietosuojan** suunnittelun ja toteuttamisen käytäntöjä
- Määräys **tarkentaa** tietoturvasuunnitelmaan tarvittavien **selvitysten sisältöä** ja **tietoturvallisuudelle** sosiaali- ja terveyspalveluissa **asetettavia vaatimuksia**

# Mikä tietoturvasuunnitelma 2/2?

Määräys 3/2021 on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uudistuvaa asiakastietolakia

- Uuden asiakastietolain ja määräysten kautta täsmennetään myös **tietojärjestelmiin kohdistuvien olennaisten vaatimusten toteutumista** sote-palveluiden järjestäjien ja tuottajien näkökulmasta
  - tietoturvasuunnitelma väline olennaisten vaatimusten täyttämisen varmistamisessa
  - sitoo yhteen sekä palvelunantajan omat käytännöt että kaikki käytössä olevat tietojärjestelmät ja ICT-palvelut
- **Tietoturvasuunnitelma ei ole julkinen** asiakirja
  - ”Tämän määräyksen mukaista tietoturvasuunnitelmaa **ei tule sisällyttää tai yhdistää** julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin.”
  - ”Tietoturvasuunnitelmaa ja siinä viitattuja liitedokumentteja **tulee käsitellä ja säilyttää ottaen huomioon tarvittava suojaaminen sivullisilta** ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto.”
- Tietoturvasuunnitelma on hyvä käytännön työväline – kokoava dokumentti, ”**kokonaisturvallisuuden toimeenpanon suunnitelma**”

# Mikä tietoturvasuunnitelma mallipohja?

Määräys 3/2021 on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uudistuvaa asiakastietolakia

- Määräyksen 3/2021 liitteenä on tietoturvasuunnitelman mallipohja, jota on uudistettu ja selkeytetty verrattuna aiemman määräyksen mukaisiin mallipohjiin
- mallipohja on tarkoitettu vapaaehtoisesti hyödynnettäväksi
  - tietoturvasuunnitelman voi laatia tarkoituksenmukaiseksi katsomallaan tavalla, kunhan suunnitelmasta tai sen liitteistä käyvät määräyksessä 3/2021 esitetyt seikat selkeästi ilmi
- mallipohjasta on määräyksen liitteeksi laadittu yksi versio
  - kooltaan ja toiminnaltaan hyvinkin erilaiset sote-palvelunantajat voivat soveltaa tai täydentää mallipohjaa omaan toimintaansa peilaten
- aiempi tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelma on päivitettävä voimassa olevan asiakastietolain mukaiseksi tietoturvasuunnitelmaksi
  - päivittämisessä on suositeltavaa lähteä liikkeelle kriittisimmistä kohteista **omassa toiminnassa tunnistettujen riskien** ja tietoturvallisuuden tilan tarkastelun kannalta

# Asiakastietolaki 27 § ja 28 §

## Asiakastietolaki 27 §

Tietoturvasuunnitelma

Palvelunantajan, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma.

Tietoturvasuunnitelmassa on oltava selvitykset, miten seuraavat asiakas- ja potilastietojen ja järjestelmien käsittelyyn liittyvät vaatimukset varmistetaan:

## Asiakastietolaki 27 §:

- 1) ... käytön vaatima **koulutus**
- 2) ... asianmukaisen käytön kannalta tarpeelliset **käyttöohjeet**
- 3) ... **käytetään** tietojärjestelmäpalvelun tuottajan antaman **ohjeistuksen mukaisesti**
- 4) ... **ylläpidetään ja päivitetään** tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti
- 5) ... **käyttöympäristö soveltuu tietojärjestelmien** asianmukaiseen sekä **tietoturvan ja tietosuojan...**
- 6) ... liitetyt **muut tietojärjestelmät** tai muut järjestelmät **eivät vaaranna...suorituskykyä** eivätkä...
- 7) ... asentaa, ylläpitää ja päivittää vain **henkilö...** tarvittava **ammattitaito** ja **asiantuntemus**
- 8) 29 § Tietojärjestelmien ja hyvinvointisovellusten käyttötarkoitus ja luokittelu:  
... **on jaoteltava** käyttötarkoitustensa ja ominaisuuksiensa perusteella **luokkiin** A ja B  
34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat **olennaiset vaatimukset**  
... Tietojärjestelmäpalvelun tuottajan on laadittava kuvaus...käyttötarkoituksesta...täyttää...olennaiset vaatimukset
- 9) ... palvelunantajalla, välittäjällä ja Kansaneläkelaitoksella on **suunnitelma...omavalvonta järjestetään ja toteutetaan** sen toiminnassa...

## Asiakastietolaki 28 §

Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu  
Sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Vastaavan johtajan on annettava kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehdittava henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä.

# Asiakastietolaki 27 1 § ja 2 § avattuna

(Tietoturvallisuuden)  
omavalvonnan kohde  
laatii Tietoturvasuunnitelman

...on oltava **selvitykset** siitä, **miten** asiakas- ja potilastietojen ja järjestelmien käsittelyyn liittyvät **vaatimukset (= velvoitteet)** varmistetaan:

Selvitykset voidaan kuvata suoraan tietoturvasuunnitelmaan tai niihin voidaan viitata tietoturvasuunnitelmassa liitedokumenteilla, linkeillä, ...



## Velvoitteet Määräyksessä 3/2021 = Asiakastietolaki 784/2021 27 § 1 momentti

- 1) henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima koulutus;
- 2) tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet;
- 3) tietojärjestelmiä käytetään tietojärjestelmäpalvelun tuottajan antaman ohjeistuksen mukaisesti;
- 4) tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti;
- 5) tietojärjestelmän käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojaan varmistavaan käyttöön;
- 6) tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia;
- 7) tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus;
- 8) 29 §:ssä tarkoitetut tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset 34 §:ssä säädetyt olennaiset vaatimukset; sekä
- 9) **palvelunantajalla, välittäjällä ja Kansaneläkelaitoksella** on suunnitelma siitä, miten omavalvonta järjestetään ja toteutetaan sen toiminnassa.

"Tietoturvasuunnitelman kohteena olevista tahoista käytetään tässä määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde tai omavalvonnan kohde."

Määräys 5/2021, tietojärjestelmien olennaisia vaatimuksia →

(Tietoturvallisuuden) omavalvonnan kohde =  
Asiakastietolaki 784/2021 27 § 1 momentti 9 kohta →

## Asiakastietolaki 784/2021 27 § 2 momentti

Ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa selvitettävä, **miten** tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät **vaatimukset** on varmistettu.

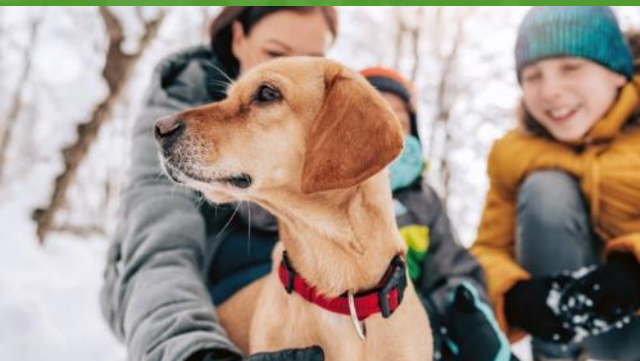
# Yhteenveto tietoturvasuunnitelmasta

- **Tietoturvasuunnitelma** on keskeinen käytännön työväline sosiaali- ja terveydenhuollon tietosuoja- ja tietoturvallisuuden suunnittelussa, toteuttamisessa ja käytännön seurannassa
- **Asiakastietolain toimeenpano ja määräykset luovat pohjaa** mm. hyvinvointialueiden tarvitsemalle tiedonhallinnalle – tietoturva- ja tietosuojakäytäntöjen yhdenmukaistaminen ja parantaminen keskeinen osa suunnittelua myös sote-uudistuksessa
- **Tietoturvasuunnitelma on** sote-uudistuksen yhteydessä erityisesti hyvinvointialueiden ja niiden palveluntuottajien organisoinnin **työväline riskienhallintaan, tietoturvallisuustyöhön, tietojärjestelmien hallinnointiin ja varautumiseen**
- **Tietoturvasuunnitelma on sovitettava organisaation omaan toimintaan** – otettava huomioon erityisesti sopimukset ja kumppanuudet
- Tietoturvasuunnitelman omavalvonta ja sen dokumentointi auttaa myös mm. **EU:n yleisen tietosuoja-asetuksen mukaisen osoitusvelvollisuuden täyttämässä**
- **Vastuu** tietoturvasuunnitelman laatimisesta ja noudattamisesta on **sote-organisaation vastaavalla johtajalla** (Asiakastietolaki 28 §)

# Tietoturvasuunnitelma

- THL Määräys 3/2021 - Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset julkaistaan Finlexissä, **jolloin ne tulevat voimaan**: FINLEX<sup>®</sup> - Viranomaisten määräyskokoelmat – Terveyden ja hyvinvoinnin laitos: <https://www.finlex.fi/fi/viranomaiset/normi/561001/>
- Määräys ja mallipohja tulevat myös saataville: <https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset>
- **Tietoturvasuunnitelmasta järjestetään koulutustilaisuus** kevättalvella 2022. Lisätietoja tulossa myöhemmin: <https://thl.fi/fi/ajankohtaista/tapahtumat/tapahtumakalenteri>
- Tämä esitys löytyy: <https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/ajankohtaista/tapahtumia-ja-koulutuksia>





**Kiitos!**