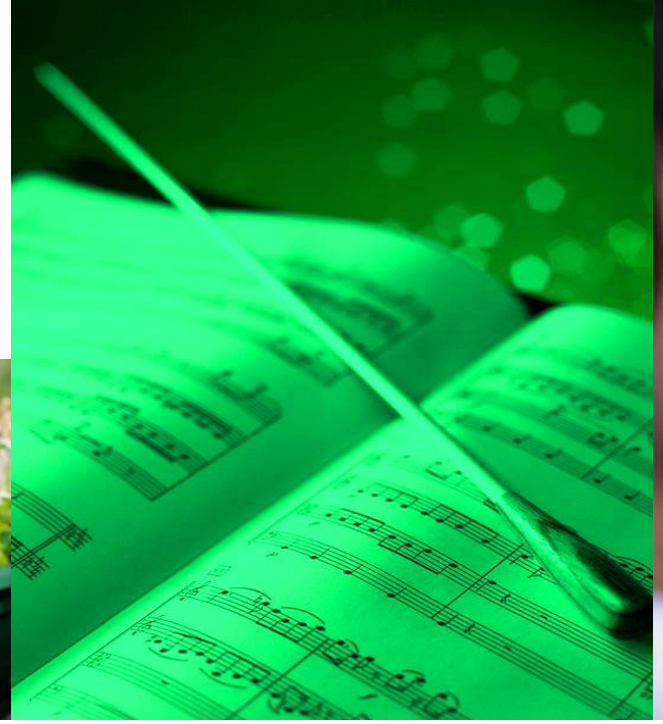


Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista sekä Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista

Asiakastietolain täytäntöönpanoa ohjaavat määräykset -infotilaisuus
9.12.2021

Juha Mykkänen

Terveyden ja hyvinvoinnin laitos

Tässä esityksessä

- Sertifiointi ja olennaiset vaatimukset – perusteet ja yleiskuva
  - Lakiperusteet
  - Määräysten sisältö - yleiskuva
  - Olennaisten vaatimusten kokonaisuus ja profiilit
  - Järjestelmien luokittelu ja sertifiointi
  - Rajaukset
- Mikä ennallaan, mikä muuttuu
  - Suhteessa aiemmin voimassa olleisiin säädöksiin
  - Lausuntokierroksen pohjalta tehdyt muutokset
- Yhteenveto




Sertifiointi ja olennaiset vaatimukset – perusteet ja yleiskuva

Asiakastietolain avainkohdat järjestelmien luokittelun, olennaisten vaatimusten ja sertifioinnin näkökulmasta

- 3 § **Määritelmät**
- 27 § Tietoturvasuunnitelma
- 29 § Tietojärjestelmien ja hyvinvointisovellusten **käyttötarkoitus** ja **luokittelu**
- 30 § Tietojärjestelmien ja hyvinvointisovellusten **rekisteröinti**
- 31 § Tietojärjestelmän ja hyvinvointisovelluksen **ottaminen tuotantokäyttöön**
- 32 § Tietojärjestelmän ja hyvinvointisovelluksen **käyttöönoton jälkeinen seuranta**
- 33 § **Tietojärjestelmäpalvelun tuottajan ja valmistajan** sekä hyvinvointisovelluksen valmistajan yleiset velvollisuudet
- 34 § Tietojärjestelmälle ja hyvinvointisovellukselle asetettavat **olennaiset vaatimukset**
- 35 § **Vaatimustenmukaisuuden osoittaminen**
- 36 § **Yhteentoimivuuden testaaminen**
- 37 § **Tietoturvallisuuden arviointi**
- 38 § Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus
- 39 § Ohjaus, valvonta ja seuranta
- 40 § Tietojärjestelmien valvonta ja tarkastukset
- 41 § Ilmoittaminen tietojärjestelmän **olennaisten vaatimusten poikkeamista**
- 52 § Siirtymäsäännökset

Määräys 4/2021 sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista

1 Määräyksen tarkoitus

2 Määräyksen soveltamisala

3 **Määritelmät**

4 Määräyksen **rajaukset** ja suhde muihin määräyksiin ja dokumentteihin

5 Tietojärjestelmien **luokittelu**

6 Tietojärjestelmän **käyttötarkoituksen** kuvaaminen ja **selvitys** olennaisten vaatimusten täyttämisestä

7 **Sertifiointiprosessi**

- 7.1 Sertifiointiprosessiin liittyvät velvoitteet
- 7.2 Yhteistestauksen sisältö ja tulokset
- 7.3 Tietoturvallisuuden arvioinnin sisältö ja tulokset

8 Tietojärjestelmän **rekisteröinti**

9 Tietojärjestelmän **käyttöönotto**

10 Vaatimustenmukaisuuden **uudistaminen**

11 Ohjaus ja neuvonta

12 Voimaantulo ja **siirtymäsäännökset**

Liite 1 Esimerkkejä järjestelmien **luokittelusta**

Liite 2 Luokkaan A kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien **muutosten** ilmoittaminen

HUOM. Tietojärjestelmän luokittelusta ja sertifioinnista vastaa tietojärjestelmäpalvelun tuottaja!

Määräys 5/2021 sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista

1 Määräyksen tarkoitus

2 Määräyksen soveltamisala

3 Määräyksen keskeinen sisältö ja rajaukset

4 Suhde muihin määräyksiin, ohjeisiin ja määrityksiin

5 Olennaiset **toiminnalliset vaatimukset**

6 Olennaiset **tietoturvallisuusvaatimukset**

7 Vähimmäisvaatimusten **profiilit**

8 Olennaisten **vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja**

9 Olennaisten **vaatimusten täyttäminen / palvelunantaja**

10 Olennaisten vaatimusten todentamisen tarkennuksia

- 10.1 Vaatimusten täyttymisen arviointi järjestelmissä, jotka eivät liity Kanta-palveluihin
- 10.2 Vaatimusten täyttymisen arviointi ja **todentamistavat** sertifioinnissa
- 10.3 Vaatimusten ja määrittelyjen **versionhallinta**
- 10.4 **Poikkeamat** vaatimustenmukaisuudesta

11 Ohjaus ja neuvonta

12 Voimaantulo ja siirtymäsäännökset

Liite 1 Olennaisten vaatimusten **soveltamisohjeet**

Liite 2 **Olennaisten vaatimusten luokitus**

Liite 3a-3g Vähimmäisvaatimusten **profiilit**

Liite 4 **Järjestelmälomake**

Olennaisten vaatimusten toteuttamisesta tietojärjestelmään ja todentamisesta vastaa valmistaja / tietojärjestelmäpalvelun tuottaja
Palvelunantajan osaltaan huolehdittava että käytetyt tietojärjestelmät täyttävät olennaiset vaatimukset ja vastaavat palvelunantajan toimintaa

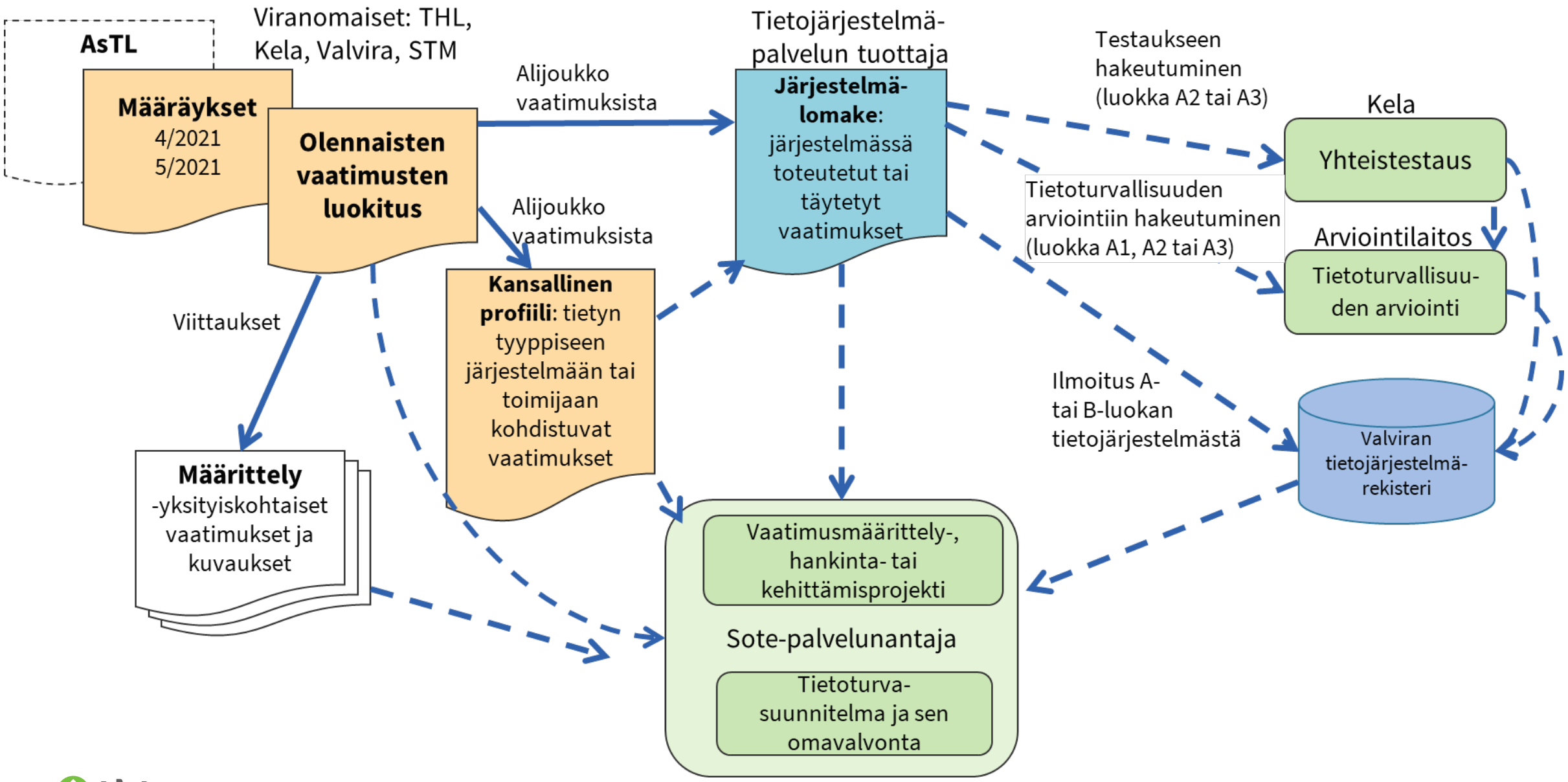
Lähtökohtia / Määräykset 4 ja 5/2021: asiakastietolain 784/2021 mukaiset sote-tietojärjestelmiin kohdistuvat olennaiset vaatimukset

- **I Toiminnalliset vaatimukset**
  - Kuvattava **käyttötarkoitus**, tietojärjestelmäpalvelun tuottajan annettava **selvitys** toiminnallisten vaatimusten täyttymisestä (A- ja B-luokan järjestelmät)
  - *Ei todenneta erikseen* osana sertifiointiprosessia, määräysten 4-5/2021 kautta selvitys voidaan antaa vertailtavalla tavalla ja sertifiointia / rekisteröintiä tukien
- **II Yhteentoimivuuden vaatimukset**
  - *Todennetaan* luokan A2 ja A3 järjestelmille (Kanta-palveluihin liittyvät) Kelan yhteistestauksen kautta
- **III Tietoturvavaatimukset**
  - *Todennetaan* luokan A (A1, A2, A3) järjestelmille tietoturvallisuuden arviointilaitoksen suorittamassa tietoturvallisuuden arvioinnissa
- Yhteentoimivuuden ja tietoturvallisuuden vaatimukset nojautuvat toiminnallisiin vaatimuksiin
  - käyttötarkoitus ja siitä annettu kuvaus, järjestelmää koskevat olennaiset vaatimukset

Olennaisten vaatimusten toteuttamisesta tietojärjestelmään vastaa tietojärjestelmäpalvelun tuottaja
Palvelunantajan on varmistettava olennaisten vaatimusten toteutuminen käyttämissään tietojärjestelmissä

Miten olennaisia vaatimuksia käytetään?

Määräys 5/2021 liite 1 luku 2 (kokoaa useita määräysten 4 ja 5 kohtia)



thl

Olennaisten vaatimusten luokitus

Määräys 5/2021 liite 2

- Kokoaa kansallisesti eri säädösten ja määrittelyjen pohjalta määritellyt olennaiset vaatimukset seuraavissa luokissa
  - **Toiminnot** (järjestelmien toiminnalliset ominaisuudet)
  - **Tietosisällöt** (järjestelmien tuottamat tai hyödyntämät tiedot)
    - erityisesti asiakastiedot, erityisesti ne joihin kohdistuu kansallisia määrittelyjä tai joita toteutetaan Kanta-palveluihin liittyvissä järjestelmissä)
  - **Tietoturvallisuusvaatimukset**
- Kukin vaatimus sisältää viittaukset sen pohjana oleviin säädöksiin tai määrittelyihin, yhteydet muihin vaatimuksiin ja sertifiointiin (yhteistestauksen testauspaketti tai tietoturva-auditoitavat vaatimukset)

Ryhmä	Id	Otsikko	Selite	Lähde	Sertifiointi	Tietosisällön muoto		Yhteydet muihin vaatimuksiin	Tarkennuksia / huomautuksia / lisätietoja
TKUV			Kuvantaminen						
	TKUV01	Kuva-aineistot	Radiologisen kuvantamisen kuva-aineistot kuten natiiviröntgentutkimukset, uä-tutkimukset, magneettitutkimukset, TT-tutkimukset, varjoainetutkimukset, ja niihin liittyvät DICOM-tutkimukset ja tutkimusobjektit	Kvarkki tekninen määrittely versio 2.1.1 / 6.6.2016 -> Kuva-aineistojen arkisto (Kvarkki) - tekninen määrittely, versio 2.3.5 / 17.04.2020; Aiempi vaiheistusasetus	Kvarkki	N	R	Toiminnot: KUV04, KUV06, KUV09, KUV11, KUV12, KUV13, KUV14	Kuvantamistutkimukseen kuuluvat kuvat eivät ole rakenteista dataa (paitsi kuva-objektia vastaavat esim. EKG-käyrät), mutta kuva-aineistoihin liittyy rakenteisia tietoja, jotka DICOM standardi määrittelee

LUONNOS

Olennaisten vaatimusten profiilit

Määräys 5/2021 liitteet 3a-3g

- Kansallisten vähimmäisvaatimusten koonti aihekohtaisesti – profiilin mukaiset vaatimukset toteutettava järjestelmissä, joissa profiilin mukainen käyttötarkoitus
- Yhdessä järjestelmässä voi olla toteutettuna useita profiileja
  - 3a Sähköisen reseptin profiilit (2 profiilia)
  - 3b Kanta-arkistopalveluihin liittyvien järjestelmien vähimmäisvaatimusprofiilit (4 profiilia)
  - 3c Potilastiedon arkiston profiilit (3 profiilia, joista 1 UUSI)
  - 3d Sosiaalihuollon asiakastiedon arkiston profiilit (julkaistaan myöhemmin)
  - 3e Kuvantamisen profiilit (5 AIEMMAT KORVAAVAA profiilia)
  - 3f Todistusten profiilit (3 profiilia)
  - 3g Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1) (1 UUSI profiili)

LUONNOS

Järjestelmien luokittelu ja riskitaso

Määräys 4/2021 luku 5 ja liite 1

- Luokittelu:
  - **A3:** ”Kanta-palveluihin liittyvät pää- ja kokonaisjärjestelmät”
    - myös *kriittiset* esim. julkisen terveydenhuollon päivystysvastuuseen liittyvät)
  - **A2:** ”Kanta-palveluihin liittyvät osajärjestelmät ja erillisjärjestelmät”
  - **A1:** ”Tietoturvallisuuden arviointia edellyttävät, joilta ei edellytetä yhteistestausta”
  - **B:** Muut asiakastietojen käsittelyyn tarkoitetut
  - Luokittelemattomat: käyttötarkoituksena ei asiakastietojen käsittely
- Lisätietoja ja tarkennuksia mm. määräys 4/2021 liitteessä 1

- Luokittelun merkitys olennaisten vaatimusten, sertifioinnin ja ilmoitusten näkökulmasta:
  - Kaikki luokkiin B, A1, A2, A3 kuuluvat: täytettävä käyttötarkoitusta vastaavat olennaiset vaatimukset, ilmoitettava Valviran tietojärjestelmärekisteriin
  - A1 lisäksi: tietoturvallisuuden arviointi, tietoturvallisuustodistus
  - A2 ja A3 lisäksi: yhteistestaus
- Järjestelmän riskitaso (perustaso / korkea) voi vaikuttaa luokitteluun ja mm. tietoturvavaatimusten todentamiseen
  - mm. asiakastietojen käsittelyn laajamittaisuus,

Sertifiointi suhteessa kehitystyöhön ja käyttöönottoihin

Määräys 5/2021 liite 1 luku 5, Määräys 4/2021 luku 7

Kehitystyö

- Vaatimusten selvittäminen ja ratkaisun suunnittelu
- Järjestelmäkehitys
- Dokumentointi
- Toimittajan oma testaus

Valmistaja / tj-palvelun tuottaja

Sertifiointi

(luokka A)

- Hakeutuminen sertifiointiin
- Yhteistestaus (luokka A2, A3)
- Tietoturvallisuuden arviointi (luokka A1, A2, A3)

Valmistaja / tj-palvelun tuottaja

Kela

Arviointi-laitos

Käyttöönotto, tuotanto ja päivitykset

- Ilmoitus Valviralle (luokka A tai B)
- Käyttöönotto, käyttöönottokoe
- Tuotantokäyttö
- Muutokset järjestelmään, muutosilmoitukset

Valvira

Valmistaja / tj-palvelun tuottaja

Kela

Sote-palvelunantaja

Kela

Arviointi-laitos

Rajauksia / määräykset 4/2021 ja 5/2021

- Määräykset 4/2021 ja 5/2021 kohdistuvat tietojärjestelmiin, ei hyvinvointisovelluksiin (joille määräys 6/2021)
- Määräykset eivät vaikuta esim. asiakastietolaissa asetettuihin sote-toimijoiden Kanta-liittymisvelvoitteiden aikatauluihin
- Määräykset kohdistuvat asiakastietolain määritelmän mukaisiin tietojärjestelmiin
  - Tietojärjestelmä tai osa sitä voi olla myös lääkinnällisten laitteiden säädösten tarkoittama lääkinnällinen laite, jolloin valmistajan huomioitava lääkinnällisten laitteiden säädösten mukaiset luokittelut ja vaatimukset – tämä arviointi riippumaton esim. asiakastietolain mukaisesta luokittelusta
  - Sertifioitavia tietojärjestelmiä eivät myöskään ole yleiskäyttöiset ohjelmistot tai alustat itsessään
- Asiakastietojärjestelmien sertifioinnissa ei ole kyse EU:n yleisen tietosuoja-asetuksen mukaisesta rekisterinpitäjään tai henkilötietojen käsittelijän sertifioinnista
- Toisiolain mukaiset käyttötarkoitukset ja Findatan määräys tietoturvallisten käyttöympäristöjen vaatimuksista eivät asiakastietolain nojalla annettujen määräysten piirissä: tieteellinen tutkimus, tilastointi, opetus, viranomaisen suunnittelu- ja selvitystehtävät




Mikä ennallaan, mikä muuttuu suhteessa aiemmin voimassa olleisiin säädöksiin

Ennallaan suhteessa aiempiin määräyksiin mm.

- Pääosa yksityiskohtaisista toiminnallisista-, tietosisältö- ja tietoturvallisuusvaatimuksista
- Tietojärjestelmäpalvelun tuottajan perusvastuut käyttötarkoituksen määrittelyssä, järjestelmän luokittelussa, sertifioinnissa ja ilmoittamisessa Valviran tietojärjestelmärekisteriin
- Olennaisten vaatimusten kohdistuminen toiminnallisuuteen, yhteentoimivuuteen ja tietoturvaan
- Olennaisten vaatimusten luokituksen, profiilien ja järjestelmälomakkeen hyödyntäminen
- Sertifiointiprosessin perusvaiheet ja vastuut

Olennaisten vaatimusten ja sertifioinnin keskeisiä muutoksia verrattuna aiempiin säädöksiin

- Järjestelmien **luokittelu** täsmentyy (B, A1, A2, A3)
  - Tietoturva-auditoitavaksi myös muita kuin Kanta-palveluihin liittyviä järjestelmiä (A1)
  - Järjestelmien käyttötarkoituksen, kriittisyyden, laajuuden ja käsiteltyjen sisältöjen huomiointi vaatimusten kohdistamisessa ja todentamisessa – järjestelmän **riskitason** huomiointi vaatimuksissa ja todentamisessa
- **Tietoturvavaatimukset** osaksi **samaa perusrakennetta** kuin toiminnalliset vaatimukset (= toiminnot ja tietosisällöt)
  - Ei erillistä tietoturvavaatimusten määräystä, poistettu päällekkäisyyksiä
  - Tietoturvavaatimuksista oma osio olennaisten vaatimusten luokitukseen (ks. määräys 5/2021 Liite 2)
  - Tietoturvavaatimukset osaksi profiileja (= järjestelmän käyttötarkoituksen aiempaa parempi huomiointi)
  - Myös **tekninen tietoturvatestaus** korkean riskitason järjestelmien todentamistavaksi
  - **Tietoturvallisuustodistuksen** roolin selkeyttäminen
- **Uusien järjestelmäratkaisujen** nykyistä parempi huomiointi, mm.
  - Palveluntuottajan oman toimintaympäristön ulkopuolelta hankittavien tai käytettävien palvelujen huomiointi tietojärjestelmiin kohdistuvissa tietoturvallisuusvaatimuksissa
  - Modulaariset järjestelmäkokonaisuudet, operatiivisen käytön tietoaltaat, jne.
- **Merkittävät poikkeamat** määritelty
- AsTL 34 §: **palvelunantajan käyttämien tietojärjestelmien** on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset
  - esim. suun terveydenhuollon palveluissa oltava käytössä Suun terveydenhuollon järjestelmäprofiilin mukaiset vaatimukset täyttävä järjestelmä

Lausuntokierroksen tuloksia / olennaisten vaatimusten ja sertifioinnin määräykset 4-5/2021

- Lausunnonantajia 34+1, satoja huomioitavia kommentteja
  - Enemmistö kokenut tarpeelliseksi ja ymmärrettäväksi
  - Monia erinomaisia kommentteja selkeyden ja sisällön parantamiseksi →
- Järjestelmien **luokitteluperusteita** (B, A1, A2, A3) selkeytetty
- **Kuvantamisen** olennaisten vaatimusten kohdistuminen muuttuu aiemmin voimassa olleisiin määräyksiin verrattuna
- Tietosuojanäkökulmasta nojaudutaan luonnosversioita selkeämmin **EU/ETA-tasoisiin käytäntöihin**, esim. tietojen käsittely ja siirto EU/ETA-alueella vastaavilla suojatoimenpiteillä kuin Suomessa
- Tiukimmat kansallisen varautumisen vaatimukset kohdistetaan tarkemmin **kriittisimmissä palveluissa** käytettäviin tietojärjestelmiin
- Useita riskipohjaisen lähestymistavan terävöittämiseen kohdistuvia lausuntoja - järjestelmän **luokittelu JA riskitaso** ohjaamaan erityisesti tietoturvavaatimusten todentamista
- Vaatimusten kohdistamista ja todentamista selkeytetään (myös eri toimittajien) **osajärjestelmistä** koostuvissa kokonaisuuksissa
- Tietojen **laadun ja yhteentoimivuuden** perusvaatimuksia täsmennetään – mm. kansallisten koodistojen käytön perusvaatimus
- Tukimateriaaliksi tulossa mm. **riskiarviotyökalu** ja vaatimukset ja profiilitiedot kokoava **koontitaulukko**

Olennaisten vaatimusten määräykset – olennaista tietojärjestelmäpalvelun tuottajan näkökulmasta

- Tietojärjestelmäpalvelun tuottajan ja valmistajan perusvastuut ja pääosa vaatimuksista eivät muutu aiemmasta, mutta omien tuotteiden ja palvelujen osalta on syytä tarkistaa ja tarvittaessa päivittää asiat:
  1. Kuvaa järjestelmän käyttötarkoitus ja määrittele järjestelmän luokka
  2. Perehdy olennaisiin vaatimuksiin
     - Mitkä profiilit ja vaatimukset (5/2021) relevantteja järjestelmän käyttötarkoituksen näkökulmasta - dokumentoi järjestelmälomakkeella
     - Hyödynnä vaatimukset kokoava materiaali
  3. Huomioi relevantit olennaiset vaatimukset järjestelmän suunnittelussa, toteuttamisessa, dokumentaatiossa, ohjeistuksissa
  4. Testaa itse ja varmista laatu, turvallisuus ja vaatimustenmukaisuus
  5. Sertifioi järjestelmä, jos se kuuluu luokkaan A1, A2 tai A3
  6. Tee ilmoitus Valviran tietojärjestelmärekisteriin ennen tuotantokäyttöönottoa
  7. Huomioi vastuut ja vaatimukset sopimuksissa (asiakassopimukset, kumppanuudet), tue asiakkaita käyttöönotossa ja olennaisten vaatimusten toteutumisen varmistamisessa
  8. Huolehdi muutoshallinnasta ja päivityksistä sekä olennaisten vaatimusten seurannasta




Yhteenveto

Määräykset 4/2021 ja 5/2021

Yhteenveto määräyksistä 4 ja 5 /2021: olennaisten vaatimusten, luokittelun ja sertifioinnin määräykset – ohjaavat ja tukevat:

- **Kokoavat** keskeisimmät säädösten ja kansallisten määritysten kautta tietojärjestelmiin, tietosuojaan ja tietoturvallisuuteen asiakastietojen käsittelyssä kohdistuvat vaatimukset
- **Tukevat tietojärjestelmien valmistajia ja tietojärjestelmäpalvelujen tuottajia** lakisääteisten vaatimusten ja velvoitteiden tulkinnassa ja täyttämisessä sekä omien ratkaisujen toiminnallisten ominaisuuksien määrittelemisessä suhteessa määrittelyihin
    - myös suhteessa kumppaneihin ja ”työnjakoon” eri järjestelmien välillä
    - esim. sama *järjestelmälomake* yhteistestauksessa, auditoinnissa ja rekisteri-ilmoituksissa
- Selkeyttävät valtakunnallisten palvelujen kehittämiseen liittyvien määrittelyjen ja niihin liittyvien kehitys-, yhteistestaus- ja sertifiointitoimenpiteiden rakennetta
    - mukaan lukien muutoshallinta ja riippuvuuksien hallinta
- **Tukevat sote-palvelujen tuottajia ja järjestäjiä** omien tietojärjestelmäratkaisujensa olennaisten vaatimusten täyttämisessä, ml. sote-uudistuksen yhteydessä tehtävä suunnitt
    - riskien hallinta, toimialasidonnaisten tietojärjestelmien keskeiset ominaisuudet
    - tietoturvallisuuden, tietosuojan ja tiedonhallinnan jatkumon muodostaminen mm. tietoturvasuunnitelmaan liittyen (ks. myös määräys 3/2021)

Tulossa

- Koulutus sote-tietojärjestelmien olennaisista vaatimuksista ja sertifioinnista 15.12.2021, ohjelmatiedot tarkentumassa THL tapahtumakalenteriin
  - Pääkohderyhmä tietojärjestelmäpalvelujen tuottajat
  - Syvempää ja yksityiskohtaisempaa läpikäyntiä useimmista tässä esityksessä näkyneistä aiheista – ei kuitenkaan kattavasti kaikista vaatimussisällöistä..
  - Alustajina asiantuntijoita / THL, Kela, Valvira
- Koulutus tietoturvasuunnitelmista (alkuvuosi 2022)

Kiitos!