



Lounais-Suomen aluehallintovirasto
Varsinais-Suomen hyvinvointialue

**Varsinais-Suomen
puuttuminen**

hyvinvointialueen

tietoturvasuunnitelman

Sisällys

ASIAN VIREILLETULO	3
SELVITYS.....	3
RATKAISU.....	4
1 Selvitykset	4
1.1 Varsinais-Suomen hyvinvointialueen selvitys	4
1.2 Lounais-Suomen aluehallintoviraston selvitys ja lausunto	5
1.3 Valviran selvitys ja lausunto	7
2 Oikeusohjeet	9
2.1 Perus- ja ihmisoikeudet.....	9
2.2 Tietosuoja-asetus.....	10
2.3 Tietosuoja laki ja hallintolaki.....	10
2.4 Tiedonhallintalaki ja sen perusteella laaditut suositukset.....	10
2.5 Sähköinen asiakastietolaki / asiakastietolaki	11
2.6 Hyvinvointialueen omavalvontaa koskeva sääntely.....	14
2.7 Valviran ja aluehallintovirastojen valvontaa koskeva sääntely	17
2.8 Terveysten ja hyvinvoinnin laitoksen määräys	18
3 Arviointi	19
3.1 Varha ja tietoturvasuunnitelman puuttumisen merkitys	19
3.2 Tietoturvasuunnitelman laatimisvelvoitteen tausta	22
3.3 Hyvinvointialueen velvoite suojata yksityiselämään kuuluvia tietoja	24
3.4 Valvonnan vireilletulo	26
4 Johtopäätökset.....	27
5 Toimenpiteet.....	28

ASIAN VIREILLETULO

Varsinais-Suomen hyvinvointialueelle (Varha) 15.11.2023 tehdyn laillisuusvalvontakäynnin yhtenä aiheena oli hyvinvointialueiden valvontaa koskeva suunnittelu ja sen toimeenpano.

Laillisuusvalvontakäynnillä saadun tiedon mukaan hyvinvointialueen omavalvontaa toteuttava Varhan hyvinvointialueen valvontakeskus oli havainnut palveluntuottajayksikköihin kohdistuneessa valvonnassaan tietoturvasuunnitelmien laatimisessa puutteita. Myöskään Varhalla itsellään ei ollut tietoturvasuunnitelmaa organisaatiotason ohjaavana dokumenttina. Tietoturvasuunnitelman puuttumisen havainneesta valvontakeskuksesta oli pyydetty Lounais-Suomen aluehallintoviraston ohjausta siihen, miten lakisääteisen dokumentin puute tulisi arvioida osana palveluntuottajien valvontaa.

Otin Varhan oman tietoturvasuunnitelman puuttumisen sekä tietoturvasuunnitelman laatimista koskevan valvonnan tutkittavaksi valtioneuvoston oikeuskanslerista annetun lain 3 §:n 1 momentin tarkoittamana omana aloitteena.

SELVITYS

Pyysin 5.3.2024 Lounais-Suomen aluehallintovirastoa selvittämään, miten Varha on noudattanut tietoturvasuunnitelman laatimiseen ja omavalvonnan toteutukseen velvoittavia säännöksiä ja mihin toimenpiteisiin aluehallintovirasto oli ryhtynyt saatuaan tiedon hyvinvointialueen tietoturvasuunnitelman puuttumisesta. Pyysin aluehallintovirastoa myös antamaan asiassa lausunnon hyvinvointialueen menettelyn lainmukaisuudesta.

Lounais-Suomen aluehallintovirasto antoi 26.6.2024 siltä pyydetyn selvityksen ja lausunnon (LSAVI/3929/2024), jonka liitteenä oli 27.5.2024 päivätty Varhan hallintojohtajan tietoturvasuunnitelmaa koskeva selvitys. Liitteenä oli esimerkkinä myös yksi salassa pidettävä tietoturvasuunnitelma (Tyks Laboratoriot).

Pyysin tämän jälkeen vielä 10.9.2024 Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviraa antamaan selvityksensä siitä, miten Valvirassa on ohjattu ja tosiasiallisesti seurattu hyvinvointialueiden tietoturvasuunnitelmien olemassaoloa, lainmukaisuutta ja niiden ajantasaisuutta. Pyysin Valviraa myös antamaan asiassa lausuntonsa Varhan ja Lounais-Suomen aluehallintoviraston antamista selvityksistä.

Valvira antoi 22.11.2024 siltä pyydetyn lausunnon (Dnro V/36761/2024).

RATKAISU

1 Selvitykset

1.1 Varsinais-Suomen hyvinvointialueen selvitys

Varha on kertonut selvityksessään, että se on vastannut sosiaali- ja terveystalvelujen sekä pelastustoimen järjestämisestä 1.1.2023 alkaen. Hyvinvointialueen muodostavat 28 kuntaa, sairaanhoitopiiri, erityishuollon palvelut sekä pelastuslaitos. Työntekijöitä on noin 24 000. Selvityksensä mukaan Varha on perinyt näiden organisaatioiden sosiaali- ja terveydenhuollon tietojärjestelmät ja toimintatavat, joita pyritään yhtenäistämään. Lähtökohtana oli 47 potilas- ja asiakastietojärjestelmää, joita on saatu vähennettyä niin, että määrä on nyt 15.

Varha on kilpailuttanut asiakas- ja potilastietojärjestelmät ja tavoitteena on, että tulevaisuudessa sillä olisi vain yksi sosiaalihuollon asiakastietojärjestelmä ja yksi perusterveydenhuollon potilastietojärjestelmä. Näiden järjestelmien käyttöönotto alkaa vuonna 2024. Tätä ennen on rakennettu pohjatyönä yhtenäistä tietoverkkoa. Tietoturvasuunnitelmaa on edellytetty jo aiemmassa sähköisessä asiakastietolaissa ja se on ollut silloin kuntien ja kuntayhtymien vastuulla. Valitettavasti kaikki eivät olleet laatineet tätä suunnitelmaa, eivätkä epäyhtenäiset kuvaukset, joiden ylläpito on vaihdellut, ole olleet hedelmällinen lähtökohta Varhan tasoisen suunnitelman laatimiseksi. Varhalla on kuitenkin esimerkiksi laboratorion kriittisiä järjestelmiä ja sairaala-apteekkia koskevat tietoturvasuunnitelmat. Todetun täydellisen tietojärjestelmä- ja tietoverkkomuutosten vuoksi ei ole kuitenkaan ollut tarkoituksenmukaista rakentaa perusteellisempaa yhtä Varhan tietoturvasuunnitelmaa vanhojen tietojärjestelmien pohjalle.

Varhan selvityksen mukaan se on lähestynyt asiaa hallintosääntönsä kautta, jonka tiedonhallintaa ja asiakirjahallinnon järjestämistä koskevassa luvussa kuvataan muun muassa tietoturvallisuusjärjestelyjä koskevat vastuut. Tämän pohjalta on laadittu tiedonhallintapolitiikka, jonka aluehallitus on hyväksynyt 6.6.2023. Kyseinen politiikka sisältää myös tietosuoja- ja tietoturvalitiikan. Politiikka kuvaa, miten Varha laatii tiedonhallintamallin ja ylläpitää sitä. Tiedonhallintamalli koostuu toimintaprosessien, tietovarantojen ja tietojärjestelmien sekä niihin liittyvien turvallisuustoimenpiteiden ja arkistointimenettelyjen kuvauksista. Ajatuksena on, että asiakastietolain mukainen tietoturvasuunnitelma koostetaan näistä ylläpidetyistä tiedoista.

Varhan näkemyksen mukaan tietoturvasuunnitelma ei ole pelkkä lain edellyttämä dokumentti, vaan pitää olla myös keinot, joilla osoitetaan kuvauksen paikkansapitävyys, arvioidaan sen valmiusaste sekä varmistetaan kuvauksen ajantasaisuus. Tämän tavoitteen saavuttamiseksi Varha on hankkinut joulukuussa 2023 työvälineen, jolla voidaan toteuttaa nämä vaatimukset. Valitettavasti työ on vielä kesken ja Varhan organisaation järjestäytyminen 34 toimijasta sekä

taloudelliset haasteet ovat hidastaneet asian valmistelua. Järjestelmästä saadaan muun muassa sekä itse tietoturvasuunnitelma että johdolle tarkoitettu raportti, joka kuvaa sen valmiusastetta. Varha on pyrkinyt määrätietoisesti laatimaan asiakastietolain mukaisen tietoturvasuunnitelman luomalla edellytykset sen laatimiseksi, ylläpitämiseksi ja tosiasialliseksi hyödyntämiseksi. Tilanne tietoturvasuunnitelman sisällön osalta on keskeneräinen. Asia on kuitenkin siltä osin hallinnassa, että valmistelutyö on käynnissä ja luodun raportointijärjestelmän ansiosta tiedetään, missä asian osalta mennään nyt ja tulevaisuudessa.

Omavalvonnan osalta Varha on todennut, että sillä on omavalvontaohjelma, joka löytyy Varhan internet-sivuilta. Ohjelma on päivitettävänä johtuen valvontalain voimaantulosta 1.1.2024 sekä siihen liittyvästä Valviran 15.5.2024 julkaisemasta määräyksestä koskien sosiaali- ja terveydenhuollon palveluntuottajan palveluyksikkökohtaisen omavalvontasuunnitelman sisältöä, laatimista ja seuranta. Varha on lisäksi ohjeistanut sosiaalihuollon omavalvontasuunnitelman laatimisesta ja kyseisessä ohjeistuksessa on myös tietosuojaan ja tietoturvaan liittyviä kohtia. Päivityksen jälkeen sekä omavalvontaohjelma että ohjeistus omavalvontasuunnitelmien laatimisesta tulevat koskemaan sekä terveydenhuoltoa että sosiaalihuoltoa.

Varhan selvityksensä liitteenä toimittaman Tyks Laboratorioiden tietoturvasuunnitelman mukaan vastuu tietoturvasuunnitelman laatimisesta on hyvinvointialuejohtajalla.

1.2 Lounais-Suomen aluehallintoviraston selvitys ja lausunto

Lounais-Suomen aluehallintoviraston selvityksen mukaan Varhan valvontakeskuksen kumppanuuspäällikkö oli 18.10.2023 lähettänyt aluehallintoviraston sosiaali- ja terveystalouden rekisteröinnit -yksikön päällikölle muun ohella tietoturvasuunnitelman puuttumista koskevan viestin, jonka tämä oli välittänyt edelleen 1.10.2023 aloittaneelle sosiaali- ja terveydenhuollon kan-
telut ja valvonnat -yksikön päällikölle. Viestissä todettiin:

”Kun yksikkökäynneillä tiedustelemme tietoturvan toteutumista ja suunnitelman mukaista toimintaa, törmäämme jatkuvasti tilanteeseen, jossa vaatimus ei nyt toteudu. Olemme linjanneet lakisääteisen ohjausdokumentaation puutteen vakavaksi poikkeamaksi, ja tämä herättää keskustelua. Suunnitelman luomisessa on Varhalla ollut haasteita, huolimatta siitä, että asiaa on toistuvasti nostettu esille.”

Aluehallintoviraston selvityksen mukaan päälliköiden tarkoituksena oli keskustella annettavasta ohjeistuksesta yhdessä. Asia jäi kuitenkin muiden kiireiden (kuten esimerkiksi kahteen yksikköön jakautuminen ja uuden päällikön aloittaminen tehtävässään sekä valvontalain voimaantuloon valmistautuminen) jalkoihin ja kumppanuuspäällikön viestiin vastaaminen valitettavasti unohtui. Kumppanuuspäällikkö ei myöskään ottanut asian tiimoilta uudelleen yhteyttä. Viestissä ei myöskään pyydetty aluehallintoviraston linjasta siihen, miten lakisääteisen dokumentin

puute tulisi arvioida osana palveluntuottajien valvontaa. Aluehallintoviraston tiedossa ei ole, että tällaista tietoturvasuunnitelman puuttumiseen liittyvää linjausta olisi pyydetty muullakaan tavoin.

Aluehallintoylilääkärit olivat kuitenkin syksyllä 2023 kiinnittäneet huomiota siihen, että aluehallintovirastolle tiedoksi tulleissa Varhan tarkastuskertomuksissa Varhan organisaation tietoturvasuunnitelman puuttuminen oli kirjattu vakavaksi poikkeamaksi. Aluehallintoylilääkärit olivat 8.11.2023 lähettäneet Varhan valvontakeskukselle (valvontakoordinaattorille ja kumppanuuspäällikölle) ohjaavan sähköpostin, jonka mukaan kyseistä puutetta ei tarvitsisi kirjata yksikköä koskevaksi vakavaksi poikkeamaksi, koska se koskee taustaorganisaatiota (Varhaa). Aluehallintoylilääkärit ovat katsoneet, että lievän poikkeaman taso olisi tältä osin riittävä.

Aluehallintoviraston selvityksen mukaan kumppanuuspäällikön sähköpostiviestin varsinainen kysymys oli: ”olisiko tietoturvasuunnitelman puute tässä kohtaa hyvinvointialueen olemassaoloa luokiteltava 31.12.2023 asti voimassa olleen sosiaali- ja terveydenhuollon järjestämisestä annetun lain (612/2021, järjestämislaki) 44 §:n mukaiseksi asiakas- ja potilasturvallisuutta vaarantavaksi puutteeksi?” Kyseisen lainkohdan mukaan hyvinvointialueen on tullut ilmoittaa välittömästi palveluja valvovalle valvontaviranomaiselle palveluntuottajan tai tämän alihankkijan toiminnassa ilmenneet asiakas- ja potilasturvallisuutta olennaisesti vaarantavat epäkohdat ja puutteet.

Aluehallintovirasto on todennut, että riippumatta siitä, että aluehallintovirastosta jäi vastaamatta kumppanuuspäällikön viestiin, valvontakeskus olisi voinut joka tapauksessa tehdä järjestämislain 44 §:n mukaisen ilmoituksen aluehallintovirastolle. Silloin asia olisi tullut virallisesti kirjaa-mon kautta vireille aluehallintovirastossa. Aluehallintovirastoon ei kuitenkaan ole saapunut järjestämislain tai sittemmin valvontalain mukaista ilmoitusta tietoturvasuunnitelman puuttumisesta. Aluehallintovirasto ei myöskään ole oma-aloitteisesti pannut vireille tietoturvasuunnitelman puuttumiseen liittyvää valvonta-asiaa. Suunnitelman puuttuminen on kuitenkin tullut yksittäisten virkamiesten tietoon eri yhteyksissä vuosina 2023 ja 2024 ja tällöin asiasta on suullisesti ja / tai mahdollisesti sähköpostitse ohjattu. Yksittäisten virkamiesten taholta tapahtunutta ohjaamista ei ole kirjattu asianhallintajärjestelmään, joten sitä ei voida jälkikäteen tarkemmin todentaa.

Asiassa saamansa selvityksen perusteella aluehallintovirasto on todennut pyynnöstäni tämän asian tutkimiseksi antamassaan lausunnossa, että Varha ei ole noudattanut sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 27 §:ssä eikä sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 77 §:ssä säädettyä velvollisuutta laatia tietoturvasuunnitelma. Aluehallintovirasto on todennut lausunnossaan, että sen näkemyksen mukaan on ymmärrettävää, että Varhan kokoisessa organisaatiossa yhteisen tietoturvasuunnitelman laatiminen on ottanut aikaa. Hyvinvointialueet ovat kuitenkin olleet toiminnassa vuoden 2023 alusta lähtien, ja velvollisuus laatia tietoturvasuunnitelma on ollut voimassa koko tämän

ajan. Aluehallintovirasto on ilmoittanut minulle antamassaan lausunnossa näkemyksensä myös, että tietoturvasuunnitelman laatiminen ja lainvastainen tilanne on kestänyt kohtuuttoman pitkään ja tietoturvasuunnitelma tulee saattaa valmiiksi viipymättä. Tietoturvasuunnitelman laatimisen tueksi on olemassa Terveyden ja hyvinvoinnin laitoksen (THL) määräys ja mallipohja, ja asiaan on annettu myös koulutusta.

1.3 Valviran selvitys ja lausunto

Valviran lausunnon mukaan valvontaviranomaiset ovat tukeneet hyvinvointialueiden, Helsingin kaupungin ja HUS-yhtymän aloittaessa vuoden 2023 alussa erityisesti niiden omavalvontaa. Valvira on järjestänyt aluehallintovirastojen kanssa 5.5.-10.11.2022 kaikille tuleville hyvinvointialueille, Helsingin kaupungille ja HUS-yhtymälle yhteensä seitsemän eri koulutus- ja infotilaisuutta, joissa aiheena on ollut muun ohella hyvinvointialueen tietoturvasuunnitelman laatimiseen liittyvät mainittuna aikana voimassa olleen sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (784/2021) mukaiset velvoitteet, mukaan lukien 27 §:n mukainen tietoturvasuunnitelman laatiminen.

Valvira järjesti 11.4.2024 valtakunnallisen webinaarin sosiaali- ja terveydenhuollon palveluntantajille 1.1.2024 voimaan tulleen uuden sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023, asiakastietolaki) mukaisista velvoitteista. Webinaarin kohderyhmässä, viestinnässä ja kutsuissa painotettiin palveluntuottajista erityisesti kaikkia hyvinvointialueita, Helsingin kaupunkia ja HUS-yhtymää.

Webinaarin yhtenä puheenvuorona oli tietoturvasuunnitelman laatimista koskeva asiakastietolain 77 §:n mukainen velvoite sekä THL:n 20.2.2024 antama määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista (2/2024).

Valvira on laatinut vuonna 2024 asiakastietolain ja sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, toisiolaki) valvontaohjelman vuosille 2024-2027. Osana tämän valvontaohjelman toimeenpanoa Valvira on suunnitellut tekevänsä asiakastietolain vaatimuksiin (mukaan lukien tietoturvasuunnitelman laatiminen ja sisältövaatimukset) ohjaus- ja arviointikäyntejä hyvinvointialueille Helsingin kaupungille ja HUS-yhtymään vuosien 2025-2026 aikana. Valviran asianhallintajärjestelmään ei ole kirjattu vuosina 2023-2024 epäkohtailmoituksia tai valvonnan yhteydessä muuten saatua tietoa siitä, että yksittäinen hyvinvointialue, Helsingin kaupunki tai HUS-yhtymä ei olisi laatinut asiakastietolain 77 §:n mukaista tietoturvasuunnitelmaa. Asianhallintajärjestelmästä tehdyn haun perusteella Valviralla ei ole ollut vuosina 2023-2024 käsiteltävänä palvelunjärjestäjän tietoturvasuunnitelman puutteita koskevia valvonta-asioita.

Valvirassa on vireillä valtakunnallinen selvitys hyvinvointialueiden, Helsingin kaupungin ja HUS-yhtymän tietoturvasuunnitelman laatimisesta, ajantasaisuudesta ja ylläpidosta vastuussa olevasta tahosta. Valvira on lähettänyt 10.-11.10.2024 selvityspyynnot kaikille hyvinvointialueille, Helsingin kaupungille ja HUS-yhtymälle. Kun kaikki selvitykset on saatu, Valvira arvioi niiden perusteella toimenpiteidensä, mukaan lukien erillisen valvonnan, tarpeen ja tekee yhteistyötä aluehallintovirastojen kanssa. Selvityksen tietoja voidaan käyttää myös aiemmin mainittujen ohjaus- ja arviointikäyntien kohteiden valinnassa.

Valvira on viitannut THL:n 20.2.2024 antamaan määräykseen (3/2024) tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Määräyksen mukaan tietoturvasuunnitelman avulla kootaan sosiaali- ja terveydenhuollon toimijoiden tietoturvaluokituskäytäntöjä. Tietoturvasuunnitelmissa on oltava selvitykset siitä, miten asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan asiakastietolain 77 §:n 1 momentin kohtien 1-9 mukaisesti.

Oleellista on varmistua siitä, miten tietoturvaluokituksen omavalvonnan kohteessa nämä asiakastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset käytännössä varmistetaan. Tietoturvaluokituksen omavalvonnan kohteen velvollisuutena on toimia laatimansa tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää ja katselmoida suunnitelmaansa sekä seurata aktiivisesti sen toteutumista. Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvaluokituksen ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta.

Tietoturvasuunnitelma muun muassa edistää asiakas- ja potilastietojen turvallista käsittelyä, parantaa ja yhdenmukaistaa sosiaali- ja terveydenhuollon toimijoiden tietosuojaa ja tietoturvaa, vahvistaa tietoturvaluokituksen ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä sekä auttaa erityisesti hallitsemaan tämän päivän digitaaliseen turvallisuuteen liittyviä riskejä. Tietoturvasuunnitelman tarkoituksena on kuvata konkreettisesti sosiaali- ja terveystietojen tuottajan tietoturva- ja tietosuojakäytäntöjä. Organisaation velvollisuutena on toimia tietoturvasuunnitelman mukaisesti, katselmoida ja ylläpitää suunnitelmaa säännöllisesti sekä seurata aktiivisesti sen toteutumista.

Tietoturvasuunnitelman laatiminen sekä suunnitelmaan kirjattujen toimintaprosessien toimeenpano, jatkuva seuranta ja päivittäminen ovat merkittävä osa hyvinvointialueiden järjestämisvastuulle kuuluvien sosiaali- ja terveystietojen omavalvonnan kokonaisuutta. Valviran 8.5.2024 antaman määräyksen 1/2024 mukaan palveluntuottajan omavalvontasuunnitelmassa on kuvattava, milloin asiakastietolain mukainen tietoturvasuunnitelma on laadittu ja päivitetty sekä kuka palveluyksikössä vastaa sen toteutumisesta. Varsinaista tietoturvasuunnitelmaa ei kuitenkaan tule liittää palveluyksikkökohtaiseen ja julkaistavaan omavalvontasuunnitelmaan.

Valvira on todennut Varhan antaman selvityksen perusteella, ettei Varha ole noudattanut aikaisemmin voimassa olleen ja nykyisen asiakastietolain mukaista tietoturvasuunnitelman laatimisvelvoitetta. Vaikka Varha on tuonut selvityksessään esiin pyrkimyksen saada aktiivisesti tietoturvasuunnitelma laadituksi, selvityksestä ei esimerkiksi ilmene toteutuksen aikataulu eivätkä toteuttamisen konkreettiset välivaiheet ja toimenpiteet sekä tietoturvasuunnitelman, seurannasta ja toimeenpanosta vastaavat tahot. Selvityksestä ei myöskään ilmene Varhan omavallonnalliset toimenpiteet sen suhteen, miten hyvinvointialue huolehtii ja varmistaa ajankohtaisesti asiakas- ja potilastietojen turvallisen käsittelyn, tietosuojan ja tietoturvan sekä hallinnoi sen järjestämisvastuulle kuuluvien palveluiden digitaaliseen turvallisuuteen liittyviä riskejä konkreettisesti toiminnoissaan. Kun huomioidaan tietoturvasuunnitelman merkitys ja sen puuttuminen 1.1.2023 lähtien, Varhan epäasianmukaista menettelyä ja puutetta ei voida pitää vähäisenä.

2 Oikeusohjeet

Tietoturvalla tarkoitetaan sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 28 kohdan määritelmän mukaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Edellä mainitun lain yksityiskohtaisten perustelujen mukaan määritelmä tarkoittaa tietojen luotamuksellisuuden, eheyden ja käytettävyyden varmistamista hallinnollisin ja teknisin toimin. Näitä tietoturvatoimia ovat esimerkiksi laitteiden ja järjestelmien pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta. Lisäksi tietoturvatoimia ovat tietoliikenteen häirinnän valvonta ja sen estäminen. ([HE 221/2013 vp](#), s. 91)

Hyvinvointialueita velvoittaa tietoturvasta huolehtimiseen varsin monitasoinen seuraavassa tarkemmin erityisesti hyvinvointialueilta vaadittavien hallinnollisten toimien osalta avattu oikeudellinen sääntely ja muut oikeuslähteet.

2.1 Perus- ja ihmisoikeudet

Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohdan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.

Perustuslain 21 §:n 2 momentin mukaan hyvän hallinnon takeet turvataan lailla.

Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen.

2.2 Tietosuoja-asetus

Henkilötietojen käsittelyyn liittyvistä yleisistä velvoitteista säädetään Euroopan unionin yleisen tietosuoja-asetuksen (2016/679) IV luvussa. Niihin kuuluvat muun muassa tietojen käsittelytoimien suunnittelu ja riskien arvioiminen, tietojen käsittelyä koskevien ohjeiden antaminen ja noudattaminen, käsittelytoimia koskevan selosteen laatiminen, tietoturvaloukkauksesta ilmoittaminen ja tietosuojavastaavan nimittäminen.

2.3 Tietosuojalaki ja hallintolaki

Tietosuoja-asetusta ja sen kansallista soveltamista yleisesti täsmennetään tietosuojalailla (1050/2018).

Hallintolain (434/2003) 6 §:n mukaisiin hallinnon oikeusperiaatteisiin kuuluvan luottamuksen-suojan mukaan viranomaisen toimien on suojattava oikeusjärjestyksen perusteella oikeutettuja odotuksia.

2.4 Tiedonhallintalaki ja sen perusteella laaditut suositukset

Sosiaali- ja terveydenhuollon järjestämisestä annetun lain (612/2021, järjestämislaki) 58 §:n 1 momentin (714/2023) mukaan hyvinvointialueen sosiaali- ja terveydenhuollon palveluiden järjestämisestä vastaava toimivaltainen viranomainen on yleisessä tietosuoja-asetuksessa tarkoitettu rekisterinpitäjä sen järjestämisvastuulle kuuluvassa toiminnassa syntyneille sekä sille kuntien ja kuntayhtymien hallinnasta siirtyneille sosiaali- ja terveydenhuollon asiakas- ja potilastiedoille. Näistä asiakas- ja potilastiedoista ja niiden käsittelystä säädetään sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa (703/2023), julkisuuslaissa ja tietosuojalaissa.

Laissa julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) säädetään tiedonhallinnan järjestämisestä ja kuvaamisesta sekä tietoturvallisuuden toteuttamisesta. Hyvinvointialu-

eet ovat kyseisen lain 4 §:n 1 momentin 5 kohdan perusteella laissa tarkoitettuja tiedonhallintayksiköitä, jotka ovat myös velvollisia laatimaan lain 5 §:ssä tarkemmin säädetyn toimintaympäristönsä tiedonhallintaa määrittelevän ja kuvaavan tiedonhallintamallin.

Tiedonhallintalain 4 §:n 2 momentin 5 kohdan mukaan tiedonhallintayksikön johdon on järjestettävä riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta.

Tiedonhallintalain perusteella laaditussa julkisen hallinnon tietoturvallisuuden arviointikriteeristöissä (Julkri, [Valtiovarainministeriön julkaisuja 2023:46](#)) käytetään hallinnollisen turvallisuuden osa-alueen käsitettä kuvaamaan niitä menetelmiä, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Osa-alue kattaa yleisiä hallinnollisen turvallisuuden, henkilöstöturvallisuuden, tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. Hallinnollisen turvallisuuden kriteereillä pyritään siihen, että organisaatiolla on riittävän hyvin toimiva tietoturvallisuuden hallintajärjestelmä sekä menettelyt sen varmistamiseksi, että tietoja käsittelevä henkilöstö toimii asianmukaisesti. Organisaation tulee myös varmistaa, että tietojen käsittelyä koskevia velvoitteita noudatetaan tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Suhteessa lainsäädäntöön Julkri on vain suositus, sillä lainsäädännön vaatimukset voidaan täyttää muutoinkin kuin Julkrissa kuvatulla tavalla.

2.5 Sähköinen asiakastietolaki / asiakastietolaki

Sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettu laki (703/2023, asiakastietolaki) on tullut voimaan 1.1.2024. Lailla on kumottu laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021, sähköinen asiakastietolaki). Asiakastietolain säätämiseen johtaneessa hallituksen esityksessä ([HE 246/2022 vp](#), s. 9) todetaan, että tiedonhallintalakia sovelletaan julkisessa sosiaali- ja terveydenhuollossa siltä osin kuin erityislainsäädännössä ei toisin säädetä. Tiedonhallintalaki sisältää sääntelyä myös tietoturvallisuudesta, kuten tietoaaineistojen turvallisuudesta ja käyttöoikeuksista.

2.5.1 Tietoturvasuunnitelmaa koskeva sääntely 1.1.–31.12.2023

Sähköisen asiakastietolain tietoturvasuunnitelmaa koskevan 27 §:n 1 momentin mukaan palveluntajan, 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:

- 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 tietosuojan 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.

Saman lain 2 momentin mukaan ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa selvitettävä, miten tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu.

Lain 3 momentin mukaan Terveiden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta.

Sähköisen asiakastietolain 28 §:ssä on säädetty tietoturvallisuuden omavalvonnan toteuttamisesta ja vastuusta. Pykälän 1 momentin mukaan 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.

Lain 39 §:ssä on säädetty valvonnasta, ohjauksesta ja seurannasta. Pykälän 1 momentin mukaan sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan yleinen suunnittelu, ohjaus ja valvonta sekä päätöksenteko merkittävien tiedonhallintahankkeiden kokonaisrahoituksesta kuuluvat sosiaali- ja terveysministeriölle.

Saman pykälän 2 momentin mukaan Terveiden ja hyvinvoinnin laitos vastaa sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan sekä 6 §:ssä tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen ja yhteisten hallinnonalakohtaisten tietovarantojen käytön ja toteuttamisen suunnittelusta, ohjauksesta ja seurannasta.

Pykälän 2 momentin mukaan sosiaali- ja terveysalan lupa- ja valvontavirasto sekä aluehallinto- virasto toimialueellaan ohjaavat ja valvovat niille säädetyn toimivallan mukaisesti osaltaan tämän lain noudattamista.

2.5.2 Tietoturvasuunnitelmaa koskeva sääntely 1.1.2024 jälkeen

Asiakastietolain tietoturvasuunnitelmaa koskevan 77 §:n 1 momentin mukaan palvelunantajan, apteekin, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma. Tietoturvasuunnitelmassa on selvitettävä, miten asiakas- ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan:

- 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 tietosuojan varmistavaan käyttöön ja käyttöympäristöön ja tietojärjestelmiin kohdistuvien riskien hallinnasta huolehditaan;
- 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 ja jonka luotettavuus on varmistettu julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 12 §:ssä tarkoitetulla tavalla, jos henkilö tehtävissään pääsee käsittelemään asiakastietoja tai jos hän muuten tehtävissään voi vaarantaa sosiaali- ja terveydenhuollon jatkuvuuden kannalta kriittisten tietojärjestelmien toimintaa;
- 8) tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset 84 §:ssä säädetty olennaiset vaatimukset; sekä
- 9) palvelunantajalla, apteekilla, välittäjällä ja Kansaneläkelaitoksella on suunnitelma siitä, miten tietoturvan ja tietosuojan omavalvonta järjestetään ja toteutetaan sen toiminnassa.

Saman pykälän 2 momentin mukaan ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan ja apteekin tietoturvasuunnitelmassa esitettävä myös selvitys siitä, miten tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu.

Pykälän 3 momentin mukaan Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä 1 ja 2 momentissa tarkoitetuista tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta.

Asiakastietolain 78 §:ssä on säädetty tietoturvallisuuden omavalvonnan toteuttamisesta ja vastuusta. Pykälän 1 momentin mukaan sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan ja apteekkarin on huolehdittava, että 77 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Palvelunantajan, apteekin ja Kansaneläkelaitoksen tulee oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin, jos joku on lainvastaisesti käsitellyt asiakastietoja.

Lain 97 §:ssä on säädetty ohjauksesta, valvonnasta ja seurannasta. Pykälän 1 momentin mukaan sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan yleinen suunnittelu, ohjaus ja valvonta sekä päätöksenteko merkittävien tiedonhallintahankkeiden rahoituksesta kuuluvat sosiaali- ja terveystieteiden ministeriölle.

Saman pykälän 30.6.2024 saakka voimassa olleen 2 momentin mukaan Terveyden ja hyvinvoinnin laitos vastaa sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan sekä 65 §:ssä tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen ja yhteisten hallinnonalakohtaisten tietovarantojen toteuttamisen ja käytön suunnittelusta, käytettävien tietorakenteiden yhteensovittamisesta, ohjauksesta ja seurannasta. Momentin sanamuotoa on muutettu 1.7.2024 alkaen lailla 307/2024 siten, että Terveyden ja hyvinvoinnin laitos on vastuussa valtakunnallisten tietojärjestelmäpalvelujen ja yhteisten hallinnonalakohtaisten tietovarantojen toteuttamisen ja käytön suunnittelusta, ohjauksesta ja seurannasta sekä käytettävien tietorakenteiden yhteensovittamisesta.

Pykälän 3 momentin mukaan tietosuojavaltuutettu, Lääkealan turvallisuus- ja kehittämiskeskus, Sosiaali- ja terveystieteiden lupa- ja valvontavirasto sekä aluehallintovirasto toimialueellaan ohjaavat ja valvovat niille säädetyn toimivallan mukaisesti osaltaan tämän lain noudattamista.

2.6 Hyvinvointialueen omavalvontaa koskeva sääntely

Sosiaali- ja terveydenhuollon järjestämisestä annetun lain (612/2021, järjestämislaki) 3 §:n 1 momentin mukaan laissa tarkoitettua sosiaali- ja terveydenhuoltoa järjestettäessä ja tuotettaessa on noudatettava, mitä sosiaali- ja terveydenhuollon yleis- ja erityislainsäädännössä säädetään.

Hyvinvointialueesta annetun lain (611/2021, hyvinvointialuelaki) järjestämisvastuuta koskevan 7 §:n 1 momentin 4 kohdan mukaan hyvinvointialue vastaa sille lailla säädettyjen tehtävien hoi-

tamisesta, hyvinvointialueen asukkaan laissa säädettyjen oikeuksien toteutumisesta ja palvelukokonaisuuksien yhteensovittamisesta sekä järjestettävien palvelujen ja muiden toimenpiteiden tuottamisen ohjauksesta ja valvonnasta.

Hyvinvointialuelain 10 §:n 2 momentin mukaan hyvinvointialueen tulee ohjata ja valvoa sen järjestämisvastuulle kuuluvaa palvelutuotantoa.

Hyvinvointialuelain 11 §:n 3 momentin mukaan aluehallintovirasto voi kantelun johdosta tutkia, onko hyvinvointialue toiminut voimassa olevien lakien mukaan.

Hyvinvointialueen omavalvonnasta säädettiin 31.12.2023 saakka järjestämislain 40 §:ssä. Sen 1 momentin mukaan hyvinvointialueen ja yksityisen palveluntuottajan on tullut järjestämislain mukaisessa toiminnassaan varmistaa omavalvonnalla tehtäviensä lainmukainen hoitaminen ja tekemiensä sopimusten noudattaminen. Hyvinvointialueen ja yksityisen palveluntuottajan on tullut omavalvonnassaan erityisesti varmistaa palvelujen saatavuus, jatkuvuus, turvallisuus ja laatu sekä asiakkaiden yhdenvertaisuus. Tehtävien ja palvelujen omavalvonta on tullut toteuttaa osana niiden järjestämistä ja tuottamista.

Vuonna 2024 voimaan tulleen sosiaali- ja terveydenhuollon valvonnasta annetun lain (741/2023, sote-valvontalaki) 23 §:n 1 momentin mukaan palvelunjärjestäjän on varmistettava omavalvonnalla sosiaali- ja terveydenhuollon tehtäviensä lainmukainen hoitaminen. Palvelunjärjestäjän on valvottava toimintaansa siten, että sosiaali- ja terveydenhuolto on sisällöltään, laajuudeltaan ja laadultaan sellaista kuin asiakkaiden ja potilaiden tarve ja turvallisuus edellyttävät. Saman pykälän 2 momentin mukaan palvelunjärjestäjän omavalvontaan kuuluu valvoa oman palvelutuotannon lisäksi eri palveluntuottajien kanssa tekemiensä sopimusten noudattamista sekä ohjata ja valvoa yksityisiä palveluntuottajia ja näiden alihankkijoita jatkuvasti palveluja tuottaessa.

Sote-valvontalain 26 §:n 2 momentin mukaan omavalvontaohjelmassa on määriteltävä, miten palvelunjärjestäjän 23 §:ssä ja palveluntuottajan 27 §:ssä tarkoitettujen veloitteiden noudattaminen järjestetään ja toteutetaan. Omavalvontaohjelmassa on todettava, miten sosiaali- ja terveydenhuollon palvelujen toteutumista, turvallisuutta ja laatua sekä asiakkaiden ja potilaiden palvelujen yhdenvertaisuuden toteutumista seurataan ja miten havaitut puutteellisuudet korjataan.

Sote-valvontalain 29 §:ssä säädetään palveluntuottajan ja henkilöstön ilmoitusvelvollisuudesta. Sote-valvontalain 29 §:n 1 momentin mukaan palveluntuottajan on ilmoitettava välittömästi salsapitosäännösten estämättä palvelunjärjestäjälle ja valvontaviranomaiselle palveluntuottajan omassa tai tämän alihankkijan toiminnassa ilmenneet asiakas- ja potilasturvallisuutta olennai-

sesti vaarantavat epäkohdat sekä asiakas- ja potilasturvallisuutta vakavasti vaarantaneet tapahtumat, vahingot tai vaaratilanteet sekä muut sellaiset puutteet, joita palveluntuottaja ei ole kyennyt tai ei kykene korjaamaan omavalvonnallisin toimin.

Saman pykälän 4 momentin mukaan ilmoituksen vastaanottaneen henkilön on ilmoitettava ja ilmoituksen tehnyt henkilö voi ilmoittaa asiasta salassapitosäännösten estämättä valvontaviranomaiselle, jos epäkohtaa tai ilmeisen epäkohdan uhkaa taikka muuta lainvastaisuutta ei korjata viivytyksettä. Valvontaviranomainen voi päättää toimenpiteistä siten kuin 38 §:ssä säädetään tai antaa 39 §:ssä säädetyn määräyksen epäkohdan poistamiseksi.

Sote-valvontalain 32 §:n 2 momentin mukaan aluehallintovirasto valvoo toimialueellaan sosiaali- ja terveystalouden järjestämisen ja tuottamisen lainmukaisuutta ja antaa siihen liittyvää ohjausta. Saman pykälän 3 momentin mukaan Valvira ohjaa aluehallintoviraston toimintaa valvonnan ja siihen liittyvän ohjauksen toimeenpanossa, yhteensovittamisessa ja yhdenmukaistamisessa.

Saman lain 33 §:n 1 momentin mukaan valvontaviranomainen ryhtyy tietoonsa tulleen valvontasian perusteella niihin toimenpiteisiin, joihin se asiakas- tai potilasturvallisuuden varmistamisen tai lain noudattamisen kannalta katsoo olevan aihetta. Saman pykälän 2 momentin mukaan valvontaan liittyvät toimenpiteet voidaan asettaa kiireellisyys- ja tärkeysjärjestykseen asiakas- ja potilasturvallisuuden tai muiden seikkojen niin edellyttäessä.

Lain 34 §:n 1 momentin mukaan valvontaviranomaisten on tarvittaessa toimittava yhteistyössä keskenään ja muiden viranomaisten kanssa hoitaessaan tässä laissa säädettyjä tehtäviä. Saman pykälän 2 momentin mukaan palvelunjärjestäjän on ilmoitettava välittömästi salassapitosäännösten estämättä valvontaviranomaiselle palveluntuottajan tai tämän alihankkijan toiminnassa ilmenneet asiakas- ja potilasturvallisuutta olennaisesti vaarantavat epäkohdat sekä asiakas- ja potilasturvallisuutta vakavasti vaarantaneet tapahtumat, vahingot tai vaaratilanteet sekä sellaiset puutteet, joita ei ole korjattu annetusta ohjauksesta huolimatta.

Lain 38 §:n 1 momentin mukaan jos sosiaali- ja terveystalouden järjestämisessä, tuottamisessa tai toteuttamisessa havaittu puute, virheellisyys, laiminlyönti tai muu epäkohta ei anna aihetta 39 §:ssä tarkoitettuihin toimenpiteisiin, valvontaviranomainen voi saattaa palvelunjärjestäjän tai palveluntuottajan, palveluyksikön vastuuhenkilön tai virheellisestä toiminnasta vastuussa olevan henkilön tietoon käsityksensä lain mukaisesta menettelystä tai kiinnittää edellä mainittujen tahojen huomiota toiminnan asianmukaiseen järjestämiseen ja tuottamiseen sekä hyvän hallinnon vaatimuksiin. Saman pykälän 2 momentin mukaan valvontaviranomainen voi myös kehottaa palvelunjärjestäjää tai palveluntuottajaa, palveluyksikön vastuuhenkilöä tai virheellisestä toiminnasta vastuussa olevaa henkilöä korjaamaan todetun puutteen tai muun epä-

kohdan. Jos edellä tarkoitettuja toimenpiteitä ei voida asian kokonaisarvioinnin vaikuttavat seikat huomioon ottaen pitää riittävinä, valvontaviranomainen voi antaa edellä mainituille tahoille huomautuksen vastaisen varalle.

Lain 39 §:n 1 momentin mukaan, jos sosiaali- ja terveyspalvelujen järjestämisessä, tuottamisessa tai toteuttamisessa havaitaan asiakas- tai potilasturvallisuutta vaarantavia puutteita tai muita epäkohtia taikka toiminta on muutoin tämän tai muun sosiaali- ja terveydenhuoltoa koskevan lain vastaista, valvontaviranomainen voi antaa määräyksen puutteiden korjaamisesta tai epäkohtien poistamisesta. Määräystä annettaessa on asetettava määräaika, jonka kuluessa tarpeelliset toimenpiteet on suoritettava. Saman pykälän 2 momentin mukaan valvontaviranomainen voi velvoittaa palvelunjärjestäjän tai palveluntuottajan noudattamaan edellä mainittua määräystä sakon uhalla tai uhalla, että palvelunjärjestäjän tai palveluntuottajan, sen palveluyksikön tai palveluyksikön osan toiminta taikka toiminnassa käytetyn laitteen tai välineen käyttö keskeytetään. Jos asiakas- tai potilasturvallisuus sitä edellyttää, valvontaviranomainen voi määrätä palvelunjärjestäjän tai palveluntuottajan tässä laissa tarkoitetun toiminnan välittömästi keskeytettäväksi tai kieltää palvelunjärjestäjän tai palveluntuottajan toiminnassa käytettävän palveluyksikön, sen osan tai laitteen käytön välittömästi.

2.7 Valviran ja aluehallintovirastojen valvontaa koskeva sääntely

Sosiaali- ja terveysalan lupa- ja valvontavirastosta (Valvira) annetun lain (669/2008) 1 §:n mukaan Valvira on sosiaali- ja terveysministeriön alainen keskusvirasto, joka edistää ohjauksen ja valvonnan keinoin oikeusturvan toteutumista ja palvelujen laatua sosiaali- ja terveydenhuollossa sekä elinympäristön ja väestön terveysriskien hallintaa. Saman lain 2 §:n mukaan viraston tehtävänä on huolehtia sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa (703/2023) sille säädetystä lupahallinnosta, ohjauksesta ja valvonnasta. Aiemman 31.12.2023 saakka voimassa olleen säädöksen 593/2022 mukaan viraston tehtävänä on ollut huolehtia sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (784/2021) sille säädetystä lupahallinnosta, ohjauksesta ja valvonnasta.

Aluehallintovirastoista annetun lain (896/2009) 2 §:n mukaan aluehallintovirastot edistävät alueellista yhdenvertaisuutta hoitamalla lainsäädännön toimeenpano-, ohjaus- ja valvontatehtäviä alueilla. Lain 4 §:ssä säädetään aluehallintovirastojen toimialasta ja tehtävistä. Pykälän mukaan aluehallintovirastot hoitavat niille erikseen säädettyjä tehtäviä muun ohella sosiaali- ja terveydenhuollon, oikeusturvan edistämisen ja toteuttamisen sekä pelastustoimen toimialoilla. Lain 6 §:n mukaan aluehallintovirasto huolehtii sille säädettyjen tehtävien hoitamisesta toimialueellaan ja käyttää sille kuuluvaa toimivaltaa siten kuin siitä tässä tai muussa laissa säädetään. Aluehallintovirasto voi kuitenkin hoitaa tehtäviä myös useamman kuin yhden viraston toimialueella.

Sote-valvontalain 5 §:n 1 momentin mukaan sosiaali- ja terveyspalveluja saa tuottaa vain palveluntuottaja, joka on 11 §:ssä tarkoitetussa Valviran ylläpitämässä valtakunnallisessa palveluntuottajien rekisterissä (Soteri) ja jonka palveluyksikkö on rekisterissä 21 §:n mukaisesti. Saman lain 3 luvussa säädetään palveluntuottajien ja palveluyksiköiden rekisteröinnistä. Lain 11 §:n 1 momentin mukaan Valvira ylläpitää valtakunnallista sosiaali- ja terveydenhuollon palveluntuottajien ja palveluyksiköiden rekisteriä (Soteri) palveluntuottajien ja sosiaali- ja terveyspalvelujen rekisteröintiä, valvontaa ja tilastointia sekä muiden viranomaisten lakisääteisiä tehtäviä varten. Lain 16 §:ssä säädetään rekisteröintiä varten annettavista tiedoista, joihin kuuluu kyseisen 16 §:n 2 momentin 9 kohdan mukaan myös tiedot ja selvitykset tietoturvasuunnitelmasta.

Sote-valvontalaki on tullut voimaan 1.1.2024. Hyvinvointialueiden osalta lain 3 luku on kuitenkin säädetty tulemaan voimaan vasta 1.1.2026. Lain 56 §:n 1 momentin mukaan sen 52 §:ssä tarkoitettu julkinen palveluntuottaja saa lain 5 §:n estämättä jatkaa toimintaansa 1.1.2024 jälkeen noudattaen asianomaisen lain säännöksiä. Julkisen palveluntuottajan on annettava valvontaviranomaiselle 16 §:ssä tarkoitetut tiedot ennen lain 3 luvun voimaantuloa 1.1.2026. Tiedot tallennetaan lain 56 §:n mukaan valtakunnalliseen palveluntuottajien rekisteriin (Soteri) maksutta viimeistään 31.12.2028.

2.8 Terveiden ja hyvinvoinnin laitoksen määräys

Asiakastietolain (703/2023) 77 §:n 3 momentin mukaan Terveiden ja hyvinvoinnin laitoksella (THL) on toimivaltaa antaa tarkempi määräyksiä tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta. Aiemmin voimassa olleessa sähköisessä asiakastietolaissa (784/2021) oli vastaava säännös 27 §:n 3 momentissa.

THL oli antanut määräyksen 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista ja uuden lain voimaan tulon jälkeen uuden [määräyksen 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista](#). Määräys tuli voimaan 22.2.2024.

Määräyksessä 3/2024 tietoturvasuunnitelman laatimiseen veloitetuista tahoista käytetään yleisnimeä tietoturvallisuuden omavalvonnan kohde. Määräyksen mukaan tietoturvallisuuden omavalvonnan kohteen velvollisuutena on toimia laatimansa tietoturvasuunnitelman mukaisesti, säännöllisesti ylläpitää ja katselmoida suunnitelmaansa sekä seurata aktiivisesti sen toteutumista. Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta. Määräyksen liitteenä on tietoturvasuunnitelman mallipohja, joka on tietoturvallisuuden omavalvonnan kohteiden tietoturvasuunnitelman laatimisen tueksi tarkoitettu esimerkinomainen dokumenttipohja. Mallipohjadokumentin rakenne on informatiivinen ja suuntaa antava eli suunnitelman tekemistä helpottava ja ohjaava.

Määräyksen 3/2024 kohdassa 3 käsitellään tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisen vastuita. Tietoturvallisuuden kohteen tulee varmistaa, että tietoturvasuunnitelmaan sisällytettävät vaatimukset toteutuvat kaikissa sen omissa palveluyksiköissä ja kaikissa muiden sen lukuun palveluiden tuottamiseen tai toteuttamiseen osallistuvien palveluntarjoajien toiminnassa mukaan lukien mahdollisten alihankintapalveluntuottajien toiminnassa. Tietoturvasuunnitelmassa olevista selvityksistä tulee näkyä kaikkien edellä kuvattujen yksiköiden ja alihankintapalveluntuottajien vastuut. Kaikkien asiakastietojen käsittelyn osapuolien vastuut tulee olla selkeästi määritelty. Jos tietoturvasuunnitelmaan kuuluvia vastuita on jonkun muun kuin tietoturvallisuuden omavalvonnan kohteen itsensä vastuulla, on vastuut määriteltävä osapuolten välisissä toimeksianto- tai muissa sopimuksissa. Sopimuksista tulee myös ilmetä, mihin toimiin osapuolet yhdessä tai erikseen tahoillaan ryhtyvät, jos tietoturvassa ilmenee puutteita, ongelmia tai toteutuneita riskejä.

Määräyksen mukaan tietoturvasuunnitelman varsinaisen sisällön tai siitä viitatuissa liitteissä esitetyn sisällön pohjalta on tarvittaessa pystyttävä todentamaan seuraavat tietoturvallisuuden omavalvontaan liittyvät asiat:

- tietoturvasuunnitelma on laadittu,
- tietoturvasuunnitelma sisältää suunnitelmalta edellytettävät asiat tämän määräyksen mukaisesti,
- tietoturvasuunnitelmassa on kuvattu, miten suunnitelmaa säännöllisesti päivitetään, katseloidaan ja
- miten sen toteutumista seurataan.

Tietoturvallisuuden omavalvonnan kohteen on pystyttävä osoittamaan tietoturvasuunnitelman olemassaolo, asianmukaisuus ja toteuttaminen esimerkiksi valvontaviranomaisille myös niissä tilanteissa, joissa se ei itse tuota palveluita.

3 Arviointi

3.1 Varha ja tietoturvallisuus

Varha on viitannut selvityksessään [hallintosääntöönsä](#), jonka tiedonhallintaa ja asiakirjahallinnon järjestämistä koskevassa luvussa kuvataan muun muassa tietoturvallisuusjärjestelyjä koskevat vastuut.

Varha on muuttanut hallintosääntöään 1.3.2024 alkaen. Varhan hallintosäännön 82 §:n mukaan hyvinvointialue on tiedonhallintalaissa tarkoitettu tiedonhallintayksikkö. Tiedonhallintayksikön tehtävänä on järjestää tiedonhallinta lain vaatimusten mukaisesti. Aluehallitus vastaa siitä, että tiedonhallinnan vastuut, käytännöt ja valvonta on määritelty hyvinvointialueen eri tehtävissä. Hallintosäännön 84 §:n mukaan aluehallitus ja hyvinvointialuejohtaja tiedonhallintaa johtavana

viranhaltijana muodostavat yhdessä tiedonhallintayksikön johdon. Tiedonhallinnasta vastaava viranhaltija johtaa aluehallituksen alaisena tiedonhallinnan valmistelun ja toteuttamisen tehtäviä. Tiedonhallinnasta vastaava viranhaltija

1. vastaa hyvinvointialueen tiedonhallintamallin valmistelusta ja täytäntöönpanosta
2. ohjaa ja kehittää hyvinvointialueen tiedonhallintaa
3. edistää tietojärjestelmien ja tietovarantojen yhteen toimivuutta
4. varmistaa tietoturvallisuuden toteuttamista hyvinvointialueen toiminnassa
5. vastaa hyvinvointialueen käyttämien tietoaineistojen ajantasaisuudesta, virheettömyydestä ja siitä, että niiden käyttökelpoisuus käyttötarkoitukseensa on varmistettu.

Varhan kummassakaan hallintosäännössä ei ole mainittu lainkaan asiakastietolain mukaista tietoturvasuunnitelmaa.

Varha on viitannut myös aluehallituksen 6.6.2023 hyväksymään tiedonhallintapolitiikkaansa, joka kuvaa, miten Varha laatii tiedonhallintamallin ja ylläpitää sitä.

Kyseisen [tiedonhallintapolitiikan](#) mukaan politiikka toimii perustana tiedonhallintamallille, henkilötietojen hallintamallille, tietoturvallisuuden hallintajärjestelmälle sekä tiedonhallintaan, tietosuojaan, tietoturvaan ja asianhallintaan liittyville toimintaohjeille, joiden tehtävänä on tarkentaa tässä politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön. Tiedonhallintapolitiikan mukaan jokaisen hyvinvointialueen viranhaltijan, työntekijän ja luottamushenkilön sekä hyvinvointialueen tietojen ja tietojärjestelmien käyttäjän on noudatettava tätä tiedonhallintapolitiikkaa ja sen pohjalta annettuja ohjeita ja määräyksiä. Hyvinvointialueen palveluntuottajien, toimittajien ja muiden ulkopuolisten tahojen, jotka käsittelevät hyvinvointialueen omistamaa tietoa työnsä tai toimeksiantonsa puitteissa, tulee myös noudattaa tätä tiedonhallintapolitiikkaa ehtona tehtäviensä mukaiselle pääsyle hyvinvointialueen tietoihin.

Varhan tiedonhallintapolitiikan tietoturvaa koskevan luvun mukaan hyvinvointialueen tiedonhallinnassa on huolehdittava asianmukaisesta tietoturvallisuudesta. Tietoturvaprosessin omistaja on tietoturvavastaava, jonka nimittää hyvinvointialuejohtaja. Hyvinvointialuejohtajalta saamiensa resurssien ja toimivaltuuksien puitteissa tietoturvavastaava vastaa tietoturvallisuuden hallinnasta, toteuttamisesta, kehittämisestä, toteutuksen valvonnasta sekä tietoturvatietoisuuden edistämisestä ja tietoturvalisesta toimintatavasta hyvinvointialueella ja sen ostamissa palveluissa sekä raportoinnista. Tietoturvavastaava raportoi hyvinvointialuejohtajalle ja aluehallitukselle. Tiedonhallintapolitiikassa on lueteltu erikseen tietoturvavastaavan yleiset tehtävät ja vastuut. Tietoturvavastaavan vastuulle on osoitettu muun ohella tietoturvalisusdokumenttien laatiminen ja päivittäminen. Lisäksi tietosuoja- ja tietoturvaryhmä muun ohella valmistelee tietoturvaan liittyvää ohjeistusta.

Tiedonhallintapolitiikassa on myös todettu, että tietoturvallisuuden varmistamiseksi aluehallitus valvoo ja johtaa tietoturvallisuuden hallinnointia, riskienhallintaa ja vaatimustenmukaisuutta sekä vaatii raportointia ja tietoa tietoturvallisuuden toteutumisesta ja nykytilasta. Hyvinvointi-aluejohtaja vastaa siitä, että tietoturvavastaavan resurssit ja toimivaltuudet ovat riittävät sekä siitä, että tietoturvatyön organisointi hyvinvointialueella on tarkoituksenmukainen, ristiriidaton ja tietoturvatyön keskeisten toimijoiden yhteistyötä edistävä.

Varhan selvityksen ja sen tiedonhallintapolitiikasta tarkemmin ilmenevän kuvauksen perusteella Varha on toiminut tiedonhallintalain mukaisten vaatimusten täyttämiseksi. Tiedonhallintapolitiikassa ei kuitenkaan ole mainintaa siitä, miten Varha olisi toteuttamassa laissa säädettyä velvollisuuttaan asiakastietolain mukaisen tietoturvasuunnitelman laatimiseksi tai miten tähän liittyvä omavalvonta olisi tarkoitus toteuttaa. Tämän perusteella jää myös epäselväksi, miten hyvinvointialueella on jaettu tietoturvasuunnitelman laatimiseen liittyvät vastuut.

Varha on selvityksessään kuvannut, kuinka se arvioi tietoturvasuunnitelmansa eri osien kypsyystasoa. Vaikka nämä voivat sinänsä toimia hyvän riskienhallinnan kannalta arvokkaana kehittämistyön seurannan ja arvioinnin tukena, tietoturvasuunnitelmasta säädetty ei tue sitä, että kyse olisi prosessista. Vaikka tietoturvasuunnitelma on omavalvontasuunnitelman tavoin kehittyvä työkalu, asiakastietolain tietoturvasuunnitelmaa koskeva sääntely ei ole luonteeltaan tarkoituksenmukaisuusperusteita joustavasti huomioivaa. Tietoturvasuunnitelmaa ei siten voitaisi laatia vasta sitten, kun hyvinvointialueen perustamisesta johtuvat tietojärjestelmien käyttöönotot olisivat valmistuneet. Tietoturvasuunnitelman tulisi kuvata kulloinkin ajankohtaista käytössä olevien tietojärjestelmien tilaa.

[Varhan tarkastuslautakunnan 16.5.2024 laaditusta vuoden 2023 arviointikertomuksesta](#) ilmenee, että tiedonhallintapolitiikassa mainittua tietoturvavastaavan sekä tietosuoja- ja tietoturvaryhmän nimeämistä oli valmisteltu, mutta lopulliset päätökset olivat olleet ainakin vielä 15.2.2024 tekemättä. Tietosuoja- ja tietoturvaryhmä olivat kokoontuneet syksystä 2023 alkaen toistaiseksi epävirallisella kokoonpanolla.

Tarkastuslautakunta oli todennut suosituksenaan, että Varhan tietosuojaan ja tietoturvaan liittyvän organisaation ja vastuuhenkilöiden virallinen vahvistaminen ja tiedonhallintamallin luominen ovat tärkeitä ja kiireellisiä toimenpiteitä. Arviointikertomuksesta ilmenee, että Varhassa oli 20.12.2023 tehdyllä hankintapäätöksellä hankittu palvelulisenssi Digiturvamalliin, jonka on ollut tarkoitus toimia Varsinais-Suomen hyvinvointialueen tiedonhallintamallin sekä tietosuoja- ja tietoturvadokumentaation laatimisen, ylläpitämisen ja jakamisen välineenä. Myöskään Varhan tarkastuslautakunta ei kuitenkaan ole ottanut kertomuksessaan kantaa tietoturvasuunnitelman puuttumiseen.

3.2 Tietoturvasuunnitelman puuttumisen merkitys

Hyvinvointialueilla sovellettava asiakastietolaki on erityislaki tiedonhallintalakiin nähden. Tietoturvasuunnitelman laatimista koskeva velvoite ei siis ole laatusuositus tai muu yleisluonteinen kuvaus tietoturvassa noudatettavista hyvän hallinnon ominaisuuksista. Sen laatimista koskeva velvollisuus on säädetty laissa ja hyvinvointialueen velvollisuus laatia tietoturvasuunnitelma on yksiselitteinen. Hyvinvointialueella on velvollisuus noudattaa myös asiakastietolain tiedonhallintalakia yksityiskohtaisempia säännöksiä muun ohella tietoturvasuunnitelman laatimisesta. Tilanne, jossa hyvinvointialue ei ole huolehtinut tästä velvoitteesta, on lainvastainen.

Hyvinvointialueiden toiminta on käynnistynyt vuoden 2023 alussa. Varhan tietoturvasuunnitelman puuttuminen on havaittu vuonna 2023, eikä kyseinen suunnitelma ole ollut Varhan selvityksen mukaan käytössä myöskään vuonna 2024.

Valvira on tuonut tämän päätöksen jaksossa 1.3 esitetyssä lausunnossaan esiin niitä asiakas- ja potilastietojen turvalliseen käsittelyyn liittyviä käytäntöjä, joita tietoturvasuunnitelma edistää. Valvira on myös todennut, että tietoturvasuunnitelma auttaa erityisesti hallitsemaan tämän päivän digitaaliseen turvallisuuteen liittyviä riskejä. Nämä riskit myös korostuvat mitä pidempään suunnitelma on organisaatiossa laatimatta ja sen mukaiset toimintamallit toteuttamatta.

Yhdyn Valviran edellä esiin tuomaan. Edellä mainitut riskit ovat vakavia. Pahimmillaan puutteelliset tietoturvakäytännöt voivat johtaa tietomurtoihin. Ne koskisivat sosiaali- ja terveydenhuoltoa ja erityisesti sen potilastietoja, jotka ovat pääsääntöisesti arkaluonteisia ja salassapidettäviä, ja voisivat koskea laajoja asiakas- ja potilasjoukkoja. Tietomurrot ovat silloin erityisen vahingollisia ja voivat aiheuttaa muun muassa henkilötietojen väärinkäyttöä, kiristämistä ja identiteettivarkauksia.

3.3 Tietoturvasuunnitelman laatimisvelvoitteen tausta

Tiedonhallintalaki ja asiakastietolaki tarkentavat hyvän hallinnon takeita, jotka perustuslain 21 §:n 2 momentin mukaan turvataan lailla. Asiakastietolain mukainen tietoturvasuunnitelma myös konkretisoi EU:n yleisen tietosuojasetuksen, tietosuojalain ja tiedonhallintalain velvoitteita sosiaali- ja terveysalalla.

Ensimmäiseen sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettuun lakiin (159/2007) lisättiin säännökset (250/2014), joiden tarkoituksena oli edistää sosiaali- ja terveydenhuollon sähköisessä tietojenkäsittelyssä tietosuojaa ja tietoturvaa sekä tietojärjestelmien yhteentoimivuutta ja toiminnallisuutta. Lain esitöiden ([HE 219/2013 vp](#), s. 1) mukaan tietojärjestelmien toimittajien ja niitä käyttävien organisaatioiden tuli ensisijassa laatujärjestelmän ja omavalvonnan keinoin huolehtia THL:n laatimien ja vahvistamien kriteerien noudattamisesta.

Sen varmistamiseksi, että jokainen sosiaali- tai terveydenhuollon tietojärjestelmiä käyttävä organisaatio ja itsenäinen ammatinharjoittaja sekä myös välityspalvelujen tuottaja on järjestänyt toimintansa asianmukaisesti, tulisi näiden laatia omavalvontasuunnitelma, jossa on selvitetty asiakas- ja potilastietojen käsittelyyn liittyvät tekijät ja näiden tietojen käsittelyssä käytettävien tietojärjestelmien asianmukaisuus. Suunnitelmassa tulee käsitellä muun muassa henkilöstön osaamiseen ja koulutukseen liittyvät asiat sekä tietojärjestelmien vaatimustenmukaisuus. Lisäksi omavalvontasuunnitelmalla tulee varmistaa, että organisaatiossa huolehditaan jatkuvasti riittävästä koulutuksesta ja seurannasta. ([HE 219/2013 vp](#), s. 10)

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (159/2007) kumottiin sähköisellä asiakastietolailla (784/2021). Tässä uudessa laissa säädettiin ensimmäisen kerran veloitteesta laatia tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma-niminen asiakirja, jossa käsitellään organisaation tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyviä keskeisiä asioita. Erillisestä tietoturvasuunnitelman laatimisesta tuli näin lain 1.11.2021 voimaan tullessa yksityiskohtaisesti säädetty tietoturvan ja tietosuojan omavalvontaa konkretisoiva lakisääteinen velvollisuus, vaikka kyseinen asiakirja oli tullut laatia myös jo aiemmin omavalvontasuunnitelman muodossa.

Lain esitöiden mukaan tietoturvasuunnitelman tarkoituksena olisi varmistaa, että palvelujenantajien, välittäjien ja Kansaneläkelaitoksen henkilökunta hallitsee käytössään olevien tietojärjestelmien käytön ja osaa ottaa huomioon asiakastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset. Lisäksi tietoturvasuunnitelmassa tulee ottaa huomioon tietojärjestelmien käyttöympäristöön, ylläpitoon ja päivitykseen liittyvät asiat sekä se, kuinka suunnitelman toteuttaminen ja suunnitelman kohteena olevien seikkojen omavalvonta järjestetään. ([HE 212/2020 vp](#), s. 113)

Tietoturvasuunnitelman laatimisella organisaatio siis luo asiakastietojen tietoturvallista käyttöä koskevan toimintasuunnitelman. Organisaation toimintaa tietoturvasuunnitelman mukaisesti valvotaan tämän jälkeen omavalvonnan keinoin. Varhan selvityksessä ei ole voitu kuvata, miten tietoturvasuunnitelmaa ja sen toteuttamista omavalvonnallisesti valvotaan, koska tietoturvasuunnitelman laatiminen itsessään on ollut kesken. Tämä herättää vakavan huolen organisaation tietoturvan tasosta. Tietoturvasuunnitelman laatimisen laiminlyömisestä myös seuraa, ettei organisaatio ole voinut tältä osin lainkaan toteuttaa omavalvontavelvoitettaan.

Koska tietoturvasuunnitelma ei ole julkinen asiakirja, hyvinvointialueen asukkailla tai ulkopuolisella valvonnalla ei ole mahdollisuutta havaita kyseistä puutetta. Hyvinvointialueella on tämänkin vuoksi poikkeuksellisen suuri vastuu, koska tietoturvasuunnitelman noudattaminen on jätetty lainsäädännössä korostetusti hyvinvointialueen omavalvonnan varaan. Varhan kohdalla valvonnassa on tietoturvan toteutumisen kannalta ratkaisevan tärkeässä asiassa aukko.

Tarkasteltaessa tietoturvasuunnitelman valvontaan liittyvää sääntelykokonaisuutta on havaittavissa, että tietoturvasuunnitelman laatimista ja valvontaa koskevaa sääntelyä on valmisteltu erillään muusta hyvinvointialueita koskevasta valvonnasta. Tätä kuvastaa se, että hyvinvointialueiden perustamisen kannalta keskeisimmässä hallituksen esityksessä puhutaan tietoturvasuunnitelmasta vain kerran. Tämäkin tapahtuu käsiteltäessä kuntien ICT-varautumista ([HE 241/2020 vp](#), s. 128), eikä tietoturvasuunnitelmaa mainita lainkaan esimerkiksi järjestämislain omavalvontaa koskevissa yksityiskohtaisissa perusteluissa. Tietoturvasuunnitelman omavalvontaa tai valvontaa ei käsitellä tarkemmin myöskään sote-valvontalain esitöissä. Tältä osin tietoturvasuunnitelma tunnistetaan asiakirjaksi, josta palveluntuottajan on annettava tiedot Soteri-rekisteröintiä varten ([HE 299/2022 vp](#), s. 97).

Koska asiakastietolain mukaista tietoturvasuunnitelmaa ei ole erikseen mainittu sote-valvontalaissa tai sen esitöissä, tämä on voinut olla omiaan hämärtämään hyvinvointialueen omavalvonnan ja valvonnan suhdetta tietoturvasuunnitelman laatimisen valvonnassa. Yksinomaan sote-valvontalain perusteella tietoturvasuunnitelman olemassaolo tulisi hyvinvointialueiden osalta systemaattisesti tarkistetuksi vasta Soteri-rekisteröinnin myötä vuonna 2026. Valviran pyynnöstäni antamasta lausunnosta kuitenkin ilmenee, että Valvira on kohdentamassa valvontaansa tietoturvasuunnitelmiin jo lokakuussa 2024 aloittamallaan selvityksellä ja edelleen vuosille 2025 ja 2026 suunnittelemallaan valvonnalla.

Jää epäselväksi, olisiko hyvinvointialueiden tietoturvasuunnitelman laatimista koskevaan velvoitteeseen kohdistunut lainkaan valvontaa ennen Soteri-rekisteröintiä.

3.4 Hyvinvointialueen velvoite suojata yksityiselämään kuuluvia tietoja

Perustuslakivaliokunta on arvioidessaan terveydenhuoltolain mukaisia potilastietorekistereitä korostanut, että potilastietorekisterin kaltaisen arkaluonteisia tietoja sisältävän rekisterin ollessa kyseessä on erityisen tärkeää varmistua siitä, että väärinkäytön estävät tietoturvajärjestelyt ovat toimivia ja käytettävissä heti, kun järjestelmä otetaan käyttöön ([PeVL 41/2010 vp](#), s. 3/II). Perustuslakivaliokunta on katsonut, että arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin kohdistuvasta tietomurrosta, tietovuodosta tai väärinkäytöstä seuraisi hyvin merkittävä perusoikeusloukkaus ([PeVL 15/2018 vp](#), s. 40)

Perustusvaliokunta on katsonut olevan lähtökohtaisesti riittävää perustuslain 10 §:n 1 momentin kannalta, että sääntely täyttää EU:n yleisessä tietosuojasetuksessa asetetut vaatimukset ([PeVL 14/2018 vp](#), s. 4). Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuojasetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkien

ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta. ([PeVL 14/2018 vp](#), s. 5)

Vuoden 2023 loppuun saakka voimassa olleen järjestämislain 40 §:n mukaan hyvinvointialueen on tullut tämän lain mukaisessa toiminnassaan varmistaa omavalvonnalla tehtäviensä lainmukainen hoitaminen. Vuoden 2024 alusta hyvinvointialueen on tullut sote-valvontalain 23 §:n 1 momentin mukaan varmistaa omavalvonnalla sosiaali- ja terveydenhuollon tehtäviensä lainmukainen hoitaminen. Momentissa on edellytetty, että palvelunjärjestäjän on valvottava toimintaansa siten, että sosiaali- ja terveydenhuolto on sisällöltään, laajuudeltaan ja laadultaan selaista kuin asiakkaiden ja potilaiden tarve ja turvallisuus edellyttävät.

Vaikka tietoturvasuunnitelman valvontaa ei mainita erikseen sote-valvontalaissa, eikä sitä ole erikseen huomioitu myöskään lain esitöissä, tietoturvasuunnitelman valvonnan voidaan katsoa kuuluvan olennaisena osana sote-valvontalain 23 §:n mukaiseen hyvinvointialueen omavalvontavelvollisuuteen huolehtia toiminnassaan asiakkaiden ja potilaiden yksityiselämään kuuluvien tietojen turvallisuudesta. Hyvinvointialueen velvoite laatia tietoturvasuunnitelma, josta on ilmettävä omavalvonnan toteuttamiseen liittyvät vastuut, voidaan johtaa myös tiedonhallintalain 4 §:n mukaisesta tiedonhallintayksikölle säädetyistä velvollisuuksista järjestää riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta.

Sote-valvontalain säätämiseen johtaneessa hallituksen esityksessä on todettu, että jo tietosuoja-asetuksessa säädetään suoria velvoitteita henkilötietojen käsittelijöille. Näitä velvoitteita ovat tietosuoja koskevat vaikutustenarvioinnit, ilmoitukset henkilötietojen tietoturvaloukkauksista, tietoturva, tietojen tuhoaminen ja auditointeihin osallistuminen. Henkilötietojen käsittelijän on lisäksi toteutettava riittävät suojatoimet sekä asianmukaiset tekniset ja organisatoriset toimenpiteet. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta ja muita suojatoimenpiteitä. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset rekisteröidyn oikeuksien suojelemiseksi. ([HE 299/2022 vp](#), s. 97–98)

Edellä mainitut esimerkit teknisistä ja organisatorisista toimenpiteistä ovat nähdäkseni juuri niitä konkreettisia toimia, joiden toteutus tulisi ilmetä asiakastietolain mukaisesta tietoturvasuunnitelmasta. Asiakastietolain 78 §:ssä hyvinvointialueen tietoturvasuunnitelmaa koskeva omavalvonta täsmentää siten edellä mainittuja valvontaan liittyviä velvollisuuksia. Niiden tulisi olla myös niin selkeitä, että koko henkilöstöllä olisi suunnitelman perusteella mahdollisuus ymmärtää omat roolinsa ja tehtävänsä tietoturvan toteuttamisessa.

3.5 Valvonnan vireilletulo

Omavalvonta on määritelty toimijan itsensä suorittamaksi oman toimintansa valvonnaksi, jota valvontaviranomainen ohjaa ja valvoo (Aluehallintovirastojen ja Valviran työnjakoa ja yhteistyötä kehittäneen työryhmän muistio, [Sosiaali- ja terveysministeriön raportteja ja muistioita 2014:24](#), s. 13)

Asiassa saatu selvitys on osoittanut, ettei Varhan tietoturvasuunnitelman valvonnan järjestäminen omavalvonnan keinoin ole ollut riittävää. Se on johtanut siihen, ettei tietoturvasuunnitelmaa ole laadittu laissa säädetyllä tavalla. Ulkopuolisen valvonnan puuttuminen on ollut myös omiaan mahdollistamaan laiminlyönnin piilossa pysymisen. Kun omavalvonnan kohteena on oma organisaatio, organisaation sisäisillä toimijoilla voi myös olla arkuutta, vääränlaista lojaalisuutta tai riippuvuutta, jonka vuoksi havaituista puutteista ei ilmoiteta ulkopuoliselle valvojalle.

Tietoturvasuunnitelman laatimisella on nähdäkseni kuitenkin myös organisaation sisäisiä toimijoita suojaava tarkoitus. Kun tietoturvasuunnitelman tarkoituksena on huolehtia siitä, että toimijoilla on tietoa ja osaamista, voidaan myös välttää osaamattomuudesta ja epätietoisuudesta johtuvia virheitä, jotka voivat johtaa virkavastuuseen. Tietoturvaan ja tietosuojaan liittyvät virheet ovat usein myös vaikeita, elleivät mahdottomia, korjata jälkikäteen.

Aluehallintovirasto on katsonut antamassaan selvityksessä, että Varhan kumppanuuspäällikön tiedustelussa on ollut kyse pyydetystä ohjauksesta. Kysymys on koskenut sitä, tulisiko havaituista tietoturvasuunnitelmien puutteista ilmoittaa välittömästi valvontaviranomaiselle asiakas- ja potilasturvallisuutta olennaisesti vaarantavana puutteena. Aluehallintovirasto on kuitenkin myös myöntänyt, että tieto Varhan tietoturvasuunnitelman puuttumisesta oli tullut myös muuta kautta sen yksittäisten virkamiesten tietoon.

Aiemmassa järjestämislain 44 §:ssä ja nykyisessä sote-valvontalain 29 §:ssä säädetään hyvinvointialueen velvollisuudesta tehdä ilmoitus valvojalle. Tällaista ilmoitusta Varha ei ole tehnyt. Sote-valvontalain 29 §:ssä säädetään myös työntekijän velvollisuudesta tehdä ilmoitus. Sosiaali- ja terveydenhuollon valvonta-asiat voivat ylipäättään tulla vireille monin eri tavoin. Valvontaviranomaisen tehtävänä on tunnistaa, milloin kyse on myös sellaisesta valvonnan kannalta merkityksellisestä ilmoituksesta, joka kertoo siitä, ettei omavalvonta toimi. On selvää, että aluehallintovirasto on saanut Varhan tietoturvasuunnitelman puuttumisesta tiedon.

4 Johtopäätökset

Tilanne, jossa hyvinvointialueella ei ole tietoturvasuunnitelmaa, on lainvastainen.

Varha on viitannut selvityksessään siihen, että sen organisaation järjestäytyminen sekä taloudelliset haasteet ovat hidastaneet asian valmistelua. Hyvinvointialueet ovat organisaation järjestäytymisen vaatimasta ajasta huolimatta laiminlyönneistään vastuussa. Viiveet organisaation järjestäytymisessä eivät myöskään poista tietoturvallisuuteen liittyviä riskejä tai tee niistä vähäisempiä hyvinvointialueen asiakkaiden kannalta. Lakia on noudatettava kaikissa olosuhteissa.

Pyytämässäni selvityksissä on osaltaan arvioitu myös laiminlyönnin vakavuutta. Varhan omavalvonnassa oli linjattu lakisääteisen ohjausdokumentaation puute vakavaksi poikkeamaksi. Varha ei olisi voinut arvioida myöskään oman tietoturvasuunnitelmansa puuttumista tästä poikkeavasti. Varhan tietoturvasuunnitelman puuttuminen on vaikuttanut myös siihen, että Varhan omavalvonnassa on todettu tietoturvasuunnitelmaan liittyviä puutteita yksiköissä, joihin se on kohdistanut omavalvontaa.

Lounais-Suomen aluehallintovirastosta annetussa ohjauksessa oli Varhan omavalvonnasta tehtyjen yhteydenottojen perusteella katsottu, ettei Varhan tietoturvasuunnitelman puuttumiseen liittyvää puutetta tarvitse kirjata yksikköä koskevaksi vakavaksi poikkeamaksi. Selvityksestä ei ilmene, että aluehallintovirasto olisi ottanut yhteydenottojen pohjalta kantaa Varhan tietoturvasuunnitelman puuttumisen aiheuttaman poikkeaman vakavuuteen. Aluehallintovirasto ei ole voinut myöskään osoittaa, millaista ohjausta se on Varhalle tältä osin antanut vai onko tällaista ohjausta annettu lainkaan.

Aluehallintovirasto ei ole myöskään ottanut oma-aloitteisesti vireille valvonta-asiana Varhan tietoturvasuunnitelman puuttumista, vaikka tieto siitä ja sen vaikutuksesta Varhan tekemän omavalvonnan toimivuuteen on tullut aluehallintoviraston virkamiesten tietoon vuoden 2023 aikana muutoin kuin järjestämislain 44 §:n mukaisena ilmoituksena. Aluehallintovirasto on pitänyt tietoturvasuunnitelman puuttumista ongelmallisena vasta kesällä 2024, kun se on pyynnöstäni antamassaan lausunnossa katsonut tietoturvasuunnitelman laatimisen ja lainvastaisen tilanteen kestäneen kohtuuttoman pitkään.

Yhdyn Valviran lausunnossaan esittämään näkemykseen siitä, ettei tietoturvasuunnitelman puuttumista voida pitää Varhan osalta vähäisenä puutteena. Kun aluehallintovirasto on saanut tiedon tietoturvasuunnitelman puuttumisesta, mutta se ei ole ryhtynyt valvontatoimiin asian johdosta, on ilmeistä, että aluehallintovirasto on tässä vaiheessa laiminlyönyt valvontatehtävänsä.

Aluehallintovirasto on antaessaan siltä pyytämäni lausunnon tässä vaiheessa kehottanut hyvinvointialuetta korjaamaan todetun puutteen. Menettely on vastannut sote-valvontalain 38 §:n 2

momentissa säädettyjä valvontaviranomaisille säädettyjä toimenpiteitä. Ennen toimenpiteisiin ryhtymistä aluehallintovirasto on kuitenkin pysynyt passiivisena, vaikka sillä on ollut tieto Varhan tietoturvasuunnitelman puuttumisesta. Kun otetaan huomioon hyvinvointialueen kokoisen organisaation tietoturvasuunnitelman merkitys sekä sen oman tietoturvan toteutumisen että omavalvonnan toimivuuden kannalta, aluehallintoviraston laiminlyöntiä ryhtyä valvontatoimiin toimivaltaisena valvontaviranomaisena ei voida pitää vähäisenä.

Selvitysten perusteella on ilmennyt, että Varha on menetellyt lainvastaisesti. Asiassa ei ole tullut esiin selvää yksittäistä vastuullista toimijaa, koska hyvinvointialuejohtaja ei ole asiakirjaselvityksen perusteella myöskään siirtänyt tietoturvasuunnitelman laatimista koskevaa vastuuta nimetyille tietoturvavastaavalle. Varhan hallintosäännön mukaan aluehallitus ja hyvinvointialuejohtaja tiedonhallintaa johtavana viranhaltijana muodostavat yhdessä tiedonhallintayksikön johdon. Kyse on ollut näin ollen hyvinvointialueen aluehallituksen ja hyvinvointialuejohtajan tiedonhallintaa johtaneena viranhaltijana tekemästä laiminlyönnistä. Varhan antamasta selvityksestä ei ilmene, että Varhan valvontakeskuksen esiin nostama havainto tietoturvasuunnitelman puuttumisestakaan olisi aiheuttanut Varhassa toimia tietoturvasuunnitelman valmiiksi saattamiseksi.

Tietoturvasuunnitelman laatimisessa on kyse toimintavelvoitteesta, jonka toteuttamisesta THL:n määräyksen mukaisesti hyvinvointialueen sisällä voi vastata vain vastaava johtaja. Tietoturvasuunnitelman tehtävänä on luoda käytännöt, joilla henkilökunta osaa toimia tietoturvan kannalta oikein sekä tavallisissa että poikkeustilanteissa. Tietoturvasuunnitelman noudattamisella voidaan myös estää sitä, että henkilökunta toimisi osaamattomuuttaan tahattomasti väärin.

5 Toimenpiteet

Varsinais-Suomen hyvinvointialueen laatima tietoturvasuunnitelma on ollut 27.6.2024 annetun selvityksen mukaan edelleen keskeneräinen. Sillä olisi kuitenkin tullut olla valmis tietoturvasuunnitelma, josta asiakastietolain mukaiset tietoturvasuunnitelmalta edellytettävät elementit ovat todettavissa, heti hyvinvointialueen toiminnan alkaessa 1.1.2023. Tietoturvasuunnitelmaa olisi tämän jälkeen tullut päivittää tietojärjestelmien vaihtuessa.

Valtioneuvoston oikeuskanslerista annetun lain 6 §:n 1 momentin mukaan, jos virkamies, julkisyhteisön työntekijä tai muu henkilö julkista tehtävää hoitaessaan on menetellyt lainvastaisesti tai jättänyt velvollisuutensa täyttämättä, oikeuskansleri voi antaa asianomaiselle huomautuksen vastaisen varalle, mikäli hän ei harkitse olevan aihetta syytteen nostamiseen. Huomautus voidaan antaa myös viranomaiselle tai muulle yhteisölle.

Annan Varsinais-Suomen hyvinvointialueelle ja Lounais-Suomen aluehallintovirastolle kummallekin huomautukset vastaisen varalle. Edellä olen kuvannut laiminlyönnin vakavuutta. Menette-

lyn arvioinnin kannalta merkityksellistä myös on, että Valvira on tiedottanut eri tavoin asiakas-tietolain velvoittaman tietoturvasuunnitelman laatimisen sisällöstä ja hyvinvointialueelle kuulu-vista velvoitteista. Tietoturvasuunnitelman laatimisvelvoite ei ole myöskään uusi asia, vaan se on koskenut jo ennen hyvinvointialuetta järjestämisvastuullisia kuntia. Tietoturvasuunnitelman puuttumisen ei siten voi katsoa johtuneen hyvinvointialueen tai aluehallintoviraston tietämättö-myydestä velvoitteen sisällöstä. Laiminlyönnin voi arvioida Varsinais-Suomen hyvinvointialueen tarkastuslautakunnan arvointikertomuksen perusteella kertovan myös hyvinvointialueen laa-jemmistakin tietosuojaan ja tietoturvaan liittyvien velvoitteiden täyttämisen puutteista.

Hyvinvointialueen tietoturvasuunnitelman puuttumisessa on ollut kyse sellaisesta sote-valvon-talain 29 §:ssä kuvatussa asiakas- ja potilasturvallisuutta olennaisesti vaarantavasta epäkoh-dasta, josta saadun ilmoituksen perusteella valvontaviranomaisena toimineen Lounais-Suomen aluehallintoviraston olisi tullut ryhtyä toimenpiteisiin. Valvontaan liittyvät toimenpiteet olisivat ol-leet myös asiakas- ja potilasturvallisuuden kannalta kiireellisiä. Aluehallintoviraston olisi lisäksi ollut syytä saattaa asia Valviran tietoon valvontaan liittyvän ohjauksen saamiseksi.

Pyydän Lounais-Suomen aluehallintovirastoa ilmoittamaan viimeistään 16.5.2025, mihin toimiin se on ryhtynyt valvoakseen sitä, että Varsinais-Suomen hyvinvointialue täyttää tietoturvasuun-nitelman laatimista koskevan velvoitteensa sekä huolehtii ja varmistaa ajankohtaisesti asiakas- ja potilastietojen tietoturvallisen käsittelyn.

Tämä asiakirja on allekirjoitettu sähköisesti.

Apulaisoikeuskansleri

Mikko Puumalainen

Vanhempi oikeuskanslerinsihteeri

Maija-Liisa Goebel