Sisällys

VERSIOHISTORIA

Päivämäärä	Versio	Muutos	Tekijä
10.6.2020	1.0	Dokumentti hyväksytty	Jenni Siermala

1. Tietotilinpäätöksen tarkoitus

Tämä on SoteDigi Oy:n ensimmäinen tietotilinpäätös. Tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja -toimenpiteitä.

Tietotilinpäätös on tarkoitettu SoteDigi Oy:n sisäiseen käyttöön johtamisen raportiksi sekä sidosryhmille tietojen käsittelyn kuvaukseksi. Se toimii myös suunnittelun ja toiminnan ohjauksen sekä raportoinnin ja johtamisen tukena. Tietotilinpäätös on myös keskeinen dokumentti EU:n yleisen tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa lakien, hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan noudattamista.

SoteDigi Oy kunnioittaa tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita. Henkilötietojen käsittelyssä noudatetaan seuraavia vaatimuksia:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

Tässä dokumentissa kuvataan, miten em. periaatteet toteutuivat SoteDigi Oy:n toiminnassa vuonna 2019.

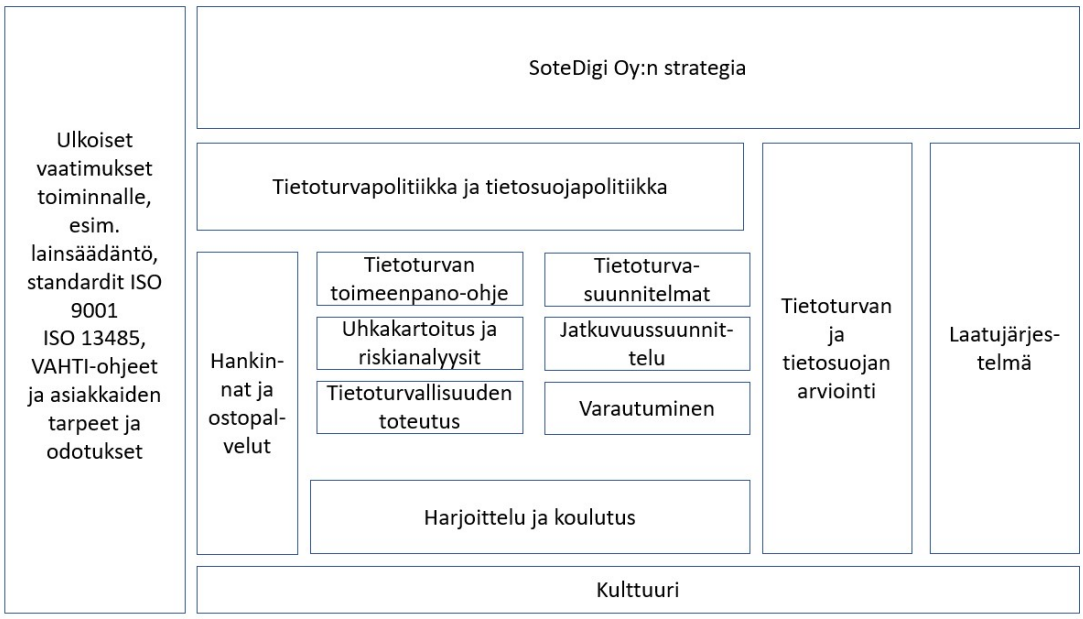
2. Tietosuojan ja tietoturvallisuuden toteuttaminen

Tässä luvussa kuvataan, miten eheys ja luottamuksellisuus tietosuojaperiaatteet toteutuvat SoteDigi Oy:n toiminnassa.

2.1 Tietoturvan organisointi

Tietosuojasta ja tietoturvallisuudesta SoteDigi Oy:ssä vastaava Toimitusjohtaja. Tietosuoja- ja tietoturva-asioista raportoidaan johtoryhmälle. SoteDigi Oy on laatinut tietosuojapolitiikan ja tietoturvapolitiikan. Yleiset tietoturvavastuut ja tiettyihin tehtäviin liittyvät tietoturvavastuut on kuvattu SoteDigi Oy:n tietoturva- ja tietosuojapolitiikoiden liittyvässä tietoturva ja tietosuojavastuut -dokumentissa. SoteDigi Oy:ssä on tietoturvapäällikkö, jonka tehtäviin lisättiin tietosuojavastaavan tehtävät. Tietosuojavastaava nimettiin Johtoryhmän kokouksessa 18.2.2019. Tietosuojavastaavan tehtävät on määritelty. Lisäksi tietosuojavastaava on suorittanut Itä-Suomen yliopiston järjestämän Osaava tietosuojavastaavakoulutuksen, joka luo pätevyyden toimia tietosuoja-asetuksessa säädettyjen tehtävien hoitamiseen.

Vuonna 2019 toteutettiin SoteDigi Oy:n tietoturvanhallintamalli ja kehitettiin palvelutuotannon tietoturva, tietosuoja ja jatkuvuudenhallintamenetelmä. Alla kuva SoteDigin tietoturvanhallintamallista.



Kuva 1, Tietoturvan hallintamalli

2.2 Tietosuojan ja tietoturvan koulutus ja ohjeistus

SoteDigi Oy:ssä hyväksyttiin tietoturvapolitiikka ja tietosuojapolitiikka. Tietosuoja- ja tietoturvapolitiikkoja täydentävät tietoturvasäännöt, henkilöstön tietoturvaohjeet, tietosuojan lomakkeet, tietosuoja- ja tietoturvaohjeet, koulutusaineistot. Henkilökunta sitoutuu salassapitoon työsopimuksessaan.

Kuva 2, Tietoturva- ja tietosuojadokumentit

SoteDigi Oy:n henkilöstö suoritti tietoturvakoulutuksen ja suoritti tietoturva- ja tietosuojatentin. Vastauksien keskiarvo oli 98%. Lisäksi johto ja esimiehet kävivät tietoturvakoulutuksen. Organisaation tieturvariskit tunnistettiin ja niille suunniteltiin näille mitigaatiot. Riskitasot hyväksyttiin johtoryhmässä ja käytiin läpi hallituksessa.

2.3 Henkilötietojen tekniset ja organisatoriset suojaustoimet

Henkilötietojen käsittelyssä käytettävien tietojärjestelmien hallinnassa noudatetaan SoteDigi Oy:n tietoturvasäännöstöä ja -ohjeita. Teknisesti tietojärjestelmät ja niiden käyttöliittymät ovat suojattu mm. palomuurilla ja SoteDigin työasemilla on virustorjuntaohjelmistot. Vimana Oy vastaa työaseman käyttöoikeuksien teknisestä toteuttamisesta. Vimana Oy toteuttaa myös teknisen tietoturvan sekä sen valvonnan.

Työasemien kovalevyt on salattu ja käytössä olevat muistitikut salataan myös työasemassa olevan salaustyökalun avulla. Lisäksi jokainen on vastuussa muistitikkujen viruksettomuudesta. Vimana Oy vastaa perustietotekniikasta, johon kuuluu työasemien ja verkkolaitteiden hankinta, käyttöönotto ja ylläpito. Työasemien asennuspalvelu on ulkoistettu Vimana Oy:n kumppanille. Sovellusten hankinnat ja asennukset sovitaan yhteistyössä Vimana Oy:n kanssa. Työasemientukitehtävissä käytettävät etäyhteydet toteutetaan salatusti Vimana Oy:n alihankkijan toimesta. Työasemien tietoliikenne turvataan VPN yhteyden avulla.

SoteDigissä on vähimpien käyttöoikeuksien periaate, jonka mukaisesti esimies valtuuttaa henkilöstölle riittävät käyttöoikeudet, siten että henkilöstöllä on työtehtäviensä laajuuden mukaiset käyttöoikeudet. SoteDigissä toteutettiin tietoturvan- ja tietosuojan omavalvontasuunnitelma, jonka mukaisesti tietoturvan ja tietosuojan toteutumista arvioidaan. Lisäksi palvelutuotannon tietoturva, tietosuoja ja jatkuvuudenhallintaohje turvaa SoteDigi Oy:n palvelun elinkaarenhallinnan. Alla kuvaus vuonna 2019 syntyneistä tietoturva- ja tietosuojadokumentaatioista.

2.4 Pseudonymisointi, anonymisointi

Pseudonymisointi (henkilötietojen käsittely siten, että niitä ei voida enää yhdistää tiettyyn henkilöön ilman erillään säilytettäviä lisätietoja). Henkilötiedot pseudonymisoidaan aina, kun henkilön suora tunnistaminen ei ole välttämätöntä. Henkilötiedon anonymisointi (henkilötiedot poistetaan siten, että tunnistaminen ja uusien tietojen yhdistäminen on mahdotonta).

SoteDigissä toteutettiin ohje tunnisteellisen tiedon ja anonymisoinnin osalta. Lisäksi päätettiin, että Tiedolla johtamisen hankkeessa on tärkeää arvioida tilanteet, joissa suorat ja epäsuorat henkilötiedot on tarpeen poistaa. Lisäksi Omaolon analytiikkaa toteutettaessa on huomioitava henkilötietojen poistaminen pseudonymisoinnin ja anonymisoinnin avulla.

2.5 Riskienhallinta ja tietoturvapoikkeamien käsittely

Vuosittain käydään läpi tietoturva- ja tietosuojariskiarviointi organisaation tasolla. Lisäksi Vaikutustenarviointi tehdään aina otettaessa käyttöön uutta teknologiaa, käsiteltäessä laajamittaisesti erityisiä henkilötietoryhmiä (EU:n yleinen tietosuoja-asetus, artiklat 9 ja 10) koskevia henkilötietoja.

Organisaation riskit käsitellään vuosittain ja toimitusjohtaja hyväksyy riskit. Vaikutuksenarvioinnin tarpeellisuusvaatimus arvioidaan omassa toiminnassa ja se toteutetaan tarvittaessa. Palvelutuotannossa toteutetaan tietoturva- ja tietosuojariskien arviointia riskisuunnitelman mukaisesti. Lisäksi palvelutuotannossa avustetaan rekisterinpitäjää ja toteutetaan vaikutuksenarviointi.

Kaikki tietoturvapoikkeamat käsitellään capa-prosessin mukaisesti. Capa prosessia on täydennetty tietoturva- ja tietosuojapoikkeamaprosessilla. Vuonna 2019 oli kaksi tietoturvapoikkeamaa. Näiden korjaavat ja ehkäisevät toimenpiteet on toteutettu sekä juurisyy selvitetty.

3. Tietovirrat

Tässä luvussa kuvataan, miten tietojen minimointi, käyttötarkoitussidonnaisuus ja säilytyksen rajoittaminen tietosuojaperiaatteina toteutuvat SoteDigin toiminnassa.

Tiedot on inventoitu ja tunnistettu. Tiedon luokittelu ja tiedonluokittelun mukainen käsittely suunniteltiin vuonna 2019. SoteDigin toimintaan velvoittavaa lainsäädäntöä ei ole tältä osin, joten tiedon luokittelu on toteutettu organisaation tarpeiden mukaan. Luokittelu on julkinen, sisäinen ja salainen. Tämän avulla voidaan kohdentaa kuhunkin tietoryhmään vaadittava käsittely ja tietoturvataso. Lisäksi tiedon säilytysajat on määritelty, jonka avulla varmistutaan siitä, että tiedon elinkaarenhallinta täyttää sille määritellyt säilytysajat.

Tietojärjestelmät on kartoitettu ja ne on määritelty tietojärjestelmä listaan. Lisäksi tietojärjestelmä kohtaisesti on määritelty:

- käyttötarkoitus
- mihin toimintoon järjestelmä liittyy
- palvelutuotteen elinkaarenhallintaan liittyvä tärkeysluokka
- tietoturvataso (vahti perustaso, korotettu tai pilvipalveluturvallisuus)
- tiedon luokittelu (julkinen, sisäinen salainen)
- kelpuutus (kyllä, ei)
- vastuut: omistaja ja pääkäyttäjä
- sijainti

Havaittiin, että palvelutuotannossa käytettävät kriittiset työvälineet Jira ja Confluencen eivät ole riittävän turvallisia toteutettaessa pilvipalvelussa. Tämän vuoksi työvälineet siirrettiin Erillisverkkojen konesaliin ja toteutettiin tiedon migraatio pilvipalvelusta.

Palvelutuotannon osalta on kuvattu tietovirrat, lokitiedot, henkilötietojen suojausvelvoite, jäljitettävyys ja läpinäkyvyys. Nämä on kuvattu kunkin palvelutuotteen tietoturva, tietosuoja ja jatkuvuudenhallinta -dokumentissa.

4. Rekisteröidyn oikeudet ja niiden toteuttaminen

Tässä luvussa kuvataan, miten rekisteröityjen oikeudet toteutuvat SoteDigi Oy:n toiminnassa (kohtuullisuus ja läpinäkyvyys tietosuojaperiaatteina).

Henkilöstön tietoturva ja tietosuojaohjeessa kuvataan henkilöstölle, mitä tarkoittaa rekisteröityjen oikeuksien toteuttaminen. Rekisteröityjä informoidaan henkilötietojen käsittelystä SoteDigin internet sivuilla olevalla tietosuojaselosteella. Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön tietosuojavastaavalle sähköpostilla tietosuoja@sotedigi.fi

4.1 Mistä henkilötiedot saadaan ja mihin niitä siirretään?

Henkilöstön ja eri sidosryhmiin kuuluvien henkilötiedot saadaan pääsääntöisesti rekisteröidyiltä itseltään. Henkilötietoja voidaan siirtää sisäisiin palveluihin esim. työsuhteen hoitamiseksi käsiteltäviä henkilötietoja. Henkilökunnan tietoja luovutetaan toiselle rekisterinpitäjälle ainoastaan asianomaisen suostumuksella tai lainsäädännön perusteella.

SoteDigi ei siirrä henkilötietoja EU tai ETA maiden ulkopuolelle.

4.2 Tietosuojaan liittyvät sopimusmallit

SoteDigi on tunnistanut tilanteet, joissa se on rekisterinpitäjä tai henkilötietojen käsittelijä. SoteDigi tekee tietosuojasopimukset henkilötietojen käsittelijöiden kanssa. SoteDigi on laatinut hankintoihin tietosuojasopimukset ja turvallisuussopimukset.

Tiedon laatu ja käytettävyys toteutuvat SoteDigin toiminnassa mm. siten, että

- käsitellään vain käyttötarkoituksen mukaisia ajan tasaisia henkilötietoja
- käyttöoikeudet on määritelty käyttäjäroolien mukaisesti
- tietosuoja ja tietoturva huomioidaan henkilötietojen käsittelyssä
- ja sitä valvotaan organisatorisin menetelmin
- tietojen elinkaari on hallinnassa ja säilytysajat sekä hävittäminen

5. Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus

Tietosuoja-asetus ei edellytä rekisterikohtaisia selosteita, vaan tietosuojaselosteita rekisterinpitäjän käsittelytoimista sekä läpinäkyvää informointia henkilötietojen käsittelystä. SoteDigissä on tietosuoja-asetuksen artiklan 30 mukainen tietosuojaselostepohja, jota hyödynnetään eri käyttötarkoituksiin.

EU:n yleinen tietosuoja-asetus EU 679/2016
Tietosuojalaki 5.12.2018/1050
Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi
Laki yksityisyyden suojasta työelämässä (759/2004)
Laki sähköisen viestinnän palveluista (68/2018)
Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
Valmiuslaki 29.12.2011/1552

Lisäksi STM on ohjeistanut seuraavasti:
SoteDigi Oy on julkisesti omistettu yhtiö ja sen tulee toiminnassaan noudattaa julkisen hallinnon toimintaperiaatteita, esimerkiksi ohjeita julkisista hankinnoista. Tämä koskee myös turvallisuutta. Samalla on kuitenkin muistettava, että vaadittava turvallisuustaso määräytyy toiminnan mukaan. Tuottaessaan sähköisiä palveluita sosiaali- ja terveydenhuollolle SoteDigi Oy:n on noudatettava tähän toimintaan liittyviä turvallisuusmääräyksiä.

Yleisessä toiminnassaan SoteDigi Oy:n tulee noudattaa VAHTI ohjeistusta. Tarjotessaan sähköisiä palveluita sosiaali- ja terveydenhuollolle SoteDigi Oy tulee noudattaa THL:n antamia ohjeita, jotka perustuvat asiakastietolakiin ja liittyvät Kanta-palveluihin, turvallisuuteen ja omavalvontaan. Lisäksi on otettava huomioon tietosuojaan ja lääkintälaitteisiin liittyvät määräykset. Näihin määräyksiin ja ohjeisiin liittyvää yksityiskohtaisempaa ohjausta antavat THL ja Valvira.

Lisäksi Kyberturvallisuuskeskus on ohjeistenut SoteDigiä seuraavasti:

Tuottaessa sähköisiä palveluja julkiselle sosiaali- ja terveydenhuollolle ja jos kyseessä on lääkinnällisten laitteiden asetuksen 2017/745/EU (MDR) mukainen lääkinnällinen laite SoteDigi Oy noudattaa STIV tietoturvatasoa.

Tietoaineistojen käsittelyä ohjaavat mm. seuraavat dokumentit:

- Tietosuojapolitiikka
- Tietoturvapolitiikka
- Tietoturvasäännöt, -ohjeet ja -prosessit
- Tietosuojaselosteiden mallipohjat
- Vaikutustenarvioinnin ohjeet ja mallipohjat

6. Seuranta ja mittaaminen

Tietosuojan ja tietoturvan tilaa SoteDigissä vuonna 2019 voidaan kuvata seuraavin tunnusluvuin.

Aihe	Määrä
Henkilötietojen tarkastus-, oikaisu- ja poistopyynnöt Tarkastuspyynnöt Oikaisupyynnöt Poistopyynnöt	0
Kieltäytymiset automaattisesta päätöksenteosta	0
Valvontaviranomaisten selvitys- ja tietopyynnöt	0
Tarpeelliset ilmoitukset valvontaviranomaiselle Tietoturvaloukkausilmoitukset	1
Käyttö- ja luovutuslokipyynnöt	0
Vakavat tietoturvapoikkeamat	0
Esille tulleet tietosuojarikkomukset ja niiden epäilyt	0
Tietojärjestelmien käyttökatkot ja niiden laajuudet	0
Tietojärjestelmien määrä	20
Rekisterit	ei arvioitu
Auditoinnit	6
Koulutukset • Henkilötön tietoturva- ja tietosuojakoulutus • Johdon ja esimiesten tietoturvakoulutus	2

Sidosryhmäyhteistyön osalta SoteDigi on mukana seuraavissa tietosuoja- ja tietoturvaryhmissä:
Jenni Siermala Vahti Toiminnan jatkuvuudenhallinta asiantuntijaryhmä PJ

7. Arviointi ja kehittäminen

SoteDigissä vuonna 2019 palkattiin tietoturvapäällikkö ja hän toteutti tietoturvanhallintamallin. Vuoden 2019 loppuun mennessä saatiin tämän lisäksi valmiiksi tietoturva- tietosuoja dokumentit, -prosessit sekä ohjeet. Henkilöstö koulutettiin näiden osalta sekä tunnistettiin riskit.

Vuonna 2019 toteutettiin tietoturva-, -tietosuoja ja jatkuvuudenhallintaprosessit palvelutuotteen elinkaarenhallintaa. Palvelutuotannossa toteutettiin vaaditut auditoinnit. Organisaatiotasoisia auditointeja ei toteutettu.

Vuoden 2019 kesäkuussa on saatu tieto, että SoteDigi Oy ja Vimana Oy yhdistyvät. Tietoturva ja tietosuojahallintamalli on tarkasteltava tällöin uuden yhtiön tarpeiden mukaiseksi. SoteDigin tulee jatkaa organisaation rekisterinpitäjävastuiden ja organisaatiotason varautumisen sekä jatkuvuudenhallintaa vaatimusten mukaiselle tasolle.