Versio 2.0, voimassa 1.1.2022 alkaen
Käsittely:
Tietosuojatyöryhmä 9.11.2021
Yhtymähallitus xx.12.2021

Tietosuoja- ja tietoturvapolitiikka

Siun soten kuntayhtymä ja konserni

Siun SOTE

Pohjois-Karjalan sosiaali- ja terveyspalvelujen kuntayhtymä
www.siunsote.fi

Sisällysluettelo

1. Johdanto

Siun sote järjestää julkiset sosiaali- ja terveydenhuollon, pelastustoimen ja ympäristöterveydenhuollon palvelut 13 kunnan alueella Pohjois-Karjalassa. Siun soten strategian[1] tavoitteena on hyvinvoiva pohjoiskarjalainen ja tehtävänä lupaus turvata pohjoiskarjalaisten arkea. Yhtenä perusedellytyksenä palveluiden ja hoidon turvallisuuden ja laadun toteutumiselle on, että huolehditaan käsiteltävien tietojen oikeista käsittelytavoista, tietojen suojaamisesta sekä digitaalisten palveluiden ja järjestelmien turvallisuudesta.

Tietosuoja- ja tietoturvapolitiikassa kuvataan ne periaatteet, tavoitteet, organisointitavat ja vastuut, joita Siun sote noudattaa tietosuojan ja tietoturvallisuuden toteuttamisessa ja kehittämisessä. Politiikallaan Siun sote sitoutuu tietosuojaa ja tietoturvallisuutta koskevan soveltuvan lainsäädännön ja viranomaisvaatimusten täyttämiseen sekä siihen, että tietosuoja ja tietoturvallisuus toteutuvat Siun sotessa, sen tuottamissa ja käyttämissä palveluissa sekä yhteistyössä sidosryhmien kanssa ja hankittaessa palveluita Siun soten ulkopuolelta.

Tietosuojalla tarkoitetaan yksityisyydensuojan sekä rekisteröidyn oikeuksien ja vapauksien toteutumista henkilötietojen käsittelyssä. Tietoturva on yksi tietosuojan toteuttamisen keino, mutta ei yksin takaa tietosuojavaatimusten toteutumista.

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä keinoja, joilla suojataan tietoa normaalioloissa sekä häiriö- ja poikkeustilanteissa. Tietoturvan keinoin suojataan kaikkea toiminnan kannalta keskeistä tietoa, ei pelkästään henkilötietoa.

Tietosuoja- ja tietoturvapolitiikka koskee Siun soten kuntayhtymää. Konserniin kuuluvia tytäryhtiöitä tietosuoja- ja tietoturvapolitiikka koskee periaatteiden ja tavoitteiden osalta. Tytäryhtiöistä Siun työterveys Oy:ltä ja Polkka Oy:ltä edellytetään kummaltakin oman politiikan laatimista toiminnan luonteen perusteella. Kaikki tytäryhtiöt myös tekevät omat toimintaansa sopeutuvat tietosuoja- ja tieturvasuunnitelmansa ja -ohjeistuksensa sekä vastaavat toimintansa tietosuojan ja tietoturvan toteutumisesta. Tytäryhtiöt raportoivat tietosuojan ja tietoturvan tilasta omille hallituksilleen kerran vuodessa tilinpäätöksen yhteydessä ja tarvittaessa.

[1] Siun soten strategia 2021–2025

2. Periaatteet ja tavoitteet

Siun sote sitoutuu kaikessa toiminnassaan seuraaviin tietosuojan ja tietoturvan periaatteisiin sekä periaatteiden mukaisiin tietosuoja- ja tietoturvatyön tavoitteisiin.

2.1 Tietojen käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- Toiminnassa noudatetaan lainsäädännön ja viranomaismääräysten ja -ohjeiden tietosuoja- ja tietoturvavaatimuksia. Toiminnan lainmukaisuus toteutuu myös yhteistyössä sidosryhmien ja ulkopuolisten palveluntuottajien kanssa.
- Henkilötietojen käsittely perustuu ennalta määriteltyihin käsittelyperusteisiin, kuten lakisääteisten velvoitteiden noudattamiseen, sopimuksiin tai henkilöiden antamiin suostumuksiin.
- Rekisteröidyille kerrotaan heidän tietojensa käsittelystä ja heidän oikeuksistaan sekä tarjotaan heille keinot käyttää oikeuksiaan.

2.2 Tietojen minimointi, käyttötarkoitussidonnaisuus ja säilytyksen rajoittaminen

- Henkilötietoja kerätään ja käsitellään vain ennalta suunniteltuja ja määriteltyjä sekä laillisia käyttötarkoituksia varten.
- Henkilötietoja säilytetään vain niin kauan kuin se on tarpeen tietojen käyttötarkoituksia varten. Säilytysajoissa huomioidaan kansallinen lainsäädäntö.

2.3 Tietojen luottamuksellisuus, turvallisuus, eheys ja saatavuus

- Tietoaineistot luokitellaan ja käsitellään luokittelun edellyttämillä tavoilla.
- Tiedot suojataan ja varmistetaan siten, että niitä pääsevät käsittelemään vain sellaiset henkilöt, jotka työtehtäviensä puolesta ovat siihen oikeutettuja.
- Tietojen käsittelyä valvotaan säännöllisesti ja ennalta suunnitellusti.
- Henkilöstön tietosuoja- ja tietoturvatietoisuutta kehitetään ja osaamisesta huolehditaan ohjeistuksin, koulutuksin ja viestinnän keinoin.
- Varautumisen ja jatkuvuuden hallinnan keinoin varmistetaan, että keskeytyksistä ja häiriöistä huolimatta toiminta ja palvelut voidaan hoitaa asiakas- ja potilasturvallisuutta vaarantamatta, ja palautuminen normaalitoimintaan tapahtuu mahdollisimman nopeasti.
- Tietojärjestelmät luokitellaan vaikuttavuuden ja kriittisyyden mukaan, jotta varautuminen erilaisiin häiriö- ja poikkeustilanteisiin voidaan kohdentaa oikein. Luokittelua käytetään myös sovittaessa palvelutasoista ICT-palveluntuottajien kanssa.
- Tietosuojariskit ja tietoturvariskit eli tiedon luottamuksellisuuden, eheyden, saatavuuden ja käytettävyyden menettämiseen liittyvät riskit sisältyvät osaksi kuntayhtymän kokonaisvaltaista riskienhallintaa.

- Palveluiden ja tietojärjestelmien tietosuoja- ja tietoturvariskit arvioidaan, ja tarvittavat suojatoimet riskien hallitsemiseksi määritellään tekemällä tietosuojan vaikutustenarviointeja mahdollisimman varhaisessa vaiheessa hankintoja tai suunniteltaessa merkittäviä muutoksia.
- Sidosryhmien ja ulkoisten palveluntuottajien kanssa solmittaviin sopimuksiin sisällytetään asianmukaiset tietosuojan ja tietoturvan vaatimukset.
- Tietosuojan ja tietoturvan toteutumista seurataan ja raportoidaan säännöllisesti kuntayhtymän osavuosikatsauksen ja tilinpäätöksen yhteydessä.

3. Organisointi ja vastuut

3.1 Johdolla on kokonaisvastuu tietosuojan ja tietoturvan toteutumisesta

Siun soten yhtymähallitus hyväksyy ja vahvistaa konsernin tietosuoja- ja tietoturvapolitiikan.

Siun soten toimitusjohtaja vastaa tietosuojan ja tietoturvan sekä näiden koordinoinnin, ylläpidon, valvonnan ja kehittämisen kokonaisuudesta. Hän nimeää rekisterien vastuuhenkilöt, ellei niitä ole laissa määritetty, vahvistaa päätöksellään tietojärjestelmien tärkeysluokituksen ja kriittisten tietojärjestelmien luettelon sekä raportoi tietosuojan ja tietoturvan kokonaisuudesta yhtymähallitukselle. Toimitusjohtajan tehtävänä on huolehtia kuntayhtymän sisäisen valvonnan ja riskienhallinnan järjestämisestä, mikä koskee myös tietosuojan ja tietoturvan asianmukaista järjestämistä. Lisäksi hän vastaa yhdessä **toimialuejohtajien** kanssa tietosuoja- ja tietoturvapolitiikan toteutuksesta hallinnollisella tasolla sekä varmistaa tietosuoja- ja tietoturvatyöhön tarvittavat resurssit.

Siun soten toimitusjohtajan nimeämä **tietosuojatyöryhmä** toimii myös tietoturvaryhmänä. Työryhmän tavoitteena on suunnitella ja kehittää Siun soten tietosuoja- ja tietoturvatyötä. Työryhmässä käsitellään keskeisiä tietosuojaohjeistuksia, tehdään tarvittavia linjauksia tietosuoja- ja tietoturva-asioissa ja käydään läpi tietosuojatyöhön liittyviä hankkeita ja ajankohtaisia asioita.

Siun soten häiriötilanne-johtoryhmä vastaa toimenpiteiden organisoinnista vakavissa tietoturvaongelmissa.

3.2 Toimialueet vastaavat tietosuojan ja tietoturvan toteutumisesta omassa toiminnassaan

Siun soten toimialuejohtajilla on ylin vastuu tietosuojan ja tietoturvallisuuden toteutumisesta omien toimialueidensa osalta.

Siun soten palvelupäälliköt ja esihenkilöt vastaavat toimintayksikkötasolla tietosuojan ja tietoturvan toteutumisesta sekä näihin liittyvien periaatteiden ja ohjeiden noudattamisesta omissa yksiköissään ja vastuualueillaan. He myös huolehtivat siitä, että tietosuoja ja tietoturva toteutuvat henkilöstöprosessin

kaikissa vaiheissa (mm. uusien työntekijöiden perehdytys, henkilöstön koulutus, käyttöoikeuksien myöntäminen) sekä vastaavat tietosuojaa ja tietoturvaa koskevasta viestinnästä henkilöstölle.

Palveluiden ja niissä käytettävien tietojärjestelmien vastuuhenkilöt vastaavat tietojärjestelmien ja niiden sisältämän tiedon tietosuojan ja tietoturvan toteutumisesta (mukaan lukien tiedon luokittelu ja tallentaminen luokituksen edellyttämään ympäristöön). He vastaavat toteuttamiensa ja suoraan ulkoiselta palveluntuottajalta hankkimiensa tietojärjestelmien tietosuoja- ja tietoturvavaatimusten toteutumisesta varmistamalla ennen hankintapäätöstä, että tietojärjestelmästä on tehty Siun sotessa EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi. Lisäksi he varmistavat, että toteutettava tai hankittava tietojärjestelmä on Siun soten kokonaisarkkitehtuurin mukainen, ja että järjestelmän jatkuvuus on huomioitu toimialueen valmiussuunnitelmassa (edellyttää järjestelmän tärkeysluokittelua). He myös nimittävät vastuullaan olevien tietojärjestelmien **pääkäyttäjät**, jotka tukevat omalta osaltaan vastuuhenkilöitä tietosuojan ja tietoturvan toteutumisessa.

Pääsääntöisesti vastuu palveluista ja tietojärjestelmistä on toimialuejohtajalla, joka voi myös delegoida vastuun tapauskohtaisesti toiselle henkilölle.

- Yhteisten potilastietojärjestelmien vastuuhenkilö on **terveys- ja sairaanhoitopalvelujen toimialuejohtaja.**
- Sosiaalipalvelujen asiakastietojärjestelmien vastuuhenkilö on **perhe- ja sosiaalipalvelujen toimialuejohtaja.**
- Pelastuslaitoksen tietojärjestelmien vastuuhenkilö on **pelastusjohtaja**.
- Ympäristöterveydenhuollon tietojärjestelmien vastuuhenkilö on **ympäristöterveydenhuollon johtaja.**
- Henkilöstöhallinnon tietojärjestelmien vastuuhenkilö on **henkilöstöjohtaja.**
- Taloushallinnon tietojärjestelmien vastuuhenkilö on **talousjohtaja.**
- Hallinnon tietojärjestelmien vastuuhenkilö on **hallintojohtaja**.

Toimialueiden palveluissa ja niissä käytettävien tietojärjestelmien osalta vastuut määräytyvät palvelun tai tietojärjestelmän käyttölaajuuden mukaan siten, että vastuuhenkilö on sen vastuualueen tai toimintayksikön esihenkilö, jonka vastuualueella palvelua tai tietojärjestelmää käytetään.

3.3 Tietosuojavastaavat toimivat tietosuojan erityisasiantuntijoina

Siun soten toimitusjohtajan nimeämät **tietosuojavastaavat** seuraavat ja valvovat henkilötietojen käsittelyä sekä tietosuojasäännösten ja -ohjeiden noudattamista kuntayhtymässä. He neuvovat ja ohjaavat henkilöstöä ja rekisteröityjä tietosuojakysymyksissä ja toimivat tietosuoja-asiantuntijoina vaikutustenarvioinnin prosessissa. Tietosuojavastaavat seuraavat tietoturvaloukkausten ilmoitusvelvollisuuden toteutumista ja toimivat yhteyshenkilöinä Siun soten ja viranomaisten välillä henkilötietojen käsittelyyn liittyvissä kysymyksissä. He toteuttavat lakisääteistä raportointia johdolle tietosuojan tilasta.

3.4 Turvallisuuspäällikkö ja digijohtaja vastaavat tietoturvatyön kokonaisuudesta

Siun soten digijohtaja, turvallisuuspäällikkö ja toimialuejohtajat valmistelevat tietojärjestelmien tärkeysluokituksen ja kriittisten tietojärjestelmien luettelon toimitusjohtajan vahvistettavaksi.

Siun soten turvallisuuspäällikkö vastaa hallinnollisen tietoturvan toteutumisesta. Hän valvoo kriittisten tietojärjestelmien luetteloiden ylläpitoa sekä sitä, että tietoturvan taso, katastrofi- ja poikkeustilavalmius vastaavat päätöksiä ja säännöksiä.

Siun soten digijohtaja vastaa teknisen tietoturvan toteutumisesta ja valvoo tietojärjestelmäpalvelujen tietoturvan tasoa. Hän huolehtii siitä, että uusien järjestelmien kehittämishankkeissa ja käyttöönotoissa huomioidaan tarvittavat tietoturva-asiat.

3.5 Henkilöstöllä on keskeinen rooli tietosuojan ja tietoturvan toteutumisessa

Jokainen Siun soten viranhaltija ja työntekijä on vastuussa tietosuojan ja tietoturvallisuuden toteuttamisesta omalta osaltaan. Jokainen sitoutuu lainsäädännön lisäksi noudattamaan Siun soten tietosuoja- ja tietoturvapolitiikan periaatteita sekä politiikan toteuttamiseen liittyviä määräyksiä, ohjeita ja toimintatapoja. Koko henkilöstö on velvollinen osallistumaan heille osoitettuun tietosuoja- ja tietoturvakoulutukseen sekä ilmoittamaan havaitsemistaan tietosuoja- ja tietoturvapoikkeamista esihenkilölleen ja tietosuojavastaaville.

3.6 Tietosuojan ja tietoturvan vastuut sidosryhmien ja palveluntuottajien toiminnassa varmistetaan sopimuksin

Ulkoiset sidosryhmät ja palveluntuottajat vastaavat omalta osaltaan tietosuojan ja tietoturvallisuuden toteutumisesta toiminnoissaan ja palveluissaan lainsäädännön mukaisesti. Siun sote varmistaa osaltaan ulkoisten toimijoiden toiminnan lainmukaisuuden palveluntuottajien kanssa sisällyttämällä toimijoiden kanssa solmittaviin sopimuksiin tietosuoja- ja tietoturvavaatimukset. Ulkopuolisten ICT-palveluntuottajien kanssa laadituissa sopimuksissa vaaditaan myös tietojärjestelmäluokituksen mukainen palvelutaso, joka palveluntuottajien tulee ottaa huomioon omissa varautumis- ja toipumissuunnitelmissaan. Siun sotella on sopimuksin varmistettu oikeus tarkastaa palveluntuottajien toimintaa.