Tietosuoja- ja tietoturvapolitiikka

Pohjois-Karjalan hyvinvointialue

Aluehallitus 30.11.2022, § 222

Sisällysluettelo

1 Johdanto

Pohjois-Karjalan hyvinvointialue (Siun sote) vastaa Pohjois-Karjalan alueen asukkaiden sosiaali- ja terveydenhuollon sekä pelastustoimen ja ympäristöterveydenhuollon palveluista. Tämä tietosuoja- ja tietoturvapolitiikka koskee koko Pohjois-Karjalan hyvinvointialuetta. Hyvinvointialueen tytäryhtiöitä tietosuoja- ja tietoturvapolitiikka koskee periaatteiden ja tavoitteiden osalta. Tytäryhtiöistä Siun työterveys Oy:ltä ja Polkka Oy:ltä edellytetään kummaltakin oman politiikan laatimista näiden toiminnan luonteen perusteella.

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

Tietosuoja- ja tietoturvapolitiikan pohjalta laaditaan hyvinvointialueen tietosuoja- ja tietoturvasuunnitelma sekä siihen pohjautuvat käytännön tason ohjeet. Hyvinvointialueen pelastustoimen toimialaa koskevat lisäksi myös oman toimialan kansalliset tietoturvaohjeistukset. Kaikki hyvinvointialueen tytäryhtiöt tekevät omat toimintaansa sopeutuvat tietosuoja- ja tieturvasuunnitelmansa ja -ohjeistuksensa, vastaavat toimintansa tietosuojan ja tietoturvan toteutumisesta sekä raportoivat tietosuojan ja tietoturvan tilasta omille hallituksilleen kerran vuodessa tilinpäätöksen yhteydessä ja tarvittaessa.

Tietosuojalla tarkoitetaan yksityisyydensuojan sekä rekisteröidyn oikeuksien ja vapauksien toteutumista henkilötietojen käsittelyssä. Yksi tietosuojan toteuttamisen keino on tietoturva, mutta sen keinoin ei pelkästään voida taata 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.

2 Periaatteet ja tavoitteet

Pohjois-Karjalan hyvinvointialue sitoutuu kaikessa toiminnassaan seuraaviin tietosuojan ja tietoturvan periaatteisiin sekä näiden 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.
- Henkilötietojen käsittelyn kohteena oleville henkilöille (rekisteröidyille) kerrotaan heitä koskevien tietojen käsittelystä, heidän tietosuojaoikeuksistaan sekä tarjotaan keinot oikeuksien käyttämiseksi.
- Henkilötietojen käsittelyssä havaitut poikkeamat tuodaan esille ja henkilötietojen tietoturvaloukkaukset dokumentoidaan. Jos loukkauksesta aiheutuu riski rekisteröidyn oikeuksille ja vapauksille, loukkauksesta tehdään ilmoitus tietosuojavaltuutetun toimistolle ja tarvittaessa rekisteröidylle itselleen.

2.2 TIETOJEN MINIMOINTI, KÄYTTÖTARKOITUSSIDONNAISUUS JA SÄILYTYKSEN RAJOITTAMINEN

- Henkilötietoja kerätään ja käsitellään vain ennalta suunniteltuja, määriteltyjä ja laillisia käyttötarkoituksia varten.
- Henkilötietoja kerätään vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden.
- Henkilötietoja säilytetään vain niin kauan kuin se on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Säilytysajoissa huomioidaan kansallinen lainsäädäntö. Säilytysajan päätyttyä henkilötiedot joko poistetaan tai anonymisoidaan.

2.3 TIETOJEN LUOTTAMUKSELLISUUS, TURVALLISUUS, EHEYS JA SAATAVUUS

- Tietoaineistot luokitellaan ja tietoja käsitellään luokittelun edellyttämillä tavoilla.
- Tiedot suojataan siten, että niitä pääsevät käsittelemään vain sellaiset henkilöt, jotka työtehtäviensä puolesta ovat käsittelyyn oikeutettuja.
- Tietojen käsittelyä sekä ohjeiden ja määräysten noudattamista valvotaan. Havaittuihin poikkeamiin puututaan, ne dokumentoidaan ja niistä raportoidaan.

- Henkilöstön tietosuoja- ja tietoturvaosaamista kehitetään perehdytyksen, koulutusten, ohjeistusten sekä tiedottamisen 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.
- Tietosuoja- ja tietoturvariskit eli tiedon luottamuksellisuuden, eheyden, saatavuuden ja käytettävyyden menettämiseen liittyvät riskit sisältyvät hyvinvointialueen kokonaisvaltaiseen riskienhallintaan.
- Henkilötietojen käsittelystä aiheutuvia riskejä tunnistetaan, arvioidaan ja hallitaan tekemällä tietosuojaa koskevia vaikutustenarviointeja, kun muun muassa hankitaan uusia palveluja, otetaan käyttöön uutta teknologiaa tai suunnitellaan merkittäviä muutoksia olemassa oleviin palveluihin tai tietojärjestelmiin.
- Sidosryhmien ja ulkoisten palveluntuottajien kanssa solmittaviin sopimuksiin sisällytetään asianmukaiset tietosuojan ja tietoturvan vaatimukset.
- Tietosuojan ja tietoturvan toteutumista sekä yleistä kyberturvallisuuden tilaa seurataan säännöllisesti. Tietosuojan ja tietoturvan toteutumisesta raportoidaan hyvinvointialueen osavuosikatsauksen ja tilinpäätöksen yhteydessä.

3 Organisointi ja vastuut

3.1 HYVINVOINTIALUE VASTAA TIETOSUOJAN JA TIETOTURVAN KOKONAISUUDESTA

Hyvinvointialue toimii rekisterinpitäjänä, kun se määrittelee toiminnassaan ja palveluissaan henkilötietojen käsittelyn tarkoitukset ja keinot, tai kun sille on laissa säädetty rekisterinpitoa koskeva tehtävä.

Hyvinvointialueen aluehallituksella on kokonaisvastuu hyvinvointialueen tietosuojasta ja tietoturvasta sekä kokonaisvaltaisesta riskienhallinnasta. Aluehallitus hyväksyy hyvinvointialueen tietosuoja- ja tietoturvapolitiikan sekä sisäisen valvonnan ja riskienhallinnan suunnitelman.

Hyvinvointialuejohtaja luo edellytykset tietosuojan ja tietoturvan asianmukaiselle toteuttamiselle hyvinvointialueella. Hyvinvointialuejohtaja vastaa tietosuoja- ja tietoturvatyön koordinoinnista, ylläpidosta, valvonnasta ja kehittämisestä sekä tietosuojan ja tietoturvan kokonaisuuden raportoinnista aluehallitukselle. Hyvinvointialuejohtaja nimeää rekisterinpitäjälle edustajat, ellei niitä ole laissa määritelty. Hyvinvointialuejohtaja on nimennyt tuekseen johtoryhmän, johon rekisterinpitäjän edustajat (toimialuejohtajat) kuuluvat. Yhdessä he

vastaavat tietosuoja- ja tietoturvapolitiikan toteutuksesta hallinnollisella tasolla sekä varmistavat tietosuoja- ja tietoturvatyöhön tarvittavat resurssit.

Rekisterinpitäjän edustajat ovat kokonaisvastuussa rekisterinpidosta ja tietovarannoista, ja he edustavat rekisterinpitäjää, kun on kyse tietosuoja-asetukseen perustuvista rekisterinpitäjän velvollisuuksista.

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

Hyvinvointialueen hallintopalveluihin sijoittuva **turvallisuuspäällikkö** vastaa hallinnollisen tietoturvan toteutumisesta. Hän valvoo kriittisten tietojärjestelmien luetteloiden ylläpitoa sekä sitä, että tietoturvan taso, katastrofi- ja poikkeustilavalmius vastaavat päätöksiä ja säännöksiä. Turvallisuusviranomaisen tehtävien osalta tietoturvan kokonaisuudesta vastaa **pelastusjohtaja** yhteistyössä digijohtajan ja turvallisuuspäällikön kanssa.

Tietosuojavastaavat ovat hyvinvointialuejohtajan nimeämiä tietosuojan erityisasiantuntijoita ja toimivat turvallisuuspäällikön alaisuudessa hallintopalveluissa. He seuraavat ja valvovat henkilötietojen käsittelyä sekä tietosuojasäännösten ja -ohjeiden noudattamista hyvinvointialueella. He neuvovat ja ohjaavat henkilöstöä ja rekisteröityjä tietosuojakysymyksissä ja toimivat asiantuntijoina vaikutustenarvioinnin prosessissa. Tietosuojavastaavat seuraavat tietoturvaloukkausten ilmoitusvelvollisuuden toteutumista ja toimivat yhteyshenkilöinä hyvinvointialueen ja viranomaisten välillä henkilötietojen käsittelyyn liittyvissä kysymyksissä. He toteuttavat lakisääteistä raportointia hyvinvointialuejohtajalle ja johtoryhmälle tietosuojan tilasta ja kehittämistarpeista.

Tietosuojatyöryhmä on hyvinvointialuejohtajan nimeämä ja turvallisuuspäällikön koordinoima työryhmä, joka toimii myös tietoturvatyöryhmänä. Työryhmän tavoitteena on suunnitella ja kehittää hyvinvointialueen tietosuoja- ja tietoturvatyötä. Työryhmässä käsitellään keskeisiä tietosuojaohjeistuksia, tehdään tarvittavia linjauksia tietosuoja- ja tietoturva-asioissa ja käydään läpi tietosuojatyöhön liittyviä hankkeita ja ajankohtaisia asioita.

Häiriötilanne-johtoryhmä on hyvinvointialuejohtajan tilannekohtaisesti koollekutsuma työryhmä, joka vastaa toimenpiteiden organisoinnista vakavissa tietoturvaongelmissa.

3.2 TOIMIALUEET VASTAAVAT TIETOSUOJAN JA TIETOTURVAN TOTEUTUMISESTA OMASSA TOIMINNASSAAN

Toimialuejohtajat ja heihin rinnastettavat **yhteisten palvelujen johtajat** vastaavat toimialueensa sekä palvelujensa tietosuojan ja tietoturvallisuuden toteutumisesta kokonaisuutena, huomioiden lainsäädännön sekä hyvinvointialueen tietoturva- ja tietosuojapolitiikan sekä ohjeistukset.

Palvelujohtajat ja palvelupäälliköt vastaavat palvelu- ja vastuualueidensa tietosuojan ja tietoturvan toteutumisesta.

Esihenkilöt vastaavat tietosuojan ja tietoturvan toteutumisesta toimintayksiköissään huomioiden monialaisen ja -ammatillisen palveluympäristön. Esihenkilöt vastaavat toimintayksiköiden työntekijöiden perehdytyksestä, osaamisen kehittämisestä, työtehtävien mukaisista henkilötietojen käsittelyoikeuksista sekä tietosuojaan ja tietoturvaan liittyvien asioiden käsittelystä yksikköpalavereissa.

Jokainen **hyvinvointialueen henkilöstöön kuuluva viranhaltija ja työntekijä** on vastuussa tietosuojan ja tietoturvallisuuden toteuttamisesta omalta osaltaan työn arjessa. Jokainen sitoutuu lainsäädännön lisäksi noudattamaan hyvinvointialueen tietosuoja- ja tietoturvapolitiikan periaatteita, politiikan toteuttamiseen liittyviä suunnitelmia, ohjeita ja toimintatapoja sekä allekirjoittamansa salassapito- ja käyttäjäsitoumuksen velvoitteita. Koko henkilöstö on velvollinen osallistumaan heille osoitettuun tietosuoja- ja tietoturvakoulutukseen sekä ilmoittamaan havaitsemistaan tietosuoja- ja tietoturvapoikkeamista esihenkilölleen ja hyvinvointialueen tietosuojavastaaville.

3.3 TIETOJÄRJESTELMIEN VASTUUHENKILÖT VASTAAVAT JÄRJESTELMIEN TIETOSUOJASTA JA TIETOTURVALLISUUDESTA

Pääsääntöisesti vastuu toimialueen tietojärjestelmistä on hyvinvointialueen **toimialuejohtajalla**, joka voi myös delegoida vastuun tapauskohtaisesti toiselle henkilölle. Vastuu voi määräytyä myös tietojärjestelmän käyttölaajuuden mukaan siten, että vastuuhenkilö on sen vastuualueen tai toimintayksikön esihenkilö, jonka alueella tai yksikössä tietojärjestelmää käytetään.

Tietojärjestelmien vastuuhenkilöt vastaavat järjestelmien ja niiden sisältämän tiedon tietosuojan ja tietoturvan toteutumisesta (mukaan lukien tiedon luokittelu ja käsittely asianmukaisesti suojatussa ympäristössä). He vastaavat hankkimiensa tietojärjestelmien tietosuoja- ja tietoturvavaatimusten toteutumisesta varmistamalla, että tietojärjestelmästä on tarvittaessa tehty EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi. Lisäksi he varmistavat, että hankittava tietojärjestelmä on hyvinvointialueen kokonaisarkkitehtuurin mukainen, ja että järjestelmän jatkuvuus on huomioitu toimialueen valmiussuunnitelmassa (edellyttää järjestelmän tärkeysluokittelua).

Vastuuhenkilöiden nimeämät **tietojärjestelmien pääkäyttäjät** huolehtivat omalta osaltaan tietosuojan ja tietoturvan toteutumisesta järjestelmissä. Pääkäyttäjät vastaavat järjestelmästä riippuen järjestelmän ylläpitotoimintojen ja käyttöoikeushallinnan toteuttamisesta sekä toimivat yhteyshenkilöinä järjestelmätoimittajaan.

Jokainen **tietojärjestelmän käyttäjä** vastaa omalta osaltaan ohjeiden noudattamisesta ja tietojärjestelmiin liittyvistä poikkeamista ilmoittamisesta esihenkilölleen.

3.4 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. Pohjois-Karjalan hyvinvointialue varmistaa osaltaan ulkoisten toimijoiden toiminnan lainmukaisuuden sisällyttämällä toimijoiden kanssa solmittaviin sopimuksiin asianmukaiset tietosuoja- ja tietoturvavaatimukset. Niistä henkilöistä, jotka käsittelevät työssään turvallisuusviranomaisten salassa pidettävää tietoa (TLII – TLIV), tai hyvinvointialueen valmiussuunnitteluun tai turvallisuuteen liittyvää salassa pidettävää tietoa, tehdään hyvinvointialueen toimesta perusmuotoiset turvallisuusselvitykset. Pelastustoimi laatii yhteistyökumppaneiden kanssa tarvittaessa turvallisuussopimukset. Ulkopuolisten ICT-palveluntuottajien kanssa laadituissa sopimuksissa vaaditaan myös tietojärjestelmäluokituksen mukainen palvelutaso, joka palveluntuottajien tulee ottaa huomioon omissa varautumis- ja toipumissuunnitelmissaan. Hyvinvointialueella on sopimuksin varmistettu oikeus tarkastaa palveluntuottajiensa toimintaa.