

Tietosuojan ja tietoturvan roolit ja vastuut

1. Pirkanmaan hyvinvointialueen aluevaltuusto

Aluevaltuusto päättää sisäisen valvonnan ja riskienhallinnan järjestämisen linjaukset, tavoitteet ja osa-alueet sekä periaatteet niiden toimeenpano-, seuranta- ja arviointimenettelyistä hyvinvointialueella ja hyvinvointialuekonsernissa (HS § 71).

2. Pirkanmaan hyvinvointialueen aluehallitus

Pirkanmaan hyvinvointialueen aluehallitus vastaa, että hyvinvointialue täyttää tietosuojalainsäädännön mukaiset velvoitteet, ja valvoo velvoitteiden toteutumista. Aluehallitus määrittelee henkilötietojen käsittelyn periaatteet ja vastuuhenkilöt (HS § 148).

Aluehallitus vastaa hyvinvointialueen konsernin kokonaisturvallisuuden hallinnasta, johon kuuluvat uhkiin varautuminen, normaaliolojen häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen (HS § 10 kohta 11). Aluehallitus vastaa myös kokonaisvaltaisen riskienhallinnan järjestämisestä (HS § 10 kohta 7).

3. Prosessin omistaja

Prosessin omistaja

1. Omistaa prosessissa käsiteltävän tiedon.
2. Vastaa, että henkilötietoa käsitellään prosessissa lainsäädännön sekä hyvinvointialueen toimintaperiaatteiden ja ohjeistusten mukaisesti.
3. Päättää tiedon käyttötarkoituksista, kerättävistä tiedoista, tallennuspaikoista ja mahdollisista luovutuksista kolmansille osapuolille.
4. Vastuuttaa tietosuoja-asetuksen 30 artiklan mukaisen selosteen käsittelytoimista laatimisen ja ylläpidon sekä hyväksyy ko. selosteen.
5. Nimeää riskienhallinnan vastuuhenkilöt prosesseissaan ja hyväksyy tietosuojan vaikutustenarvioinnit (DPIA).
6. Vastaa prosessissaan, että rekisteröidyillä on mahdollisuus käyttää oikeuksiaan, ja vastuuttaa tietopyyntöjen yhteyspisteen.
7. Hyväksyy käyttöoikeuksien hallinnan periaatteet prosessissaan sekä vastuuttaa käsittelyyn käytettävien tietojärjestelmien käyttöoikeuksien hallinnan ja seurannan.



8. Vastuuttaa ja varmistaa riittävän henkilötietojen käsittelyn valvonnan.
9. Päättää henkilötietojen tietoturvaloukkauksien ilmoittamisesta valvontaviranomaiselle ja rekisteröidyille sekä merkittävistä poikkeamista (kyberturvallisuuslain 11§ ja asiakastietolain 90 §:n mukaisesti) ilmoittamisesta valvontaviranomaiselle.
10. Hyväksyy henkilötietojen siirrot ETA-alueen ulkopuolelle.
11. Vastuuttaa ja varmistaa, että henkilötietojen käsittelystä laaditaan kirjalliset ohjeet ja henkilöstö saa riittävää koulutusta tietojen käsittelyssä.
12. Voi hyväksyä tai hylätä tietojärjestelmän käyttöönoton tai päättää keskeyttää sen käytön prosessissaan.

3.1 Hyvinvointialuejohtaja

Hyvinvointialuejohtaja vahvistaa tietosuoja- ja tietoturvaohjausryhmän toiminnan. Hyvinvointialuejohtaja vastaa tehtäviinsä liittyvistä koko hyvinvointialuetta koskevista rekistereistä (mm. Pirkanmaan hyvinvointialueen ilmoituskanava / Whistleblowing).

3.2 Konsernijohtaja

Konsernijohtaja vastaa strategisten järjestämistoimintojen useiden eri rekisteröityjen ryhmiä koskevista rekistereistä.

3.3 Vaikuttaminen ja viestintä -vastuualueen johtaja (oto)

Viranhaltija vastaa hyvinvointialuetasoisesta strategisesta turvallisuuden, riskienhallinnan ja varautumisen turvallisuuden johtamisesta, ohjaamisesta ja kehittämisestä.

3.4 Vastaava johtajaylilääkäri

Vastaava johtajaylilääkäri vastaa potilasrekistereistä (mm. potilasrekisteri ml. ensihoidon rekisteri, työterveyshuollon potilasrekisteri, lääkinnällisen kuntoutuksen ja erikoissairaanhoidon ostopalvelujen rekisteri).

3.5 Vastaava sosiaalihuollon johtaja

Vastaava sosiaalihuollon johtaja vastaa sosiaalihuollon rekistereistä (mm. sosiaalihuollon asiakasrekisteri).

3.6 Hr-johtaja

Hr-johtaja vastaa henkilöstöhallinnon rekistereistä (mm. henkilöstöasioiden rekisteri, rekrytointirekisteri).

3.7 Hallintojohtaja

Hallintojohtaja vastaa hallintotoiminnan henkilörekistereistä (mm. luottamushenkilörekisteri).

3.8 Tukipalvelujohtaja

Tukipalvelujohtaja nimeää tehtäväalueensa asiantuntijat tietosuoja-, tietoturva- ja tekninen arkkitehtuuriryhmään.

3.9 Talousjohtaja

Talousjohtaja vastaa talous- ja laskentapalveluissa käsiteltävistä henkilötiedoista (mm. vammaispalvelujen kuljetustiedot).

3.10 Pelastusjohtaja

Pelastusjohtaja vastaa pelastuspalvelujen tehtäväalueella käsiteltävistä henkilötiedoista (mm. pelastuslaitoksen valvontarekisteri, pelastustoimen toimenpiderekisteri), pl. ensihoidon potilasrekisteri.

3.11 Hankintajohtaja

Hankintajohtaja vastaa hyvinvointialueen hankintatoimessa käsiteltävistä henkilötiedoista.

3.12 Kiinteistöjohtaja

Kiinteistöjohtaja vastaa hyvinvointialueen Kiinteistöpalvelut -vastuualueella käsiteltävistä henkilötiedoista (mm. kameravalvonta).

3.13 Tietohallintojohtaja

Tietohallintojohtaja vastaa tietoturvasta yleisesti niiltä osin, mitä tässä dokumentissa ei ole todettu kuuluvan muiden tahojen vastuulle.

Lisäksi tietohallintojohtaja:

- Vastaa tietohallinnon johtamisesta sekä tietojärjestelmien ja digitaalisten ratkaisujen kehittämisestä.
- Varmistaa, että tietohallinto tukee hyvinvointialueen eri palvelujen tavoitteita.
- Raportoi tietosuojasta ja tietoturvallisuudesta hyvinvointialueen johtoryhmälle, aluehallitukselle ja aluevaltuustolle.
- Vastaa hyvinvointialueen tietojärjestelmäarkkitehtuurin toteuttamisesta ja ICT-infrastruktuurin tietoturvallisuudesta.
- Vastaa ICMT-puitesopimuksen ja muiden merkittävien ICMT-sopimusten osalta, että tietoturvallisuus on asianmukaisesti huomioitu ja vastuuttaa sopimusten valvonnan.
- Vastaa tietosuojaa ja tietoturvaa koskevien yleisohjeistusten ajantasaisuudesta ja koulutusten tarjoamisesta yhteistyössä muiden prosessien omistajien kanssa.

Tietohallintojohtaja toimii hyvinvointialueen tietosuoja- ja tietoturvaohjausryhmän puheenjohtajana ja vahvistaa tietosuoja-, tietoturva- ja teknisen arkkitehtuuriryhmän toiminnan.

Tietohallintojohtaja vastaa tietohallinnon henkilökistereistä (mm. hyvinvointialueen digitaalisten palvelujen rekisteri, keskitetty käyttövaltuuksien hallinta- ja lokirekisteri).

4. Biopankista vastaava henkilö

Biopankista vastaava henkilö vastaa biopankkitoiminnan rekisterien ja tietokantojen ylläpitämisestä, yhdistämisestä ja suojaamisesta.

Biopankista vastaava henkilö vastaa yksityisyyden suojan varmistamisesta näytteitä ja niihin liittyviä tietoja käsiteltäessä.

5. Tytäryhtiön johto

Tytäryhtiön johto vastaa tietosuojan ja tietoturvan toteutumisesta lainsäädännön sekä hyvinvointialueen politiikkojen ja ohjeistusten mukaisesti, kun tytäryhtiö käsittelee hyvinvointialueen asiakas- ja potilastietoja tai muita henkilötietoja. Tytäryhtiön johto on vastuussa henkilötietojen käsittelystä tytäryhtiön rekisterinpitoon kuuluvien tietojen osalta. Tytäryhtiön politiikat eivät saa olla ristiriidassa hyvinvointialueen tietosuoja- ja tietoturvapoliitiikan kanssa.

6. Tehtäväaluejohtaja/ Palvelulinjajohtaja

Tehtäväaluejohtaja (mikäli tehtäväalueella on palvelulinjajohtaja, palvelulinjajohtajaa päättää tämän osion mukaisista asioista)

- Vastaa tehtäväalueen omassa ja ostopalvelutuotannossa tietosuojan ja tietoturvan toteutumisesta lainsäädännön sekä hyvinvointialueen politiikkojen ja ohjeistusten mukaisesti mm. siitä, että tehtäväalueen henkilöstöllä on riittävä osaaminen,

mahdollisuus riittävään kouluttautumiseen sekä ohjeistus ja asianmukaiset työkalut henkilötietojen lainmukaiseen käsittelyyn.

- Nimeää tehtäväalueen tietosuoja- ja tietoturvan vastuuyhteyshenkilön sekä vastuualueille tarvittavan määrän tietosuoja- ja tietoturvan yhteyshenkilöitä. Mikäli vastuualueita ei ole, nimetään tietosuoja- ja tietoturva yhteyshenkilöt toimialueille.
- Nimeää tehtäväalueen asiantuntijat tietosuoja-, tietoturva- ja tekninen arkkitehtuuriryhmään.

Soten palvelulinjajohtaja

- Vastaa palvelulinjansa omassa ja ostopalvelutuotannossa tietosuoja- ja tietoturvan toteutumisesta lainsäädännön sekä hyvinvointialueen politiikkojen ja ohjeistusten mukaisesti mm. siitä, että palvelulinjan henkilöstöllä on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen sekä ohjeistus ja asianmukaiset työkalut henkilötietojen lainmukaiseen käsittelyyn.
- Nimeää palvelulinjan tietosuoja- ja tietoturvan vastuuyhteyshenkilön sekä vastuualueille tarvittavan määrän tietosuoja- ja tietoturvan yhteyshenkilöitä. Mikäli vastuualueita ei ole, nimetään tietosuoja- ja tietoturva yhteyshenkilöt toimialueille.
- Nimeää palvelulinjan asiantuntijat tietosuoja-, tietoturva- ja tekninen arkkitehtuuriryhmään.

Toimialue- ja vastuualuejohtajat vastaavat edellä mainituista tehtävistä oman toimi-/vastuualueensa osalta yhteisten linjausten mukaisesti.

Vastuualuejohtaja nimeää myös ICT-yhdys henkilön, tunnustilaajan sekä vahvistaa ulkopuolisen palveluntuottajan ICT-tilaajan vastuualueen osalta.

Mikäli palvelulinjalla ei ole toimialuetta, asiasta päättää ja vastaa vastuualuejohtaja.

7. Tietosuoja- ja tietoturvan vastuuyhteyshenkilö

Tietosuoja- ja tietoturvan vastuuyhteyshenkilö koordinoi ja seuraa tietosuoja- ja tietoturvan toteutumista sekä kehittää ja lisää tietosuoja- ja tietoturvatietoisuutta edustamallaan alueella.

Vastuuyhteyshenkilö toimii tiiviissä yhteistyössä alueensa yhteyshenkilöiden sekä hyvinvointialueen tietosuojavastaavan ja tietoturvavastaavan kanssa. Hän tuo esille havaitsemansa tietosuoja- ja tietoturvariskit ja poikkeamat sekä arvioi tietosuojaan ja tietoturvaan liittyviä riskejä yhdessä hyvinvointialueen tietosuojavastaavan ja tietoturvavastaavan kanssa.

8. Tietosuoja- ja tietoturvan yhteyshenkilö

Tietosuoja- ja tietoturvan yhteyshenkilö seuraa tietosuoja- ja tietoturvan toteutumista sekä kehittää ja lisää tietosuoja- ja tietoturvatietoisuutta edustamallaan alueella.

Yhteyshenkilö toimii tiiviissä yhteistyössä palvelulinjansa vastuuyhteyshenkilön sekä hyvinvointialueen tietosuojavastaavan ja tietoturvavastaavan kanssa. Hän tuo esille havaitsemansa tietosuoja- ja tietoturvariskit ja poikkeamat sekä arvioi tietosuojaan ja tietoturvaan liittyviä riskejä yhdessä hyvinvointialueen tietosuojavastaavan ja tietoturvavastaavan kanssa.

9. Esihenkilöt

Hyvinvointialueen esihenkilöt vastaavat, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen sekä ohjeistus ja asianmukaiset työkalut henkilötietojen lainmukaiseen käsittelyyn.

Esihenkilö vastaa, että alainen on osallistunut pakollisiin tietosuoja- ja tietoturvakoulutuksiin. Esihenkilöltä odotetaan esimerkillistä ja vastuullista tietosuoja- ja tietoturvakäyttäytymistä. Hänen tehtävänä on valvoa tietosuojaan ja tietoturvan toteutumista henkilöstönsä työssä sekä raportoida tietosuojaan ja tietoturvan vaarantumiset ja poikkeamat periaatteista tai ohjeistuksista omalle esihenkilölleen ja/tai tietosuoja- tai tietoturvavastaavalle.

10. Henkilöstö

Hyvinvointialueen henkilöstö, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä sitoutuvat noudattamaan hyvinvointialueen tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen ehtoja allekirjoittaessaan sopimuksen ja toimimaan sen mukaisesti. Jokaisen työntekijän tulee myös suorittaa hyväksytysti tietosuoja- ja tietoturvakoulutus voimassa olevan koulutussuunnitelman mukaisesti. Jokaisen työntekijän vastuulla on raportoida havaitsemansa tietosuojaan tai tietoturvan vaarantuminen tai poikkeamat periaatteista tai ohjeistuksista omalle esihenkilölleen ja tietosuojavastaavalle tai tietoturvavastaavalle.

11. Tietojärjestelmän vastuuhenkilö

Tietojärjestelmän vastuuhenkilö huolehtii tietojärjestelmän elinkaaren hallinnasta, tietosuojaan ja tietoturvan toteuttamisesta – kuten tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta – sekä lakisääteisten seurantaraaporttien laatimisesta.

Raportoi heikkouksista ja poikkeamista prosessin omistajalle. Vikatilanteista ja käyttökatkoista tiedottaminen yhdessä teknisen omistajan ja yhteyshenkilön kanssa.

Tietojärjestelmän vastuuhenkilö on aina hyvinvointialueen palveluksessa oleva henkilö. Tietojärjestelmän vastuuhenkilö nimetään siitä yksiköstä, jonka toimintaa ja tietojenkäsittelyä varten palvelu tai järjestelmä on hankittu. Yhteisten ja yleiskäyttöisten tietojärjestelmien vastuuhenkilö nimetään tietohallinnosta.

12. Tietojärjestelmän tekninen omistaja

Tietojärjestelmän tekninen omistaja huolehtii tietojärjestelmän vastuuhenkilön ohjauksessa ja yhteistyössä tietojärjestelmän elinkaaren hallinnasta sekä tietosuojan ja tietoturvan toteuttamisesta, kuten

- riskienhallinnan toteuttamisesta, sisältäen riittävän dokumentaation,
- tiedon eheyden varmistamisesta,
- tietoturvan ja käyttöoikeuspolitiikan toteutumisen valvonnasta,
- sovelluksen ylläpitotoiminnoista ja yhteydenpidosta järjestelmätoimittajaan, ja
- vikatilanteista ja käyttökatkoista tiedottaminen yhdessä yhteyshenkilön kanssa.

Tietojärjestelmän tekninen omistaja voi olla palveluntoimittajan palveluksessa oleva henkilö.

13. Tietojärjestelmän yhteyshenkilö (esimerkiksi pääkäyttäjä)

Tietojärjestelmälle voidaan tarvittaessa nimetä yhteyshenkilö, joka toimii yhteistyössä tietojärjestelmän vastuuhenkilön ja teknisen omistajan kanssa. Yhteyshenkilön tehtäviin voivat kuulua esimerkiksi tietojärjestelmän käyttöoikeuksien hallinta (tilausoikeudellinen) tai järjestelmän käyttäjien ohjeistus.

Yhteyshenkilöä ei tarvitse nimetä, jos tietojärjestelmällä on yleinen tukikanava (kuten Omni-tuki) hoitamassa edellä mainittuja tehtäviä. Yhteyshenkilö voi olla palveluntoimittajan palveluksessa oleva henkilö.

14. ICT-yhdyshenkilö

Jokaisella vastuualueella on ICT-yhdyshenkilö ja hänellä korkeintaan kaksi varahenkilöä. ICT-yhdyshenkilön tehtävät on määritelty tarkemmin käyttövaltuus- ja pääsynhallintaperiaatteessa.

Mikäli vastuualueita ei ole, toimialuejohtaja määrittää ict-yhdyshenkilöiden määrän ja tarpeen.

15. Ulkopuolisen palveluntuottajan ICT-tilaaja

Ulkopuoliselle palveluntuottajalle nimetään tarvittaessa oma ICT-tilaaja ja hänelle tarvittava määrä varahenkilöitä, tai voidaan sopia, että ICT-tilaukset tehdään hyvinvointialueen ICT-yhdyshenkilön kautta. Vastuunjako sovitaan ostopalvelusopimuskohtaisesti ja seuranta tapahtuu yhteistyömallin mukaisesti. ICT-tilaajan tehtävät on määritelty tarkemmin käyttövaltuus- ja pääsynhallintaperiaatteessa.

16. Hyvinvointialueen tunnustilaaja

Tunnustilaaja huolehtii vastuualueen käyttäjätunnusten ja järjestelmien käyttöoikeuksien tilauksesta ja hallinnoimisesta, pois lukien niiden palveluntuottajien tilauksista, joille on nimetty oma tunnusmanageri. Tunnustilaajan rooli on

vastuualuetasoinen. Tunnustilaajia voidaan nimettävä tarvittava määrä turvaamaan tunnustilausprosessi vastuualueella. Tunnustilaajan tehtävät on määritelty tarkemmin käyttövaltuus- ja pääsynhallintaperiaatteessa.

Mikäli vastuualuetta ei ole, toimialuejohtaja määrittää tunnustilaajien määrän ja tarpeen.

17. Ulkopuolisen palveluntuottajan tunnusmanageri

Tunnusmanageri on ulkopuolisen palveluntuottajan tunnusten ja käyttöoikeuksien tilaaja. Tunnusmanageri voidaan nimetä sellaisille Pirkanmaan hyvinvointialueen tai hyvinvointialueen tytäryhtiöiden ulkopuolisille palveluntuottajille, jotka käyttävät Pirhan potilas- tai asiakastietojärjestelmiä. Rooli on palveluntuottaja-, yksikkö- tai palvelukohtainen. Tunnusmanagereita tulee olla riittävästi sujuvan toiminnan varmistamiseksi. Tunnusmanagerin tehtävät on määritelty tarkemmin käyttövaltuus- ja pääsynhallintaperiaatteessa.

18. Tietosuojavastaava

Hyvinvointialueen tietosuojavastaava toimii EU:n yleisen tietosuoja-asetuksen sekä sosiaali- ja terveydenhuollon erityislainsäädännön tarkoittamana tietosuojavastaavana. Tietosuojavastaava tukee organisaation erityisasiantuntijana yksiköiden johtoa ja henkilökuntaa tietosuoja-asioissa.

Tietosuojavastaava auttaa hyvinvointialuetta toteuttamaan tietosuojalainsäädännön mukaiset velvoitteet henkilötietojen käsittelyssä, suojaamisessa ja valvonnassa sekä toimii yhteyspisteenä rekisteröidyille ja viranomaisille. Lisäksi tietosuojavastaava antaa pyydettyä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta tietosuoja-asetuksen 35 artiklan mukaisesti.

Tietosuojavastaava raportoi tietosuojan tilasta ja kehittämistarpeista suoraan hyvinvointialueen prosessista vastaavalle henkilölle.

19. Pelastuspalvelujen tietosuojavastaava

Pelastuspalvelujen tietosuojavastaava toimii EU:n yleisen tietosuoja-asetuksen tarkoittamana tietosuojavastaavana. Tietosuojavastaava tukee organisaation erityisasiantuntijana johtoa ja henkilökuntaa tietosuoja-asioissa. Tietosuojavastaava auttaa pelastuspalveluita toteuttamaan tietosuojalainsäädännön mukaiset velvoitteet henkilötietojen käsittelyssä, suojaamisessa ja valvonnassa sekä toimii yhteyspisteenä rekisteröidyille ja viranomaisille.

Lisäksi tietosuojavastaava antaa pyydettyä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta tietosuoja-asetuksen 35 artiklan mukaisesti.

Pelastuspalvelujen tietosuojavastaava raportoi tietosuojan tilasta ja kehittämistarpeista suoraan prosessista vastaavalle henkilölle.

20. Tietoturvavastaava

Tietoturvavastaava valvoo organisaation erityisasiantuntijana hyvinvointialueen hallinnollisen ja teknisen tietoturvallisuuden toteutumista ja raportoi sen toteutumisesta. Hän vastaa tietoturvan tason arvioinnista, kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietoisuuden edistämisestä organisaatiossa, tietoturvaohjeistamisesta ja -tiedottamisesta.

Tietoturvavastaava toimii tietosuoja-, tietoturva- ja tekninen arkkitehtuuriryhmän puheenjohtajana. Tietoturvavastaava raportoi tietoturvan tilasta ja kehittämistarpeista tietohallintojohtajalle.

21. Pelastuspalvelujen tietoturvavastaava

Pelastuspalvelujen tietoturvavastaava valvoo organisaation erityisasiantuntijana pelastuspalvelujen hallinnollisen ja teknisen tietoturvallisuuden toteutumista ja raportoi sen toteutumisesta. Hän vastaa tietoturvan tason arvioinnista, kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietoisuuden edistämisestä organisaatiossa, tietoturvaohjeistamisesta ja -tiedottamisesta.

Pelastuspalvelujen tietoturvavastaava raportoi tietoturvan tilasta ja kehittämistarpeista esihenkilölleen.

22. Arkistopäällikkö

Arkistopäällikkö johtaa asiakirjahallintoa ja arkistopalveluja, joiden tehtävänä on varmistaa päätearkistoissa olevien asiakirjojen käytettävyys sekä pitkäaikais- ja pysyvässä säilytys, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää asiakirjat päätearkistosta vuosittain säilytysajan päättymisen jälkeen.

Arkistopäällikkö vastaa, että alueen kunnan kanssa on laadittu tietoaineistojen yhteishallintaa koskeva sopimus silloin, kun hyvinvointialueelle kuuluvaa aineistoa säilytetään edelleen kunnalle kuuluvassa tai kunnalta vuokratuissa tiloissa.