12.5.2023

Varsinais-Suomen hyvinvointialueen tiedonhallintapolitiikka

Hyväksytty: Aluehallitus 6.6.2023 § 223 dnro VARHA/10761/07.00.00/2023

Sisällys

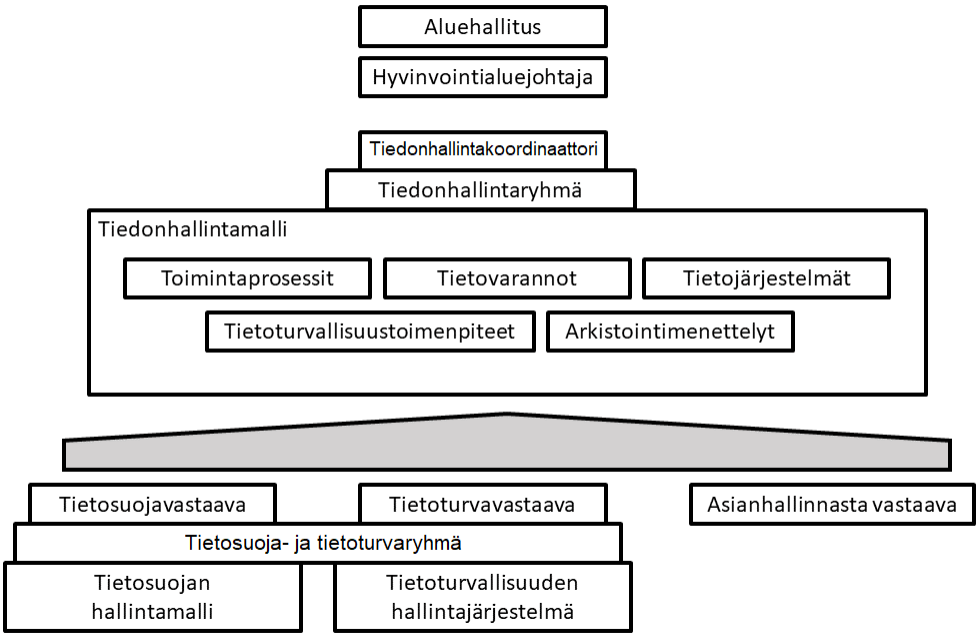
1. Soveltamisalue

Varsinais-Suomen hyvinvointialue on tiedonhallintalaissa (906/2019) tarkoitettu tiedonhallintayksikkö. Tiedonhallintayksikön tehtävänä on järjestää tiedonhallinta lain vaatimusten mukaisesti. Tiedonhallintalaki edellyttää, että tiedonhallintayksikkö ylläpitää tiedonhallintamallia palveluiden, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi. Tiedonhallintamalli tukee Varsinais-Suomen hyvinvointialueen strategiaa sen vaikuttavuustavoitteen toteuttamisessa, mm. asiakas-ja potilastietojärjestelmien konsolidoinnissa ja uusien digipalveluiden käyttöönotossa.

Varsinais-Suomen hyvinvointialueen aluehallitus määrittelee ja vahvistaa tässä tiedonhallintapolitiikassa tiedonhallintaan liittyvät periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Varsinais-Suomen hyvinvointialueen tiedonhallinnassa, sen toteuttamisessa ja kehittämisessä. Tiedonhallintapolitiikka 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.

Tiedonhallintapolitiikka kattaa hyvinvointialueen kaikkeen toimintaan liittyvät tietojenkäsittelyn tehtävät sekä hyvinvointialueen omistaman ja hallinnoiman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta. Jokaisen hyvinvointialueen viranhaltijan, työntekijän ja luottamushenkilön sekä hyvinvointialueen tietojen ja tietojärjestelmien käyttäjän on noudatettava tätä tiedonhallintapolitiikkaa ja sen pohjalta annettuja ohjeita ja määräyksiä. Hyvinvointialueen palvelutuottajien, toimittajien ja muiden ulkopuolisten tahojen, jotka käsittelevät hyvinvointialueen omistamaa tietoa työnsä tai toimeksiantonsa puitteissa, tulee myös noudattaa tätä tiedonhallintapolitiikkaa ehtona tehtäviensä mukaiselle pääsylle hyvinvointialueen tietoihin.

2. Määritelmiä



Kuva 1. *Tiedonhallinnan käsitteet ja ylimmät vastuut.*

Tiedonhallintamalli kuvaa toimintaympäristön tiedonhallinnan sisältäen

1) toimintaprosessien,
2) tietovarantojen,
3) tietojärjestelmien,
4) tietoaineiston arkistointimenettelyjen ja
5) tietoturvallisuustoimenpiteiden kuvaukset.

Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi. Suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä tulee tehdä **muutosvaikutusten arviointi** koskien tiedonhallinnan vastuita, tietovarantojen yhteentoimivuutta ja tarvittavia muutostoimenpiteitä. Lisäksi muutoksen yhteydessä on arvioitava rekisteröityjen tietosuojaan vaikuttavat tekijät EU:n yleisen tietosuoja-asetuksen mukaisesti.

Toimintaprosessilla tarkoitetaan viranomaisen asiankäsittely- tai palveluprosessia.

Tietovarannolla tarkoitetaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettäviä tietoaineistoja sisältävää kokonaisuutta, jota käsitellään tietojärjestelmien avulla tai manuaalisesti.

Tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä.

Asianhallinnalla tarkoitetaan organisaation toimintaprosesseihin sisältyvien asioiden ja niihin liittyvien asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista, arkistointia ja hävittämistä sekä asiakirjatietojen hallintaa.

Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.

Asiakirjajulkisuuskuvaus sisältää julkisen kuvauksen organisaation asiarekisterin ja tietojärjestelmien sisältämistä tiedoista tietopyyntöjen esittämiseksi.

Tietosuoja on osa lain takaamaa yksityisyyden suojaa, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on varmistaa, että henkilötietoja käsitellään lainmukaisesti ja vain silloin, kun niiden käsittelyyn on lainmukainen peruste.

Tietosuojan hallintamallilla tarkoitetaan toiminta- ja ohjausmallia, jonka mukaisesti henkilötietojen käsittelyä ohjeistetaan, toteutetaan, valvotaan ja kehitetään sekä osoitetaan tietosuojaperiaatteiden ja lainsäädännön noudattaminen organisaation kaikessa toiminnassa.

Tietoturvallisuudella tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus.

- Luottamuksellisuus: Tietoon on pääsy vain sellaisilla tahoilla, joilla on tietoon oikeus.
- Eheys: Tieto ei muutu ilman oikeutetun tahon sallittuja muutostoimia.
- Saatavuus: Tieto on tarvittaessa siihen oikeutettujen tahojen saatavilla.

Tietoturvan määritelmän mukainen tieto kattaa kaiken organisaation tiedon kaikissa muodoissaan. Tietoa voidaan käsitellä sähköisesti, manuaalisesti, ihmisten välisissä keskusteluissa, etäneuvotteluissa ja muilla tavoilla.

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan riskien arviointiin perustuvaa johtamisjärjestelmän osaa, jonka tarkoituksena on suunnitella, toteuttaa, seurata, noudattaa, arvioida, ylläpitää ja kehittää tietoturvallisuutta.

3. Tiedonhallinnan ylin vastuu

Tiedonhallintalaissa (906/2019) on säädetty tiedonhallintayksikön velvollisuudeksi laatia ja ylläpitää tiedonhallintamallia. Varsinais-Suomen hyvinvointialueen hallintosäännön 74 § mukaisesti aluehallitus vastaa siitä, että tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut on määritelty, asiaan kuuluvat ohjeet ovat olemassa, asiaan liittyvää koulutusta on tarjolla, tarvittavat työvälineet ovat olemassa ja riittävä valvonta on järjestetty. Hallintosäännön 76 § mukaan aluehallitus ja hyvinvointialuejohtaja tiedonhallintaa johtavana viranhaltijana muodostavat yhdessä tiedonhallintayksikön johdon.

Varsinais-Suomen hyvinvointialue on myös arkistolain mukainen arkiston muodostaja. Hallintosäännön 75 § mukaan aluehallitus vastaa siitä, että arkistotoimen lainmukaisten tehtävien vastuut, käytännöt ja valvonta on määritelty hyvinvointialueen viranomaisen tehtävissä. Aluehallitus määrää hyvinvointialueen asiakirjahallintoa, arkistotointa ja arkistonmuodostusta johtavan viranhaltijan, antaa tarkemmat määräykset asiakirjahallinnon hoitamisesta, päättää tiedonohjaussuunnitelman yleisistä periaatteista ja nimeää arkistonmuodostajat.

Hyvinvointialueen asiakirjahallintoa, arkistointia ja arkistonmuodostusta johtavana viranhaltijana toimii hyvinvointialueen asianhallintapäällikkö.

4. Tiedonhallintakoordinaattori ja tiedonhallintaryhmä

Hyvinvointialueella toimii tiedonhallintakoordinaattori, jonka hyvinvointialuejohtaja nimittää. Tiedonhallintakoordinaattori raportoi hyvinvointialuejohtajalle.

Tiedonhallintakoordinaattorin tehtäviin kuuluu

- tiedonhallintamallin mukaisten kuvausten koostaminen ja ylläpidosta huolehtiminen,
- muutosvaikutustenarviointia koskevan prosessin määrittäminen,
- tietojärjestelmien toiminnan ja yhteentoimivuuden edistäminen, tietovarantojen yhteentoimivuuden varmistaminen sekä tiedonhallintaan liittyvien prosessien yhteistyön koordinointi, niin että tietoaineistot ovat ajantasaisia, virheettömiä ja käyttötarkoitukseensa sopivia
- varmistaa, että tiedonhallinnan vaatimukset otetaan huomioon hankinnoissa ja sopimuksissa
- varmistaa, että tietojärjestelmien käytöstä, käyttöoikeuksista ja poikkeusoloihin varautumisesta on ajantasainen ohjeistus,
- hyvinvointialueen toiminnan seuranta, ohjaaminen ja kehittäminen tiedonhallinnan kannalta
- tiedonhallintaan liittyvän lainsäädännön muutosten seuranta ja lakimuutosten aiheuttamien toimenpiteiden koordinointi hyvinvointialueen toiminnassa.

Tiedonhallintakoordinaattori vastaa tämän tiedonhallintapolitiikan ja sen muutosten valmistelusta aluehallituksen päätettäväksi.

Tiedonhallintakoordinaattorin apuna toimii tiedonhallintaryhmä, jonka hyvinvointialuejohtaja nimittää. Tiedonhallintakoordinaattori toimii tiedonhallintaryhmän puheenjohtajana. Tiedonhallintaryhmä tukee tiedonhallintakoordinaattoria tehtäviensä hoitamisessa.

5. Hyvinvointialueen toimintaprosessit

Hyvinvointialueen toiminta perustuu toimintaprosesseihin. Hyvinvointialuejohtaja vastaa siitä, että organisaation toiminta on järjestetty tarkoituksenmukaisella ja lainmukaisella tavalla prosesseihin ja että prosesseilla on omistajat. Prosessikuvausten laatimisesta ja muutosvaikutusten arviointien laatimisesta vastaa kyseisen prosessin omistaja ja kuvausten yhtenäiseen malliin ohjaa hyvinvointialueen järjestämisen palvelut. Hyvinvointialueen prosessit kuvataan keskitettyyn järjestelmään muutosvaikutustenarvioinnin mahdollistamiseksi.

6. Tietovarannot ja tietojärjestelmät

Hyvinvointialueen toiminnassa kertyy paljon toimintaan liittyvää tietoa, esimerkiksi potilas- ja asiakastietoa, henkilöstöhallinnollista tietoa, taloudellista, rakennetun ympäristön ja materiaalisten resurssien tietoa ja muuta. Eri tietoryhmiin kohdistuu erilaisia lainsäädännöllisiä, hallinnollisia, tietosuojaan ja tietoturvaan liittyviä sekä muita vaatimuksia. Tietoa hyödynnetään ensisijaisesti niissä käyttötarkoituksissa (prosesseissa), joissa tieto alun perin kertyy ja mihin tarkoituksiin sitä käsitellään. Tiedolla on myös useita mahdollisia toissijaisia käyttötarkoituksia, eli muita käyttötarkoituksia kuin mitä varten ne on alun perin

tallennettu, kuten tieteellinen tutkimus, kehittämistoiminta, tiedolla johtaminen ja mahdolliset muut käyttötarkoitukset. Tiedon toissijaisiin käyttötarkoituksiin hyödyntämisen mahdollistaminen tulee huomioida jo tietojärjestelmäratkaisuja hankittaessa.

Hyvinvointialueen tietovarannoilla ja niiden käsittelyyn käytettävillä tietojärjestelmillä tulee olla omistajat. Hyvinvointialuejohtaja päättää tietovarantojen ja tietojärjestelmien omistajista. Nämä ovat pääosin samoja henkilöitä, jotka vastaavat toimintaprosesseista, joita tietojärjestelmät ja niissä käsiteltävät tiedot tukevat. Tietovarantojen ja tietojärjestelmien omistajan vastuisiin ja tehtäviin kuuluvat

- vastuu tietojen laadusta,
- vastuu tiedon lainmukaisesta ja kohtuullisesta käsittelystä sekä lainmukaisesta ja asiallisesta luovuttamisesta joko kolmansille osapuolille tai toissijaisiin käyttötarkoituksiin,
- vastuu tietojen käyttöoikeuksien määrittelystä sekä
- vastuu siitä, että tietosuoja ja tietoturvallisuus toteutuvat kyseisten tietojen käsittelyssä hyvinvointialueen voimassa olevien käytäntöjen mukaisesti.

Hyvinvointialueen tietojen toisiokäytön, kuten tiedolla johtamisen ja tutkimus- ja opetuskäytön, vastuuhenkilö on hyvinvointialuejohtaja. Tiedonhallintamallissa määritellään hallinnolliset reunaehdot hyvinvointialueen prosesseissa syntyvän tiedon hyödyntämisestä laissa sosiaali- ja terveystietojen toissijaisesta käytöstä määritellyissä ja muissa toissijaisissa käyttötarkoituksissa.

7. Tietojärjestelmien hallinta

Hyvinvointialueen toimintaprosessien ja tiedonhallinnan tukena hyödynnetään erilaisia tietojärjestelmiä. Tietojärjestelmien hallintaprosessin omistaja on hyvinvointialueen tietohallintojohtaja.

Tietojärjestelmien hallintaprosessin omistaja tukee hyvinvointialueen toimintaprosessien omistajia siinä, että hankitut ja tuotetut tietojärjestelmät ovat toimintaprosessien vaatimusten ja tarpeiden mukaisia. Tietojärjestelmien hallintaprosessin omistaja vastaa hyvinvointialueen tietojärjestelmien tilaajan edustajana tietojärjestelmiin ja tietoliikenneratkaisuihin liittyvien vaatimusten määrittelyn koordinoinnista. Määrittelyssä on huomioitava hyvinvointialueen yleiset tietosuojaa ja tietoturvaa koskevat linjaukset. Tietojärjestelmien hallintaprosessin omistaja valvoo tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteutumista.

8. Asianhallinta

Hyvinvointialueen tiedonhallinnassa on huolehdittava asianhallinnasta siten, että asiankäsittely, asiakirjahallinta ja arkistointi on toteutettu asianmukaisesti ja lainmukaisesti ja että tietoaineistojen käsittelystä löytyvät ajantasaiset ohjeet. Viranomaisen käsittelyssä olevista ja olleista asioista ylläpidetään asiarekisteriä, johon rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Hyvinvointialue järjestää myös muun kuin asiankäsittelyn yhteydessä muodostuvan tietoaineiston hallinnan asianmukaisesti. Hyvinvointialueen tiedonohjaus- ja arkistonmuodostussuunnitelmilla ohjataan asiakirjojen käsittelyä ja säilyttämistä huomioiden tietoaineistojen erilaiset säilytysajat ja -muodot.

Hyvinvointialue laatii asiakirjajulkisuuden toteuttamiseksi asiakirjajulkisuuskuvauksen, jossa kuvataan hyvinvointialueen hallinnoimat tietovarannot ja asiarekisteri.

Kaikki tietoaineistot pyritään muuttamaan sähköiseen muotoon helposti saataville.

Asianhallintaan liittyvien prosessien omistaja on asianhallintapäällikkö.

9. Tietosuoja

Hyvinvointialueen tiedonhallinnassa on huolehdittava asianmukaisesta henkilötietojen tietosuojasta. Hyvinvointialueen toiminnassa syntyneiden henkilötietojen käsittelytarkoitus määritellään toimintayksikkökohtaisesti. Aluehallitus määrää henkilötietojen käsittelyn vastuuhenkilöt. Aluehallituksella on vastuu tietosuojalainsäädännön mukaisten velvoitteiden täyttämisestä ja velvoitteiden noudattamisen valvonnasta sekä tietosuojavastaavien nimeämisestä. Tietosuojaprosessin omistaja on hyvinvointialuejohtaja.

9.1 Tietosuojan tavoitteet ja periaatteet

Henkilötietojen käsittelyyn hyvinvointialueella sovelletaan seuraavia periaatteita:

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys: Henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi.

Käyttötarkoitussidonnaisuus: Henkilötietoja käsitellään suunnitellun, tietyn, nimenomaisen ja laillisen käyttötarkoituksen mukaisesti.

Tietojen minimointi: Henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää.

Täsmällisyys: Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä.

Säilytyksen rajoittaminen: Henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika.

Eheys ja luottamuksellisuus: Henkilötietojen käsittelyssä varmistetaan henkilötietojen asianmukainen turvallisuus, kuten eheys ja luottamuksellisuus.

Hyvinvointialueen toiminnassa noudatetaan **sisäänrakennetun ja oletusarvoisen tietosuojan** periaatetta. Se tarkoittaa, että hyvinvointialueen toiminnassa on otettava edellä mainitut tietosuojaperiaatteet huomioon ja sisällytettävä ne kaikkiin henkilötietojen käsittelyn vaiheisiin mahdollisimman varhaisessa vaiheessa. Ne on otettava huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja ja prosesseja tai kehitetään tietojärjestelmiä sekä silloin, kun olemassa olevien käsittelytoimien tai järjestelmien laajuus, luonne tai tarkoitus muuttuu. Tietosuojan toteuttamisessa hyvinvointialue varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan, ja että lainsäädännön noudattaminen on osoitettavissa asianmukaisen ja ajantasaisen dokumentaation avulla.

Hyvinvointialueen lähtökohtana tietosuojassa on riskilähtöisyys. Hyvinvointialue rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa hyvinvointialueen riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka.

9.2 Tietosuojan organisointi ja vastuut

Tietosuojaa johtaa ja valvoo hyvinvointialueen aluehallitus. Hyvinvointialuejohtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuojavastaavan ja tietosuoja- ja tietoturvaryhmän.

Hyvinvointialueen tietosuojavastaava toimii tietosuojan erityisasiantuntijana, joka valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä antaa neuvoja ja tietoja tietosuojasääntelyn mukaisten velvollisuuksien noudattamisessa osallistumalla mm. henkilöstölle järjestettäviin koulutuksiin. Tietosuojavastaava raportoi hyvinvointialuejohtajalle ja aluehallitukselle. Tietosuojavastaavan asema organisaatiossa on riippumaton.

Tietosuojavastaavan tehtävät:

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat tietosuoja-asetuksen ja muiden tietosuojasäännösten mukaisia velvollisuuksia
- seurata, että noudatetaan tietosuoja-asetusta ja muita tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset
- antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta
- tehdä yhteistyötä tietosuojaviranomaisen kanssa
- toimia tietosuojaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä

Tietosuoja- ja tietoturvaryhmä osallistuu tietosuojan kehittämisen suunnitteluun ja toimeenpanon valmisteluun. Tietosuoja- ja tietoturvaryhmä ylläpitää tietosuojan kehittämissuunnitelmaa, valmistelee tietosuojaan liittyvää ohjeistusta, tiedottaa tietosuojatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietosuojatyön osaksi organisaation operatiivista toimintaa.

Tietosuoja- ja tietoturvaryhmän alaryhmänä toimii tietosuoja- ja tietoturvayhteyshenkilöiden alaryhmä. Sen tehtävänä on edistää tietosuoja- ja tietoturvanäkemyksen huomioimista kaikessa organisaation toiminnassa. Tavoitteena on aktiivinen tiedonvaihto ja kehittäminen alueen tai tukipalveluiden henkilötietojen käsittelystä.

Jokaisella henkilörekisterillä tai henkilötietojen käsittelytoimella on oltava vastuuhenkilö, jonka vastuulla on huolehtia siitä, että henkilötietojen käsittely on suunniteltu ja dokumentoitu tietosuojaperiaatteet huomioiden, ja että tietosuojavelvollisuuksien noudattamisesta huolehditaan tarvittavin teknisin ja organisatorisin toimenpitein.

Henkilöstöhallinnolliset esihenkilöt vastaavat alaistensa toimintatavan tietosuojalainsäädännön mukaisuudesta hyvinvointialueella ja omissa yksiköissään annettujen ohjeiden mukaisesti. Jokainen hyvinvointialueella henkilötietoja käsittelevä, on vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Hyvinvointialuejohtaja voi antaa tarkempia ohjeita tietosuojan vastuista ja menettelytavoista toimintaohjeella.

9.3 Tietosuojan toteuttaminen

Tietosuojan toteuttamista hyvinvointialueella ohjataan tietosuojan hallintamallilla, joka sisältää ohjeet, tietosuojaprosessit ja tietosuojalainsäädännön edellyttämän dokumentaation.

Hyvinvointialue toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi, joiden avulla varmistetaan mm., että:

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta,
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen,
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville,
- taataan rekisteröityjen oikeuksien toteutuminen sekä
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Perustettaessa EU:n yleisen tietosuoja-asetuksen mukaista rekisteröidyille korkean tietosuojariskin aiheuttavaa rekisteriä, sen osalta tulee tehdä tietosuojaa koskeva vaikutustenarviointi. Arviointi tehdään tietosuojavastaavan avustuksella sovitun mallin mukaisesti. Lähtökohtaisesti korkean riskin rekistereitä ovat mm. kaikki erityisiä henkilötietoryhmiä (arkaluonteiset tiedot) koskevat rekisterit.

Hyvinvointialueen järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Hyvinvointialue voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Hyvinvointialue valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Hyvinvointialueen ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Hyvinvointialue rekisterinpitäjänä sisällyttää tietosuojan myös projektinhallinta- ja kehittämismallinsa osaksi.

Hyvinvointialueella on määritetty toimintaprosessit ja ohjeet tilanteisiin, joissa rekisteröidyt käyttävät tietosuoja-asetuksen mukaisia tietosuojaoikeuksiaan, kuten oikeuttaan saada pääsy henkilötietoihinsa.

Hyvinvointialue huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja tiedottamisen kautta. Organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

10. Tietoturva

Hyvinvointialueen tiedonhallinnassa on huolehdittava asianmukaisesta tietoturvallisuudesta. Tietoturvaprosessin omistaja on tietoturvavastaava, jonka nimittää hyvinvointialuejohtaja.

10.1 Tietoturvatoiminnan tavoitteet ja periaatteet

Hyvinvointialueen tietoturvatoiminnan päämääränä on turvata hyvinvointialueen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden luvaton ja oikeudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi tulee varautua toiminnan keskeyttäviin poikkeamatilanteisiin ja niistä toipumiseen.

Tietoturvallisuus on huomioitava kaikessa toiminnassa jo suunnitteluvaiheessa, ja se tulee sisällyttää oletusarvoisena ja sisäänrakennettuna osana hyvinvointialueen kaikkeen toimintaan. On huolehdittava toimintaympäristön tietoturvallisuustilan jatkuvasta seurannasta ja tietoturvariskien hallinnasta sekä niihin perustuvista tietoturvallisuustoimenpiteistä. Tietoturvallisuus on varmistettava kaiken tiedon osalta koko sen elinkaaren ajan.

10.2 Tietoturvallisuuden organisointi ja vastuut

Hallintosäännön 76 § mukaan hyvinvointialuejohtaja varmistaa tietoturvallisuuden toteuttamista hyvinvointialueen toiminnassa. Tätä varten hän nimeää tietoturvavastaavan ja tietosuoja- ja tietoturvaryhmän.

Hyvinvointialuejohtajalta saamiensa resurssien ja toimintavaltuuksien puitteissa tietoturvavastaava vastaa tietoturvallisuuden hallinnasta, toteuttamisesta, kehittämisestä, toteutuksen valvonnasta sekä tietoturvatietoisuuden edistämisestä ja tietoturvallisesta toimintatavasta hyvinvointialueella ja sen ostamissa palveluissa sekä raportoinnista. Tietoturvavastaava raportoi hyvinvointialuejohtajalle ja aluehallitukselle. Tietoturvavastaavan tehtävät:

Yleiset tehtävät
- tiedonhallintayksikön ja sen toimintaympäristön tietoturvallisuuden tilan seuranta
- tiedonhallintayksikön tietoturvasäännösten noudattamisen seuranta ja havaittujen puutteiden raportointi
- tiedonhallinnan muutosten arvioinnin tekemiseen liittyvien neuvojen antaminen pyydettäessä
- viranomaisten yhteyshenkilönä toimiminen tietoturvallisuuteen liittyvissä asioissa
- tietoturvallisuutta koskevien tietojen ja neuvojen antaminen johdolle ja henkilöstölle

Vastuut
- tiedonhallintamallissa ja tietoturvallisuuden hallintajärjestelmässä kuvattujen tietoturvallisuusjärjestelyjen asianmukaisuuden valvonta
- tietoturvallisuustoimenpiteiden mitoittaminen tiedonhallintayksikön tietoturvalinjausten mukaisesti
- tietoturvallisuuden arviointi ja ulkoisten arviointien koordinointi
- tietoturvallisuusdokumenttien laatiminen ja päivittäminen
- tietoturvatietoisuuden edistäminen ja tietoturvallisten toimintatapojen noudattaminen tiedonhallintayksikössä ja sen ostamissa palveluissa
- hyvinvointialueen yleinen tietoturvaohjeistus ja -koulutus sekä tietoturva-asioista tiedottaminen
- tietoturvallisuuden yleisen tilanteen seuraaminen
- laitteisto- ja ohjelmistoturvallisuuden periaatteiden määrittäminen
- hankintojen tietoturvallisuusvaatimusten määrittely ja niiden noudattamisen seuranta
- tietoturvallisuuden mittaamisen määrittäminen ja tulosten raportointi
- tietoturvallisuuden kehittämissuunnitelmien tekeminen
- tietoturvallisuuden toimeenpanon koordinointi

- merkittävien tietoturvapoikkeamien käsittely johdon kanssa käyttäen tarvittaessa ulkopuolista asiantuntemusta

Tukitehtävät

- tiedonhallintayksikön riskienhallinnan tukeminen selvittämällä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti
- tietojärjestelmien omistajien ja vastuuhenkilöiden tukeminen tietoturvatoimenpiteiden suunnittelussa
- säännöllinen keskustelu tiedonhallintayksikön toimintojen kanssa tietoturvallisuuskysymyksistä
- tiedonhallintayksikön tietosuojavastaavan tukeminen tietoturvallisuutta koskevissa asioissa
- osallistuminen tiedonhallintayksikön ICT-varautumiseen ja toiminnan jatkuvuuden hallintaan

Tietosuoja- ja turvaryhmä avustaa tietoturvan kehittämissuunnitelman laatimisessa, valmistelee tietoturvaan liittyvää ohjeistusta, tiedottaa tietoturvatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietoturvatyön osaksi organisaation operatiivista toimintaa.

Jokaiselle tietojärjestelmälle nimetään omistaja. Tietojärjestelmän omistajan velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten kuten kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn määrittely sekä käyttöoikeuksien määrittely, myöntäminen ja valvonta yhteistyössä tietovarantojen omistajien kanssa kuin myös tietojärjestelmän ja sen liittymien kuvaaminen hyvinvointialueen tiedonhallintamalliin.

Tietoturvallisuuden toteutumisen varmistamiseksi aluehallitus valvoo ja johtaa tietoturvallisuuden hallinnointia, riskienhallintaa ja vaatimustenmukaisuutta sekä vaatii raportointia ja tietoa tietoturvallisuuden toteutumisesta ja nykytilasta. Hyvinvointialuejohtaja vastaa siitä, että tietoturvavastaavan resurssit ja toimintavaltuudet ovat riittävät sekä siitä, että tietoturvatyön organisointi hyvinvointialueella on tarkoituksenmukainen, ristiriidaton ja tietoturvatyön keskeisten toimijoiden yhteistyötä edistävä.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esihenkilö. Hän huolehtii yksikön uusien työntekijöiden perehdyttämisestä.

Jokainen hyvinvointialueen työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä ovat omalta osaltaan vastuussa tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta voimassa olevan ohjeistuksen mukaisesti.

10.3 Tietoturvallisuuden toteuttaminen

Tietoturvan toteuttaminen tapahtuu tietoturvallisuuden hallintajärjestelmällä, jonka perustuu tietoturvariskien arviointiin ja tietoturvan jatkuvaan parantamiseen. Lähtökohtana on hyvinvointialueen organisaation sekä sen sisäisen ja ulkoisen toimintaympäristön ymmärtäminen. Suojattava tieto-omaisuus tulee kartoittaa sekä ymmärtää sidosryhmien tarpeet ja odotukset, mukaan lukien lakisääteiset vaatimukset, viranomaisvaatimukset ja sopimusvelvoitteet. Tietoturvariskit arvioidaan ja käsitellään dokumentoidusti. Käytetyt tietoturvallisuuden hallintakeinot dokumentoidaan. Tietoturvan toteuttamista seurataan valituin mittarein. Tärkeää on myös organisaation tietoturvatietoisuuden lisääminen ja viestintä tietoturva-asioista. Itse hallintajärjestelmän toimintaa arvioidaan mm. sisäisin auditoinnein. Olennainen osa hallintajärjestelmää ovat säännölliset johdon katselmukset, joissa käydään läpi tietoturvatavoitteiden täyttyminen, olennaiset tapahtumat ja poikkeamat sekä tietoturvallisuuden parantamismahdollisuudet.

Keskeisiä tietoturvallisuuden hallintakeinoja ovat henkilöstön tietosuoja- ja tietoturvakoulutus, pääsynhallinta tietojärjestelmiin ja tietojenkäsittelytiloihin, tietoturvapoikkeamien seuranta ja niiden hallintaprosessit, varmuuskopiointi, kriittisten järjestelmien vikasietoisuus, muutosten hallinta sekä yhteistyökumppaneiden sopimusehdot.

11. Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Hyvinvointialueella on määritetty toimintaprosessi tietoturvapoikkeamiin sekä henkilötietojen tietoturvaloukkauksiin.

Tietoturvapoikkeamat ja henkilötietojen tietoturvaloukkaukset ilmoitetaan, käsitellään ja dokumentoidaan voimassa olevan ohjeistuksen mukaisesti. Tietoturvapoikkeamat ja henkilötietojen tietoturvaloukkaukset ilmoitetaan tarvittaessa valvonta- ja muille viranomaisille voimassa olevan kansallisen ja kansainvälisen lainsäädännön ja ohjeistuksen mukaisesti.

Henkilötietojen tietoturvaloukkauksen sattuessa hyvinvointialueella on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturva-loukkaus on tullut ilmi, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, ilmoitetaan rekisteröidylle loukkauksesta ilman aiheetonta viivytystä.

12. Rikkomukset ja seuraamukset

Tiedonhallintapolitiikan, tietosuojaa ja tietoturvallisuutta koskevan sitoumuksen sekä muiden tiedonhallintaa, tietoturvaa ja tietosuojaa ohjaavien periaatteiden ja ohjeiden toteutumista ja noudattamista seurataan. Periaatteiden, ohjeistuksen sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietoturvarikkomusten sekä henkilötietojen tietoturvaloukkausten mahdollisiin seuraamuksiin sovelletaan toimintaohjetta. Tietoturvarikkomukset ja henkilötietojen tietoturvaloukkaukset raportoidaan tietoturvavastaavalle, tietosuojavastaavalle ja hyvinvointialuejohtajalle.