Pirkanmaan hyvinvointialueen tietosuoja- ja tietoturvaperiaate

Käsittely:

Hallinnon johtotiimi 9.9.2025
Tietosuoja-, tietoturva- ja tekninen arkkitehtuuri-ryhmä 17.9.2025
Pelastus- ja ensihoitopalveluiden johtoryhmä 1.10.2025
Tietosuojan ja tietoturvan ohjausryhmä 3.10.2025
Konsernipalveluiden johtoryhmä 8.10.2025
Sote-palvelut johtoryhmä 8.10.2025
Tukipalvelujen johtoryhmä 15.10.2025
Hyvinvointialueen johtoryhmä 21.10.2025
Tiedonhallintaryhmä 24.10.2025
Aluehallituksen aamukoulu 3.11.2025
Aluehallitus 12.1.2026

Sisällys

1. Tausta ja tarkoitus

Käsittelemme Pirkanmaan hyvinvointialueen (jatkossa hyvinvointialue) palveluissa runsaasti luottamuksellisia ja salassa pidettäviä henkilötietoja, kuten sosiaalihuollon asiakastietoja, potilastietoja, pelastustoiminnan tietoja ja henkilöstötietoja, sekä toimintaan liittyviä tietoja, jotka ovat lainsäädännön perusteella suojattavia. Hyvinvointialueen ydintehtävät sekä asiakas- ja potilasturvallisuus edellyttävät tietosuojan ja tietoturvan toteutumista kaikissa olosuhteissa.

Tietosuoja- ja tietoturvaperiaate on aluehallituksen ja ylimmän johdon hyväksymä asiakirja, jossa otetaan kantaa tietosuojan ja tietoturvan ylläpitämiseen ja kehittämiseen. Periaate määrittelee ne periaatteet, tavoitteet, vastuut sekä seurannan ja valvonnan, joita noudatamme hyvinvointialueella potilaidemme, asiakkaidemme, työntekijöidemme ja yhteistyökumppaneidemme yksityisyyden suojan, luottamuksellisuuden, oikeusturvan ja tiedonhallinnan tehokkuuden sekä tietoturvallisuuden varmistamiseksi. Tietosuoja- ja tietoturvaperiaate täydentävät hyvinvointialueen tietoturvasuunnitelma sekä muut yksityiskohtaiset linjaukset, päätökset ja ohjeet.

Tietosuoja ja tietoturva ovat osa päivittäistä toimintaamme. Tietosuoja- ja tietoturvaperiaate koskee koko hyvinvointialuekonsernia ja kattaa kaikki hyvinvointialueen toimintaan liittyvät tietojenkäsittelytehtävät. Periaatteen ja ohjeistuksen mukaista toimintaa noudatetaan soveltuvin osin myös hyvinvointialueen tytäryhtiöissä. Henkilöstöllä tarkoitetaan tässä periaatteessa hyvinvointialueen ja sen tytäryhtiöiden henkilöstöä.

Tietosuoja ja tietoturva on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Hyvä tiedonhallinta edellyttää toimintamme pitkäjänteistä suunnittelua, jatkuvaa kehittämistä, seurantaa ja erilaisiin uhkatilanteisiin varautumista. Varmistamme tietosuoja- ja tietoturvatavoitteiden toteutumisen sovituilla toimintatavoilla ja käytänteillä, jotka perustuvat muiden muassa jatkuvaan riskien arviointiin, henkilöstön kouluttamiseen ja ohjeistamiseen sekä henkilötietojen käsittelyn sisäiseen ja ulkoiseen valvontaan. Näiden lisäksi varmistamme henkilötietojen ja muun salassa pidettävän tiedon riittävän suojaamisen sekä hallinnollisin että teknisin tietoturvakeinoin.

2. Määritelmät

Tietosuoja asettaa säännöt, joiden mukaan tulee toimia aina henkilötietoja käsiteltäessä, ja tietoturva tarjoaa ne keinot, joilla henkilötietoja suojataan. Käsitteinä nämä kulkevat käsi kädessä, eikä tietosuojaa ole ilman tietoturvaa. Kun tietosuojasta huolehditaan asianmukaisesti, tulee myös tietoturva henkilötietojen käsittelyssä väistämättä huomioiduksi.

2.1 Tietosuoja

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn (henkilön, jonka tietoja käsitellään) oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Henkilötietojen käsittelyn on aina perustuttava lakiin. Henkilötietojen käsittelyn on oltava asianmukaista ja tapahduttava aina tiettyä tarkoitusta varten joko asianomaisen henkilön suostumuksella tai muulla laissa säädetyllä perusteella.

Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty, ja tarvittaessa saada virheelliset tiedot korjatuiksi tai poistetuiksi.[1] Riippumaton viranomainen, tietosuojavaltuutettu, valvoo henkilötietojen suojaa koskevien säännösten noudattamista.

Tietosuojaan liittyvät keskeiset käsitteet, kuten **henkilötieto, erityiset henkilötietoryhmät, henkilötietojen käsittely, rekisterinpitäjä, henkilötietojen käsittelijä, tietosuojavastaava ja rekisteröity**, määritellään EU:n yleisessä tietosuoja-asetuksessa (679/2016, GDPR).

2.2 Tietoturva

Tietoturva kattaa fyysiset, hallinnolliset, toiminnalliset, tekniset ja muut keinot, joilla suojataan hyvinvointialueen tiedot, palvelut, tietojärjestelmät ja tietoliikenne niin normaalitilanteissa, normaaliolojen häiriötilanteissa kuin poikkeusoloissakin. Tietoturvalla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus:

- **Luottamuksellisuus** tarkoittaa, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla.
- **Eheys** tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa, mihin liittyy keskeisesti mm. tiedon muuttumattomuuden varmistaminen.
- **Saatavuus** tarkoittaa, että tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

3. Ohjaavat säädökset

Tietosuojaa ja tietoturvaa ohjataan säädöksin, määräyksin, ohjein ja suosituksin. Keskeiset tietosuojaa ja tietoturvaa ohjaavat säädökset ja suositukset on koottu tämän periaatteen liitteeseen 1.

Lainsäädännön lisäksi on noudatettava muita hyvinvointialueelle hyväksyttyjä tietosuojaan ja tietoturvaan liittyviä ohjeita ja määräyksiä. Hyvinvointialueen omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietosuoja- ja tietoturvaperiaatteen tai voimassa olevan lainsäädännön kanssa siten, että tietosuoja tai tietoturva heikkenee.

4. Tietosuojaan ja -turvallisuuteen kohdistuvat uhat ja riskienhallinta

Tietosuojaan ja -turvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja saatavuudelle.

[1] Tietosuojalainsäädännön mukaisista rekisteröidyn oikeuksiin liittyvistä tietopyynnöistä on erotettava julkisuuslain mukaiset tietopyynnöt, joista hyvinvointialueella on eri ohjeistuksensa.

Digitaalisten palvelujen ja ratkaisujen käyttö lisääntyy osana palvelutarpeen arviointia, diagnosointia, hoitoa ja näihin liittyvien palvelujen tuottamista. Esimerkiksi pilvipalvelujen mukanaan tuomat erilaiset kyberuhat tarkoittavat nopeatahtisia muutostarpeita myös tietosuoja- ja tietoturvavaatimusten toteuttamiseen.

Henkilöstön kouluttaminen ja turvallisuuskulttuurin ylläpitäminen on tärkeää, jotta voidaan välttää osaamattomuudesta ja ymmärtämättömyydestä aiheutuvat uhat henkilötietojen käsittelylle ja tietoturvallisuudelle. Merkittäviä uhkia ovat muiden muassa virheellisesti toimivat ohjelmistot ja laitteet, tekniset ongelmat, tietojen kalastelut, haittaohjelmat, palvelunestohyökkäykset, kyberhyökkäykset sekä tietomurrot. Merkittäviä uhkia voi liittyä myös ulkopuolisten palveluntuottajien toimintaan, mikäli palveluntuottajien kanssa ei ole tehty sopimuksia, joissa huomioidaan tietosuoja, tietoturva ja varautuminen sekä rikkomuksiin liittyvät sanktiot. Uhka aiheutuu myös siitä, jos tehtyjen sopimusten noudattamista ei valvota.

Riskienhallinta on lakisääteinen osa julkisen organisaation johtamista ja toimintaa: Pirkanmaan hyvinvointialueen kaltaisella julkisella organisaatiolla riskienhallinnan perusteet lähtevät jo hyvän hallinnon periaatteista sekä muista lainsäädännön asettamista yksityiskohtaisemmista velvoitteista. Yksittäisten riskienhallinnan osa-alueiden osalta asetetaan useita tarkentavia velvoitteita myös muussa lainsäädännössä. Kyberturvallisuuslaki (124/2025), tiedonhallintalaki (906/2019) ja EU:n yleinen tietosuoja-asetus (679/2016) velvoittavat selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamaan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Riskienhallintaa toteutetaan hyvinvointialueen aluevaltuuston hyväksymän sisäisen valvonnan ja riskienhallinnan perusteiden sekä aluehallituksen hyväksymän riskienhallintasuunnitelman periaatteiden mukaisesti kaikilla osa-alueilla. Nämä muodostavat yhdessä hyvinvointialueen riskienhallintapolitiikan. Tietosuojasta ja tietoturvasta sekä laajemmin tietotekniikkaan liittyvien riskien hallinnasta huolehditaan jokaisessa prosessissa, projektissa ja tietojärjestelmässä.

5. Tietosuojan ja tietoturvallisuuden merkitys ja toteuttaminen

5.1 Turvattavat kohteet

Hyvinvointialueen toiminnassa turvattavia kohteita ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan. Tiedonhallintalain ja kyberturvallisuuslain mukaisesti hyvinvointialueen on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojensa ja tietojärjestelmiensä tietoturvallisuus koko niiden elinkaaren ajan. Tavoitteena on operatiivisten järjestelmien ja tietoverkon toiminnan turvaaminen sekä palvelujen tuottaminen niin normaali- kuin poikkeusoloissakin.

5.2 Tietosuoja- ja tietoturvaperiaatteet

Noudatamme hyvinvointialueen kaikessa toiminnassa seuraavia yleisiä tietosuoja- ja tietoturvaperiaatteita:

- Tietosuoja ja tietoturva ovat koko henkilöstön asia ja osa hyvinvointialueen päivittäistä toimintaa ja riskienhallintaa.
- Jokainen esihenkilö varmistaa, että tietosuoja- ja tietoturvamääräykset ja -ohjeet perehdytetään ja koulutetaan hänen alaiselleen henkilöstölle.
- Henkilötietojen käsittelyn tulee olla suunniteltua eikä henkilötietoja saa käsitellä muihin kuin etukäteen määriteltyihin tarkoituksiin.
- Luottamukselliset, arkaluonteiset ja muut salassa pidettävät tiedot kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
- Prosesseilla, tiedolla ja järjestelmillä on nimetyt omistajat ja muut vastuuhenkilöt. Tietosuojaan ja tietoturvaan liittyvä ohjaus, valvonta ja seuranta kuvataan ja vastuutetaan tämän tietosuoja- ja tietoturvaperiaatteen liitteessä 2.
- Tietosuoja ja tietoturva on huomioitava riittävän tarkasti sopimuksissa ja sopimusten toimeenpanoa tulee seurata.
- Tietosuojan ja tietoturvan huomioiminen on keskeinen osa muuta turvallisuuden ylläpitoa ja kehittämistä, tilasuunnittelua ja palvelujen kehittämistä.

Tietosuoja- ja tietoturvaperiaatteita noudattamalla voimme muun muassa suojata tietoja erilaisilta uhkilta, varmistaa toimintamme jatkuvuuden ja minimoida toiminnalliset riskit.

5.3 Tietosuojan ja -turvallisuuden toteutumista tukevia käytäntöjä

Tietosuoja- ja tietoturvatyön tavoitteena on luoda tietoturvakulttuuri, joka suojaa tietoja sekä toteuttaa arvojamme ja tavoitteitamme hyvinvointialueella. Hyvä tietosuoja- ja tietoturvataso saavutetaan tietosuoja- ja tietoturvaperiaatteen sekä periaatteiden, suunnitelmien ja ohjeistuksen mukaisilla toimintaperiaatteilla ja mekanismeilla. Hyvää tietosuoja- ja tietoturvatasoa hallitaan ja seurataan jatkuvan kehittämisen periaatteita noudattaen.

Tietojärjestelmien hankinta- ja kehitysprojekteissa toteutetaan tietoturvan ja teknisen arkkitehtuurin arvioprosessi (tietoturva-arvio). Tietoturva-arvioiden tekoon liittyvät tarkat periaatteet on kuvattu erillisessä linjauksessa. Arvioinneissa käytetään tarvittaessa ulkopuolisten asiantuntijoiden apua, ja prosessissa arvioidaan arkkitehtuuri- ja tietoturvavaatimusten toteutuminen. Riskitason perusteella valitaan kokonaisuuteen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Kun hankimme uusia tietojärjestelmiä, huomioimme erityisesti tietojärjestelmien käytettävyyden, toimivuuden ja laadukkuuden.

Tietojärjestelmien toimintaa ja käyttöä tulee valvoa, jotta varmistetaan niiden asianmukainen ja turvallinen käyttö sekä suojataan arkaluontoisia tietoja. Valvonta sisältää teknisiä toimenpiteitä, kuten pääsynhallintaa ja lokitietojen seurantaa, sekä hallinnollisia toimia, kuten käytäntöjen ja ohjeistusten luomista ja niiden noudattamisen valvontaa. Tietojärjestelmien ja tietojen käyttö on sallittua vain työtehtävien edellyttämässä laajuudessa, tai sopimusten ja lupien mukaisten tehtävien hoitamiseen, kun kyse on sopimus- ja yhteistyökumppaneistamme.

Riskilähtöisyys ohjaa myös henkilötietojen käsittelyä hyvinvointialueella ja on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Henkilötietojen käsittelyn riskejä arvioidaan, ja mikäli käsittelystä aiheutuu todennäköisesti korkeita riskejä henkilöiden oikeuksille ja vapauksille, laaditaan tietosuojan vaikutustenarviointi (DPIA, data protection impact assessment) ennen käsittelyn aloittamista. Vaikutustenarviointi on jatkuvan riskienhallinnan työkalu, jolla hallitaan henkilötietojen käsittelyyn liittyviä riskejä. Henkilötietojen siirtoon EU:n tai ETA-alueen ulkopuolelle kohdistuu erityisiä vaatimuksia, ja hyvinvointialueella noudatettavat menettelyt näissä tilanteissa määritellään erillisessä ohjeessa.

Henkilötietojen käsittely ja käytettävät tietojärjestelmät on kuvattu tietosuoja- ja tietojärjestelmäselosteilla. Tietosuojaselosteita käytetään hyvinvointialueella rekisteröityjen informointiin, joista keskeisimmät julkaistaan pirha.fi-sivustolla.

Hyvinvointialue voi ulkoistaa osan henkilötietojen käsittelystään sopimus- ja yhteistyökumppaneille. Valitsemme sopimuskumppaneiksemme vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat ajantasaisia tietosuoja- ja kyberturvallisuuslain sekä tiedonhallintalainsäädännön velvoitteita. Henkilötietojen käsittelyn ulkoistuksiin liittyvissä sopimuksissa täytyy laatia henkilötietojen käsittelysopimus. Myös salassapito- ja turvallisuussopimus solmitaan aina, kun hyvinvointialue tekee uuden sopimuksen. Hyvinvointialueella on sopimushallintaohje, jossa määritellään sopimusten valmisteluun, hyväksymiseen, toimeenpanoon ja elinkaareen liittyvät tehtävät ja vastuut.

Tietosuojasta ja -turvasta viestitään hyvinvointialueen viestintäohjeistuksen mukaisesti. Viestintä keskittyy ohjaukseen, neuvontaan ja tietoisuuden lisäämiseen, jotta poikkeamatilanteissa osataan toimia oikein ja parhaimmillaan välttää niistä useimmat. Häiriötilanteessa perustetaan hyvinvointialueen häiriötilannejohtoryhmä, joka sopii viestintävastuista ja pääviesteistä.

6. Tietosuoja- ja tietoturvatoimintojen organisoituminen

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

Aluehallitus vastaa, että hyvinvointialue täyttää tietosuojalainsäädännön mukaiset velvoitteet, ja valvoo velvoitteiden toteutumista. Hallitus määrittelee henkilötietojen käsittelyn periaatteet ja vastuuhenkilöt. Aluehallitus vastaa hyvinvointialueen konsernin kokonaisturvallisuuden hallinnasta, johon kuuluvat uhkiin varautuminen, normaaliolojen häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen. Aluehallituksen tehtävänä on huolehtia hyvinvointialueen sisäisestä valvonnasta ja riskienhallinnan järjestämisestä.

Prosessin omistaja – hyvinvointialuejohtaja, konsernijohtaja, Vaikuttaminen ja viestintä -vastuualueen johtaja (oto), vastaava johtajaylilääkäri, vastaava sosiaalihuollon johtaja, hr-johtaja, hallintojohtaja, tukipalvelujohtaja, talousjohtaja, pelastusjohtaja, hankintajohtaja, kiinteistöjohtaja, tietohallintojohtaja – omistaa prosessissaan käsiteltävän tiedon. Hän vastaa, että henkilötietoja käsitellään prosessissa lainsäädännön sekä hyvinvointialueen toimintaperiaatteiden ja ohjeistusten

mukaisesti. Prosessin omistaja päättää tiedon käyttötarkoituksista, kerättävistä tiedoista ja mahdollisista luovutuksista kolmansille osapuolille.

Yksittäisten työntekijöiden ja viranhaltijoiden roolit ja vastuut hyvinvointialueen tietosuojan ja tietoturvallisuuden toteuttamisessa on kuvattu tarkemmin tämän periaatteen liitteessä 2.

7. Toiminta häiriötilanteissa ja poikkeusoloissa

Pirkanmaan hyvinvointialueen valmiussuunnittelun tavoitteena on varautua ennalta erilaisiin normaaliajan toimintaa häiritseviin tai niitä vaarantaviin häiriötilanteisiin ja poikkeusoloihin. Toimintamallien tulee olla etukäteen suunniteltuja ja johtamisjärjestelmän toimiva. Suunnittelun, toimivan järjestelmän ja tehokkaan johtamisen avulla voimme reagoida nopeasti tarkoituksenmukaisin keinoin yllättäviinkin normaalista poikkeaviin tilanteisiin. Riskienhallinnalla tunnistamme, arvioimme ja hallitsemme tavoitteidemme saavuttamista uhkaavia tekijöitä.

Toiminnan jatkuvuus turvataan valmiussuunnitelmin, jotka sisältävät toimintaohjeet häiriötilanteen aikaiseen toimintaan ja mahdollistavat nopean toipumisen. Valmiussuunnittelussa huomioidaan toiminnan mahdolliset riskit ja prioriteetit. Tietojärjestelmiin ja tietojen käsittelyyn liittyvissä suunnitelmissa, järjestelyissä ja ohjeissa varaudutaan tietoturvallisuutta ja tietosuojaa koskevien laiminlyöntien, vahinkojen tai virheiden jälkikäteisselvittämiseen. Mahdollisia häiriö- ja poikkeustilanteita harjoitellaan säännöllisesti yhdessä palveluntoimittajien kanssa.

Häiriöistä ja heikkouksista ilmoittamisen tarkoituksena on toiminnan luottamuksellisuuden ja tietoturvallisuuden parantaminen. Puutteiden huomaaminen ajoissa voi auttaa välttämään vakavia seurauksia. Tietosuoja- ja tietoturvahäiriöiden ja -heikkouksien hallinta on prosessi, johon sisältyy jokaista hyvinvointialueen henkilöstöön kuuluvaa koskeva velvollisuus ilmoittaa havaitsemistaan puutteista. Prosessi sisältää myös puutteiden arvioinnin, välittömät korjaukset ja tapahtuman juurisyyn poistamisen silloin kun se on mahdollista.

8. Tietosuoja- ja tietoturvatietoisuus ja -osaaminen

Tietosuoja- ja tietoturvakoulutusvaatimukset koskevat koko hyvinvointialueen henkilöstöä. Tietosuojan ja tietoturvallisuuden tulee olla sisällytettynä perehdytysprosessiin. Pakollista koulutusta järjestetään koko henkilöstölle vähintään kahden vuoden välein. Lisäksi työntekijän tai viranhaltijan roolin tai tehtävien mukaista kohdennettua koulutusta järjestetään tarpeen mukaan.

Jokaisen hyvinvointialueen tietojärjestelmien käyttäjän on hyväksyttävä tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus ennen kuin hänelle myönnetään pääsy tietojärjestelmiin. Sitoumus sisältää hyvinvointialueen keskeiset tietosuoja- ja tietoturvakäytännöt.

9. Seuranta ja puuttuminen

Kaikki tietosuoja- ja tietoturvatapahtumat rekisteröidään ja raportoidaan. Tahallinen ohjeiden ja määräysten noudattamatta jättäminen katsotaan rikkomukseksi. Havaitusta väärinkäytöksestä tai pistokokeena havaitusta väärinkäytöksestä raportoidaan ja tiedotetaan lähintä esihenkilöä,

prosessin omistajaa sekä muita tarvittavia vastuuhenkilöitä väärinkäytöksestä riippuen. Väärinkäytökset on sanktioitu ja menettelytavat on kuvattu henkilöstöhallinnon ohjeistuksessa.

10. Tietosuojan ja tietoturvallisuuden hallintamalli

Tietosuoja- ja tietoturvaperiaate on osa hyvinvointialueen tietosuojan ja tietoturvan hallintamallia. Hallintamalliin kuuluvat kaikki tietosuojan ja tietoturvallisuuden hallintaan tarvittavat toimintatavat, hallintakeinot ja dokumentit. Hallintamallin avulla toteutetaan tietosuojan ja tietoturvan hallintaa ja seurantaa sekä arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Tavoitteena on hallintamallin kehittäminen ja sen myötä riittävän tietosuoja- ja tietoturvatason ylläpitäminen. Liitteessä 3 on lueteltu esimerkkejä tärkeimmistä hallintajärjestelmään kuuluvista toimintamalleista.

11. Tietosuoja- ja tietoturvaperiaatetta täydentävät dokumentit

Tietosuoja- ja tietoturvaperiaatetta täydentävät hyvinvointialueen tietoturvasuunnitelmat sekä yksityiskohtaiset linjaukset, päätökset ja ohjeet, kuten

- Tietosuoja- ja tietoturvaohjeet
- Tietosuojaa, tietoturvaa ja teknistä arkkitehtuuria koskevat linjaukset
- Käyttövaltuusperiaate
- Lokiperiaate ja ohje lokivalvonnasta
- Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja tietoturva-arvioinnista
- Ohjeet henkilötietojen tietoturvaloukkauksen ja tietoturvapoikkeaman hallinnasta

Tietosuojavastaava ja tietoturvavastaava seuraavat ohjeiden sisältöä ja ajantasaisuutta.

12. Periaatteen hyväksyminen ja ylläpito

Tietosuoja- ja tietoturvatyössä onnistuminen edellyttää hyvinvointialueen johdon sitoutumista työn tukemiseen. Hyvinvointialueen hallitus on hyväksynyt tämän tietosuojaa ja tietoturvaa koskevan periaatteen henkilöstöä sitovaksi säännöksi **1.3.2026 alkaen.**

Hyvinvointialueen tietosuojan ja tietoturvan ohjausryhmä vastaa tietosuoja- ja tietoturvaperiaatteen ajantasaisuudesta ja tarkistaa sen säännöllisesti muutostarpeita vastaavaksi. Periaatetta päivitetään vähintään 4–5 vuoden välein.