Pirkanmaan hyvinvointialueen tietosuoja- ja tietoturvapolitiikka

Käsittely:
Pirhan ja PSHP:n tietosuoja-, tietoturva- ja tekninen arkkitehtuuriryhmä 21.9.2022
Pirhan tietosuojaryhmä 22.9.2022
Pirhan ja PSHP:n tietosuojan ja tietoturvan ohjausryhmä 11.10.2022
Tukipalvelujen johtoryhmä 12.10.2022
Hyvinvointialueenjohtoryhmä 18.102022
Aluehallitus 24.10.2022

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

Tietosuoja ja tietoturva ovat osa päivittäistä toimintaamme. Tietosuoja- ja tietoturvapolitiikka koskee koko hyvinvointialuekonsernia ja kattaa kaikki hyvinvointialueen toimintaan liittyvät tietojenkäsittelytehtävät. Politiikan ja ohjeistuksen mukaista toimintaa edellytetään myös hyvinvointialueen tytäryhtiöiltä, osakkuus- ja osaomistusyhtiöiltä sekä yhteistyö- ja sopimuskumppaneiltamme.

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

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. 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 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 politiikan 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 tietoturvapolitiikan tai voimassa olevan lainsäädännön kanssa siten, että tietosuoja tai tietoturva heikkenee.

4. Tietosuojaan ja -turvallisuuteen kohdistuvat uhat

Tietosuojaan ja -turvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja saatavuudelle. Hyvinvointialueen aloittaessa toimintansa 1.1.2023 yhteiset toimintatavat hakevat vielä muotoaan, eikä organisaatiolla todennäköisesti ole yhdenmukaisia tapoja hoitaa turvallisuusasioita. Myös henkilöstön mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys voivat aiheuttaa merkittävän uhan hyvinvointialueen tietosuojalle ja -turvalle.

Aiemmin sovitut erilaiset toimintamallit palveluntuottajien kanssa voivat muodostaa uhan. Merkittäviä uhkia voi liittyä myös ulkopuolisten palvelujen tuottamiseen, mikäli palveluntuottajien kanssa ei ole tehty sopimuksia, joissa huomioidaan tietoturva, tietosuoja ja varautuminen sekä rikkomuksiin liittyvät sanktiot. Merkittävä uhka aiheutuu myös siitä, jos tehtyjen sopimusten noudattamista ei valvota.

Tiedonhallintalaki (906/2019) ja EU:n yleinen tietosuoja-asetus (679/2016) velvoittavat selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamaan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Jokaisessa prosessissa, projektissa ja tietojärjestelmässä on huolehdittava tietosuojaan ja tietoturvaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta. Edellytyksenä on, että turvallisuuskulttuuri nivotaan osaksi toimintaa, ja että hyvinvointialueen rakenteet mahdollistavat tämän.

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 mukaisesti hyvinvointialueen on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien 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 tietoturvapolitiikan liitteessä 2.
- Tietoturva ja tietosuoja on huomioitava riittävän tarkasti sopimuksissa ja sopimusten toimeenpanoa tulee seurata.

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 tietoturvapolitiikan sekä periaatteiden, suunnitelmien ja ohjeistuksen mukaisilla toimintaperiaatteilla ja mekanismeilla. Hyvää tietosuoja- ja tietoturvatasoa hallitaan ja seurataan jatkuvan kehittämisen periaatteita noudattaen.

Käytämme tietosuojan ja tietoturvan toteuttamisessa tarvittaessa ulkopuolisten asiantuntijoiden apua. Tietoturvan ja tietosuojan vaatimusten toteutuminen tietojärjestelmissä ja palveluissa on suositeltavaa tarkastaa eli auditoida ulkopuolisella asiantuntijataholla tai sisäisesti jo määrittelyvaiheessa, ja pakollista se on ennen kuin uusi tietojärjestelmä tai palvelu otetaan tuotantokäyttöön. Kun hankimme uusia tietojärjestelmiä, huomioimme erityisesti tietojärjestelmien käytettävyyden, toimivuuden ja laadukkuuden.

Tietojärjestelmien toimintaa ja käyttöä tulee valvoa. Tietojärjestelmien ja tietojen käyttö on sallittua vain työtehtävien edellyttämässä laajuudessa, tai sopimusten ja lupien mukaisten tehtävien hoitamiseen, kun kyse on sopimus- ja yhteistyökumppaneistamme.

Hyvinvointialue voi ulkoistaa osan henkilötietojen käsittelystä sopimus- ja yhteistyökumppaneille. Valitsemme sopimuskumppaneiksemme vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat ajantasaisia tietosuoja- ja tiedonhallintalainsäädännön velvoitteita. Henkilötietojen käsittelyn ulkoistuksiin liittyvissä sopimuksissa täytyy laatia henkilötietojen käsittelysopimus (yleinen tietosuojasopimus). Suuririskisessä henkilötietojen käsittelyssä täytyy myös laatia tietosuojan vaikutustenarviointi (DPIA, data protection impact assessment) ennen käsittelyn aloittamista. Yleinen salassapito- ja turvallisuussopimus solmitaan aina, kun hyvinvointialue tekee uuden sopimuksen.

6. Tietosuoja- ja tietoturvatoimintojen organisoituminen

Pirkanmaan hyvinvointialueen hallitus vastaa, että hyvinvointialue täyttää tietosuojalainsäädännön mukaiset velvoitteet, ja valvoo velvoitteiden toteutumista. Hallitus määrittelee henkilötietojen käsittelyn periaatteet ja vastuuhenkilöt. Hallitus vastaa hyvinvointialueen konsernin kokonaisturvallisuuden hallinnasta, johon kuuluvat uhkiin varautuminen, normaaliolojen häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen.

Prosessin omistaja – konsernipalvelujohtaja, johtajaylilääkäri, sosiaalihuollon vastuuviranhaltija, henkilöstöjohtaja, hallintojohtaja, talousjohtaja, pelastustoimen johtaja – omistaa prosessissaan käsiteltävän tiedon. Hän vastaa, että henkilötietoa käsitellään prosessissa lainsäädännön ja hyvinvointialueen toimintaperiaatteiden sekä ohjeistusten mukaisesti. Prosessin omistaja päättää tiedon käyttötarkoituksista, kerättävistä tiedoista ja mahdollisista luovutuksista kolmansille osapuolille.

Yksittäisten työntekijöiden, viranhaltijoiden ja toimielinten roolit hyvinvointialueen tietosuojan ja tietoturvallisuuden toteuttamisessa on tarkemmin kuvattu liitteessä 2 - Tietosuojan ja tietoturvallisuuden vastuut.

7. Toiminta häiriötilanteissa ja poikkeusoloissa

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

Toiminnan jatkuvuus tulee turvata valmiussuunnitelmalla, joka sisältää häiriöiden ennalta ehkäisemisen ja mahdollistaa niistä nopean toipumisen. Valmiussuunnittelussa tulee erityisesti huomioida 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. Oikean asenteen luominen ilmoittamiseen onkin eräs häiriöiden ja heikkouksien hallinnan haasteista. 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.

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 määräajoin tietoturvasuunnitelman mukaisesti. Työntekijän tai viranhaltijan roolin tai tehtävien mukaista kohdennettua koulutusta järjestetään tarpeen mukaan.

Ajantasaiset tietosuoja- ja tietoturvaohjeet ovat luettavissa hyvinvointialueen intranetissä. Tietosuojavastaava ja tietoturvavastaava seuraavat ohjeiden sisältöä ja ajantasaisuutta.

Tietojärjestelmän käyttäjän on hyväksyttävä tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus ennen kuin hänelle myönnetään pääsy tietojärjestelmiin.

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 tietoturvapolitiikka 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 ja dokumenteista.

11. Politiikan hyväksyminen ja ylläpito

Tietosuoja- ja tietoturvatyössä onnistuminen edellyttää hyvinvointialueen johdon sitoutumista työn tukemiseen. Hyvinvointialueen hallitus on hyväksynyt tämän tietosuojaa ja tietoturvaa koskevan politiikan henkilöstöä sitovaksi säännöksi pp.kk.vvvv.

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