

Peruspalvelukuntayhtymä Kallio

TIETOSUOJAPOLITIikka

## **Johdanto**

Tietosuojapolitiikassa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja menetelmät organisaatiossa. Näiden periaatteiden ja menetelmien avulla Peruspalvelukuntayhtymä Kallion tavoitteena on varmistaa palvelujen korkea laatu sekä korkea tietosuojan taso.

Lähtökohtaisesti kaikki viranomaisen toiminta on julkista. Toisaalta laki myös edellyttää, että henkilön yksityisyydensuoja on turvattava. Tämän yksityisyydensuojan takaamiseksi kaikki peruspalvelukuntayhtymä Kallion hallussa olevat henkilöä koskevat tiedot on suojattu. Henkilötietoja käsittelevät vain tietoihin oikeutetut henkilöt, niitä luovutetaan ainoastaan henkilön itsensä suostumuksella ja niitä käsitellään siten, että ulkopuolisilla ei ole mahdollisuutta päästä tietoihin käsiksi.

Tietojenkäsittelyn turvallisuus on kuntayhtymän toiminnan jatkuvuuden ja palveluiden laadun kannalta erittäin tärkeää. Tietosuoja on oleellinen osa tietoturvallisuutta.

Peruspalvelukuntayhtymä Kallion johto ja koko henkilöstö on sitoutunut tietoturvalliseen toimintaan ja toimii tässä asiakirjassa julkaistujen periaatteiden mukaisesti. Jokainen on tietoinen tietoturvallisuudesta ja sen merkityksestä, koulutettu ja ammattitaitoinen toimimaan turvallisella tavalla.

Tämä tietosuojapolitiikka on hyväksytty Peruspalvelukuntayhtymä Kallion yhtymähallituksessa 10.4.2014 ja se astuu voimaan 1.5.2014 korvaten yhtymähallituksen hyväksymän edellisen version.

## **Tietosuojapolitiikan kattavuus**

Tietosuojapolitiikka kattaa kuntayhtymän kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät. Jokaisen Kallion viranhaltijan, työntekijän, opiskelijan ja luottamushenkilön sekä toimintayksikön tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietosuojapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä.

Tätä politiikkaa sovelletaan myös kuntayhtymässä työskentelevään vuokratyövoimaan ja konsultteihin sekä muihin sidosryhmiin. Asiakkaiden ja muiden sidosryhmien välisissä sopimuksissa ja tietoturvakäytäntöjen toteuttamisessa on vähimmäisvaatimuksena tämä politiikka.

Tietosuojan hallintamenetelmät kohdistuvat kaikkeen henkilötietojen käsittelyyn sekä manuaaliseen että sähköiseen ja pitävät sisällään myös puhutun ja kirjoitetun tiedon.

## **Tietosuojan tavoitteet ja periaatteet**

Tietosuoja on oleellinen osa tietoturvallisuutta. Sillä tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista.

Lainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä.

Laissa säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa liittyen.

Henkilökunnan toimintaa ohjaavat lain ja määräysten mukaiset velvollisuudet ja oikeudet sekä näiden lisäksi sosiaali- ja terveydenhuollon ammattietiikka, johon sisältyy vastuu hyvästä toimintatavasta ja velvollisuus tietojen salassapidosta ja vaitiolosta.

### **Organisointi ja vastuut**

Peruspalvelukuntayhtymä Kallion yhtymähallitus suunnittelee, ohjaa ja valvoo kuntayhtymän tietoturvallisuutta osana palvelujen laatua ja vastaa tietosuojapolitiikan julkaisusta. Tietohallintoa johtaa Hallinto- ja tukipalvelujen toimialajohtaja, joka vastaa kokonaisturvallisuudesta.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ja laki sähköisestä lääkemääräyksestä edellyttävät, että jokainen sosiaali- ja terveydenhuollon palvelujen antaja nimeää tietosuojavastaavan, jonka tehtävänä on erityisasiantuntijana auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja tietosuojaan taso, jonka avulla voidaan rakentaa ja säilyttää luottamus rekisteröidyn ja rekisterinpitäjän välille. Tietosuojavastaava koordinoi tietosuojatyon toteutusta ja vastaa tietosuojaan koulutuksesta ja raportoinnista.

Tietosuojaryhmä, joka on osa tietoturvaryhmää, edustaa tietoturvaluustoimintaa, jolla varmistetaan kuntayhtymän toimialojen henkilörekisterien tietosuojaan toteuttaminen. Tietosuoja-ryhmä valmistelee tietosuojaan kuuluvat asiat Peruspalvelukuntayhtymä Kallion johtoryhmän käsittelyn jälkeen toimialajohtajien hyväksyttäväksi.

Jokainen Peruspalvelukuntayhtymä Kalliossa tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan.

### **Tietoturvallisuuden ja tietosuojaan toteuttaminen**

Tietoturvallisen toiminnan toteuttaminen perustuu Peruspalvelukuntayhtymä Kallion yhtymähallituksen hyväksymään tietoturva- ja tietosuojapolitiikkaan. Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka sisältää hallinnollisia, fyysisiä ja teknisiä ratkaisuja ja niiden avulla varaudutaan tietoihin kohdistuviin uhkiin sekä pyritään vähentämään tietoturvariskejä.

Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien tietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton.

Tietoihin ja tietojärjestelmiin pääsy on tarkoin määritelty. Henkilöillä on tietojen saantioikeus vain silloin, kun siihen on olemassa peruste. Tietoja saa käsitellä vain siinä käyttötarkoituksessa ja laajuudessa kuin on välttämätöntä. Tämän lisäksi myönnettävät pääsyoikeudet riippuvat henkilön roolista.

Tietojärjestelmiä käyttävät henkilöt tunnustetaan ja todennetaan siten, että henkilön esiintymisen toisena ei ole mahdollista. Käytössä on tarvittavat käyttäjätunnus-, salasana-, toimikortti- ja PIN -koodimenettelyt. Kaikkia normaalista poikkeavia tapahtumia ja tilanteita valvotaan ja seurataan.

Henkilötietojen käyttöä ja luovutuksia on seurattava. Seuraamisvelvoite tarkoittaa muun muassa, että kaikista tietojärjestelmän avulla tapahtuvista tietojen käytöstä ja luovutuksista tallentuu automaattinen lokimerkintä. Jos luovutus tapahtuu paperisena tai muuna ei-sähköisenä menettelmänä, tulee kaikki luovutukset kirjata myös tietojärjestelmään.

Henkilökunnan tietoturvan ja tietosuojan osaamisen taso mitataan määräajoin verkkopohjaisessa koulutus- ja osaamisympäristössä.

### **Tietojen luokittelun, säilytyksen ja luovutuksen periaatteet**

Lainsäädännön perusteella Peruspalvelukuntayhtymä Kallio voi saada haltuunsa potilasta/asiakasta koskevia tietoja useista lähteistä. Hoito- ja palvelusuhteen aikana tietoja saadaan potilaalta/asiakalta itseltään ja niitä syntyy hoito- ja palvelutapahtuman yhteydessä. Säilytyksessä voi olla tietoja potilaan/asiakkaan edellisistä hoito- ja palvelusuhteista. Niitä voi olla vastaanotettu muilta hoito- ja palveluyksiköiltä tai muilta viranomaisilta. Jos tietojen suojaamiseksi näitä tietoja tarvitsee ryhmitellä erillisiksi kokonaisuuksiksi esimerkiksi säilytystä tai luovutusta varten, näin voidaan tarpeen mukaan tehdä.

Tietojen säilytyksestä on säädetty arkistolaissa ja tietojen säilyttämisestä on erikseen annettu asetuksia ja ohjeita. Henkilötietoja koskevat erilaiset säilytysvaatimukset. On myös erikseen säädetty, milloin vanhat tiedot täytyy poistaa. Väärien, vanhentuneiden ja virheellisten tietojen käsittely on kielletty, ja näiden oikaiseminen on tehtävä tarpeen mukaan.

Henkilötietoja voidaan luovuttaa ainoastaan potilaan/asiakkaan nimenomaisella suostumuksella. Hoitohenkilökunnalla on tietty oikeus käsitellä potilaan/asiakkaan tietoja ilman hänen lupansa. Näitä tilanteita voivat olla esimerkiksi potilaan tajuttomuustila vaikeassa loukkaantumisessa, potilaan vajaakykyisyys päättää itse asiasta tai oikeusviranomaisen määräämä pakkokeino. Tietoja voidaan luovuttaa ilman suostumusta myös lainsäädännöstä tulevan tietojensaantioikeuden perusteella.

Säilytykseen ja luovutukseen liittyvistä määräyksistä noudatetaan kulloinkin voimassa olevia lakeja ja asetuksia sekä sosiaali- ja terveysministeriön henkilöstölle antamia määräyksiä ja ohjeita.

### **Lait ja asetukset**

Lainsäädäntö suojaa henkilötietoja usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Peruspalvelukuntayhtymä Kallion tietoturvan ja tietosuojan hallintakäytäntöjen tulee kaikilta osin noudattaa lakeja ja asetuksia, sopimusten velvoitteita ja turvallisuusvaatimuksia.

Tietoturvallisuudesta, arkaluonteisten tietojen käsittelystä ja erityisesti asiakas-/potilastiedoista on säädetty useassa eri laissa, joista tässä yhteydessä oleellisimmiksi voidaan katsoa

- o laki viranomaisen toiminnan julkisuudesta (621/1999)
- o henkilötietolaki (523/1999)
- o laki yksityisyyden suojasta työelämässä (759/2004)
- o laki potilaan asemasta ja oikeuksista (785/1992)
- o laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- o laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- o sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)
- o arkistolaki (831/1994)
- o laki sähköisestä asiointista viranomaistoiminnassa (13/2003)
- o sähköisen viestinnän tietosuojalaki (516/2004)
- o laki sähköisestä lääkemääräyksestä (61/2007) ja sosiaali- ja terveysministeriön asetus sähköisestä lääkemääräyksestä (485/2008)

## **Rikkomukset ja seuraamukset**

Jokainen Peruspalvelukuntayhtymä Kallion tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan hyväksytyjä käytösääntöjä, tietoturva- ja tietosuojaohjeita. Tietosuojapolitiikkaa sekä siihen liittyviä ohjeita vastaan havaitut rikkomukset raportoidaan organisaation johdolle ja tietosuojavastaavalle. Rikkomuksen tekijä saatetaan edesvastuuseen teostaan ja häntä vastaan ryhdytään rikkomuksen luonteen vaatimiin toimenpiteisiin. Vakaviin tietosuojarikkomuksiin liittyvä sisäinen ja julkinen tiedottaminen hoidetaan tapauskohtaisesti johdon tai johdon valtuuttaman henkilön toimesta.