



Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan kuntayhtymän tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa kuntayhtymä toimii rekisterinpitäjänä.

Kuntayhtymän palveluiden perustana ovat kuntalaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn kuntayhtymän toimintaympäristöissä. Kuntayhtymän palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Kuntayhtymän toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Henkilötietojen käsittelyn suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvien osin poikkeusoloihin. Erityisesti huolellista ennakkovalmistelua edellyttävät ne tilanteet, joissa henkilötietojen käsittelyä ohjataan sopimuksilla.

Tietoturvallisuus ja tietosuoja on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Yhtymähallitus tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Poliitiikka toimii perustana kuntayhtymän tietosuoja koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön. Tietoturvat toiminnan periaatteet on määritelty kuntayhtymän tietoturvapoliitiikassa.

Tietosuojapolitiikka koskee koko organisaatiota ja sen henkilöstöä mukaan lukien niitä kuntayhtymän sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kuntayhtymän omistamaa tai hallinnoimaa tietoa. Poliitiikka kattaa kuntayhtymän omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt virheelliset tai tarpeettomat tiedot oikaistuiksi tai poistetuiksi.

Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen turvaaminen siten, että niiden luottamuksellisuus, eheys ja käytettävyys/saatavuus voidaan taata ja osoittaa toteutuneen.

* Luottamuksellisuus: Tieto on vain siihen oikeutettujen saatavilla.

* Eheys: Tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.

* Käytettävyys/saatavuus: Tieto on saatavilla aina sitä tarvittaessa.



Tietosuojan tavoitteet ja periaatteet

Kuntayhtymän lähtökohtana tietosuojassa on riskilähtöisyys. Kuntayhtymä rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa kuntayhtymän riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Kuntayhtymä toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Kuntayhtymän toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä erityisesti potilastyössä ja lisäksi mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Kuntayhtymän tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- * henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- * henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- * henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- * henkilötietojen käsittely toteutetaan täsmällisesti
- * henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- * henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

Tietosuojan organisointi ja vastuut

Kuntayhtymän tietosuojaa johtaa ja valvoo yhtymähallitus. Yhtymähallitus päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuojavastaavan. Potilastietosuojan ja -turvan osa-alueesta vastaa johtava lääkäri.

Organisaation tietosuojavastaava toimii tietosuojan erityisasiantuntijana, joka valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä vastaa neuvonnasta ja kouluttamisesta tietosuoja-asioissa. Tietosuojavastaava raportoi organisaation johdolle tietosuojan toteutumisesta.



Kuntayhtymässä toimii tietosuojatyöryhmä tietosuojan kehittämisen suunnittelua ja toimeenpanon valmistelua varten. Tietosuojaryhmä ylläpitää tietosuojan kehittämissuunnitelmaa, valmistelee tietosuojaan liittyvää ohjeistusta, tiedottaa tietosuojatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietosuojatyön osaksi kuntayhtymän operatiivista toimintaa.

Kunkin henkilörekisterin vastuuhenkilön on huolehdittava siitä, että tietosuojalainsäädännön edellyttämät velvoitteet ko. rekisterinpidon osalta tulevat hoidettua. Henkilörekisterin vastuuhenkilön tehtävänä on päättää henkilörekisteriin kohdistuvan tarkastusoikeuden käytöstä tai käytön epäämisestä sekä virheen oikaisuvaatimuksen aiheuttamista toimenpiteistä. Potilastietojen tarkastusoikeutta koskevien pyyntöjen käsittely on ohjeistettu tarkemmin potilasasiakirjaohjeistossa.

Henkilöstöhallinnolliset esimiehet vastaavat alaistensa tietosuojalainsäädännön mukaisesta toiminnasta kuntayhtymässä ja omassa yksikössään annettujen ohjeiden mukaisesti. Jokainen organisaatiossa tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Kuntayhtymän rekisterihallinnon vastuut ja menettelytavat määritellään tarkemmin kuntayhtymän rekisterihallinnosta annetussa ohjeessa.

Tietosuojan toteuttaminen

Kuntayhtymä haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia.

Tietosuojan toteuttamisessa kuntayhtymä haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Kuntayhtymän järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuoja-vaatimukset. Sovellettavat tietosuoja-vaatimukset 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.

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

Kuntayhtymän 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.



Kuntayhtymä ohjeistaa ulkoistettua henkilötietojen käsittelijää kyseistä tarkoitusta varten tehdyllä ohjeistuksella. Samaa ohjeistusta sovelletaan myös kuntayhtymän oman henkilöstön kohdalla.

Kuntayhtymä rekisterinpitäjänä sisällyttää tietosuojan myös projektinhallintamallinsa osaksi.

Kuntayhtymässä on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

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

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Kuntayhtymässä on määritetty toimintaprosessi ja ohje liittyen toimintaan henkilötietoihin kohdistuvien tietoturvaloukkausten tapahtuessa. Prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa.

Henkilötietojen tietoturvaloukkauksen sattuessa kuntayhtymällä on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

Rikkomukset ja seuraamukset

Jokainen kuntayhtymän tietojärjestelmien käyttäjä on sitoutunut noudattamaan kuntayhtymän tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla tietosuojasitoumuksen. Tietosuojasitoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietosuojarikkomusten mahdollisiin seuraamuksiin sovelletaan toimintaohjetta ja tietosuojarikkomukset raportoidaan kuntayhtymän johdolle ja tietosuojavastaavalle.

Tietosuojapolitiikan ajan tasalla pitäminen ja muutokset

Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon kuntayhtymän tietosuojan kehittämis- sekä tietosuojapolitiikan päivitystyössä. Päivittämisestä vastaa kuntayhtymän tietosuojatyöryhmä. Tietosuojapolitiikka hyväksytään yhtymähallituksessa valtuustokausittain.