



KAINUUN
hyvinvointialue

Tietosuojapolitiikka

Kainuun hyvinvointialue



Sisällysluettelo

1	Johdanto	1
2	Tietosuojan määritelmä	1
3	Tietosuojan tavoitteet ja periaatteet	2
4	Tietosuojan organisointi ja vastuut	2
5	Tietosuojan toteuttaminen	3
6	Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus	4
7	Rikkomukset ja seuraamukset	4

Kainuun hyvinvointialueen tietosuojapolitiikka

1 Johdanto

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

Hyvinvointialueen palveluiden perustana ovat potilaidemme ja asiakkaidemme tarpeet. Hyvinvointialueen palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömyydestä ja turvallisesta toiminnasta. Hyvinvointialueen toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Henkilötietojen käsittelyn suunnittelussa ja ohjaamisessa tulee varautua eritasoisin toimintahäiriöihin sekä mahdollisiin poikkeusoloihin.

Tietoturvallisuus ja tietosuoja on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Kainuun hyvinvointialue tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Poliitiikka toimii perustana hyvinvointialueen tietosuojaan koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön. Tietoturvaturvatoiminnan periaatteet on määriteltävä hyvinvointialueen tietoturvapoliitikassa.

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

2 Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Henkilötietojen käsittelyn on oltava asianmukaista ja 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 muutetuiksi 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 saatavuus voidaan taata ja osoittaa toteutuneen.

- tietojen luottamuksellisuus: tieto on vain siihen oikeutettujen saatavilla.
- tietojen eheys: tieto on oikeaa ja eheää, eikä ole muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- tietojen saatavuus: tieto on saatavilla aina sitä tarvittaessa.

3 Tietosuojaan tavoitteet ja periaatteet

Hyvinvointialueen lähtökohtana tietosuojassa on riskien tunnistaminen. Hyvinvointialue rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet.

Riskin tunnistamisen merkitys korostuu, kun rekisterinpitäjä määrittää teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuojaan toteutuminen henkilötietojen käsittelyssä. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojaan toteuttamiseksi, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta ja muita suojaustoimenpiteitä.

Tietosuojaan riskien hallinta on osa hyvinvointialueen riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Organisaatio toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojaan 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.

Hyvinvointialueen toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojaan periaatetta. Tietosuoja otetaan huomioon perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa.

Hyvinvointialueen tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- henkilötietojen käsittelyn ohjeistaminen
- henkilöstön tietosuojakoulutukset
 - henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
 - henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
 - henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarpeellinen lainmukainen aika
- henkilötietoja sisältäville asiakirjoille määritellään säilytysajat
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

4 Tietosuojaan organisointi ja vastuut

Tietosuojaan johtaa ja valvoo Kainuun hyvinvointialueen aluehallitus. Hyvinvointialuejohtaja päättää rekisterinpidon ja tietosuojaan kokonaisuudesta antamalla tietosuojaan ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuojavastaavan ja tietoturva- ja tietosuojayöryhmän.

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

Hyvinvointialueella toimii tietoturva- ja tietosuojatyöryhmä, jonka tehtävänä on tietosuojan suunnittelu ja kehittäminen. Tietoturva- ja tietosuojatyöryhmä, valmistelee tietosuojaan liittyviä ohjeistuksia, tiedottaa tietosuojatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietosuojatyön osaksi organisaation operatiivista toimintaa.

Esihenkilöt vastaavat oman yksikkönsä henkilöstön osaamisesta ja henkilötietojen käsittelystä tietosuojalainsäädännön sekä organisaatiossa annettujen ohjeiden mukaisesti. Jokainen alueen tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Hyvinvointialueen rekisterihallinnon vastuut ja menettelytavat määritellään tarkemmin hyvinvointialueelle laadittavasta rekisterihallinnon ohjeesta.

5 Tietosuojan toteuttaminen

Hyvinvointialue toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen ja muun lainsäädännön vaatimuksia. Tietosuojan toteuttamisessa varmistetaan tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Hyvinvointialueen tietojärjestelmien ja ohjelmistojen hankinta- ja käyttöönottoprosesseissa 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.

Hyvinvointialue voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Hyvinvointialue valitsee sopimuskumppanikseen sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa ja toteuttavat tietosuoja-asetuksen vaatimukset.

Henkilötietojen käsittelyä sisältävissä hankinnoissa tietosuojaan liittyvät vaatimukset liitetään osaksi tarjouspyyntöä.

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

Hyvinvointialueella on käytössä toimintaprosessit ja ohjeet, jotka liittyvät rekisteröityjen oikeuksien toteuttamiseen, joita ovat henkilötietojen tarkastusoikeus ja oikeus vaatia virheellisen tiedon oikaisua. Prosessin mukaista toimintatapaa noudatetaan tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan tai haluavat kopiot asiakirjoista, jotka sisältävät heidän omia henkilötietojaan. Toimintatapaa noudatetaan myös silloin, kun rekisteröity esittää organisaatiolle omia henkilötietoja koskevan virheellisen tiedon korjaamisvaatimuksen (oikaisuoikeuden toteuttaminen).

Hyvinvointialue huolehtii henkilöstön riittävästä tietosuojaosaamisesta kouluttamalla ja tiedottamalla henkilökuntaa. Organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin.

Hyvinvointialueella on laadittu tietosuojaan liittyviä ohjeita, joiden sisältöjä koulutetaan henkilöstölle ja jotka ovat luettavissa hyvinvointialueen intrassa. Käyttöoikeudet eri järjestelmiin myönnetään käyttäjähallintaprosessin kautta ja käyttöoikeudet myönnetään voimassa olevien työtehtävien mukaisesti.

6 Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Hyvinvointialueella on määritetty toimintaprosessi tilanteisiin, joissa havaitaan tai todetaan henkilörekisteririkkomusepäily, johon liittyy henkilötietoihin kohdistuva tietoturvaloukkaus. Prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa.

Henkilötietojen tietoturvaloukkauksen sattuessa hyvinvointialueella on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaiselle sekä rekisteröidylle.

Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus 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.

7 Rikkomukset ja seuraamukset

Jokainen hyvinvointialueen tietojärjestelmien käyttäjä ja organisaation työntekijä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla salassapito- käyttäjäsitoumuksen työsuhteen alkaessa. Esimies ja työntekijä käyvät läpi tietosuoja- ja käyttäjäsitoumuksen ja sen merkityksen organisaation toiminnassa.

Tietosuojasitoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään käyttölokien seuranta- ja valvontasuunnitelman (liitteen 1) mukaisesti. Tietoturva- ja tietosuojarikkomusten mahdollisiin seuraamuksiin sovelletaan organisaation määrittämien tietoturva- ja tietosuojarikkomusten seuraamustaulukon mukaisia toimia (liite 2). Tietosuojarikkomukset raportoidaan hyvinvointialueen johdolle ja tietosuojavastaavalle.

Liitteet: Liite 1 Käyttölokien seuranta- ja valvontasuunnitelma
Liite 2 Tietoturva- ja tietosuojarikkomusten seuraamustaulukko