TIETOSUOJAPOLITIIKKA

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Paimion kaupungin tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa Paimion kaupunki tai sen tytäryhtiöt toimivat rekisterinpitäjänä.

Paimion kaupungin palveluiden perustana ovat Paimiolaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn kaupungin organisaation ja sen konsernin toimintaympäristöissä. Palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Henkilötietojen käsittelyn suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Erityisesti huolellista ennakkovalmistelua edellyttävät tilanteet, joissa henkilötietojen käsittelyä ohjataan sopimuksilla.

Tietoturvallisuus ja tietosuoja on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Kaupungin johto tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana tietosuojaa koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön. Tietoturvatoiminnan periaatteet on määritelty kaupungin tietoturvapolitiikassa.

Tietosuojapolitiikka koskee koko organisaatiota ja sen henkilöstöä mukaan lukien konsernin sekä niitä Paimion kaupungin sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kaupungin 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 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.

- Luottamuksellisuus: Tieto on vain siihen oikeutettujen saatavilla.
- Eheys: Tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Saatavuus: Tieto on saatavilla aina sitä tarvittaessa.

Tietosuojan tavoitteet ja periaatteet

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

Paimion kaupunki 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.

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

Kaupungin 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

Paimion kaupungin tietosuojaa johtaa ja valvoo kaupungin johtoryhmä. Kaupunginjohtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuojavastaavan sekä tietosuojaryhmän. Terveyskeskus kuntayhtymän tietosuojavastaava toimii yhteistyössä kaupungin tietosuojaorganisaation kanssa. Kaupungin tietosuojavastaava toimii tietosuojan erityisasiantuntijana, joka valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä vastaa neuvonnasta ja kouluttamisesta tietosuoja-asioissa. Tietosuojavastaava raportoi johtoryhmälle tietosuojan toteutumisesta. Tietosuojavastaavan asema organisaatiossa on riippumaton.

Kaupungissa 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 organisaation operatiivista toimintaa.

Kunkin henkilörekisterin vastuuhenkilön on huolehdittava siitä, että tietosuojalainsäädännön edellyttämät velvoitteet ko. rekisterinpidon osalta tulevat hoidettua.

Henkilöstöhallinnolliset esimiehet vastaavat alaistensa toimintatavan tietosuojalainsäädännön mukaisuudesta organisaation antamien ohjeiden mukaisesti. Jokainen Paimion kaupungissa tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä ovat vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Tietosuojan toteuttaminen

Paimion kaupunki 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 Paimion kaupunki haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

Paimion kaupungin järjestelmä- ja sovelluskehitysprosesseissa 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. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Paimion kaupunki voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Paimion kaupunki 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.

Paimion kaupungin 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.

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

Paimion kaupunki rekisterinpitäjänä sisällyttää tietosuojan myös projektinhallintamallinsa osaksi.

Paimion kaupungissa 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.

Paimion kaupunki huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja tiedottamisen kautta. Organisaatioon 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

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

Henkilötietojen tietoturvaloukkauksen sattuessa Paimion kaupungilla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturva-loukkaus 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.

Rikkomukset ja seuraamukset

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