SUONENJOEN KAUPUNKI

TIETOSUOJA- JA TIETOTURVAPOLITIIKKA

Kaupunginhallitus 7.5.2018 § 89

Sisällys

Johdanto

Suonenjoen kaupunki tuottaa päätuotteenaan hyvinvointipalveluja Suonenjoen kaupungin asukkaille. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn. Tietojen digitalisoituessa enimmässä määrin ja tietosuojaan liittyvän lainsäädännön muuttuessa, edellytetään tietosuoja- ja tietoturva ajattelun ottamista osaksi jokaisen kaupungin palveluksessa olevan viranhaltijan ja työntekijän sekä luottamushenkilön päivittäistä työskentelyä. Myös ulkopuolisten toimijoiden ja toimittajien tulee sitoutua Suonenjoen kaupungin tietoturva- ja tietosuojapolitiikkaan.

Tietoturva- ja tietosuojapolitiikka määrittää ne **periaatteet**, **toimintatavat**, **vastuut**, **toimivallat**, **valvonnan ja seuraamusjärjestelmän**, joita noudatetaan Suonenjoen kaupungin tietoturvan ja tietosuojan toteuttamisessa ja kehittämisessä. ”**Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohje**” kuvaa ja ohjeistaa sen, miten tehtävät käytännössä hoidetaan. Suonenjoen kaupunki haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä.

Tietosuojapolitiikan avulla turvataan Suonenjoen kaupungin asiakkaiden, työntekijöiden ja muiden sidosryhmien oikeudet yksityisyyteen. Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus.

Tietoturva- ja tietosuojapolitiikan periaatteet

Suonenjoen kaupungin johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Politiikkaa tarkennetaan erillisillä ohjeilla. Ei riitä, että toimitaan *oletusarvoisesti* tietosuoja-asetuksen mukaisesti, vaan meidän *pitää myös pystyä se osoittamaan*.

Tietosuojassa ei ole kysymys rajoituksista oikeuksiin saada tietoja vaan toimenpiteistä, joilla henkilön yksityisyys suojataan **aina** henkilötietoja käsitellessä.

- **Henkilötietoja** ovat kaikki sellaiset tiedot, jolla henkilö voidaan suoraan tai epäsuorasti tunnistaa ja yksilöidä. Esimerkiksi nimi, osoite, henkilötunnus, sähköpostiosoite, verkkotunnistetiedot, tallentava kameravalvonta.

- **Henkilötietojen käsittelyä** ovat kaikki toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Esimerkiksi henkilötietojen tallennus, muokkaus, säilytys, luovuttaminen, poistaminen.

Rekisterinpitäjän on aina määriteltävä käsittelyn peruste huolellisesti. Henkilötietojen käsittelyn on aina oltava perusteltua, asianmukaista ja tapahduttava tiettyä tarkoitusta varten asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Henkilötietoja käsitellään tietosuojaperiaatteiden mukaisesti, rekisteröidyn oikeuksia toteuttaen.

Erityisiin henkilötietoryhmiin kuuluvien tietoja käsitellään vain, kun tietojen käsittelemiseen on olemassa lakiin perustuva käsittelyn perusta. Henkilötietojen käsittelyssä varmistetaan alaikäiseltä tietoja kerättäessä vanhempien suostumus henkilötietojen käsittelemiseen sen mukaisesti kuin lainsäädäntö edellyttää.

Rekisterinpitäjän velvollisuudet

Suonenjoen kaupungin **rekisterinpitäjinä toimivat kaupunginhallitus sekä lautakunnat.** Rekisterinpitäjä määritellään tehtävien hoidon säännösten ja määräysten mukaisesti. Rekisterinpitäjällä on ylin vastuu rekisterissään olevista henkilötiedoista, käsittelyn suunnittelusta ja toteutuksesta. Rekisterinpitäjä on pystyttävä osoittamaan muun muassa viranomaisille, että esimerkiksi henkilötietojen käsittelyn periaatteita on noudatettu niin, että toiminta on lainmukaista, kohtuullista ja läpinäkyvää.

Jokaisella rekisterinpitäjällä on dokumentoituna henkilötietojen käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden toteuttamisen käytännöt:

- Palvelu-/ toimikohtaiset ”**selosteet henkilötietojen käsittelytoimista**” sekä ”**tietosuojaselosteet**”.
- Mahdolliset ”**toimiala- /palvelukohtaiset ohjeistukset”**, joiden avulla voidaan huomioida suoritettavan henkilötietojen käsittelyn erityispiirteet
- ”**Riskienarvioinnit**”, ja ”**vaikutustenarvioinnit**” merkittävimmille toiminnoille

Rekisterinpitäjällä on vastuu oman organisaation riittävästä osaamisesta ja sisäisistä ohjeistuksista. Tietosuojan ja tietoturvan toteuttaminen ja ylläpitäminen ovat osa jokaisen henkilöstöön kuuluvan työtehtäviä ja niihin liittyviin vastuita. ”**Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohje”** löytyy intran tietosuoja- ja tietoturva sivustolta.

Riskianalyysi ja vaikutusten arviointi

Tietosuojariskienhallinta on osa Suonenjoen kaupungin riskienhallintaprosessia. Kukin lautakunta rekisterinpitäjänä arvioi tuottamiensa palveluiden henkilötietojen käsittelyyn liittyvät riskit. Riskianalyysissa tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Riskitason määrityksellä vältetään matalariskisen toiminnan ylisäätely ja vastaavasti tunnistetaan merkittävän tason riskit, jotka on raportoitava kaupungin johdolle saakka. Riskitekijöiden tunnistaminen toimii pohjana myös tarkoituksenmukaisten tietojärjestelmien ja tietoverkkojen tietoturvaratkaisujen käyttämiselle sekä tietosuojakäytännöille. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy.

Suonenjoen kaupunki toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi myös tietosuojan vaikutustenarviointeja. Vaikutustenarviointi vaaditaan vain tilanteessa, jossa henkilötietojen käsittelyyn liittyy erityisiä riskejä käsittelytapojen, käsittelyn laajuuden tai käsiteltävien tietojen luonteen vuoksi. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Rekisteröidyn oikeudet

Tietosuoja-asetus määrittää rekisterinpitäjän velvollisuuksien ohella myös rekisteröidylle oikeuksia. Rekisteröidyllä on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen. Rekisteröidyn oikeudet on kuvattu dokumenteissa ”**Tietosuojaselosteet**”.

Henkilötietojen käsittelyyn liittyviä toimintoja suunniteltaessa on myös huomioitava, että käsittelyn oikeusperuste vaikuttaa jonkin verran siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeus siirtää tiedot järjestelmästä toiseen ja vastustamisoikeus liittyvät vain osaan käsittelyperusteista. Osana henkilötietojen käsittelytoimintojen suunnittelua rekisterinpitäjän tulisi selvittää, mitä rekisteröidyn oikeuksia käytössä oleviin käsittelyn perusteisiin liittyy ja miten rekisteröityjen oikeuksien toteuttaminen käytännössä toteutetaan.

Rekisteröityjen tietopyyntöprosessi

Suonenjoen kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Ohje on nimeltään ”**Rekisteröidyn oikeudet**” ja se löytyy Intranetistä Tietoturva ja Tietosuoja-sivuilta. Tämän prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

Henkilötietojen käsittelyn läpinäkyvyys

Suonenjoen kaupunki informoi rekisteröityä henkilötietojen käsittelystä kerätessään henkilötietoja sekä julkaisemalla kaupungin internet-sivuilla tietoa henkilötietojen käsittelytoimenpiteistä.

Henkilötietojen käsittelijä = ulkopuolinen toimija

Hankinnoissa ja sopimuksissa, joissa välittömästi tai välillisesti on kyse henkilötietojen käsittelystä, on huomioitava tietosuoja-asetuksen edellytykset sopimuksille. Henkilötietojen käsittelijällä tarkoitetaan kaupungin ulkopuolista tahoa, sopimuskumppania, joka käsittelee kaupungin henkilötietoja rekisterinpitäjän lukuun, esimerkkinä ostopalvelut ja tietojärjestelmätoimittajat. Vastuu henkilötietojen asianmukaisesta käsittelystä ei siirry palveluntuottajalle, vaan se säilyy rekisterinpitäjällä. Rekisterinpitäjä on juridisessa vastuussa rekisteristä ja määrää rekisterin käytöstä.

Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä. Sopimuskumppaniksi valitaan vain sellaisia toimijoita, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Henkilötietojen käsittelijän vastuu määritetään kirjallisella sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään. Sopimuksessa on määriteltävä vähintään käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. Tarkemmat ohjeet löytyvät ”**Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohjeesta”**.

Tietoturva

Tietoturvallisuudella tarkoitetaan tiedon, tietojärjestelmien ja tietoliikenteen suojaamista niin, että minimoidaan tietoihin, toimintaan ja palveluihin liittyvät riskit. Tietoturva koostuu tiedon käytettävyydestä, eheydestä, luottamuksellisuudesta, saatavuudesta, kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvan peruskäsitteet ovat:

- Tietojen eheys: Tieto on oikeaa ja eheää. Tietoja ei voi tahallisesti tai tahattomasti muuttaa.
- Tietojen luottamuksellisuus: Tieto on vain sen käyttöön oikeutettujen saatavilla ja suojattu muulta käytöltä, esimerkiksi käyttöoikeudet
- Käytettävyys: Tieto on saatavilla aina sitä tarvittaessa.
- Lisäksi tietoon käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan, esimerkiksi lokitiedostot

Tärkeät toiminnot pyritään suojaamaan kaikissa häiriötilanteissa varmistaen palveluiden käytettävyys mahdollisimman lyhyellä toipumisajalla.

”**Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohje**” kuvaa ja ohjeistaa sen, miten tehtävät käytännössä hoidetaan tietoturva-asiat huomioiden.

Toiminta häiriötilanteissa ja ilmoitusvelvollisuus

Henkilötietojen käsittelyn häiriötilanteella, eli tietoturvaloukkauksella, tarkoitetaan tilannetta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi jokin ylimääräinen taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkauksissa, tai epäiltäessä

tietoturvaloukkausta, noudatetaan ”**Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohjeessa**” kuvattua toimintaprosessia. Ohje löytyy intran tietosuoja- ja tietoturva sivustolta.

Henkilötietojen tietoturvaloukkauksen sattuessa tietosuojavastaava tekee asetuksen mukaiset ilmoitukset valvontaviranomaisen sekä rekisteröidyn suuntaan.

Tietosuojan ja tietoturvan raportointi

Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain raportoinnilla johdolle, ”**Tietotilinpäätös**”. Tietosuojan osalta raportissa selvitetään miten tietosuojaperiaatteita, rekisterinpitäjän velvollisuuksia ja rekisteröidyn oikeuksia on noudatettu. Tietoturvan osalta selvitetään miten tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta on huolehdittu. Arvioinnin tavoite on varmistaa palveluiden jatkuvuus ja toiminnan laatu.

Organisaatio ja vastuut

Tietosuoja- ja tietoturvatyö ovat osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietosuojan ja tietoturvan ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä vastuuhenkilöitä. Kaupungilla on nimettynä tietoturvavastaava, tietosuojavastaava sekä sosiaalipalveluiden tietosuojavastaava. Kaupunginjohtaja perustaa ja nimittää kaupungin tietosuoja- ja tietoturvatyöryhmän.

Rooli	**Vastuu**
Kaupunginhallitus	Hyväksyy tietosuoja- ja tietoturvapolitiikan ja tietotilinpäätöksen
Kaupunginjohtaja	Perustaa ja nimeää tietosuoja ja -turvaryhmän
Hallintojohtaja	Valmistelee ja ylläpitää tietosuoja- ja tietoturvapolitiikkaa Ohjeistaa ja koordinoi koko kaupungin tietosuoja- ja tietoturvatyötä Johtaa tietosuoja- ja tietoturvaryhmää Suunnittelee tietosuoja- ja tietoturva koulutuksen yhdessä tietosuoja- ja tietoturvaryhmän kanssa
ICT-palvelut	Järjestää ICT-palvelut ja avustaa riskienhallinnassa ja tietoturvan teknisissä ratkaisussa
Tietosuoja- / tietoturvaryhmä	Määrittää tietosuoja ja –turvaratkaisuja sekä ohjeistaa toimialoja Suunnittelee, organisoi ja seuraa tietosuojakoulutuksia Jäsenet toimivat yhdyshenkilöinä toimialoilleen
Tietosuojavastaava	Seuraa tietosuoja-asetuksen noudattamista Valvoo organisaation järjestelmien tietosuojan toteutumista Osallistuu riskienarviointien ja tarvittaessa vaikutustenarviointien tekemiseen Osallistuu tietosuojaperiaatteiden määrittelyyn Raportoi ylimmälle johdolle tietosuojan tilasta Neuvoo ja opastaa tietosuoja-asioissa Käsittelee tietosuojapuutteet ja poikkeamat sekä poikkeustilanteet Tekee yhteistyötä valvontaviranomaisen kanssa Vastaa järjestelmistä kerättävien/muodostuvien lokitiedostojen hallinnasta
Tietoturvavastaava	Valvoo organisaation järjestelmien tietoturvan toteutumista Koordinoi poikkeustilanteet Raportoi ylimmälle johdolle tietoturvan tilasta Kehittää ja valmistelee tietoturvaohjeet ja -käytäntöjä

	Avustaa johtoa ja yksiköitä tietoturva-asioiden toimeenpanossa Osallistuu tietoturvaperiaatteiden määrittelyyn Käynnistää tietoturvapuutteiden ja poikkeamien käsittelyn Vastaa järjestelmistä kerättävien/muodostuvien lokitiedostojen hallinnasta
Henkilötietojen käsittelijä (ulkoistettu)	Käsittelee henkilötietoja huolellisesti kaupungin lukuun kirjallisen sopimuksen ja rekisterinpitäjän ohjeiden mukaisesti.
Toimialajohtajat	Hallitsee oman toimialansa tietosuojan ja tietoturvan erityispiirteet ja lainsäädännön, ja Vastaa näiden pohjalta annetuista tarkennetuista ohjeista Tietoturva- ja tietosuoja-asioiden johtaminen, resursointi ja valvonta Huolehtii tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsyn-valvonnasta Huomioi tietosuojan ja tietoturvan hankinnoissa ja sopimuksissa Varmistaa tietosuojaan ja tietoturvaan tarvittavan osaamisen henkilöstölle Nimeää jäsenen tietosuoja- ja tietoturvaryhmään Toteuttaa riskiarvioinnit ja tarvittaessa vaikutustenarvioinnit sekä suunnittelee toiminnan häiriötilanteissa yhdessä tietosuojavastaavien ja ICT-palveluiden kanssa Nimeää pääkäyttäjät vastuulla olevien järjestelmien osalta Määrittää rekisterin vastuuhenkilöt Huolehtii raportointiin tarvittavien tietojen tuottamisesta
Esimies	Huolehtii henkilöstönsä riittävästä perehdytyksestä ohjeisiin Vastaa yksikkönsä osalta tietosuojan ja tietoturvan toteutumisesta Hakee käyttöoikeudet ja ilmoittaa niiden poistamisesta pääkäyttäjille Huolehtii, että henkilöstöllä on riittävä tietosuoja/-turva osaaminen Raportoi välittömästi havaituista poikkeamista tietosuojavastaavalle
Työntekijän/viranhaltijan vastuut	Noudattaa tietosuoja- ja tietoturvaohjeistusta Käsittelee henkilötietoja vain sovitussa käyttötarkoituksessa Raportoi välittömästi havaituista poikkeamista tietosuojavastaavalle

Dokumentointi

Tietosuoja-asetuksen mukaan rekisterinpitäjän on pystyttävä osoittamaan, että tietosuojaperiaatteita noudatetaan. Suonenjoen kaupungissa tietosuojan ja –turvan toteutuminen varmistetaan seuraavilla asiakirjoilla:

- Tietosuoja- ja tietoturvapolitiikka
- Suonenjoen kaupungin henkilöstön tietosuoja ja –turvaohje
- Toimiala- /palvelukohtaiset ohjeistukset
- Rekisteriselosteet (tietojärjestelmät)
- Selosteet henkilötietojen käsittelytoimista
- Tietosuojaselosteet
- Riskienarvioinnit, ja mahdolliset vaikutustenarvioinnit
- Rekisteröidyn oikeudet
- Tietotilinpäätös