

# Tiedonhallinta- politiikka

KH 26.1.2026



## Sisällys

1 Tiedonhallintapolitiikka .....	3
1.1 Tiedonhallintapolitiikan tarkoitus ja soveltamisala .....	3
1.2 Tiedonhallintaa ohjaava sääntely .....	3
2 Tiedonhallinta .....	4
2.1 Tiedonhallinnan periaatteet ja tavoitteet .....	4
2.2 Asianhallinta ja palvelujen tiedonhallinta .....	4
2.2.1 Asianhallinta .....	5
2.2.2 Palvelujen tiedonhallinta .....	5
2.3 Säilytys ja arkistointi .....	6
3 Tiedon suojaaminen .....	7
3.1 Tietoturva .....	7
3.2 Tietosuoja .....	9
3.3 Tietoturva ja tietosuoja hankinnoissa .....	10
3.4 Lokitietojen käsittely .....	11
3.4 Salassapito, vaitiolovelvollisuus ja hyväksikäyttökielto .....	12
3.5 Toiminta häiriötilanteissa .....	13
4 Tiedonhallinnan roolit ja vastuut .....	13
4.1 Kaupunginhallituksen vastuu .....	14
4.2 Toimielinten vastuut .....	14
4.3 Hallintojohtajan vastuu .....	15
4.4 Toimialajohtajan vastuu .....	15
4.5 Toimistopäällikkö .....	16
4.6 Asiakirjahallinnon vastuuhenkilö .....	16
4.7 Tietoturvavastaava .....	16
4.8 Tietosuojavastaava .....	17

4.9 Esihenkilöt .....	18
4.10 Henkilöstö ja luottamushenkilöt .....	18
4.11 Tiedonhallintaryhmä .....	18
4.12 Asianhallintatiimi .....	19
4.13 Henkilötietojen käsittelijä (ulkoistettu) .....	19
<b>5 Tiedonhallinnan kuvaukset ja toteutus .....</b>	<b>19</b>
5.1 Tiedonhallintamalli .....	19
5.2 Tiedonhallinnan muutosvaikutusten arviointi .....	20
5.3 Asiakirjajulkisuuskuvaus .....	21
5.4 Tiedonohjaussuunnitelma .....	21
5.5 Tietotilinpäätös .....	21
5.6 Tietosuojan riski- ja vaikutustenarvioinnit .....	22
5.7 Tietosuojaselosteet .....	22
5.8 Henkilötietojen tietoturvaloukkauseilmoitus .....	22
5.9 Tekoälyn eettiset periaatteet .....	23

# 1 Tiedonhallintapolitiikka

## 1.1 Tiedonhallintapolitiikan tarkoitus ja soveltamisala

Suonenjoen kaupunginhallitus vastaa siitä, että tiedonhallintalain mukaiset vastuut, käytännöt ja valvonta on määritelty kunnassa. Tiedonhallintapolitiikka tarkoittaa Suonenjoen kaupungin hallintosäännön määräyksiä tiedonhallinnan toteuttamiseen liittyen. Poliitiikka määrittelee ne periaatteet, tavoitteet, toimintatavat, vastuut ja valvonnan, joita noudatetaan Suonenjoen kaupungin tiedonhallinnan, sekä tietoturvan ja tietosuojan, toteuttamisessa ja kehittämisessä.

Tiedonhallintapolitiikka kattaa Suonenjoen kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta. Se toimii kaupungin tiedonhallinnan perustana ja sitä voidaan täsmentää erillisillä ohjeilla.

Tiedonhallintapolitiikka koskee koko Suonenjoen kaupunkia ja sen henkilöstöä sekä konserniyhteisöjä niiltä osin, kun ne toimivat kunnan lakisääteisten tehtävien piirissä. Myös ulkopuolisten toimijoiden ja toimittajien tulee sitoutua Suonenjoen kaupungin tiedonhallintapolitiikkaan. Tarkoitus on, että tietosuoja- ja tietoturva-ajattelu on osa jokaisen päivittäistä työskentelyä.

## 1.2 Tiedonhallintaa ohjaava sääntely

Kansallinen lainsäädäntö asettaa kunnalle raamit turvalliseen tiedon käsittelyyn. Lainsäädännön lisäksi on noudatettava kunnan hallintosäännön määräyksiä, Kansallisarkiston antamia ohjeita ja määräyksiä, kuntaliiton suosituksia ja ohjeita sekä kunnan omia asiakirjojen käsittelyyn liittyviä ohjeita ja neuvoja.

- Tiedonhallintalaki: valtakunnalliset periaatteet viranomaisten tietojen käsittelyyn ja tiedonhallinnan kuvaamiseen
- Julkisuuslaki: salassapito ja tiedonsaantioikeus viranomaisen asiakirjoihin
- Hallintolaki: hallintoasioiden käsittely ja hyvä hallinto
- Arkistolaki: arkistointiin ja arkistoitujen aineistojen säilyvyyden turvaamiseen liittyvät velvoitteet
- Digipalvelulaki: digitaalisten palvelujen järjestäminen, tarjoaminen ja saavutettavuus
- Laki sähköisestä asioinnista viranomaistoiminnassa: sähköisen asioinnin menettelyt
- EU:n yleinen tietosuoja-asetus ja tietosuojalaki: henkilötietojen käsittely ja suojaus

Lisäksi on noudatettava muita mahdollisia toimialakohtaisia erityislainsäädäntöjä.

## 2 Tiedonhallinta

### 2.1 Tiedonhallinnan periaatteet ja tavoitteet

Suonenjoen kaupunki järjestää asukkailleen sekä lakisääteisiä että itsehallintonsa mukaisesti ottamiaan palveluja. Toiminnan monimuotoisuuden myötä myös kaupungin käsittelemä tieto on hyvin vaihtelevaa ja vaatii monenlaista käsittelyä erilaisissa järjestelmissä. Tiedonhallinnan tarkoitus on varmistaa sekä digitaalisessa että analogisessa muodossa olevien tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely. Tieto on pystyttävä hallitsemaan koko sen elinkaaren ajan, tiedon synnystä tiedon tuhoamiseen tai arkistointiin. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

*Tiedon elinkaari*



Tiedon on pystyttävä tukemaan kaupungin toimintaa ja päätöksentekoa sekä julkisuusperiaatteen toteuttamista. Oikein toteutettuna tiedonhallinta, mukaan lukien tietosuoja ja tietoturva, mahdollistavat muodostetun ja kerätyn tiedon aikaisempaa tehokkaamman hyödyntämisen ja kustannussäästöt. Organisaation jokaisella henkilöllä tulee olla yleiskuva organisaation tiedonhallinnan sekä tietoturvan ja tietosuojan periaatteista, keskeisistä prosesseista, rooleista ja vastuista.

### 2.2 Asianhallinta ja palvelujen tiedonhallinta

Kaikki viranomaisen asiakirjat on voitava antaa niihin oikeutetulle vaivattomasti, myös ne, jotka syntyvät palveluja tuottaessa asiakäsittelyprosessin ulkopuolella. Asiakirja voi olla paperimuotoinen, sähköinen tai muuta vastaavaa informaatiota sisältävä. Tiedonhallintalaki rajaa asiakirjan käsitteen viranomaisten toiminnan julkisuudesta annetun lain 5 §:n tarkoitettuun asiakirjaan.

Viranomaisen on pystyttävä tunnistamaan, mitkä tiedonhallintayksikön asiakirjat syntyvät asiakäsittelyssä ja mitkä palveluissa:

- Sellaiset asiat, joissa tehdään ratkaisu, esimerkiksi päätös tai lupa, kuuluvat asiakäsittelyyn

- Palvelu tuotetaan ilman asiankäsittelyprosessia, eikä siihen liity hallinnollisia päätöksiä tai muutoksenhakua. Palvelujen asiakirjat tuotetaan palveluntuottajan ja asiakkaan välisessä asioinnissa tai sisäisessä palvelussa jonkin tehtävän suorittamiseksi.

## 2.2.1 Asianhallinta

Tiedonhallintalain mukaan tiedonhallintayksikön (Suonenjoen kaupunki) on ylläpidettävä viranomaisen käsittelyssä olevista ja olleista asioista asiarekisteriä, johon viipymättä rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Edellä mainittujen tietojen lisäksi asiarekisteriin on kirjattava metatietoja, joiden vähimmäisvaatimuksista säädetään myös tiedonhallintalaissa. Kyseisiä metatietoja ovat esimerkiksi asiakirjan saapumistapa ja -ajankohta.

Asiarekisteriä ylläpidetään asianhallintajärjestelmässä. Huomioitavaa on, että asiaa voidaan käsitellä myös asianhallintajärjestelmän ulkopuolella operatiivisissa järjestelmissä. Tällöin kyseisten käsittelyvaiheiden tiedot olisi oltava myös löydettävissä asiarekisteristä asiankäsittelyn kulkua kuvaavina tietoina.

Viranomaisen asioiden rekisteröimisen tarkoituksena on tukea viranomaisen toiminnan avoimuutta, kansalaisten tiedonsaantia ja vaikuttamismahdollisuuksia. Hyvään hallintoon kuuluu myös, että asiankäsittelyn on oltava joutuisaa, seurattavissa ja todennettavissa. Asianhallintajärjestelmässä asioiden luokittelua tehdään kaupungin tiedonohjaussuunnitelman mukaisesti.

## 2.2.2 Palvelujen tiedonhallinta

Palvelujen tiedonhallinta -käsite tiedonhallintalaissa kohdistuu siihen tietoaaineistoon, joka jää tiedonhallintayksikön asiarekisterin eli asianhallinnan ulkopuolelle. Palvelujen tiedonhallinta tapahtuu pääosin kunnan operatiivisissa tietojärjestelmissä. Tiedonhallintaa jäsennetään ja tuetaan tiedonhallintamallilla.

Suonenjoen kaupunki tuottaa suuren määrän erilaisia palveluja, joten syntyvien asiakirjojenkin määrä on suuri. Tiedonhallintalain mukaan myös tämän tietoaaineiston hallinta on järjestettävä siten, että asiakirjojen ja muiden tietojen muodostuminen palvelua tuottaessa voidaan jälkikäteen todentaa. Lisäksi tavoitteena on, että tietoaaineistosta muodostettavat asiakirjat ovat haettavissa jollakin tietokokonaisuudet yksilöivällä tunnukseksi, jotta tiedot voidaan antaa siihen oikeutetulle vaivattomasti.

Jokaisen palvelualueen tulee tunnistaa, mitä tietoaineistoja palvelussa kertyy. Samoin kuin asiakäsittelyn yhteydessä, myös palveluja tuottaessa muodostuvien asiakirjojen tuottamista, vastaanottamista, säilyttämistä, käyttöä, hävittämistä ja arkistointia on valvottava.

## 2.3 Säilytys ja arkistointi

### Säilytys

Tiedonhallintalaissa tietoaineistojen säilyttämisaikojalla tarkoitetaan tietoaineistojen säilyttämistä niin kauan kuin niitä tarvitaan alkuperäisiin käyttötarkoituksiin sekä oikeusturvan toteuttamiseksi ja virkavastuun todentamiseksi. Jos tietoaineistojen tai asiakirjojen säilytysajasta ei ole säädetty laissa, säilytysaikoja määritettäessä on otettava huomioon:

- tietoaineiston alkuperäisen käyttötarkoituksen mukainen tarpeellisuus viranomaisen toiminnassa;
- luonnollisen henkilön tai oikeushenkilön etujen, oikeuksien, velvollisuuksien ja oikeusturvan toteuttaminen ja todentaminen;
- sopimuksen tai muun yksityisoikeudellisen oikeustoimen oikeusvaikutus;
- vahingonkorvaus- sekä rikosoikeudelliset vanhentumisajat.

Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvalisella tavalla. Säilytysajat on kuvattu Suonenjoen kaupungin tiedonohjaussuunnitelmaan (TOS).

Tiedonohjaussuunnitelma muodostaa arkistolain säättämän arkistonmuodostussuunnitelman sekä analogisille että sähköisille aineistoille, ja se on integroitu asianhallintajärjestelmään.

### Arkistointi

Arkistointivaiheessa aineiston käyttö on etupäässä tutkimuskäyttöä. Tietoaineistoa ei enää arkistoinnin jälkeen käsitellä alkuperäiseen käyttötarkoitukseensa. Arkistoinnista eli arkistotoimen järjestämisestä säädetään arkistolaissa. Suonenjoen kaupunki vastaa sen toiminnassa syntyvien ja Kansallisarkiston pysyvään säilytykseen määrittämien asiakirjatietojen arkistoinnista. Arkistoon sisältyy vanha paperiarkisto, sekä jatkuvasti kertyvä digitaalinen aineisto. Vaikka sähköinen arkistointi on "tämän päivän" ensisijainen tapa arkistoida, on edelleen huolehdittava myös analogisen paperiarkiston osalta sen aineiston käytettävyydestä ja säilyvyydestä.

## 3 Tiedon suojaaminen

Tietojen digitalisoituessa ja käsiteltävän tietomäärän lisääntyessä, edellytetään tietosuojaja- ja tietoturvaajattelun ottamista osaksi jokaisen viranhaltijan, työntekijän sekä luottamushenkilön päivittäistä työskentelyä. Tietosuojaja muodostuu säännöistä ja periaatteista, ja tietoturva on keinoja (työkaluja) näiden sääntöjen noudattamiseen. Myös ulkopuolisten toimijoiden ja toimittajien tulee sitoutua tietoturvan ja tietosuojan huomioimiseen toiminnassaan. Tietosuojasta ja -turvan käytännön toteuttamisesta on laadittu erillinen ohje.

Tietoaineistot sisältyvät pääasiassa tietojärjestelmiin, joissa niitä myös käsitellään, jonka vuoksi tietojärjestelmien hallinta on osa tiedonhallintaa. Tietojärjestelmien ja niihin sisältyvien tietoaineistojen tietoturvallisuuden varmistaminen kuuluu olennaisena osana tiedonhallintaan, jonka lisäksi analogisessa muodossa olevien tietoaineistojen turvallisuudesta on huolehdittava.

Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Suonenjoen kaupungilla on kaupunginhallituksen nimeämät tietosuojavastaava sekä tietoturvavastaava, joiden tehtävänä on seurata ja arvioida sekä kehittää ja ohjeistaa tietosuojaan ja tietoturvaan liittyvissä asioissa. Tavoitteena on turvata tiedon turvallinen käsittely ja rekisteröityjen oikeuksien toteutuminen.

Asiakkaiden, työntekijöiden ja yhteistyökumppanien tulee voida luottaa siihen, että heidän tietojensa käsitellään turvallisesti ja vastuullisesti.

### 3.1 Tietoturva

Tietoturva on olennainen osa tiedonhallintaa. Tietoturvallisuus on laaja käsite, josta usein käytetään myös termejä digiturvallisuus tai kyberturvallisuus. Koska kokonaisuuteen sisältyy muitakin kuin digitaalisia asioita, esim. toimitilaturvallisuus, paperisten asiakirjojen säilytys ja henkilöstön koulutus, tässä dokumentissa käytetään termiä tietoturva. Tiedonhallintalain mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tietoturva tarkoittaa hallinnollisia, toiminnallisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus. Tietoturvalla tähdätään jatkuvuuden varmistamiseen ja tietoihin liittyvien riskien minimoimiseen.

- Luottamuksellisuus – Tiedot ovat vain oikeutettujen henkilöiden käytettävissä.
- Eheys – Tiedon on oltava oikeaa, ajantasaista, muuttumatonta ja suojattu teknisiltä ja fyysisiltä vahingoilta.
- Saatavuus – Tiedon on oltava käyttökelpoisessa muodossa ja saatavilla. Saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu.

Tietojärjestelmien käyttöoikeudet on määriteltävä siten, että ne perustuvat käyttäjien tehtäviin liittyviin käyttötarpeisiin. Käyttöoikeudet on pidettävä ajan tasalla. Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen avulla voidaan selvittää myös henkilötietojen väärinkäyttöä.

Suonenjoen kaupungin on seurattava jatkuvasti toimintaympäristön tietoturvallisuuden tilaa ja varmistettava tietoaaineistojen ja tietojärjestelmien tietoturvallisuus. Tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojen käsittely on suunniteltava siten, että asiakirjojen julkisuus ja salassapito voidaan vaivatta toteuttaa. Tiedonhallintalain mukaisesti tietojenkäsittelyyn kohdistuvat riskit on selvitettävä ja mitoitettava tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti.

Varmistukset suojaavat tiedon saatavuuden ja käytännön työnteon. Suonenjoen kaupunki huolehtii itsellä ylläpidettyjen järjestelmien varmuuskopioinnista järjestelmien kriittisyyden mukaan ja ulkoistetut palvelujen tuottajat vastaavat omien palveluidensa varmistuksesta.

Yksi tärkeimmistä tietoturvallisuuden osa-alueista on henkilöstön osaaminen. Tiedonhallintalain mukaan tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on ajantasaiset ohjeet tietoaaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvaluustoimenpiteistä sekä poikkeusoloihin varautumisesta. Tarjolla on oltava koulutusta ajantasaisista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista. Käyttäjien pitää osata toimia oikein käsitellessään tietoa ja lisäksi heidän pitää osata käyttää tietojärjestelmiä turvallisesti. Koska toimintaympäristö ja järjestelmät muuttuvat jatkuvasti, tulee myös koulutuksen olla jatkuvaa ja kaupungin on varmistettava henkilöstönsä osaaminen koulutuksella.

Kriittiset toiminnot ja palvelut (=ydintoiminta) on tunnistettava ja niiden jatkuvuus on pystyttävä turvaamaan normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa.

Varautumistoimenpiteitä ovat esimerkiksi koulutus, harjoitukset ja riskien arviointi. On myös

huolehdittava, että toiminnan kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys testataan riittävän säännöllisesti.

Salassa pidettävien tietojen siirto yleisessä tietoverkossa tulee toteuttaa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä. Salassa pidettävien tietojen vastaanottaja on myös varmistettava tai tunnistettava riittävän tietoturvallisesti ennen kuin tämä pääsee käsittelemään kyseisiä tietoja.

Tietoturvyössä täytyy aina muistaa tarkoituksenmukaisuus ja oikein mitoitettujen toimenpiteiden.

Täydellisen tietoturvan tavoitteluun saa uppoamaan lähes loputtomasti rahaa. Tietoturvatyötoimenpiteet suhteutetaan riskiarviointien avulla käytettävissä oleviin resursseihin.

## 3.2 Tietosuojaja

Tietoaineistoissa olevat tiedot sisältävät usein henkilötietoja. Tietosuojaja on perusoikeus, jolla taataan oikeus henkilötietojen suojaan ja lainmukaiseen käsittelyyn. Tietosuojasta säädetään tietosuojalain asetuksessa, tietosuojalain ja erityislainsäädännössä.

**Henkilötiedoilla** tarkoitetaan kaikkia sellaisia tietoja, joilla henkilö voidaan suoraan tai epäsuorasti tunnistaa ja yksilöidä. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

**Henkilötietojen käsittelyä** ovat kaikki toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Esimerkiksi henkilötietojen tallennus, muokkaus, säilytys, luovuttaminen, poistaminen. Henkilötietoja käsiteltäessä, on aina otettava huomioon tietosuojan periaatteet, joista keskeisimmät ovat:

- Lainmukaisuus ja läpinäkyvyys: Henkilötietojen käsittelyssä on noudatettava selkeitä sääntöjä ja informoitava rekisteröityjä.
- Tietojen minimointi: Vain tarpeellisia tietoja saa kerätä ja käsitellä.
- Oikeusperusteisuus: Tietojen käsittelylle on oltava laillinen peruste.
- Riskiperusteinen lähestymistapa: Organisaatioiden on arvioitava käsittelyyn liittyvät riskit ja toteutettava suojatoimet niiden mukaisesti.

Henkilötietoja käsiteltäessä on aina toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan tietosuojan toteutuminen. Teknisiä toimenpiteitä ovat sovellusten, järjestelmien ja palveluiden tietoturvamäärittelyt, tietojen salauksen tekniset määrittelyt, monivaiheinen tunnistautuminen ja muut tietoturvatyömenpiteet. Organisatorisia toimenpiteitä ovat henkilötietojen käsittelyä koskevat ohjeet, käyttövaltuushallinta, käytönvalvonta, hankinta- ja sopimusmenettelyjen noudattaminen, henkilötietojen tietoturvaloukkausprosessin noudattaminen.

Suonenjoen kaupungin rekisterinpitäjiä ovat kaupunginhallitus sekä lautakunnat. Rekisterinpitäjä määrittää tehtävien hoidon säännösten ja määräysten mukaisesti. Rekisterinpitäjällä on ylin vastuu tietosuojan toteuttamiseen liittyen. Se vastaa osaltaan rekisterissään olevista henkilötiedoista ja niiden käsittelyn suunnittelusta ja toteutuksesta. Huomioitavaa on, että vastuu henkilötietojen asianmukaisesta käsittelystä ei siirry esimerkiksi palveluntuottajalle, vaan se säilyy rekisterinpitäjällä. Rekisterinpitäjä on juridisessa vastuussa rekisteristä ja määrää rekisterin käytöstä. Tässä tapauksessa sopimuskumppani on vain *henkilötietojen käsittelijä*, joka käsittelee kaupungin henkilötietoja rekisterinpitäjän lukuun, esimerkkinä ostopalvelut ja tietojärjestelmätoimittajat.

Rekisteröidyllä, eli henkilötietojensa käsittelyn kohteella, on aina oikeus tutustua niihin tietoihin, joita hänestä on kerätty. Tarvittaessa hän voi myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen. Rekisteröidyn oikeudet määräytyvät sen mukaan, mikä on henkilötietojen käsittelyn peruste. Rekisteröidyn oikeudet on kuvattu kaupungin ylläpitämässä ”Tietosuojaselosteissa”, jotka julkaistaan kaupungin verkkosivuilla.

### 3.3 Tietoturva ja tietosuoja hankinnoissa

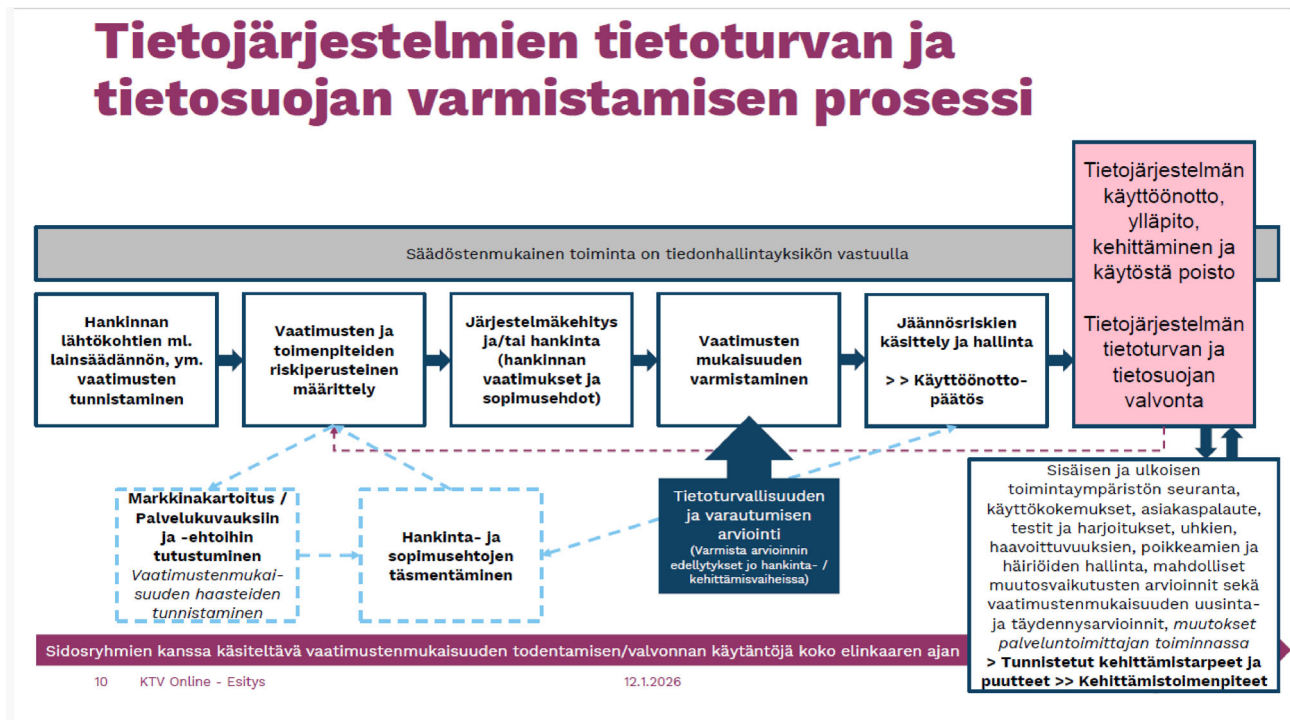
Tiedonhallintalain mukaan viranomaisen on varmistettava hankinnoissaan, että hankintaan liittyen on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Tietosuoja-asetuksen mukaan organisaatiot saavat käyttää vain sellaisia henkilötietojen käsittelyä suorittavia toimittajia, jotka voivat antaa riittävät takeet siitä, että lainsäädäntöä noudatetaan ja kaikkien oikeudet on huomioitu.

Hankinnoissa ja sopimuksissa, joissa käsitellään henkilötietoja, on huomioitava tietosuoja-asetuksen edellytykset sopimuksille. 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.

Lähes kaikkien palvelu- ja järjestelmähankintojen kohdalla tapahtuu henkilötietojen käsittelyä. Henkilötietoja joko siirretään suoraan palvelutoimittajalle käsiteltäviksi tai sitten palvelua tuotettaessa toinen osapuoli saa pääsyn organisaation henkilötietoihin. Järjestelmätoimituksissa – etenkin pilvipalveluissa – on lähes väistämätöntä, että henkilötiedot annetaan toiselle organisaatiolle ylläpidettäväksi ja säilytettäväksi.

Toimittajalta tulee vaatia tiettyä tietoturvasoaa sekä ymmärrystä tietosuojan merkityksestä. Hankinnan vaikutukset henkilötietojen käsittelytoiminnan riskeihin on aina arvioitava. Tarvittaessa tehdään vaikutustenarviointi.

Suonenjoen kaupungilla on erillinen ”Suonenjoen kaupungin hankintastrategia ja -ohjeet” dokumentti, jota kuuluu noudattaa kaikissa hankinnoissa.



### 3.4 Lokitietojen käsittely

Tiedonhallintalain mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen avulla pystytään havaitsemaan mahdollisia tietomurtoja ja selvittämään tapahtumien kulkua jälkikäteen.

Loki voi sisältää myös henkilötietoja, jolloin niiden käsittelyssä on noudatettava EU:n tietosuojasetusta. Asetuksen mukaan henkilötietojen on oltava rajoitettuja suhteessa niihin käyttötarkoituksiin, joita varten niitä käsitellään. Järjestelmän sisältämistä henkilötiedoista on laadittava tietosuojaseloste. Liian yksityiskohtainen tapahtumaseuranta yhdistettynä henkilöiden identiteetteihin saattaa rikkoa yksilön tietosuojaa.

Suonenjoen kaupunki kerää lokitietoja useimmista tietojärjestelmistään. Lokitietojen keräys, säilytysaika ja muut niitä koskevat tiedot dokumentoidaan asianmukaisesti.

Lokitietoja tarkastetaan säännöllisesti rutiinitarkastuksissa sekä tarpeen mukaan. Tarkastukset tekee tiedonhallintaryhmä yhdessä järjestelmän pääkäyttäjän ja/tai vastuuyksikön esihenkilön kanssa. Pistotarkastettavat järjestelmät valitaan satunnaisesti tai esimerkiksi järjestelmän tärkeyden, arvioitujen riskien ja aiempien tarkistusten perusteella. Tarkastuksista tehdään tarkastusraportti. Lokitietojen seurannasta raportoidaan kaupungin johdolle.

## 3.4 Salassapito, vaitiolovelvollisuus ja hyväksikäyttökielto

Julkisuuslaissa säädetään salassapitovelvoitteesta, joka sisältää salassapitovelvollisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon. Tiedonhallintalain mukaisesti kaupungin on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.

- **Salassapitovelvollisuus** tarkoittaa kieltoa näyttää tai luovuttaa sivulliselle salassa pidettävää asiakirjaa tai sen kopiota tai tulostetta tai antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi. Näyttämisellä ei tarkoiteta pelkästään aktiivista asiakirjan näyttämistä. Sivullisella tarkoitetaan jokaista, jonka tehtäviin asian käsittely ei kuulu. Asiakirjan salassapitovelvollisuus edellyttää huolehtimista myös siitä, ettei sivullinen pääse näkemään salassa pidettäviä asiakirjoja. Salassapitovelvollisuus sisältää myös velvollisuuden pitää salassa se, että salassa pidettävä asiakirja on olemassa, jos pelkkä tieto asiakirjan olemassaolosta voi paljastaa salassa pidettävän seikan.
- **Vaitiolovelvollisuus** tarkoittaa kieltoa paljastaa asiakirjan tai tiedon sisällöstä kertomalla siitä sivulliselle. Vaitiolovelvollisuus koskee myös sellaista tallettamatonta tai kirjoittamatonta tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä. Vaitiolovelvollisuuden säilyttämiseksi on kiinnitettävä huomiota myös siihen, etteivät sivulliset tahattomastikaan pääse tai joudu kuulemaan salassapidettäviä asioita. Tietosuojalaissa säädetään henkilötietojen käsittelyyn

liittyvästä vaitiolovelvollisuudesta. Säännöksen mukaan joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta taikka toisen liikesalaisuudesta, ei saa oikeudettomasti ilmaista sivulliselle näin saamiaan tietoja eikä käyttää niitä omaksi tai toisen hyödyksi tai toisen vahingoksi.

- **Hyväksikäyttökielto** tarkoittaa kieltoa käyttää salassa pidettäviä tietoja omaksi tai toisen hyödyksi tai toisen vahingoksi. Tietoja ei saa käyttää, vaikka käyttö ei johtaisikaan siihen, että salassa pidettävä tieto samalla paljastuu ulkopuoliselle.

## 3.5 Toiminta häiriötilanteissa

Suonenjoen kaupungin toiminta kriisitilanteissa perustuu valmiuslain (1552/2011) mukaiseen valmiussuunnitteluun. Toimialat ja konserniyhtiöt laativat kukin valmiussuunnitelman omalta osaltaan. Suunnittelussa tulee varautua pieneen, keskisuureen ja suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Koska tietotekniikka on nykyään tärkeä osa lähes kaikkea toimintaa, tulee jokaisen vastualueen ottaa valmiussuunnittelussa huomioon toiminta tilanteessa, jossa tietojärjestelmät eivät ole käytettävissä.

Suonenjoen kaupunginvaltuusto hyväksyy kaupunkikonsernia koskevat Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Kaupungin tieto- ja viestintäteknisen infrastruktuurin tai tietojärjestelmien toimintaa, tietoturvaa tai tietosuoja uhkaavissa tilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava kaupungin johdolle. Tietoturva- ja tietosuojarikkomukset käsitellään tapauskohtaisesti. Tietohallinnolla on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite uhkatilanteen vahinkojen minimoimiseksi. Tietohallinto informoi asianosaisia ja kaupungin johtoa suoritetuista toimenpiteistä ja mahdollisista jatkotoimenpiteistä mahdollisimman pian.

## 4 Tiedonhallinnan roolit ja vastuut

Suonenjoen kaupunki on tiedonhallintalaissa tarkoitettu tiedonhallintayksikkö, jonka tehtävänä on järjestää tiedonhallinta lain vaatimusten mukaisesti. Seuraavassa määritelty tiedonhallinnan roolit ja vastuut huomioiden erikseen asiakirjahallinto ja arkisto sekä tietosuoja ja tietoturva.

## 4.1 Kaupunginhallituksen vastuu

Suonenjoen kaupunki on julkisen hallinnon tiedonhallinnasta annetussa laissa tarkoitettu tiedonhallintayksikkö. Suonenjoen kaupunginhallitus toimii hallintosäännön mukaisesti tiedonhallintayksikön johtona, jolla on kokonaisvastuu tiedonhallinnan ja asiakirjahallinnan sekä tietosuoja- ja tietoturvan järjestämisestä. Kaupunginhallitus määrittelee tiedonhallintaan liittyvät vastuut ja huolehtii siitä, että tiedonhallintalain mukaiset vaatimukset täyttyvät tiedonhallinnassa.

Kaupunginhallitus:

- määrää asiakirjahallintoa ja arkistointia johtavan viranhaltijan
- nimeää tietoturva- ja tietosuojavastaavan
- hyväksyy tiedonhallintapolitiikan, tiedonhallintamallin kuvauksen sekä tietotilinpäätöksen
- vastaa sisäisen valvonnan ja riskienhallinnan järjestämisestä

## 4.2 Toimielinten vastuut

Kaupunginvaltuusto, kaupunginhallitus, lautakunnat sekä henkilöstöjaosto vastaavat omalta osaltaan tiedonhallintaan liittyvien tehtävien hoitamisesta, jotka on säädetty kunnallisten viranomaisten vastuulle tiedonhallintalaissa tai muissa tiedonhallintaa koskevissa laeissa.

Toimielimet ovat viranomaisen ominaisuudessaan arkistolaisissa tarkoitettuja arkistonmuodostajia sekä Euroopan unionin yleisessä tietosuoja-asetuksessa tarkoitettuja rekisterinpitäjiä, joiden mukaisesti toimielin vastaa oman toimialansa toiminnasta:

- toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuojasääntelyä
- panee tarvittaessa täytäntöön asianmukaiset tietosuoja koskevat toimintaperiaatteet
- vastaa toimialalla muodostuvien asiakirjojen ja niitä vastaavien tietojen osalta arkistonmuodostajille kuuluvien tehtävien hoitamisesta.

Hallintosäännön mukaisesti:

- lautakunnat huolehtivat toimialan tietoaineistojen ja asiakirjatietojen käsittelyn suunnittelusta ja toteuttamisesta annettujen määräysten ja ohjeiden mukaisesti sekä nimeävät vastuuhenkilön toimialallaan.

## 4.3 Hallintojohtajan vastuu

Hallintojohtaja on kaupunginhallituksen määräämä asiakirjahallintoa ja arkistotointa johtava viranhaltija, joka vastaa kokonaisvaltaisesti tiedonhallinnasta, asiakirjahallinnosta ja arkistoinnista sekä niihin liittyvistä toimista. Hallintosäännön mukaisesti hallintojohtaja:

- vastaa kaupunginhallituksen asiakirjahallinnon viranomaistehtävien valmistelusta ja täytäntöönpanosta
- ohjaa ja kehittää asiakirjahallintoa osana kaupungin tiedonhallintaa
- hyväksyy tiedonkäsittelyn, säilytyksen ja arkistoinnin ohjeistuksen
- hyväksyy kaupungin tiedonohjaussuunnitelmat
- vastaa keskusarkistosta ja pysyvästi säilytettävistä asiakirjatiedoista
- laatii kaupungin asiakirjahallinnon ohjeen ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä
- huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta

Lisäksi hallintojohtaja ohjeistaa ja koordinoi koko kaupungin tietosuoja- ja tietoturvatyötä.

## 4.4 Toimialajohtajan vastuu

Toimialajohtaja vastaa hallintosäännön mukaisesti oman toimialansa toiminnasta sekä johtaa ja kehittää sen toimintaa. Toimialojen tiedonhallinta ja sen soveltaminen sekä asiakirjahallinnon ja arkistotoimen toteuttaminen ja hoitaminen on kunkin toimialan johtavan viranhaltijan vastuulla.

Toimialajohtaja vastaa sisäisen valvonnan toteutumisesta ja riskienhallinnasta toimialueellaan.

Toimialajohtaja:

- johtaa, resursoi ja valvoo tietoturva- ja tietosuoja-asioissa sekä varmistaa tarvittavan osaamisen henkilöstölleen
- seuraa toimintaympäristönsä tietoturvallisuuden tilaa ja varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuuden koko niiden elinkaaren ajan
- hallitsee oman toimialansa erityispiirteet ja -lainsäädännön ja vastaa näiden pohjalta annetuista tarkennetuista ohjeista
- huomioi tietosuojan ja tietoturvan hankinnoissa ja sopimuksissa
- toteuttaa riskiarvioinnit ja tarvittaessa vaikutustenarvioinnit, sekä suunnittelee toiminnan häiriötilanteissa, yhdessä tietosuojavastaavan ja ICT-palveluiden kanssa

- määrittää tietojärjestelmien pääkäyttäjät

## 4.5 Toimistopäällikkö

Toimistopäällikkö vastaa tiedonhallinnan ja asianhallinnan prosesseista ja kehittämisestä.

Toimistopäällikkö:

- ohjeistaa ja neuvoo tiedonhallinnassa
- järjestää tiedonhallinnan tiedonhallintalain mukaisesti
- ylläpitää tiedonhallintaan liittyvää dokumentointia
- ylläpitää ja kehittää kaupunginarkiston toimintaa ja aineistoja
- toteuttaa tiedonhallinnan muutoksenvaikutuksen arviointeja
- toimii asianhallintatiimin tiiminvetäjänä

## 4.6 Asiakirjahallinnon vastuuhenkilö

Asiakirjahallinnon vastaavien henkilöiden tehtävänä on:

- huolehtia kirjattavien asioiden/asiakirjojen diarioinnista
- huolehtia hallussaan olevien asiakirjojen ohjeiden mukaisesta säilyttämisestä ja arkistoinnista siihen asti, kunnes asiakirjat siirretään järjestettyinä kunnan päätearkistoon tai hävitetään
  - siirtää pitkäaikaisesti ja pysyvästi säilytettävät asiakirjat asiamukaisesti järjestettyinä ja luetteloituina päätearkistoon ohjeiden mukaisesti
  - tuhoaa toimialansa asiakirjat säilytysajan päätyttyä
- osallistua tiedonohjaussuunnitelman laatimiseen ja ylläpitoon, sekä valvoa ja ohjata tiedonohjaussuunnitelman noudattamista
- oikeaksi todistaa toimielimen hallinnassa olevista asiakirjoista annettavat otteet ja jäljennökset

## 4.7 Tietoturvavastaava

Tietoturvavastaava seuraa Suonenjoen kaupungin toimintaympäristönsä tietoturvallisuuden tilaa ja varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuuden ja valvoo organisaation järjestelmien tietoturvan toteutumista.

Tietoturvavastaava:

- koordinoi tietoturvan poikkeustilanteet
- raportoi ylimmälle johdolle tietoturvan tilasta
- kehittää ja valmistelee tietoturvaohjeita ja -käytäntöjä
- avustaa johtoa ja yksiköitä tietoturva-asioiden toimeenpanossa
- osallistuu tietoturvaperiaatteiden määrittelyyn
- käynnistää tietoturvapuutteiden ja poikkeamien käsittelyn
- vastaa järjestelmistä kerättävien/muodostuvien lokitiedostojen hallinnasta
- seuraa tietosuoja/-turvakoulutusten suorittamista
- huolehtii, että toiminnan kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys testataan riittävän säännöllisesti
- toteuttaa riskiarviointia tietoturvallisuuden osalta ja mitoittaa tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti
- osallistuu tarvittavaan dokumentointiin tietoturvan osalta

Suonenjoen kaupungin ICT-palvelut avustaa riskienhallinnassa ja tietoturvan teknisissä ratkaisuisissa.

## 4.8 Tietosuojavastaava

Tietosuojavastaavan työtä määrittää ja ohjaa Euroopan unionin yleinen tietosuoja-asetus, jonka 39 artiklassa säädetään tämän tehtävistä.

Tietosuojavastaava:

- seuraa tietosuoja-asetuksen noudattamista – valvoo henkilötietojen käsittelyn ja henkilötietojen suojan toteutumista
- ylläpitää tietosuojaa koskevia ohjeistuksia
- toteuttaa riskienarviointia sekä tarvittaessa vaikutustenarviointia ja kehittää tietosuojaa riskienhallinnan näkökulmasta
- vastaa rekisteröityjen tarkastuspyyntöihin
- osallistuu tietosuojaperiaatteiden määrittelyyn ja raportoi ylimmälle johdolle tietosuojan tilasta
- käsittelee tietosuojapuutteet ja poikkeamat sekä poikkeustilanteet
- tekee yhteistyötä valvontaviranomaisen (tietosuojavaltuutettu) kanssa
- osallistuu lokitietojen hallintaan

- osallistuu dokumentointiin tietosuojan osalta

## 4.9 Esihenkilöt

Esihenkilöt vastaavat yksikkönsä osalta tiedonhallinnan toteutumisesta. He huolehtivat henkilöstönsä riittävästä perehdytyksestä annettuihin ohjeisiin sekä tietoturva- ja tietosuojavastuisiin. Esihenkilö varmistaa, että tietoja käsitellään lainsäädännön mukaisesti. Esihenkilöt huolehtivat, että käyttöoikeudet on määritelty työtehtävien mukaisesti ja ne ovat ajantasaiset.

## 4.10 Henkilöstö ja luottamushenkilöt

Jokaisen työntekijän, viranhaltijan sekä luottamushenkilön on velvollisuus perehtyä ja noudattaa ajantasaista ohjeistusta tietojenkäsittelystä. Lisäksi jokaisen on varmistettava käsittelemänsä tiedon käytettävyyden, oikeellisuuden, suojaamisen ja säilyminen. Henkilötietoja käsitellään vain sovitussa käyttötarkoituksessa ja havaituista poikkeamista on raportoitava tietosuojavastaavalle.

## 4.11 Tiedonhallintaryhmä

Tiedonhallintaryhmä kehittää, seuraa ja raportoi tiedonhallintaan, tietoturvaan ja tietosuojaan liittyvien veloitteiden toteutumista Suonenjoen kaupungilla. Lisäksi ryhmä koordinoi konsernitason tasolla tiedonhallintaan liittyvien veloitteiden edellyttämiä toimenpiteitä, ohjeistusta ja koulutusta. Ryhmää johtaa hallintojohtaja.

Tiedonhallintaryhmän tehtävänä on:

- valmistella tiedonhallintaan liittyvät kaupunginhallituksen hyväksyttäväksi menevät asiakirjat
- suunnitella ja seurata tiedonhallintaan liittyviä ohjeistuksia ja koulutuksia
- tukea kaupungin johtoa tiedonhallintalakikokonaisuuden toimeenpanossa ja toimenpiteiden toteuttamisessa
- tarkastaa lokitietoja
- valvoo hankittavia järjestelmiä ja niiden sopimuksia tietosuojan ja tietoturvan osalta
- koordinoi ja valvoo tiedonhallinnan muutoksenvaikutuksen arviointeja
- koordinoi ja valvoo riskiarviointia tietoturvan ja tietosuojan osalta, huomioiden mahdolliset vaikutustenarvioinnit

- varmistaa säädösten vaatima dokumentaatio (mm. tiedonhallintamalli ja tietotilin päätös)

## 4.12 Asianhallintatiimi

Asianhallintatiimin tarkoituksena on kehittää ja yhtenäistää kaupungin asianhallintaa. Tiimin vastuulle kuuluu koko tiedon elinkaari, huomioiden myös tietopyynnöt. Asianhallintatiimi koostuu eri toimialojen toimistosihteereistä ja tiiminvetäjänä toimii toimistopäällikkö. Tiimissä mahdollisesti esille tulleet parannus- ja kehityskohteet raportoidaan asiakirjahallintoa ja arkistointia johtavalle viranhaltijalle, hallintojohtajalle.

## 4.13 Henkilötietojen käsittelijä (ulkoistettu)

Ulkoinen henkilötietojen käsittelijä on yritys tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun sen ohjeiden mukaisesti. Rekisterinpitäjä päättää tietojen käsittelyn tarkoituksista ja keinoista ja ulkoinen käsittelijä hoitaa itse käsittelytehtäviä. Vastuu asianmukaisesta käsittelystä säilyy rekisterinpitäjällä, vaikka käsittely olisi ulkoistettu. Käsittelijä on vastuussa vain jos se toimii vastoin ohjeita tai asetuksia.

# 5 Tiedonhallinnan kuvaukset ja toteutus

Tiedonhallinnan dokumentointia varten Suonenjoen kaupungille on hankittu erillinen järjestelmä, jonka avulla voidaan kokonaisvaltaisesti seurata kaupungin tiedonhallinnan, tietoturvan ja tietosuojan tilannetta. Järjestelmästä voidaan tuottaa myös tiedonhallintalain sekä tietosuojasetuksen mukaisia raportteja. Järjestelmässä julkaistaan henkilöstölle ohjeita ja koulutuksia tiedonhallintaan liittyen.

## 5.1 Tiedonhallintamalli

Tiedonhallintalain mukaisesti Suonenjoen kaupunki tiedonhallintayksikkönä ylläpitää toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia.

Tiedonhallintamallin tarkoitus on palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelu ja toteuttaminen, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttaminen, moninkertaisen tietojenkeruun vähentäminen, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttaminen sekä tietoturvallisuuden ylläpitäminen.

Kaupunginhallitus on hyväksynyt 9.6.2025 Suonenjoen kaupungin tiedonhallintamallin kuvauksen. Tiedonhallintamallia ylläpidetään ja päivitetään erillisessä järjestelmässä. Päivitystarve tulee esimerkiksi muutosvaikutusarviointien kautta.

Tiedonhallintamalliin sisällytetään vähintään seuraavat tiedot:

- **Toimintaprosessit** ja niistä vastaavat viranomaiset, sekä prosessien keskinäiset sidokset.
- **Tietovarannot** ja niistä vastaavat viranomaiset, sekä tietovarantojen sidokset toimintaprosesseihin ja tietojärjestelmiin. Lisäksi tiedot tietovarannon käyttötarkoituksesta, keskeisistä tietoryhmistä ja tietojen luovutuskohteista.
- **Tietoaineistot** ja tiedot niiden säilytysajasta, arkistoon siirtämisestä, arkistointitavasta ja arkistopaikasta tai tuhoamisesta. Edellä mainitut arkistointitoimenpiteet voidaan esittää myös erillisessä arkistolain mukaisessa arkistonmuodostussuunnitelmassa tai tiedonohjaussuunnitelmassa, joka liitetään osaksi tiedonhallintamallia.
- **Tietojärjestelmät** ja niistä vastaavat viranomaiset. Lisäksi tiedot tietojärjestelmän käyttötarkoituksesta, tietojärjestelmän liittymistä muihin tietojärjestelmiin ja liittymissä käytettävistä tiedonsiirtotavoista.
- **Riskien hallinta ja tietoturvallisuustoimenpiteet.**

## 5.2 Tiedonhallinnan muutosvaikutusten arviointi

Tilanteissa, joissa kaupungin toimintaan on tulossa sellaisia hallinnollisia muutoksia tai keskeisten tietojärjestelmien hankintoja, vaihdoksia taikka käytöstä poistamisia, joilla on olennaista vaikutusta tiedonhallintaan, tulee tehdä tiedonhallinnan muutosvaikutusten arviointi.

Tiedonhallintalain mukaisesti arvioinnissa on tarkasteltava millä tavalla muutokset tulevat vaikuttamaan tiedonhallinnan vastuisiin, tietoturvallisuusvaatimukseen ja -toimenpiteisiin, tietoaineistojen muodostamiseen ja luovutustapoihin, asianhallintaan ja palvelujen tiedonhallintaan sekä asiakirjojen säilyttämiseen, arkistointiin, tuhoamiseen, julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin. Arvioinnissa on otettava huomioon myös tietovarantojen yhteentoimivuus ja hyödynnettävyys tietoaineistoja muodostettaessa ja käytettäessä.

## 5.3 Asiakirjajulkisuuskuvauk

Asiakirjajulkisuuskuvauksen avulla kerrotaan Suonenjoen kaupungin asiakkaille, miten Suonenjoella hallitaan tietoaineistoja, joita syntyy viranomaisen asiankäsittelyssä ja palveluja tuottaessa. Kuvauksen tavoitteena on auttaa asiakkaita tietopyynnön sisällön yksilöinnissä ja tietopyynnön kohdistamisessa oikealle taholle. Asiakirjajulkisuuskuvauk on täydentyvä asiakirja, jota päivitetään säännöllisesti. Asiakirjajulkisuuskuvauk pohjautuu tiedonhallintamallin tietoihin. Asiakirjajulkisuuskuvauk julkaistaan yleisessä tietoverkossa siltä osin kuin sen tiedot eivät ole salassa pidettäviä.

## 5.4 Tiedonohjaussuunnitelma

Tiedonohjaussuunnitelma (TOS) ohjaa kaupungin tietoaineistojen käsittelyä ja arkistointia. Se täyttää arkistolain viranomaisilta edellyttämien arkistonmuodostussuunnitelman vaatimukset. TOS:aa ylläpidetään sähköisesti tiedonohjausjärjestelmässä (TOJ). TOJ on integroitu asianhallintajärjestelmään, niin, että se antaa järjestelmään viedyille asioille automaattisesti muun muassa käsittelyvaiheita ja säilytysaikoja.

## 5.5 Tietotilinpäätös

Kaupunginhallitukselle tulee tuoda vuosittain tilinpäätöskäsittelyn yhteydessä tiedoksi tietotilinpäätös. Tietotilinpäätös on osa tiedolla johtamista ja antaa kokonaiskuvan organisaation tiedonhallinnan sekä tietosuojan ja tietoturvan toteutumisesta. Tietotilinpäätökseen kootaan edelliseltä kalenterivuodelta keskeisimmät havainnot, toteutumat ja arvioinnit yleisesti tiedonhallinnasta. 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.

Tietotilinpäätöstä käytetään yhtenä keinona Euroopan unionin yleisen tietosuojasetuksen vaatiman osoitusvelvollisuuden toteuttamisessa.

## 5.6 Tietosuojaan riski- ja vaikutustenarvioinnit

Tietosuojariskienhallinta on osa Suonenjoen kaupungin riskienhallintaprosessia. Kukin lautakunta rekisterinpitäjänä arvioi tuottamiensa palveluiden *henkilötietojen käsittelyyn liittyvät riskit*.

Riskianalysissa tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Riskitason määrityksellä vältetään liian raskaat toimenpiteet matalariskisten toimintojen suojaamiseksi ja vastaavasti tunnistetaan merkittävän tason riskit, jotka on raportoitava kaupungin johdolle saakka. Riskitekijöiden tunnistaminen toimii pohjana myös tarkoituksenmukaisten tietojärjestelmien ja tietoverkkojen tietoturvatkaisuun käyttämiselle sekä tietosuojakäytännöille. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy.

Suonenjoen kaupunki toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi myös tietosuojaan vaikutustenarviointeja. Vaikutustenarviointi vaaditaan tilanteissa, 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.

## 5.7 Tietosuojaselosteet

Euroopan unionin yleisen tietosuoja-asetuksen mukaisesti rekisterinpitäjän on informoitava rekisteröityjä henkilötietojen käsittelystä mahdollisimman läpinäkyvästi. Läpinäkyvän informoinnin toteuttamiseksi tulee kaupungin palveluista, joissa käsitellään henkilötietoja, laatia ja ylläpitää ajantasaisia tietosuojaselosteita, jotka pidetään nähtävillä yleisessä tietoverkossa tai palveluissa itsessään. Suonenjoen kaupungin tietosuojaselosteet on julkaistu kaupungin verkkosivuilla.

## 5.8 Henkilötietojen tietoturvaloukkausilmoitus

Tietoturvaloukkauksella tarkoitetaan käytännössä häiriötilannetta, jonka seurauksena henkilötietoja mahdollisesti tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Tietoturva- ja tietosuojarikkomukset eli tietoturvaloukkaukset käsitellään aina tapauskohtaisesti.

Tietoturvaloukkauksesta, tai läheltä piti tilanteesta, on heti ilmoitettava esihenkilölle ja tietoturva ja tietosuojavastaaville. Ilmoituksen lisäksi on aina täytettävä ”ilmoitus tietoturvan häiriötilanteesta” -lomake, koska kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet on dokumentoitava, riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa. Lomake löytyy kaupungin intrasta. Dokumentointivelvollisuuden tai ilmoituksen tekemisen laiminlyöminen on tietosuoja-asetuksen vastaista. Dokumentointivelvollisuuden piiriin kuuluvat myös tietojärjestelmään kohdistuneen tietoturvaloukkauksen osalta tapahtuma-ajan lokitiedot.

Rekisterinpitäjän on arvioitava, millainen riski tietoturvaloukkauksesta on aiheutunut vuodon kohteena olevalle henkilölle. Tietosuojavastaava tekee asetuksen mukaiset ilmoitukset valvontaviranomaisen sekä rekisteröidyn suuntaan riskiarvion perusteella:

- Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto. Ilmoitus on tehtävä 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi.
- Henkilötietojen tietoturvaloukkauksesta on ilmoitettava aina rekisteröidylle, jos se aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisterinpitäjän on tällöin ilmoitettava asiasta ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua. Jos rekisteröityihin ei voida ottaa yhteyttä henkilökohtaisesti, on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä.

## 5.9 Tekoälyn eettiset periaatteet

Tiedon tehokkaan hyödyntämisen edellytyksenä on systemaattinen tiedonhallinta. Tekoälyn avulla monia työvaiheita tiedon hallinnassa ja hyödyntämisessä voidaan nopeuttaa ja tehostaa.

Tekoälyn eettiset periaatteet on kuvattu kaupunginhallituksen hyväksymässä ”Tekoälypalvelujen käyttö Suonenjoen kaupungissa” -ohjeessa. Tekoälypalvelujen käyttö Suonenjoen kaupungissa -ohjeeseen on kuvattu tekoälyjärjestelmien käyttöönotto ja käyttö Suonenjoen kaupungin toiminnassa huomioiden vaikutustenarviointit, eettiset periaatteet sekä Euroopan unionin tekoälyasetus.