



Naantalin kaupunki

TIETOTILINPÄÄTÖS

vuodelta 2025

9.3.2026 tiedonhallintasuunnittelija ja tietosuojavastaava Laura Sundqvist, kaupunginjuristi
Turo Järvinen ja tietoturvapäällikkö Juha Riekkinen

[hyväksyntä KH 16.3.2026 § xx]

Sisällys

1. Tietosuojavastaavan katsaus.....	3
2. Tietotilinpäätöksen tarkoitus	4
3. Tietosuoja-asioiden vastuunjako Naantalissa.....	4
3.1. Kaupunginhallitus	4
3.2. Tietosuojavastaava	4
3.3. Tietoturva- ja tietosuojaryhmä	4
4. Rekisteröidyn oikeuksien toteuttaminen	5
4.1. Rekisteröidyn informointi	5
4.2. Tietosuojaselosteet	5
4.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt	5
4.3.1. Oikeus saada pääsy tietoihin	6
4.3.2. Oikeus tiedon oikaisemiseen	6
4.3.3. Poistopyynnöt.....	6
4.3.4. Oikeus käsittelyn rajoittamiseen	7
4.3.5. Oikeus siirtää tiedot järjestelmästä toiseen	7
4.3.6. Vastustamisoikeus	7
4.3.7. Oikeus riitauttaa automaattinen yksittäispäätös	7
4.3.8. Oikeus tehdä valitus valvontaviranomaiselle	7
5. Selosteet käsittelytoimista	8
6. Tietoturva	8
7. Tietosuojaa koskevat vaikutustenarvioinnit	8
8. Sisäänrakennettu ja oletusarvoinen tietosuoja.....	9
9. Sopimukset ja hankinnat	10
10. Lainsäädäntö, koulutus ja ohjeistus	10
10.1. Henkilötietojen käsittelyä koskeva lainsäädäntö.....	12
10.2. Henkilötietojen käsittelyä koskevat koulutukset.....	12
10.3. Henkilötietojen käsittelyä koskeva ohjeistus	12
11. Henkilötietojen tietoturvaloukkaukset	12
12. Valvontaviranomaisten selvitys- ja tietopyynnöt.....	13
13. Tietosuojatyön kehittämistarpeet	13

1. Tietosuojavastaavan katsaus

Tällä tietotilinpäätöksellä osoitetaan, miten tietosuoja ja tietoturva ovat toteutuneet Naantalın kaupungin toiminnassa vuonna 2025. Tietotilinpäätös kokoaa yhteen tiedonhallinnan ja tietosuojan keskeiset periaatteet sekä toiminnan. Sen tarkoituksena on antaa läpinäkyvä kokonaiskuva siitä, miten Naantalın kaupunki huolehtii vastuullisesti hallussaan olevista tiedoista ja varmistaa niiden lainmukaisen käsittelyn. Tietotilinpäätös auttaa myös tunnistamaan kehittämiskohteita sekä kartoittamaan, mitä toimenpiteitä tarvitaan tietosuojan parantamiseksi.

Naantalın kaupungin tietotilinpäätöksestä käy ilmi, että tietosuojatyön kehittäminen on luonteeltaan jatkuvaa. Tietosuojatyö on entistä laaja-alaisempaa ja tiiviisti sidoksissa digitalisaatioon, tiedonhallintaan sekä uuteen sääntelyyn. Esimerkiksi tekoälyn yleistyminen sekä EU:n tekoälyasetus tuovat mukanaan uusia arviointi- ja dokumentointitarpeita. Lisäksi meneillään on myös tietosuojalainsäädännön kokonaisuudistus, joka on osa pääministeri Orpon hallitusohjelmaa.

Kuntaliitto on käynnistänyt tietosuojan perusohjeistus kunnille -hankkeen (2025–2026), jonka tarkoituksena on auttaa kuntia tulkitsemaan tietosuojan peruskäsitteitä sekä organisoimaan tietosuojatyön vastuita entistä paremmin ja yhdenmukaisemmin kuntalaisten tietojen suojaamiseksi. Uuden tietosuojan perusohjeistuksen laatiminen ei onnistu ilman sidosryhmien laajaa osallistumista ja panostusta, ja sen takia olemme Naantalista myös mukana viemässä projektia eteenpäin.

Tämän lisäksi olemme tiiviisti mukana Digi- ja väestötietoviraston VAHTI-verkoston työryhmien toiminnassa. Alan asiantuntijat työskentelevät työryhmissä yhdessä, osallistuvat ajankohtaisten julkaisujen laadintaan, kehittävät omaa osaamistaan ja edistävät organisaatioidensa digitaalista turvallisuutta.

Meillä tietosuojan ja tietoturvan vastuuhenkilöt sekä tietoturva- ja tietosuojaryhmän jäsenet ovat kaikki osaavia ja sitoutuneita työhönsä. Kaupungilla on toimivat prosessit rekisteröidyn oikeuksiin liittyviin pyyntöihin ja tietoturvaloukkauksiin. Henkilöstöä koulutetaan kattavasti tietosuoja- ja turva-asioihin uudistetulla digitaalisella oppimisympäristöllä. Kaupungin intranet-sivuilla on lisäksi koottu tietosuoja koskevat selkeät, käytännönläheiset ja työtä tukevat ohjeet, jotta jokainen tietää, miten toimia henkilötietojen käsittelyn eri tilanteissa. Lisäksi Digturvamalli-järjestelmän pääkäyttäjät järjestivät sekä uusille että vanhoille käyttäjille suunnatun koulutuksen ja työpajan järjestelmän käytöstä.

Tietoturva- ja tietosuojaryhmä yhdessä johdon kanssa osallistui TAISTO 2025 tietosuoja- ja tietoturvaloukkausten hallinnan harjoitukseen. Harjoituksessa harjoitellaan häiriö- ja poikkeamatilanteissa toimimista kuvitteellisten tilanteiden avulla. Harjoituksessa kokeilimme toimintamalliemme ja ohjeistuksiemme toimivuutta käytännössä, kun kyseessä oli jokin uhkatilanne, kuten kalastelukampanja, haittaohjelma tai kriittinen haavoittuvuus.

Kaupungille on aiemmin laadittu oma Tietosuojakäsikirja, jota on viimeksi päivitetty vuonna 2025. Tietosuojakäsikirjassa kerrotaan perustietoa tietosuojalainsäädännöstä sekä ohjeistetaan toteuttamaan tietosuojalainsäädännön toimenpiteitä. Käsikirja on tarkoitettu ohjeeksi kaikille, jotka työssään käsittelevät henkilötietoja – eli suurimmalle osalle kaupungin työntekijöistä.

Tietosuojatyö on kaupungin asukkaita varten. Heillä on oikeus luottaa siihen, että Naantalın kaupunki käsittelee heidän henkilötietojensa lainsäädännön edellyttämällä tavalla. Hyvin hoidettu tietosuojatyö näkyy asukkaille turvallisina ja sujuvin palveluina, avoimuutena, luotettavuutena sekä oikeuksien toteutumisena. Näin ollen on tärkeää, että panostamme jatkossakin tietosuojatyöhön sekä jatkamme hyvää linjaa kehittämällä tietosuojatyötä uudet teknologiat, toimintatavat ja lakiuudistukset huomioiden.

2. Tietotilinpäätöksen tarkoitus

Tietotilinpäätös on keskeinen osa tietosuojan toteutumisen seuranta ja EU:n yleisen tietosuoja-asetuksen (EU 2016/679) määrittelemää osoitusvelvollisuutta (art. 5). Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.

Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Tietotilinpäätös on osa tätä dokumentointia, ja se koostaa yhteen, mitä Naantalin kaupungilla on käytännössä tehty tietosuojan toteuttamiseksi.

Osoitusvelvollisuuden toteuttamisen lisäksi tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa, arvioi tietosuojan ja tietoturvan toteutumista, tarkastelee tietosuojan valvontaa ja esittelee kehityskohteita. Tietotilinpäätös on kunnan johdolle tarkoitettu tietosuojan seurannan ja kehittämisen työkalu ja sitä voidaan käyttää sisäisen ja ulkoisen valvonnan apuvälineenä.

Tietotilinpäätös on suunnattu laajalle kohdeyleisölle kaupungin johdosta esimiehiin, asiantuntijoihin, työntekijöihin ja kaupungin asukkaisiin. Tietotilinpäätöstä laadittaessa on otettu huomioon tietosuojavaltuutetun toimiston ohjeistus tietotilinpäätöksen laatimisesta.

3. Tietosuoja-asioiden vastuunjako Naantalin kaupungilla

Tietosuoja-asioiden vastuunjako on määritelty kaupungin tietosuojalinjauksissa. Toimialojen johdolla on vastuu toiminnan lainmukaisuudesta henkilötietojen käsittelyssä.

3.1. Kaupunginhallitus

Hallintosäännön mukaisesti kaupunginhallitus vastaa siitä, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista.

3.2. Tietosuojavastaava

Tietosuoja-asetus velvoittaa kaikkia julkishallintoon kuuluvia organisaatioita nimittämään tietosuojavastaavan. Tietosuojavastaavan tehtäviin kuuluu organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä, tietosuoja-asetuksen noudattamisen valvonta, mukaan lukien tähän liittyvät tarkastukset, yhteistyö valvontaviranomaisen (tietosuojavaltuutetun toimisto) kanssa ja rekisteröityjen (kuntalaiset ja asiakkaat) oikeuksien toteuttamisen tukeminen. Tietosuojavastaava raportoi suoraan kaupungin johdolle, ja hänen asemansa organisaatiossa on autonominen ja riippumaton. Tietosuojavastaavan sijaisena toimii kaupunginjuristi. Tietosuojavastaavan henkilötiedot on julkistettava ja ne on ilmoitettava valvontaviranomaisella.

3.3. Tietoturva- ja tietosuojaryhmä

Naantalin kaupunki on nimennyt helmikuussa 2021 uuden tietoturva- ja tietosuojaryhmän, joka seuraa tietoturvan ja tietosuojan tilaa, linjaa niiden kehittämistä sekä omalta osaltaan jalkauttaa kaupungin yhteisiä toimintatapoja toimialoille. Ryhmän kokoonpanon muodostavat eri toimialojen asiantuntijat.

Tietoturva- ja tietosuojaryhmän kokoonpanoa päivitettiin vuonna 2025 henkilömuutosten vuoksi. Vuoden 2025 aikana tietoturva- ja tietosuojaryhmä kokoontui 4 kertaa.

4. Rekisteröidyn oikeuksien toteuttaminen

Tietosuoja-asetuksen mukaan rekisterinpitäjän velvollisuuksiin kuuluu rekisteröidyn oikeuksien toteuttaminen. Henkilötietojen käsittelyperuste määrittää, mitä oikeuksia rekisteröidyllä on. Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien käyttöä ja huolehdittava siitä, että oikeudet toteutuvat tehokkaasti.

4.1. Rekisteröidyn informointi

Naantalin kaupungin internetsivuilla informoidaan rekisteröityjä tietosuoja-asioissa osoitteessa naantali.fi/tietosuoja. Sivulla annetaan yleisinformaatiota Naantalin kaupungin henkilötietojen käsittelystä sekä kerrotaan rekisteröidyn oikeuksista ja niiden toteuttamisesta. Lisäksi sivulta löytyy myös tietosuojaselosteet, joissa kerrotaan henkilötietojen käsittelystä tietovarantokohtaisesti. Sivulla kerrotaan myös Naantalin kaupungin tietosuojavastaavan yhteystiedot.

4.2. Tietosuojaselosteet

Naantalin kaupunki kerää ja käsittelee henkilötietoja eri käyttötarkoituksiin. Henkilötietojen käsittelyssä noudatetaan EU:n yleistä tietosuoja-asetusta sekä muuta henkilötietojen käsittelyä koskevaa lainsäädäntöä. Henkilötietojen käsittely perustuu aina käsittelyperusteeseen, kuten rekisterinpitäjän lakisääteiseen velvoitteeseen, yleistä etua koskevaan tehtävään tai julkiseen valtaan. Kaupungin rekisterinpitäjillä on velvollisuus informoida rekisteröityjä henkilötietojen käsittelystä. Naantalin kaupungin käsittelemiä henkilötietoja koskevat tietosuojaselosteet ovat osa tätä informointia. Tietosuojaselosteet on julkaistu kaupungin verkkosivuilla osoitteessa naantali.fi/tietosuoja.

Tietosuojaselosteista ilmenee seuraavat tiedot:

- rekisterinpitäjän ja tämän edustajan yhteystiedot
- tieto siitä, mitä henkilötietoja käsitellään
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- tieto henkilötietojen säännönmukaisista luovutuksista
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- henkilötietojen tietolähteet
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä

Tietosuojaselosteita on ajantasaistettu osana kaupungin tiedonhallintamallin laatimista. Tiedonhallintamalli on hyväksytty kaupunginjohtajan päätöksellä 24.11.2022 § 93. Tietosuojaselosteita päivitetään tarvittaessa ja tiedonhallintamallin vastuuhenkilöt katselmoivat selosteiden tietosisältöä vuosittain osana tiedonhallintamallin päivityssykliä.

4.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt

Rekisteröidyllä on oikeuksia liittyen omiin henkilötietoihin ja niiden käsittelyyn. Rekisteröidyllä henkilöllä on:

- Oikeus saada pääsy tietoihin
- Oikeus tiedon oikaisemiseen
- Oikeus tietojen poistamiseen
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus
- Oikeus riitauttaa automaattinen yksittäispäätös
- Oikeus tehdä valitus valvontaviranomaiselle

4.3.1. Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus pyytää Naantalin kaupungilta pääsy häntä itseään koskeviin henkilötietoihin. Rekisteröidyllä on oikeus tarkastaa, mitä häntä koskevia henkilötietoja asiakasrekisteriin on tallennettu tai ettei rekisterissä ole häntä koskevia tietoja. Huoltajalla on pääsääntöisesti oikeus tarkastaa myös lastaan koskevat tiedot.

Tarkastuspyyntö tehdään henkilökohtaisesti käynnin yhteydessä tai omakätisellä allekirjoituksella tai vastaavalla tavalla varmennetulla asiakirjalla tai henkilökohtaisesti rekisterinpitäjän luona. Asiakkaan henkilöllisyys varmennetaan ennen tietojen antamista. Asiakkaalla on oikeus tutustua ja nähdä itseään koskevat asiakastiedot ja pyynnöstä saada kopiot niistä kirjallisena. Pääsääntöisesti tarkastusoikeus toteutetaan siinä yksikössä, jossa tiedot ovat syntyneet. Tiedot tulee antaa ilman aiheutonta viivästystä. Jos tarkastusoikeus evätään, asiakkaalle annetaan kirjallinen kieltäytymistodistus, jossa mainitaan kieltäytymisen syyt. Asiakkaalla on oikeus saattaa asia tietosuojavalvottuun ratkaistavaksi.

Vuoden 2025 aikana Naantalin kaupungille saapui yksi omien henkilötietojen tarkastuspyyntö.

4.3.2. Oikeus tiedon oikaisemiseen

Rekisteröidyllä on oikeus pyytää Naantalin kaupungilta häntä itseään koskevien epätarkkojen ja virheellisten henkilötietojen oikaisemista ilman aiheutonta viivytystä.

Asiakkaan tulee pyynnössään yksilöidä ja perustella tarkasti, mitä tietoa vaaditaan korjattavaksi ja mikä on asiakkaan mielestä oikea tieto ja millä tavalla korjaus pyydetään tekemään. Asiakastietoja voidaan myös korjata täydentämällä niitä asiakkaan näkemyksellä asiasta. Asiakkaan henkilöllisyys varmennetaan ennen tietojen oikaisemista.

Vuoden 2025 aikana Naantalin kaupungille ei tullut omien tietojen oikaisupyyntöjä.

4.3.3. Poistopyynnot

Rekisteröidyllä on tietyissä tapauksissa oikeus saada kaupunki poistamaan häntä koskevat tiedot. Oikeus tietojen poistamiseen, eli oikeus tulla unohdetuksi tarkoittaa rekisteröidyn oikeutta pyytää kaupunkia poistamaan esimerkiksi häntä koskevat vanhentuneet henkilötiedot. Mikäli rekisteröidyllä on oikeus tietojensa poistamiseen, ne on poistettava ilman aiheutonta viivytystä. Oikeus tietojen poistamiseen on kuitenkin rajoitettu. Oikeutta tietojen poistamiseen ei ole, jos käsittely perustuu kaupungin lakisääteisen velvoitteen noudattamiseen, liittyy yleistä etua koskevan tehtävän suorittamiseen tai kaupungille kuuluvan julkisen vallan käyttämiseen.

Vuodelta 2025 ei raportoitu henkilötietojen poistopyyntöjä.

4.3.4. Oikeus käsittelyn rajoittamiseen

Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty. Tällainen tilanne voi tulla kyseeseen, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan siihen asti, kunnes kaupunki voi varmistua tietojen paikkansapitävyydestä.

Vuoden 2025 aikana Naantalin kaupungille ei tullut henkilötietojen käsittelyn rajoittamispyyntöjä.

4.3.5. Oikeus siirtää tiedot järjestelmästä toiseen

Jos rekisteröity on toimittanut kaupungille omia henkilötietojaan, hänellä on oikeus siirtää ne toiselle rekisterinpitäjälle, kuten toiselle kunnalle. Kyseinen oikeus tulee ainoastaan sovellettavaksi silloin, jos henkilötietojen käsittely perustuu sopimukseen tai suostumukseen, ja jos käsittely suoritetaan automaattisesti. Tämä oikeus ei tule sovellettavaksi silloin, kun käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai kaupungille kuuluvan julkisen vallan käyttämistä varten. Oikeus siirtää tiedot järjestelmästä toiseen koskee vain rekisteröidyn toimittamia tietoja.

4.3.6. Vastustamisoikeus

Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan. Vastustamisoikeus tulee sovellettavaksi silloinkin, kun käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen, julkisen vallan käyttämiseen, rekisterinpitäjän tai kolmannen osapuolen oikeutettuun etuun. Tässä tapauksessa tietojen käsittely jatkuu vain, jos käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, jonka kaupunki voi osoittaa. Käsittelyä saa jatkaa myös silloin, jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Vastustamisoikeutta ei ole, jos henkilötietojen käsittely perustuu kaupungin lakisääteiseen velvoitteeseen. Henkilötietojen käsittelyä ei siten voi vastustaa esimerkiksi silloin, kun on kyse koulun oppilaiden tai varhaiskasvatuksessa olevien lapsien ja heidän huoltajien rekisteristä.

Vuonna 2025 henkilötietojen käsittelyn vastustamisvaatimuksia ei raportoitu.

4.3.7. Oikeus riitauttaa automaattinen yksittäispäätös

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

Naantalin kaupungilla ei ole vuonna 2025 ollut käytössä automaattista päätöksentekomenettelyä, eikä kaupungille ei ole tullut yhteydenottoja koskien automaattiseen henkilötietojen käsittelyyn perustuvan päätöksen kohteeksi joutumista.

4.3.8. Oikeus tehdä valitus valvontaviranomaiselle

Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuojaa-asetusta. Suomessa valitus tehdään tietosuojavaltuutetun toimistoon.

5. Selosteet käsittelytoimista

Rekisterinpitäjän on ylläpidettävä selosteita käsittelytoimista (tietosuoja-asetuksen 30 artiklan mukaiset selosteet). Selosteet käsittelytoimista ovat yleisiä kuvauksia siitä, miten rekisterinpitäjä käsittelee henkilötietoja. Selosteet käsittelytoimista laaditaan kaupungin sisäiseen käyttöön sekä valvontaviranomaista varten. Selosteissa kerrotaan:

- rekisterin tai palvelukokonaisuuden nimi
- rekisterinpitäjä ja yhteystiedot
- tietosuojavastaava ja hänen yhteystietonsa
- henkilötietojen käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä
- kuvaus henkilötietoryhmistä
- vastaanottajaryhmät
- tietojen säilytysajat
- kuvaus teknisistä ja organisatorisista turvatoimista
- tieto henkilötietojen säännönmukaisista luovutuksista EU/ETA-alueen ulkopuolelle
- viittaus henkilötietojen käsittelijän kanssa solmittuun käsittelyä koskevaan sopimukseen

Seloste käsittelytoimista tuotetaan tiedonhallintamallin tiedoista.

6. Tietoturva

Tietosuoja ei pystytä toteuttamaan ilman hyvää tietoturvaa, sillä tärkeä osa tietosuoja on henkilötietojen asianmukainen tekninen turvaaminen. Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Tietoturvatyökalut, kuten käyttöoikeuksien hallinta ja käyttöoikeusrajaukset, järjestelmälokukset, auditoinnit sekä kyky taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa, ovat teknisiä toimenpiteitä, joilla pyritään varmistamaan tietosuojan toteutuminen.

Jos rekisteröity on toimittanut kaupungille omia henkilötietojaan, hänellä on oikeus siirtää ne toiselle rekisterinpitäjälle, kuten toiselle kunnalle. Kyseinen oikeus tulee ainoastaan sovellettavaksi silloin, jos henkilötietojen käsittely perustuu sopimukseen tai suostumukseen, ja jos käsittely suoritetaan automaattisesti. Tämä oikeus ei tule sovellettavaksi silloin, kun käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai kaupungille kuuluvan julkisen vallan käyttämistä varten. Oikeus siirtää tiedot järjestelmästä toiseen koskee vain rekisteröidyn toimittamia tietoja.

Naantalin kaupungissa on nimetty tietoturvapäällikkö, joka edistää tietoturvallisuuden toteutumista kaupungissa. Tietoturvavastaavia ei nimetä erikseen, vaan palvelualueiden johtajat ovat vastuuhenkilöitä ja voivat tarvittaessa delegoida tehtävän vastuuta alaspäin. Kaupunginhallitus on 20.2.2017 § 55 hyväksynyt Naantalin kaupungille tietoturvapoliittikan.

7. Tietosuoja koskevat vaikutustenarvioinnit

Tietosuoja koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä. Tietosuoja-asetuksen mukaan arvioinnin on sisällettävä vähintään järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, arvio käsittelytoimien

tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä sekä suunnitellut toimenpiteet riskeihin puuttumiseksi. Vaikutustenarvioinnin tuloksena syntyy näkemys tarvittavista hallintakeinoista, joita tarvitaan pienentämään riskitasoa ja varmistamaan asetuksen vaatimusten toteuttaminen.

Naantalin kaupungin tiedonhallinnan muutosvaikutusten arvioinnin prosessi on hyväksytty tiedonhallinnan ohjausryhmässä. Toimintakauden aikana aloitettiin tietosuojan vaikutustenarviointien (DPIA) laatiminen. Alla olevasta kuvasta näkyy, että tietosuoja koskevien vaikutustenarviointien määrä on kasvanut tasaisesti vuoden 2025 aikana, ja jatkaa kasvua edelleen. Kokonaisuutena Naantalin kaupunki on siirtynyt tilanteeseen, jossa vaikutustenarviointien toteuttaminen on systemaattista, kattavaa ja vakiintuneesti sisällytetty osaksi kaupungin tietosuojan ja riskienhallinnan kokonaisuutta.

Arviointeja laaditaan sekä Digiturvamallissa että Ilona IT:n DPIA-työkalun avulla. Arvioinnit ovat luonteeltaan laajoja, ja niitä laaditaan pääasiassa yhteistyöverkostossa muiden korkeakoulujen, kuntien ja ammatillisten oppilaitosten kanssa. Kun organisaatiot toteuttavat arviointeja yhdessä, työnteko on tehokasta, näkökulmat monipuolisia, työmäärä jakaantuu ja dokumentaation laatu paranee. Arvioinneissa on nyt keskitytty erityisesti perus- ja lukio-opetuksen järjestelmiin. Tällaisissa järjestelmissä käsitellään esimerkiksi alaikäisten henkilötietoja, joita on EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan suojeltava erityisen tarkasti.



8. Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa lähestymistapaa, jossa tietojärjestelmien suunnittelussa ja henkilötietojen käsittelytoimissa otetaan tietosuoja keskeisesti huomioon alusta alkaen. Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ohjaavat rekisterinpitäjää toimimaan henkilötietoja käsiteltäessä rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla. Periaatteita ovat:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen
- Eheys ja luottamuksellisuus

Naantalin kaupunki noudattaa toiminnassaan näitä edellä mainittuja periaatteita. Henkilötietojen käsittely perustuu aina käsittelyperusteeseen ja kerromme rekisteröidylle avoimesti, mitä heitä koskevia tietoja kerätään ja käsitellään. Henkilötietojen käsittelyn tarkoitus on ennalta suunniteltu ja määritelty ennen käsittelyn aloittamista. Käsitteltävät henkilötiedot ovat täsmällisiä ja päivitettyjä emmekä käsittele henkilötietoja turhaan.

Henkilötietojen elinkaaren hallinnalla varmistutaan siitä, että henkilötietoja käsitellään vain niin kauan, kuin on niiden käyttötarkoituksen kannalta tarpeellista. Lisäksi pyritään huolehtimaan siitä, että henkilötiedot poistetaan ja asiakirjat hävitetään sen jälkeen, kun määritelty säilytysaika on päättynyt. Henkilötietojen säilytysaikoja on määritelty osana yleisiä tietojen säilytysaikoja muun muassa kaupungin tiedonohjaussuunnitelmassa ja tiedonhallintamallissa. Tiedonhallintamallin kautta tiedot tulevat myös tietosuoja koskevaan dokumentaatioon, kuten tietosuojaselosteille ja selosteeseen käsittelytoimista.

9. Sopimukset ja hankinnat

Arvioitaessa tietosuoja-asetuksen asettamia velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella, kun joku muu (kuten kaupungin palveluntuottaja) käsittelee tietoja rekisterinpitäjän (kaupunki) puolesta. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään. Tietosuoja-asetuksessa säädetään sopimisvelvoitteen lisäksi tietosuoja koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia.

Naantalin kaupunki hyödyntää hankinnoissaan alkukeväästä 2025 julkaistuja Valtiovarainministeriön ylläpitämiä JYSE/JIT henkilötietojen käsittelyn ehtoja ja henkilötietojen käsittelytoimien kuvauksia, jotka ovat tarkoitettu käytettäväksi osana julkisen hankintojen yleisiä sopimusehtoja ja julkisten hallinnon IT-hankintojen yleisiä sopimusehtoja. Liitteet on tarkoitettu hankintoihin, jossa toimittaja (käsittelijä) käsittelee tilaajan henkilötietoja tilaajan (rekisterinpitäjän) lukuun osana hankittavaa palvelua.

Tämän lisäksi Naantalin kaupungille on laadittu myös uusi IT-hankintojen yleiset pakolliset vaatimukset - taulukko. Taulukkoa tulee käyttää hankinnan ehtona, toteutettaessa ja/tai kilpailutettaessa mitä tahansa IT-hankintaa, jossa järjestelmä toimii ulkoisen palveluntuottajan ympäristössä (SaaS). Taulukko on kattava, käsittäen muun muassa palvelunhallinnan, käyttöönottoprojektin, vaatimustenmukaisuuden ja tietosuojan sekä tietoturvan.

Osana tiedonhallintamallia kerätään tietoja siitä, mitkä tahot toimivat henkilötietojen käsittelijöinä, ja onko näiden tahojen kanssa sovittu henkilötietojen käsittelystä. Ennen tietosuoja-asetuksen voimaantuloa tehtyihin sopimuksiin muutokset tehdään viimeistään uuden sopimuskauden alkaessa.

10. Lainsäädäntö, koulutus ja ohjeistus

EU:n yleinen tietosuoja-asetus (EU) 2016/679 (General Data Protection Regulation, GDPR) tuli sovellettavaksi 25.5.2018. Asetus on suoraan sovellettavaa lainsäädäntöä. Sen tavoitteena on vahvistaa henkilötietojen suojaa, lisätä henkilötietojen käsittelyn läpinäkyvyyttä rekisteröidylle, joiden tietoja käsitellään, sekä antaa heille enemmän mahdollisuuksia hallita omien henkilötietojensa käsittelyä.

Digitalisaation edetessä tietosuojan merkitys korostuu. Tietosuoja-asetus pyrkii vastaamaan digitalisaation ja globalisaation mukanaan tuomiin tietosuojakysymyksiin ja -haasteisiin. Tietosuojalaki (1050/2018) tuli voimaan 1.1.2019. Se on henkilötietojen käsittelyyn sovellettava yleislaki, ja se täydentää sekä täsmentää

tietosuoja-asetuksen säännöksiä. Lisäksi henkilötietojen käsittelyä ohjaavat monet muut lait, kuten laki viranomaisen toiminnan julkisuudesta (621/1999, julkisuuslaki) ja erityislainsäädäntö.

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. **Organisatorisiin** toimenpiteisiin sisältyvät muun muassa koulutukset ja ohjeistukset, joita kaupungin henkilötietoja käsitteleville työntekijöille annetaan.

Naantalin kaupungin GDPR-vaatimustenmukaisuus on vahvistunut merkittävästi vuoden 2025 aikana. Alla olevasta kuvasta näkyy, että vaatimustenmukaisuuden taso oli keväällä 2025 noin 35–40 pisteen tasolla, ja kehitys on tuolloin ollut maltillista. Syksyyn 2025 mennessä taso nousi hieman yli 45 pisteen, mikä kuvastaa perusvaatimusten jäsentymistä ja toiminnan tasoittumista. Merkittävin parannus tapahtui alkuvuonna 2026, jolloin vaatimustenmukaisuuden toteutuminen lähti voimakkaaseen nousuun: helmikuussa indeksi hyppäsi noin 45 pisteestä lähes 80 pisteeseen, ja maaliskuussa taso saavutti asetetun tavoitetaso 80+.

Tämä kaikki kertoo siitä, että Naantalin kaupunki on systemaattisesti vahvistanut tietosuoja- ja tietoturvakäytäntöjään, päivittänyt prosessejaan sekä parantanut dokumentaatiota ja osoitusvelvollisuuden toteutumista. Nykytilassa Naantalin kaupunki täyttää jo hyvin GDPR-vaatimustenmukaisuuden kokonaisuuden ja kehityskaari osoittaa selvästi, että kaupunki on siirtynyt perusvaatimuksista kohti järjestelmällistä, kattavaa ja jatkuvasti paranevaa tietosuojan hallintamallia.



10.1. Henkilötietojen käsittelyä koskeva lainsäädäntö

Kaupungin työntekijät joutuvat käsittelemään henkilötietoja työssään monenlaisiin käyttötarkoituksiin. Suurin osa henkilötietojen käsittelystä kunnassa perustuu lakiin sekä yleistä etua koskevaan etuun tai

julkiseen valtaan. Laissa ei tarvitse suoraan sanoa, että henkilötietoja saa käsitellä, vaan kunnalla on tehtävään perustuva oikeus henkilötietojen käsittelyyn eli laissa määrätyn tehtävän hoitaminen edellyttää henkilötietojen käsittelyä.

10.2. Henkilötietojen käsittelyä koskevat koulutukset

Perusohjeistus tietosuojasta ja –turvasta toteutetaan Naantalin kaupungilla jatkuvana verkkokoulutuksena, joka uudistettiin kokonaan vuonna 2025. Kaikkien Naantalin kaupungin palveluksessa olevien tulee suorittaa tietosuojaan ja tietoturvaan liittyvät koulutuskokonaisuudet. Koulutukset uusitaan säännöllisesti. Verkkokoulutuksien suorittamista seurataan raportoinnilla esimiehille. Palvelualat perehdyttävät henkilötietoja käsittelevän henkilökuntansa tietosuoja-asetuksen mukaiseen toimintaan sekä valvovat sen noudattamista.

10.3. Henkilötietojen käsittelyä koskeva ohjeistus

Naantalin kaupungin tietosuojakäsikirja on laadittu sekä päivitetty ja se palvelee niin kuntalaisia kuin henkilöstöä. Palvelualat ohjeistavat henkilökuntaa tietojärjestelmiensä edellyttämien henkilötietojen käsittelyjen osalta.

Hallintopalveluissa on laadittu ohjeistus henkilötietojen käsittelystä kaupungin hallinnossa sekä julkaisemisesta toimielinten ja viranhaltijoiden päätöksissä ja päätösten julkaisemisessa avoimessa tietoverkossa. Asian käsittelyssä julkaistaan vain asian käsittelyn kannalta välttämättömät henkilötiedot ja henkilötiedot poistetaan muutoksenhakuajan jälkeen.

Maankäyttöosastolla on oma ohjeistus koskien kiinteistötietojärjestelmästä luovutettavia tietoja. Yksityishenkilönä olevan maanomistajan yhteystiedot saa luovuttaa vain lainhuutotodistuksella, jonka kaupungilta voi tilata vain omistaja itse. Muussa tapauksessa lainhuutotodistus on tilattava Maanmittauslaitoksesta. Yrityksen tai yhdistyksen yhteystiedot saadaan luovuttaa suoraan kaupungin järjestelmistä.

Rakennuslupien julkipanolistassa esitettävistä tiedoista on laadittu oma ohjeistus, jonka mukaan julkipanolistassa ilmoitetaan vain seuraavat tiedot: päätöspykälä, lupatunniste, kiinteistötunniste, osoite ja toimenpide.

11. Henkilötietojen tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti. Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

Rekisterinpitäjän on arvioitava, millainen riski tietoturvaloukkauksesta on aiheutunut vuodon kohteena olevalle henkilölle. Arvio määrittää tietoturvaloukkauksesta seuraavia toimenpiteitä. Tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetulle ja kohteena olevalle rekisteröidylle, mikäli loukkauksesta voi aiheutua riski luonnollisten henkilöiden vapauksille ja oikeuksille. Tietoturvaloukkausten varalta kaupungilla on menettelyohjeistus, ja käytössä on sähköinen kanava tietoturvaloukkauksista

ilmoittamiseksi. Dokumentoimme kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet.

Vuoden 2025 aikana sattui yksi henkilötietojen tietoturvaloukkaus, josta tehtiin ilmoitus tietosuojavaltuutetun toimistoon. Ilmoitus sekä tarvittavat toimenpiteet tehtiin viipymättä, minkä tuloksena loukkauksesta ei ehtinyt aiheutua haittaa rekisteröidyille. Tietosuojavaltuutetun toimisto katsoi, että ilmoitus ei antanut aihetta ryhtyä enempiin toimenpiteisiin, sillä rekisterinpitäjä oli toteuttanut kaikki mahdolliset tietoturvaloukkauksen edellyttämät toimenpiteet.

12. Valvontaviranomaisten selvitys- ja tietopyynnöt

Tietosuojavaltuutettu on Suomen kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Tietosuojavaltuutetun toimisto saattaa lähettää rekisterinpitäjille selvityspyyntöjä erilaisissa tilanteissa, joissa selvitetään henkilötietojen käsittelyn lainmukaisuutta, esimerkiksi tietoturvaloukkauksien yhteydessä. Vuonna 2025 tietosuojavaltuutetun toimistolta ei saapunut selvitys- tai tietopyyntöjä.

13. Tietosuojatyön kehittämistarpeet

Yksi tietotilinpäätöksen keskeisistä tehtävistä on nostaa esille ongelmakohtia ja kehittymisen paikkoja tietosuojatyössä.

Ajankohtaisia tietosuojatyön kehittämistarpeita:

1. Tekoälyn käytön lisääntyminen ja sen vaikutukset tietosuojaan:
tietosuojatyössä pitää entistä enemmän kiinnittää huomiota kehittämistarpeisiin, jotka keskittyvät tekoälyn hallintaan, sääntelyn monimutkaisuuteen ja teknisiin suojamenetelmiin.
Perusoikeusvaikutustenarviointi (FRIA) tulee tehdä EU:n tekoälyasetuksen mukaan ennen mahdollisten suuririskisten tekoälyjärjestelmien käyttöönottoa. Naantalissa kaupungilla on mahdollisuus tehdä FRIA-arviointia yhteistyössä Ilona IT: sovelluskirjaston kautta.
2. Lainsäädäntö- ja ohjeistusmuutosten huomioiminen Naantalissa kaupungin toiminnassa: tietosuojalainsäädännössä ja sen ohjeistuksessa on tapahtumassa merkittäviä muutoksia, jotka keskittyvät erityisesti kansalliseen sääntelyyn ja EU:n yleisen tietosuoja-asetuksen (GDPR) soveltamiseen tarkentamiseen. Muutosten tavoitteena on muun muassa selkeyttää henkilötietojen käsittelyä koskevaa sääntelyä ja edistää viranomaisen tiedon liikkuvuutta.

3. Riskienhallinta: jatketaan keskeisten ja kriittisten tietojärjestelmien ja sovellusympäristöjen osalta riskienhallintasuunnitelmien laatimista.
4. Ydintiedonhallinta-projektin edistäminen: kaupungin eri järjestelmissä (esim. taloushallinto, henkilöstöhallinto, asiakaspalvelu, tekninen toimi) on paljon päällekkäistä ja hajautunutta tietoa. Selvitetään kaupungin ydintieto, sen sijainti, hallinnointi ja integraatiot. Master Data Managementin (MDM) avulla luodaan yksi luotettava lähde keskeisille liiketoiminnan tietokokonaisuuksille, kuten asiakkaille, tuotteille ja sijainneille.