

Naantalin kaupungin

TIETOTILINPÄÄTÖS VUODELTA 2018

25.5.2019 Turo Järvinen ja Juha Riekkinen

[hyväksyntä KH 17.6.2019 § xxx]

1 TIE TOTILINPÄÄTÖKSEN TARKOITUS NAANTALIN KAUPUNGISSA.....	1
2 TIE TOVARANNOT	3
3 TIE TOJENKÄSITTELYN NYKYTILA.....	5
4 TIE TOSUOJAN JA TIE TOTURVAN TOTEUTUMINEN.. Virhe. Kirjanmerkkiä ei ole määritetty.	
5 TIE TOSUOJAN PROSESSIT JA VALVONTA.....	8
6 TIE TOSUOJAN JA -TURVAN KEHITTÄMISKOHTEET	8

1 TIETOTILINPÄÄTÖKSEN TARKOITUS NAANTALIN KAUPUNGISSA

Tässä tietotilinpäätöksessä kuvaamme keskeisiä toimenpiteitä, kuinka Naantalissa huolehdimme asiakkaidemme tiedosta ja yksityisyydestä. Tietotilinpäätöksen aikajana kulkee toukokuusta 2018 toukokuun loppuun 2019, sekä tulevaisuuden kehittämiseen ja painopisteisiin

EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 eteenpäin. Tietosuojalainsäädännön uudistuksella pyritään antamaan ihmisille enemmän oikeuksia omien tietojensa hallintaan. Samalla yhteisillä pelisäännöillä rakennetaan luottamusta digitaalisiin palveluihin, kun yrityksiltä vaaditaan enemmän läpinäkyvyyttä datan käsittelyyn. Yleinen tietosuoja-asetus koskee lähtökohtaisesti kaikenlaista henkilötietojen käsittelyä. Se sisältää säännökset rekisteröidyn oikeuksista sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Tietosuoja-asetuksen rinnalla sovelletaan kansallista tietosuojalakia, joka korvasi 1.1.2019 lukien aiemman henkilötietolain.

Tietosuoja-asetuksen painottama osoittamisvelvollisuus merkitsee kaupungin näkökulmasta aikaisempaa kattavampaa dokumentaatiota. Vaikka dokumentaation tuottaminen tarkoittaa lisätyötä, on siitä viime kädessä hyötyä asiakkaalle ja kaupungille itselleen, kun riskienhallinta ja suunnitelmallisuus korostuvat digitaalisia palveluita rakennettaessa.

Kaupungilla on oltava kokonaisvaltainen kuva sen hallussa olevista henkilötiedoista:

- Mitä, miten ja mihin tarkoitukseen henkilötietoja kerätään?
- Ovatko kaikki tiedot tarpeellisia?
- Mikä on oikeusperuste henkilötietojen käsittelylle?
- Kuinka henkilötietoja käsitellään ja säilytetään?
- Kuinka henkilötietojen käsittelyä valvotaan?
- Kuinka on hoidettu henkilötietojen luovutukset ja siirrot
- Mitä henkilötiedoille tapahtuu käyttötarkoituksen päättymisen jälkeen?
- Kuinka hyvin rekisteröidyn oikeudet toteutuvat?

1.1 Tietotilinpäätöksen tarkoitus

Jatkossa vuosittain laadittava Naantalın kaupungin 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.

Tietotilinpäätöksen koonnista vastaa tietosuojaryhmä. Tietotilinpäätöstä laatiessa on huomioitu tietosuojavaltuutetun toimiston ohjeistus sekä kunnan tietosuojavastaavan saama koulutus.

1.2 Organisaation kuvaus

Naantalın kaupungissa oli vuonna 2018 keskimäärin 1200 päätoimista työntekijää, joista vakituisia oli 970. Määräaikaisia työntekijöitä oli 251.

Kaupungin työntekijät joutuvat käsittelemään henkilötietoja työssään mm. tietojärjestelmissä ja henkilörekistereissä. Suurin osa henkilötietojen käsittelystä kunnassa perustuu lakiin sekä yleistä etua koskevaan etuun tai julkiseen valtaan.

Viimekädessä vastuu toiminnan lainmukaisuudesta sekä tietosuojan ja tietoturvan toteutumisesta on organisaation johdolla. Kaupungissa on nimettynä tietosuojatyöryhmä, joka omalta osaltaan valvoo tietosuojan toteutumista sekä kehittää tietosuojatyötä kunnassa.

Tietosuojavastaavan rooli korostuu tietosuojatyössä. Hän toimii mm. yhdyshenkilönä henkilötietojen käsittelijöille (kaupungin työntekijät), rekisteröidyille (kuntalaiset) ja valvontaviranomaiselle (tietosuojavaltuutettu). Tietosuojavastaavan tehtäviin kuuluu myös asiantuntijana ja tiedottajana toiminen, tietosuoja-asetuksen ja -lain noudattamisen valvominen sekä kouluttajana ja neuvonantajana toimiminen.

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

2 TIETOVARANNOT

2.1 Tietosuojaselosteet

Kaupungin tietovarannot koostuvat useista rekistereistä. Naantalissa on vuosina 2017 - 2018 aikana päivitetty selosteet henkilötietoja sisältävistä rekistereistä. Tietosuojaselosteet löytyvät kunnan verkkosivuilta ja ne on laadittu tietosuojavaltuutetun ohjeiden mukaan.

Tietosuojaselosteet ovat osa kunnan tiedottamisvelvollisuutta ja tietosuojaselosteesta käyvät ilmi henkilötietojen käsittelyn tarkoitus, rekisterin tietosisältö, tietolähteet, tietojen säilyttäminen ja rekisteröidyn oikeudet.

Tietosuojaselosteiden päivittäminen on rekisterinpitäjän vastuulla.

2.2 Henkilötietojen käsittely

2.2.1 Yleisiä käsitteitä

Henkilötiedon käsittelynä pidetään merkintää, jonka perusteella henkilö voidaan tunnistaa. Henkilö voidaan tunnistaa suoraan tai epäsuorasti eli myös tietoja yhdistämällä.

Henkilötietojen käsittelynä pidetään kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin, kuten henkilötietojen kerääminen, tallentaminen, käyttäminen, muuttaminen ja poistaminen. Henkilörekisteri on henkilötietoja sisältävä tietojoukko esim. paperinen nimilista tai asiakastietojen hallintaan käytettävä ohjelmisto. Kaupungilla on myös yhteisrekistereitä, jolloin samaa rekisteriä käyttävät palvelun tarjoaja ja palvelun tuottaja.

Tietosuoja-asetuksessa on määritelty erityiset henkilötiedot, joiden käsittely saattaa aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille. Kunnassa erityisiä tietoja käsitellään etenkin perusturvapalveluissa. Tietosuoja laki on määritellyt Suomessa lapsen iäksi 13 vuotta, jolloin alle 13 vuotiaan henkilötietoja ei saa käsitellä ilman huoltajan suostumusta.

2.2.2 Käsittelyperuste

Tietosuoja-asetuksessa on määritelty henkilötietojen käsittelyperusteet. Kunnassa henkilötietojen käsittely perustuu usein lakisääteisen velvoitteen noudattamiseen tai 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.

Rekistereiden käyttöoikeudet on määritelty työtehtävien mukaan. Henkilötietoja sisältävät asiakirjat ja manuaaliset rekisterit tulee säilyttää aina lukitussa tilassa. Tietokoneella olevat tiedostot ja tietojärjestelmät tulee säilyttää henkilökohtaisen käyttäjätunnuksen ja salasanan takana. Käyttäjätunnukset ja salasanat on pidettävä vain omana tietona. Salasanan turvallisuus tulee varmistaa. Henkilökohtaiset tunnukset mahdollistavat tarvittaessa lokitietojen tarkastamisen. Henkilöstöä on myös ohjeistettu lukitsemaan tietokone ja äylaitteet poistuttaessa niiden luota.

Henkilötietoja sisältävät paperit ja tiedostot tulee hävittää asianmukaisesti. Papereiden hävittämiseen tulee käyttää tietoturva-astiaa. Tiedostoja tietokoneelta poistaessa tulee huolehtia myös varmuuskopioiden poistaminen.

Viranhaltijat ja työntekijät, jotka käsittelevät työssään erityisiä henkilötietoja, allekirjoittavat salassapito- ja vaitiololupauksen.

3 TIETOJENKÄSITTELYN NYKYTILA KAUPUNGISSA

3.1 Lomakkeet ja asiakirjat

Kaupungilla on käytössään tarkastuspyyntö- ja korjaamisvaatimuslomakkeet rekisteröityjen oikeuksien tarkastamisen varmistamiseen.

3.2 Kuntalaisille tiedottaminen

Tietosuoja-asetuksen voimaan tultua on kaupungin verkkosivuille lisätty oma osionsa tietosuojasta. Sivuilta löytyvät tulostettavassa muodossa olevat rekisteröidyn tietopyyntölomake ja tietojen oikaisulomake sekä terveys- ja sosiaalipalvelujen lomakkeet.

Kaupungin sivuilta löytyvät myös tietoturva- ja suojapolitiikka.

3.3 Koulutukset ja tiedottaminen henkilöstölle

Tietosuojatyöryhmä osallistui valtakunnalliseen Taisto18-harjoitukseen, jossa harjoiteltiin kuvitteellista tietoturva- ja tietosuojamurtoa.

Henkilöstölle järjestetään koulutusta tietosuojaan ja tietoturvaan liittyvissä asioissa. Koulutus voi olla joko itse opiskeltavien materiaalien muodossa, kuten verkkokoulutus. Tietosuojaohjeet ja tietosuojakoulutusvideot ovat koko henkilöstön saatavilla intrasta.

4 TIETOSUOJAN JA TIETOTURVAN TOTEUTUMINEN

4.1 Organisaatio ja vastuut

Julkisen sektorin toimijoilla on velvollisuus nimetä tietosuojavastaava. Tietosuojavastaavan tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Tietosuojavastaavan tehtävänä on myös toimia yhteyshenkilönä sekä rekisteröidyille että valvontaviranomaisille henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaavan yhteystiedot on julkistettava ja ne on ilmoitettava valvontaviranomaiselle. Tietosuojavastaava ei kuitenkaan ole vastuussa henkilötietojen käsittelyn lain mukaisuudesta, vaan vastuu kuuluu edelleen organisaation johdolle. Sosiaali- ja terveydenhuollossa tietosuojavastaava on nimetty erikseen.

Kaupunginjohtaja on viranhaltijapäätöksellä 31.1.2017 § 10 määritellyt tietoturvapoliittikkaan ja – turvallisuuteen liittyvät vastuut ja roolit seuraavasti:

tietoturvapäällikkö	tietohallintopäällikkö Juha Riekkinen
turvallisuuspäällikkö	ei nimetä
tietosuojavastaava	kaupunginlakimies Turo Järvinen (kaupunkitasolla)
tietosuojavastaava	(soten osalta lakisäätäinen) Susanne Kekkonen
tietoturvavastaavat	ei nimetä erikseen. (Virastopäälliköt ovat vastuuhenkilöitä ja voivat tarvittaessa delegoida tehtävän vastuita alaspäin.)

Kaupunginhallitus on 20.2.2017 § 55 hyväksynyt Naantalın kaupungille tietoturvapoliitikan.

4.2 Tietosuojan ja tietoturvan ohjeistus

Tietoturvallisuus ja tietosuoja perustuvat lainsäädäntöön ja normiohjaukseen. Vastuu tietoturvalisuudesta ja siihen liittyvä osaaminen kuuluu omalta osaltaan jokaiselle organisaatiossa.

Tietosuojalla tarkoitetaan yksilön tietojen käsittelyä ja oikeutta yksityisyyteen omien henkilötietojenkäsittelyssä. Siihen sisältyy oikeudet tarkastaa ja korjata sekä vaatia poistettavaksi tarpeeton

tieto. Tietosuojan tarkoituksena on myös varmistaa yksilön perusoikeuksiensa säilyminen tietojen käsittelyn koko elinkaaren ajan.

Tietoturva on yksi tietosuojan toteuttamisen keino. Tietoturvallisuuden tarkoitus on suojata tietoa aineisto (sähköiset sekä paperiset) ja tietojärjestelmät. Tietoturvallisuuden tavoitteena on varmistaa, että tiedot ovat vain niiden käytössä, joilla on siihen oikeus (luottamuksellisuus), silloinkin he niitä tarvitsevat (käytettävyys) ja tieto on oikeassa muodossa eikä ole muuttunut hallitsemattomasti (eheys).

Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus on tärkeä osa perehdytystä; jokainen kaupungin työasemia käyttävä on ne hyväksynyt. Kaikki materiaalit ovat luettavissa intrassa. 4.3 Henkilötietoihin liittyvät tietopyynnot

Sosiaalitoimeen tuli vuonna 2018 kolmekymmentä (30) omien tietojen tarkastus- tai korjauspyyntöä.

Terveyspalveluihin tehtiin vuonna 2018 kahdeksan omien tietojen tarkastuspyyntöä, kaksitoista vainajan tietojen luovutus, viisi potilastietojen korjauspyyntöä sekä yhdeksän rekisteritietojen käsittelyn tarkastuspyyntöä. Muihin kaupungin toimintoihin kohdistuvia tietopyyntöjä ei tullut lainkaan.

5 TIETOSUOJAN PROSESSIT JA VALVONTA

5.1 Tietojen tarkistaminen, korjaaminen ja poistaminen

Rekisteröidyllä on oikeus nähdä omat tietonsa henkilörekistereissä ja oikeus virheellisten tietojen oikaisemiseen tai tietyissä tapauksissa poistamiseen. Pyyntö tulee aina esittää kirjallisesti ja omakätisesti allekirjoitettuna tai muutoin luotettavasti tunnistautumalla. Lomakkeita saa tulostettua kaupungin internetsivuilta.

5.2 Tietoturvaloukkaus

Tietoturvaloukkauksella tarkoitetaan tilanteita, joiden seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, luovutetaan luvattomasti, tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Rekisterinpitäjän tulee suojata henkilötiedot, mutta samalla laatia toimintaohjeet tietoturvaloukkaustilanteita varten.

Kaupungissa on laadittu ohjeistusta tietoturvaloukkauksia varten. Henkilötietoihin liittyvistä tietoturvaloukkauksista on ilmoitettava valvontaviranomaiselle 72 tunnin kuluessa loukkauksen ilmitulosta sekä lain edellyttämässä tilanteissa kyseiselle rekisteröidylle henkilölle. Tietosuoja vastaava tiedottaa tarvittaessa tietoturvaloukkauksesta kaupunginjohtajan johtoryhmää.

6 TIETOSUOJAN JA -TURVAN KEHITTÄMISKOHTEET

Henkilöstön tietosuoja ja tietoturvaa koskevien tietojen ylläpito on jatkuvaa työtä. Vuonna 2019 on käytössä uusi verkkopohjainen itseopiskeluohjelma.

Tavoitteena on tietoturva- ja suojaohjeistuksen kehittäminen selkeäksi kokonaisuudeksi.

Jatkossa hankinnoissa ja sopimuksissa joissa käsitellään henkilötietoja, tulee ottaa tietosuoja-asetus huomioon. Sopimusten liite koskien henkilötietojen käsittelyä tulee laatia erikseen.

Tietosuoja vastaavat osallistuvat vuoden aikana sopiviin koulutuksiin tietotason ylläpitämiseksi.

Verkostoitumista seudun tietosuoja vastaavien kanssa on syytä edistää esimerkiksi kehittämällä yhdessä oppimista sekä hyvien mallien jakoa.

Tavoitteena on tietosuoja- ja tietoturva-asioiden ajaminen sekä pitäminen osana kaikkien arki-työtä.