



Naantalin kaupunki

TIETOTILINPÄÄTÖS

25.5.2020 – 24.5.2021

10.6.2021 tietosuojavastaava Turo Järvinen ja tieturvapäällikkö Juha Riekkinen
[hyväksyntä KH 21.6.2021 § xx]

Sisällys

1. Tietosuojavastaavan katsaus.....	3
2. Tietotilinpäättöksen tarkoitus	3
3. Tietosuojaja-asioiden vastuunjako Naantalin kaupungilla.....	3
3.1. Kaupunginhallitus	4
3.2. Tietosuojavastaava	4
3.3. Tietosuojatyöryhmä.....	4
3.4. Tietosuojaa koskevat vastuut palvelualueilla.....	4
4. Rekisteröidyn oikeuksien toteuttaminen	4
4.1. Rekisteröidyn informointi	4
4.2. Rekisteriselosteet.....	4
4.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt	5
4.3.1. Tarkastuspyynnöt	5
4.3.2. Oikaisupyynnöt	5
4.3.3. Poistopyynnöt.....	6
4.3.4. Rajoittamisoikeus	6
4.3.5. Vastustamisoikeus	6
4.3.6. Riitauttamisoikeus	6
5. Selosteet käsittelytoimista	7
6. Tietoturva	7
7. Tietosuojaa koskevat vaikutustenarvioinnit	8
8. Käsiteltävät henkilötiedot ja niiden elinkaaren hallinta	8
9. Sopimukset ja hankinnat	8
9.1. Ennen tietosuojaja-asetuksen voimaantuloa tehdyt sopimukset	8
9.2. Tietosuojaja-asetuksen voimaantulon jälkeen tehdyt sopimukset ja hankinnat.....	9
10. Lainsäädäntö, koulutus ja ohjeistus.....	9
10.1. Henkilötietojen käsittelyä koskeva lainsäädäntö.....	9
10.2. Henkilötietojen käsittelyä koskevat koulutukset.....	9
10.3. Henkilötietojen käsittelyä koskeva ohjeistus	9
11. Henkilötietojen tietoturvaloukkaukset	9
12. Valvontaviranomaisten selvitys- ja tietopyynnöt.....	10
13. Tietosuojatyön kehittämistarpeet	10

1. Tietosuojavastaavan katsaus

Tällä tietotilinpäätöksellä osoitetaan, miten tietosuoja ja tietoturva ovat toteutuneet Naantalın kaupungin toiminnassa aikavälillä 25.5.2020-24.5.2021.

Tästä Naantalın kaupungin kolmannesta tietotilinpäätöksestä käy ilmi, että kaupunki on edelleen kehittänyt tietosuojatyötä muun muassa ulkopuolisen asiantuntijatahon suorittaman arvioinnin ja toimenpide-ehdotusten perusteella. Yhtenä toimenpiteenä on ollut alkuvuodesta 2021 uuden tietoturva- ja tietosuojaryhmän perustaminen, johon kuuluvat kaikkien toimialojen johdon edustajat tietohallinnon, riskien hallinnan, asianhallinnan ja tietosuojavastaavien lisäksi.

Tietosuojan ja tietoturvan vastuuhenkilöt sekä tietosuojatyöryhmä ovat kaikki osaavia ja sitoutuneita työhönsä. Kaupungilla on toimivat prosessit rekisteröidyn oikeuksiin liittyviin pyyntöihin ja tietoturvaloukkauksiin. Sopimuksissa ja hankinnoissa, joissa käsitellään henkilötietoja, kaupungilla on oma tietosuoja- ja salassapitoliite. Henkilöstöä koulutetaan kattavasti tietosuoja- ja turva-asioihin käyttöön otetulla uudella verkkopohjaisella itseopiskeluohjelmalla. Kaupungilla on tietosuojan intranet -sivut, joilta löytyy selkeä ohjeistus tietosuojakysymyksiin.

Tietoturvatyöryhmä yhdessä johdon kanssa osallistui TAISTO20 -tietoturva- ja -suojaharjoitukseen. Harjoitus simuloi hyökkäystä organisaation tietojärjestelmään ja tietosuojaloukkausta sekä organisaation toimintavalmiuksia poikkeaman johdosta ja selvittämiseksi.

Kaupungille on ajanjaksolla laadittu oma Tietosuojakäsikirja.

Tietosuojatyö on kaupungin asukkaita varten. Heillä on oikeus luottaa siihen, että kaupungilla käsitellään heidän henkilötietojaan lainsäädännön edellyttämien tavoin. Näin ollen on tärkeää, että Naantalın kaupunki panostaa jatkossakin tietosuojatyöhön sekä jatkaa hyvää linjaansa tässä työssä kehittämällä sitä kaudella ilmenneiden tarpeiden osalta.

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 Naantalın 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 Naantalın kaupungilla

Tietosuoja-asioiden vastuunjako on määritelty kaupungin tietosuojalinjauksissa.

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 (tietosuojavaltuutettu) kanssa ja rekisteröityjen (kuntalaiset) oikeuksien toteuttamisen tukeminen. Tietosuojavastaavan henkilötiedot on julkistettava ja ne on ilmoitettava valvontaviranomaisella. Naantalın kaupunkiin on nimetty vielä erikseen sosiaali- ja terveydenhuollon tietosuojavastaava.

3.3. Tietoturva- ja tietosuojaryhmä

Naantalın 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.

3.4. Tietosuojaa koskevat vastuut palvelualoilla

Palvelualojen johdolla on vastuu toiminnan lainmukaisuudesta henkilötietojen käsittelyssä. Lisäksi kuhunkin palvelualaan on nimetty tietosuojan vastuhenkilö, joka toimii yhteyshenkilönä oman organisaationsa ja tietosuojavastaavan välillä.

4. Rekisteröidyn oikeuksien toteuttaminen

4.1. Rekisteröidyn informointi

Naantalın kaupunki antaa rekisteröidylle tarvittavan informaation kaupungin internetsivuilla. Sivulla annetaan yleisinformaatiota henkilötietojen käsittelystä Naantalın kaupungilla sekä kerrotaan rekisteröidyn oikeuksista ja niiden toteuttamisesta. Lisäksi sivuilla on rekisteriselosteet, joissa kerrotaan henkilötietojen käsittelystä rekisterikohtaisesti. Sivulla kerrotaan myös Naantalın kaupungin tietosuojavastaavan ja Naantalın kaupungin sosiaali- ja terveystietojen tietosuojavastaavan yhteystiedot.

4.2. Rekisteriselosteet

Naantalın kaupunki kerää henkilötietoja eri rekistereihin tietojen käyttötarkoituksen mukaan. Kaikista Naantalın kaupungin rekistereistä on laadittu rekisteriselosteet, joista ilmenee seuraavat tiedot:

- rekisterin nimi
- rekisterinpitäjän ja tämän edustajan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- rekisterin tietosisältö
- tieto henkilötietojen säännönmukaisista luovutuksista
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- henkilötietojen tietolähteet

Rekisteriselosteet on julkaistu Naantalın kaupungin verkkosivuilla. Palvelualueiden tietosuojan vastuhenkilöt huolehtivat rekisteriselosteiden laadimisesta. Selosteet tehdään kaupungin rekisteriselostepohjalle. Rekisteriselosteet on laadittu tietosuojavaltuutetun ohjeiden mukaan. Rekisteriselosteiden päivittäminen on rekisterinpitäjän vastuulla.

4.3. Rekisteröidyn oikeuksiin liittyvät pyynnöt

Rekisteröidyillä on oikeuksia liittyen omiin henkilötietoihinsa ja niiden käsittelyyn. Rekisteröidyillä 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. Tarkastuspyynnöt

Rekisteröidyillä henkilöllä on oikeus pyytää Naantalın kaupungilta pääsy häntä itseään koskeviin henkilötietoihin. Rekisteröidyillä 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. Pyyntöä varten on laadittu lomake, joka löytyy Naantalın internetsivuilta

[Omien tietojen tarkastuspyyntö](#)

[Pyyntö vainajan tietojen luovuttamiseksi](#)

[Rekisteritietojen käsittelyn tarkastuspyyntö](#)

ja toimintayksiköstä. Asiakkaan henkilöllisyys varmennetaan ennen tietojen antamista.

Sosiaalitoimeen tuli ajanjaksolla 25.5.2020-24.5.2021 yhteensä 25 omien henkilötietojen tarkastuspyyntöä. Terveyspalveluihin tehtiin ajanjaksolla 131 omien tietojen tarkastuspyyntöä sekä 42 lokitietopyyntöä.

Terveyspalveluille tehtiin 22 tietojen korjauspyyntöä.

Sivistyspalveluihin omien henkilötietojen tarkastuspyyntöjä saapunut yksi.

4.3.2. Oikaisupyynnöt

Rekisteröidyllä henkilöllä on oikeus pyytää Naantalın kaupungilta häntä itseään koskevien epätarkkojen ja virheellisten henkilötietojen oikaisemista ilman aiheetonta viivytystä.

Pyyntöä varten on laadittu lomake, joka löytyy Naantalın internetsivuilta

[Potilasrekisteriin tallennetun tiedon korjausvaatimus](#)

ja toimintayksiköstä. Asiakkaan tulee pyynnössään yksilöidä ja perustella tarkasti, mitä tietoa vaaditaan korjattavaksi ja mikä on asiakkaan mielestä oikea tieto ja millä tavalla korjaus pyydetään tekemään. Asiakkaan henkilöllisyys varmennetaan ennen tietojen oikaisemista.

Terveyspalveluihin tehtiin ajanjaksolla 22 potilasrekisteriin tallennetun tiedon korjausvaatimusta, joista seitsemän johti korjaukseen.

4.3.3. Poistopyynnöt

Joissakin poikkeustapauksissa, esimerkiksi jos tietojen käsittely on perustunut henkilön suostumukseen ja henkilö peruuttaa suostumuksensa, henkilöllä on oikeus saada tietonsa poistetuiksi eli tulla unohdetuksi. Oikeutta tietojen poistamiseen ei ole, jos käsittely perustuu kaupungin lakisääteisen veloitteen noudattamiseen, liittyy yleistä etua koskevan tehtävän suorittamiseen tai kaupungille kuuluvan julkisen vallan käyttämiseen.

Henkilötietojen poistopyyntöjä raportoitiin sivistyspalveluista yksi.

4.3.4. Rajoittamisoikeus

Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty.

Henkilötietojen käsittelyn rajoittamispyyntöjä ei ole tullut kaupungille yhtään.

4.3.5. Vastustamisoikeus

Rekisteröidyllä henkilöllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Henkilötietojen käsittelyn vastustamisvaatimuksia ei raportoitu.

4.3.6. Riitauttamisoikeus

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.

Kaupungille ei ole tullut yhtäkään yhteydenottoa koskien automaattiseen henkilötietojen käsittelyyn perustuvan päätöksen kohteeksi joutumista.

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

Palvelualueiden tietosuojan vastuuhenkilöt laativat selosteet käsittelytoimista hyödyntäen kaupungin mallipohjaa ja erillistä ohjetta. Tietosuojavastaavan tulee tarkastaa selosteet.

6. Tietoturva

Tietoturva liittyy läheisesti tietosuojaan. 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.

Naantalissa 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 Naantalissa kaupungille tietoturvapoliittikan.

7. Tietosuojaa koskevat vaikutustenarvioinnit

Tietosuojaa 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.

8. Käsiteltävät henkilötiedot ja niiden elinkaaren hallinta

Henkilötietojen elinkaaren hallinnalla pyritään varmistamaan, että henkilötietoja käsitellään vain niissä tarkoituksissa, jotka on määritelty rekisteriselosteessa (käyttötarkoitussidonnaisuus). Lisäksi pyritään huolehtimaan siitä, että henkilötiedot poistetaan ja asiakirjat hävitetään sen jälkeen, kun määritelty säilytysaika on päättynyt.

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 tietosuojaa koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia.

9.1. Ennen tietosuoja-asetuksen voimaantuloa tehdyt sopimukset

Palvelualat ovat selvittäneet sopimuksia, joiden perusteella joku toinen toimija (kuten palveluntuottaja) käsittelee henkilötietoja kaupungin lukuun. Kartoitustyö keskittyi tietosuoja-asetuksen voimaan tullessa jo olemassa oleviin sopimuksiin.

Sopimusten kartoitustyö on valmis ja sopimukset käydään jatkossa läpi muutaman vuoden välein.

9.2. Tietosuoja-asetuksen voimaantulon jälkeen tehdyt sopimukset ja hankinnat

Rekisterinpitäjän ja käsittelijän välisiin sopimuksiin ja hankintoihin on laadittu erillinen tietosuoja- ja salassapitoliite, jossa on määritelty henkilötietojen käsittelyn edellytykset. Lähtökohtaisesti Naantalın kaupungin kaikkiin uusiin sopimuksiin ja hankintoihin, joiden perusteella käsittelijä käsittelee henkilötietoja kaupungin lukuun, käytetään mallin mukaista liitettä.

10. Lainsäädäntö, koulutus ja ohjeistus

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.

10.1. Henkilötietojen käsittelyä koskeva lainsäädäntö

Kaupungin työntekijät joutuvat käsittelemään henkilötietoja työssään muun muassa tietojärjestelmissä ja henkilörekistereissä. 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. Kaikkien Naantalin kaupungin palveluksessa olevien tulee suorittaa tietosuojaan ja tietoturvaan liittyvät koulutusosiot. Koulutukset uusitaan säännöllisesti. Verkkokoulutuksien suorittamista seurataan raportoinnilla esimiehille. Palvelualat perehdyttävät henkilötietoja käsittelevän henkilökuntansa tietosuojasetuksen mukaiseen toimintaan sekä valvovat sen noudattamista.

10.3. Henkilötietojen käsittelyä koskeva ohjeistus

Tietosuojakäsikirja on laadittu 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.

Terveyspalveluissa on omaa ohjeistusta potilastietojen käsittelystä ja luovuttamisesta.

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 julkipanelistassa esitettävistä tiedoista on oma ohje. Sen mukaan julkipanelistassa 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.

Tietoturvaloukkausten varalta kaupungilla on valmisteltu menettelyohjeistus, ja käytössä on tietojärjestelmä tietoturvaloukkauksista ilmoittamiseksi.

Raportoituja tietoturvaloukkauksia oli hallintopalveluissa kaksi ja terveyspalveluissa kaksi. Hallintopalvelujen tapauksissa oli kyse kokousasiakirjoissa olevien henkilötietojen julkaisemisesta kaupungin verkkosivuilla. Henkilötiedot poistettiin verkkosivuilta viipymättä asian ilmi tultua ja loukkauksista tehtiin ilmoitukset asianosaisille henkilöille sekä tietosuojavaltuutetun toimistolle.

Terveyspalvelujen tapauksessa on kyse ollut väärän asiakkaan tietoihin kohdistuneesta kirjauksesta, joka on korjattu ja ilmoitettu asiakkaalle, mikäli tiedoissa on ollut jokin sellainen tieto, josta toinen henkilö olisi voinut tunnistaa hänet Omakannasta väärää tietoa lukiessa.

12. Valvontaviranomaisten selvitys- ja tietopyynnöt

Tietosuojavaltuutettu on Suomen kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Tietosuojavaltuutetun toimisto saattaa lähettää rekisterinpitäjille selvityspyyntöjä esimerkiksi tilanteissa, joissa tietosuojavaltuutetun toimistolle on ilmoitettu tietoturvaloukkauksesta ja siitä tarvitaan selvennystä.

Tietosuojavaltuutetun toimistolta ei ole saapunut selvitys- tai tietopyyntöjä.

13. Tietosuojatyön kehittämistarpeet

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

Jo edellisellä kaudella 2019 kehittämiskohteina nousi esiin seuraavaa:

1. Tarkentaa ja päättää tietoturvatyön organisoimisesta, ohjaamisesta, vastuista ja tehtävistä koko kaupunkikonsernin osalta.
2. Päätetään tietoturva-asioiden sisäisestä auditoinnista sekä tietoturvan ja tietosuojan osalta vuosiraportoinnista.
3. Varmistetaan vuosittain riittävän tietoturvakoulutuksen tarjoamisesta kaupungin henkilökunnalle sekä uuden työntekijän perehdytyksessä.
4. Keskeisten ja kriittisten tietojärjestelmien ja sovellusympäristöjen osalta riskienhallintasuunnitelmien laatiminen.
5. Varmistetaan, että kaikki kaupungin palvelusopimuskumppanit sitoutuvat noudattamaan palvelutoiminnassaan EU-tietosuoja-asetuksen tietoturva- ja tietosuojavaatimuksia.
6. Päivitetään kuntalaisten informointia tietosuoja-asioitten osalta. Korvataan nykyiset rekisteriselosteet tietosuojaselosteilla kaupungin www-sivulle.

Yllä mainittujen kehittämiskohteiden osalta on ryhdytty tai jo tehty toimenpiteitä tarkastelukaudella ja työtä jatketaan edelleen tulevalla kaudella.