

VANTAAN KAUPUNGIN TIETOTILINPÄÄTÖS

2019



Vantaa
Vanda

SISÄLLYSLUETTELO

JOHDANTO.....	3
TIETOSUOJAVASTAAVAN RAPORTTI VUODELTA 2019	5
TOIMIALOJEN JA PALVELUALUEIDEN RAPORTIT.....	13
Sosiaali- ja terveydenhuollon toimiala.....	13
Sivistystoimen toimiala	14
Maankäytön, ympäristön ja rakentamisen toimiala.....	16
Kaupunginjohtajan toimiala.....	16
Taloussuunnittelu	16
Elinkeinopalvelut	17
Kaupunginkanslia.....	17
Sisäinen tarkastus.....	18
Viestintä	19
Henkilöstökeskus	19
Konserni- ja asukaspalveluiden toimiala	20
Asukaspalvelut.....	20
Hankintakeskus.....	21
Tietohallinto.....	21
Vantaan työterveys liikelaitos.....	22
TIETOTILINPÄÄTÖKSEN LIITTEET	24
Liite 1: Vuoden 2019 tietotilin päätöksen rakenne.....	24
Liite 2: Vantaan kaupungin henkilötietojen tietoturvaloukkaukset 2019 toimialoittain	25

JOHDANTO

Vantaan kaupungin ensimmäinen tietotilinpäätös tehtiin vuodelta 2018. Ensimmäisessä tietotilinpäätöksessä kuvattiin henkilötietojen käsittelyä kaupungissa ja sitä, miten EU:n yleisen tietosuoja-asetuksen soveltaminen kaupungissa käynnistyi. EU:n yleistä tietosuoja-asetusta alettiin soveltaa EU:n jäsenmaissa 25.5.2018. Kaupunginhallituksessa ensimmäinen tietotilinpäätös käsiteltiin 29.4.2019.

Vuoden 2019 tietotilinpäätöksessä on nostettu erityisesti esiin kaksi tärkeää asiaa, *vaikutustenarvioinnit* ja *tietoturvaloukkaukset*. Toimialojen raportit rakentuvat seuraavien asiakokonaisuuksien ympärille:

- Tietosuoja toimialalla/tulosalueella vuonna 2019
- Alkukartoitus ja vaikutustenarvioinnit
- Tietoturvaloukkaukset
- Ohjeistukset

Vaikutustenarvioinnit ovat tietosuojan sisäänrakentamisen kannalta ensiarvoisen tärkeässä asemassa. Ne ovat pohja sille, että kaikissa prosesseissa tietosuoja tulee otettua huomioon ja toiminta on lainmukaista. Vaikutustenarvioinnit ovat pakollinen toimenpide, jota EU:n tietosuoja-asetus edellyttää. Niiden tekemättä jättäminen on lainvastaista ja rangaistavaa.

Tietoturvaloukkaukset ovat seurausta siitä, että kaikilta osin ei ole toimittu oikein. Pääasiallisesti on kyse yksittäisen työntekijän *tahattomasta virheestä* eli on toimittu huolimattomasti. Tämän tyyppisiä tietoturvaloukkauksia voidaan vähentää yleisellä tietosuojakoulutuksella ja tietosuojaosaamista lisäämällä.

Toinen pääasiallinen tietoturvaloukkausten tyyppi on *rakenteellinen tietoturvaloukkaus*. Rakenteellisia tietoturvaloukkauksia ovat esimerkiksi järjestelmät, jotka on otettu käyttöön ilman, että niiden tietosuoja on selvitetty kunnolla tai järjestelmään liittyviä tietojenkäsittelyprosesseja ei ole suunniteltu loppuun asti tietosuojan näkökulmasta. Tällöin on kyseessä koko ajan päällä oleva tietoturvaloukkaus, ja tietoturvaloukkausten määrä voi olla tällöin huomattava. Vaikutustenarvioinnit ovat ensisijainen työkalu tämänkaltaisten tietoturvaloukkausten eliminoimiseen.

Vakavia seurauksia aiheuttavat *ulkopuolisen tahon tekemät tietoturvaloukkaukset*. Ulkopuolisen tahon tekemissä tietoturvaloukkauksissa tietoja hakkeroidaan, järjestelmään pääsee haittaohjelma tai järjestelmä joutuu kyberhyökkäyksen kohteeksi. Vantaan kaupunki on tähän asti onnistunut torjumaan suurimittaiset hyökkäykset.

Jotta jatkossa tähän myös pystyttäisiin, tulee tietoturvan tasoon panostaa. Parantamalla kaupungin tietoturvan tasoa ja ennakoimalla uhkia kaupunki voi merkittävästi laskea riskiä joutua hyökkäyksen kohteeksi ja estää sellaisen onnistumisen.

Tietosuojavastaavan vuosittainen kokonaiskatsaus keskittyy neljään tietosuojan sisänrakentamisen kannalta kriittiseen kysymykseen: tietosuojakoulutukset, tietosuojatyöryhmät, vaikutustenarvioinnit ja tietoturvaloukkaukset.

Tämän julkaistavan version lisäksi tietotilinpäätyksestä on laadittu laajempi ja perusteellisempi versio, jonka saa nähtäväksi pyydettäessä.

TIETOSUOJAVASTAAVAN RAPORTTI VUODELTA 2019

EU:n yleistä tietosuoja-asetusta alettiin soveltaa kaikissa EU:n jäsenmaissa 25.5.2018. EU:n tietosuoja-asetusta täydentävää kansallista tietosuojalakia alettiin soveltaa 1.1.2019. Vuosi 2019 on ollut siten myös merkittävä tietosuojalainsäädännön uudistamisen kannalta. Se on ollut ensimmäinen vuosi, jolloin sekä EU:n tietosuoja-asetus että kansallinen tietosuojalainsäädäntö on ollut sovellettavana.

Vantaan kaupungissa tietosuojalainsäädännön asettamien velvollisuuksien sisäänrakentaminen kaupungin prosesseihin on käynnissä, ja kaupungissa ollaan menossa kohti entistä parempia tietosuojakäytänteitä. Tietosuojan sisäänrakentaminen kaikkiin prosesseihin vaatii paljon työtä ja resursseja, jotta Vantaan kaupunki pysyisi kuntien kärkipäässä hyvin hoidetussa henkilötietojen käsittelyssä ja suojauksessa.

Raportissa on nostettu esille neljä kokonaisuutta, jotka ovat tietosuojan sisäänrakentamisen kannalta välttämättömiä: tietosuojakoulutukset, tietosuojatyöryhmät, vaikutustenarvioinnit ja tietoturvaloukkaukset. Tietosuojaosaamista kasvattamalla ja vaikutustenarviointeja tekemällä saadaan minimoitua tietojenkäsittelyyn liittyvät riskit ja näin tietoturvaloukkauksien määrä vähenee.

TIETOSUOJAKOULUTUKSET

Vuoden 2019 tietosuojakoulutus kaupungin henkilöstölle järjestettiin valtuustosalissa kaupungintalolla 20.11.2019. Koulutus videoitiin, ja materiaali on katsottavissa tallenteena kaupungin omilta intrasivuilta. Esiemiesten on suositeltu varaavan alaisilleen aikaa tallenteen katsomiseen. Näin lisätään yhdeltä osin työntekijöiden tietoisuutta henkilötietojen käsittelystä ja siihen liittyvistä uhkatekijöistä. Vuoden 2020 syksyllä on tarkoitus saada toteutettua koko kaupungin henkilökuntaa koskeva tietosuojatesti, jonka jokainen henkilötietoja käsittelevä kaupungin työntekijä olisi velvollinen suorittamaan hyväksytysti.

TIETOSUOJATYÖRYHMÄT

Kaupungin tietoturva- ja tietosuojatyöryhmän tehtävänä on valmistella kaupunkia koskevia tietoturvaan ja tietosuojaan liittyviä ohjeita sekä antaa suosituksia ja kannanottoja edellä mainituista asioista. Kaupungin tietosuojavastaava toimii ryhmän

puheenjohtajana, ja kaupunginjohtaja nimeää työryhmän jäseniksi toimialojen edustajat. Vuonna 2019 tietoturva- ja tietosuojatyöryhmä kokoontui 10 kertaa.

Tietosuojan jalkauttamisessa ja sisäänrakentamisessa toimialojen ja palvelualueiden tietosuojavastuuhenkilöt ovat keskeisessä asemassa. Heidän tehtävänä on jalkauttaa tietosuojaa koskeva ohjeistus ja tietosuojatyöryhmässä sovitut käytänteet oman toimialansa/palvelualueensa prosesseihin. Ilman heidän aktiivista panostaan ja puuttumista epäkohtiin ei tietosuojaa saada sisäänrakennettua toimialan/palvelualueen prosesseihin. Osalla tietosuojavastuuhenkilöitä tietosuoja on sisällytetty heidän työtehtäviinsä. Tietosuoja tulisi sisällyttää kaikkien vastuuhenkilöiden työtehtäviin, ja ennen kaikkea varata riittävästi aikaa tehtävän suorittamiseen.

Pääkaupunkiseudun tietosuojatyöryhmään kuuluvat Vantaan, Helsingin, Espoon ja Kelan tietosuojavastaavat. Työryhmässä käsitellään kaupunkeja ja Kelaa koskevia tietosuoja-asioita. Asioiden yhdessä käsittelemisestä saadaan paljon hyötyä, koska kaikkia kaupunkeja koskevat samat säännöt ja velvollisuudet. Resursseja säästyy ja lainsäädännön tulkinnat ja linjaukset pystytään pitämään yhtenäisinä. Vuonna 2019 työryhmä kokoontui 7 kertaa.

TIETOSUOJAN VAIKUTUSTENARVIOINNIT

Mikä on tietosuojan vaikutustenarviointi?

Tietosuojan vaikutustenarviointi on EU:n yleisen tietosuoja-asetuksen mukainen pakollinen toimenpide, jolla arvioidaan suunnitellun käsittelytoimen vaikutuksia henkilötietojen suojalle. Vaikutustenarvioinnilla pyritään tunnistamaan, arvioimaan, vähentämään ja hallitsemaan henkilötietojen käsittelyyn liittyviä riskejä. Kyse on eräänlaisesta itsearviointityökalusta henkilötietojen käsittelyyn liittyvien riskien hallitsemiseksi.

Vaikutustenarvioinnin tarkoituksena on:

- Kuvata henkilötietojen käsittelyä
- Arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta
- Arvioida käsittelyn riskejä
- Määritellä toimenpiteet riskien hallintaan.

Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa. Vaikutustenarviointi on keskeinen työkalu EU:n tietosuoja-asetuksen mukaisen osoitusvelvollisuuden toteen näyttämässä.

Vaikutustenarviointi on tehtävä myös käsittelytoimille, jotka on jo aloitettu ennen tietosuoja-asetuksen soveltamista, jos kyseisiin käsittelytoimiin on asetuksen mukaan tehtävä vaikutustenarviointi.

Mitä hyötyä tietosuojan vaikutustenarvioinnista on?

Vaikutustenarviointien tekeminen *edistää tietosuojaa*. Kaikkien henkilötietoja käsittelevien on tiedettävä mitä henkilötietoja he käsittelevät, miten henkilötietoja tulee käsitellä, minne henkilötietoja saa tallentaa ja miten niitä voidaan luovuttaa tietoihin oikeutetuille. Tulevien virheiden määrää pystytään vaikutustenarvioinnin avulla huomattavasti vähentämään.

Vaikutustenarviointien tekeminen *kasvattaa luottamusta* henkilötietojen käsittelyyn. Kuntalaiset ja henkilökunta voivat luottaa siihen, että tietoja käsitellään lainmukaisesti ja vain siinä määrin kuin se kulloinkin on tarpeellista.

Vaikutustenarviointi on tärkeä väline *tietojen elinkaaren hallintaan*. Tiedämme, mitä henkilötietoja eri prosesseissa käsitellään, kun asiat on heti alussa dokumentoitu.

Vaikutustenarvioinnin ottaminen mukaan kaikkiin prosesseihin heti alkuvaiheessa tuo *kustannussäästöjä*. Puutteiden varhainen korjaaminen on kustannuksiltaan huomattavasti edullisempaa kuin jälkikäteinen korjaaminen

Kuka vastaa tietosuojan vaikutustenarvioinnin tekemisestä?

Rekisterinpitäjän (Vantaan kaupunki) tehtävänä on tietosuoja-asetuksen mukaan varmistaa, että vaikutustenarviointi on tehty. Tietosuojan vastuut on määritelty kaupungin hallintosäännössä. Hallintosäännön mukaan apulaiskaupunginjohtaja vastaa toimialan tietosuojasta ja tulosaluejohtaja tulosalueen tietosuojasta. Vaikutustenarvioinnit kuuluvat yhtenä osana hallintosäännön mukaisiin tietosuojavastuisiin. Vuoden 2020 alusta voimaan tullut uusi hallintosääntö ei tuonut muutosta tietosuojaa koskeviin vastuisiin muuten kuin että tulosaluejohtajien vastuu on siirtynyt 1.1.2020 alkaen palvelualuejohtajille.

Resurssit vaikutustenarvioinnin tekemiseen

Vaikutustenarvioinnit vaativat paljon resursseja. Tietoturva- ja tietosuojapolitiikassa on määritelty resurssien järjestämisestä. Poliitiikan mukaan apulaiskaupunginjohtajien tulee huolehtia riittävästä tietoturvan ja tietosuojan resursoinnista toimialallaan, ja tulosalueiden johtajat (mukaan lukien liikelaitokset) ja tulosyksiköiden

päälliköt ovat vastuussa tietoturvasta ja tietosuojasta oman tulosalueensa ja tulosyksikkönsä osalta. Johtajien ja päälliköiden tulee järjestää riittävä resursointi tietoturvan ja tietosuojan toteutumiseksi omassa yksikössään.

Jokaisella hankkeella tai prosessilla tulee olla omistaja ja vastuhenkilö, jonka tehtävänä on viedä hanketta tai prosessia eteenpäin. Hänen tehtävänsä on huolehtia myös tietosuojan huomioimisesta kyseisessä hankkeessa tai prosessissa. Vaikutustenarviointi on työkalu, jolla hankkeen tai prosessin tietosuojaa arvioidaan ja hallitaan.

Toimialoille on nimetty tietosuojan vastuhenkilöt, joiden tehtävänä on ohjata ja avustaa vaikutustenarviointien tekemisessä. Kaupungin tietosuojavastaava toimii toimialojen tietosuojasta vastaavien henkilöiden apuna.

Milloin vaikutustenarviointi tulee tehdä?

Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun on luultavaa, että käsittelystä seuraa yksilöiden oikeuksiin ja vapauksiin liittyvä korkea riski.

Vaikutustenarviointi on tehtävä:

- Tietosuoja-asetuksessa yksilöidyissä käsittelytilanteissa
- Tietosuojaviranomaisen luetteloimissa käsittelytilanteissa
- Kansallisen lainsäädännön määrittämässä tilanteissa (asetuksen salliman kansallisen liikkumavaran puitteissa).

Vaikutustenarviointi on erittäin käyttökelpoinen työkalu myös muissa kuin pakollisissa tilanteissa. Henkilötietojen käsittelyyn sisältyy aina riskejä, ja riskit on syytä arvioida ja käydä systemaattisesti läpi ja miettiä asiaankuuluvat riskienhallintakeinot.

Vaikutustenarviointi tulee sisällyttää prosessiin mahdollisimman aikaisessa vaiheessa ja tehdä sitä prosessin edetessä. Näin helpottuu riskienhallintakeinojen sekä tietosuoja-asetuksen mukaisten sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden noudattaminen. Samoin saadaan minimoitua taloudelliset kustannukset.

Vaikutustenarviointi ei ole kertaluontoinen tehtävä, vaan jatkuva riskien tunnistamisen ja hallitsemisen prosessi. Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista ja sitä on päivitettävä aina kun riskit, prosessit, toiminta tai tekniikka muuttuu.

Milloin vaikutustenarviointia ei tarvitse tehdä?

Vaikutustenarviointia ei tarvitse tehdä, jos katsotaan, että henkilötietojen käsittely ei todennäköisesti aiheuta luonnollisen henkilön oikeuksien ja vapauksien kannalta korkeaa riskiä tai samankaltaisesta käsittelystä on jo tehty vaikutustenarviointi.

Vantaan kaupunki käsittelee asiakkaiden ja henkilöstön henkilötietoja laajamittaisesti. Erityisesti sosiaali- ja terveydenhuollon sekä kasvatuksen ja opetuksen toimialoilla käsitellään asiakkaiden erityisen arkaluontoisia henkilötietoja. Kyseisillä toimialoilla vaikutustenarviointi tulee tehdä käytännössä kaikissa henkilötietojen käsittelyprosesseissa ja hankkeissa. Samoin henkilöstöpalvelut käsittelee kaupungin työntekijöiden henkilötietoja, joihin sisältyy erityisen arkaluontoisia henkilötietoja, jolloin myös vaikutustenarvioinnin pakollisuuden kriteerit täyttyvät käytännössä aina.

Vaikutustenarvioinnin tekemisen laiminlyönti

Vaikutustenarvioinnin tekeminen on siis pakollista, kun lainsäädännössä määritellyt kriteerit täyttyvät. Valtaosassa kaupungin eri prosesseissa nämä edellytykset täyttyvät. Mikäli vaikutustenarviointia ei ole tehty silloin kun se olisi tullut tehdä, on laiminlyöty lainsäädännön asettamat velvollisuudet.

EU:n tietosuoja-asetuksen mukaisia hallinnollisia sakkoja ei Suomen lainsäädännön mukaan voida määrätä julkishallinnolle. Vaikutustenarvioinnin laiminlyömisestä seuraamukset menevät yleisen virkavastuun mukaisesti. Viranomaisia sitoo hallinnon lainmukaisuusperiaate, ja lainmukainen henkilötietojen käsittely kuuluu viranomaisissa työskentelevien virkavelvollisuuksiin.

Virkamiehen asemaan kuuluu myös rikosoikeudellinen virkavastuu, kurinpidollinen virkavastuu sekä vahingonkorvausvastuu. Lisäksi viranomaisen toiminnasta voidaan kannella, ja laillisuusvalvojat valvovat viranomaisten ja virkamiesten toiminnan lainmukaisuutta.

Vaikutustenarvioinnin ohjeistus kaupungissa

EU:n tietosuoja-asetusta alettiin soveltaa 25.5.2018. Vaikutustenarviointeja on Vantaalla tehty EU:n tietosuoja-asetuksen soveltamisesta alkaen. Ohjeistusta on tehty paloissa, ja käytäntöjä hiottu asetuksen soveltamisen alkamisesta lähtien.

Laajan ja kattavan vaikutustenarviointiohjeistuksen valmistelu aloitettiin vuonna 2019. Ohjeistusta valmisteltiin toimialojen tietosuojavastuuhenkilöistä koostuvassa pienryhmässä. Kaupungin tietoturva- ja tietosuojatyöryhmässä ohjeistusta käsiteltiin

4 kertaa. Ohjeistuksen valmistuttua toimialojen ja tulosalueiden tietosuojavastuuhenkilöille järjestettiin työpaja, jossa ohjeistusta käytiin läpi. Tietosuojavastuuhenkilöt ovat avainasemassa ohjeistuksen jalkauttamisessa käytäntöön. Kaupungin johtoryhmässä ohjeistus käsiteltiin ja hyväksyttiin 20.10.2019.

Vaikutustenarviointien käynnistyminen Vantaalla

Tietosuojan sisäänrakentaminen kaikkiin kaupungin prosesseihin, joissa käsitellään henkilötietoja, on iso ja jatkuva prosessi. Vaikutustenarviointit ovat tietosuojan sisäänrakentamisessa avainasemassa. Vuonna 2019 kaupungissa ollaan vielä vaikutustenarviointien sisäänrakentamisen alkuvaiheessa. Prosessi on kuitenkin lähtenyt hyvin liikkeelle, ja tietoisuus vaikutustenarvioinnin pakollisuudesta ja tärkeydestä on pääasiallisesti ymmärretty ja tiedostettu sekä johdon että vaikutustenarviointiprosessiin osallistuvien työntekijöiden keskuudessa.

Suurin ongelma vaikutustenarviointien käynnistymisessä on epäselvyys prosessin omistajuudesta. Prosessille tulee löytää omistaja, joka vastaa siitä, että myös tietosuoja huomioidaan prosessissa. Tietosuojan osalta vastuut menevät kuten muutkin prosessin vastuut. Prosessin omistajan tehtävänä on järjestää vaikutustenarviointiin liittyvät kokoukset ja työpajat. Prosessin omistaja tuntee myös parhaiten asiantuntijat, joita kokouksissa ja työpajoissa tarvitaan. Toimialojen/palvelualueiden tietosuojavastuuhenkilöt ohjaavat vaikutustenarviointiprosessia.

Ennakkokuuleminen

Jos tietosuojan vaikutustenarviointi osoittaa, että henkilötietojen käsittelystä aiheutuu korkea riski rekisteröidylle, eikä rekisterinpitäjä saa omilla toimenpiteillään riskiä pienemmäksi, tulee tietosuojaviranomaista kuulla ennen käsittelyn aloittamista. Tällainen tilanne voi olla esimerkiksi silloin, kun riskinä on, että rekisteröity voi joutua kärsimään huomattavasta tai peruuttamattomasta seurauksesta.

Ennakkokuulemisessa tietosuojaviranomainen (tietosuojavaltuutettu) antaa kirjalliset ohjeet toimenpiteistä, joihin tulee ryhtyä riskin alentamiseksi. Rekisterinpitäjän tulee toteuttaa kyseiset toimenpiteet, jotta henkilötietojen käsittely olisi laillista.

TIETOTURVALOUKKAUKSET

Milloin on kyseessä henkilötietojen tietoturvaloukkaus?

Henkilötietojen tietoturvaloukkauksesta on säädetty EU:n yleisessä tietosuojasetuksessa. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka luvaton pääsy tietoihin. Henkilötietojen tietoturvaloukkaus voi olla tahallinen tai se voi myös johtua huolimattomasta tietojenkäsittelystä.

Mitä vaikutuksia tietoturvaloukkauksella voi olla sen kohteeksi joutuneelle?

Tietoturvaloukkaus voi aiheuttaa sen kohteeksi joutuneelle fyysisiä, aineellisia tai aineettomia vahinkoja. Kiireessä ja huolimattomuudessa tehty virhe voi johtaa yksittäisen henkilön kohdalla vakaviin seurauksiin. Tämän vuoksi henkilötietojen huolelliseen käsittelyyn täytyy kiinnittää erityistä huomiota.

Tietoturvaloukkauksen kohteeksi joutuneelle ilmoittaminen

Henkilötietojen loukkauksen kohteeksi joutuneille tulee ilmoittaa tietoturvaloukkauksesta mahdollisimman nopeasti, mikäli loukkaus aiheuttaa *korkean riskin* rekisteröidyn oikeuksille tai vapauksille.

Ilmoitus tietosuojavaltuutetulle

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta *voi aiheutua riski* luonnollisten henkilöiden oikeuksille ja vapauksille. Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto.

Palveluntuottajan tietoturvaloukkaus

Palveluntuottajan (henkilötietojen käsittelijä) tulee ilmoittaa tietoturvaloukkauksesta ensin rekisterinpitäjälle (Vantaan kaupunki), jollei ole erikseen sovittu, että palveluntuottaja voi ilmoittaa tietoturvaloukkauksista suoraan tietosuojavaltuutetun toimistolle. Vastuu ilmoituksen tekemisestä säilyy kuitenkin Vantaan kaupungilla.

Kaupungin ohjeistus tietoturvaloukkauksiin

Kaupungin on rekisterinpitäjänä suojattava henkilötiedot siten, että riski tietoturvaloukkauksille olisi mahdollisimman pieni. Tämän lisäksi on kuitenkin varauduttava mahdollisiin tietoturvaloukkauksiin laatimalla ohjeet tietoturvaloukkaustilanteita

varten. Kaupungissa on laadittu ohjeistus tietoturvaloukkauksien havaitsemiseen ja toimimiseen tietoturvaloukkauksen tapahduttua.

Kaupungissa tapahtuneet tietoturvaloukkaukset vuonna 2019

Kaupungissa tehtiin vuonna 2019 tietoturvaloukkaus ilmoituksia yhteensä 154 kertaa. Ilmoituksista suurin osa on tapahtunut sosiaali- ja terveydenhuollon toimialalla. Käsiteltävien henkilötietojen määrä on sosiaali- ja terveydenhuollon toimialalla ylivoimaisesti suurin, kuten myös henkilötietoja käsittelevien työntekijöiden määrä. Lisäksi uuden asiakas- ja potilastietojärjestelmä Apotin käyttöönotto on aiheuttanut sosiaali- ja terveydenhuollon toimialalla tietoturvaloukkauksia. Ilmoituskynnys voi vaihdella toimialoittain. Ilmoitusten määrä ei suoraan kerro sitä, että tietoja olisi toimialalla käsitelty huolimattomasti. Potilastietojen ja sosiaalihuollon asiakastietojen käsittely on ollut lainsäädännössä jo pitkään tiukasti säänneltyä, ja sosiaali- ja terveydenhuollon toimialalle on kehittynyt vahva toimintakulttuuri tietosuojaosaston osalta. Valtakunnallisestikin sosiaali- ja terveydenhuollon sektorilta tulee paljon ilmoituksia.

Tietoturvaloukkausten dokumentointi

Rekisterinpitäjänä kaupungin on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset. Dokumentointivelvollisuus tulee suoraan EU:n tietosuoja-asetuksesta. Vantaalla kaikki tietoturvaloukkausilmoitukset toimitetaan kaupungin kirjaamoon, jossa ne kirjataan asiakirjahallintajärjestelmään

LOPUKSI

Teknologia kehittyy koko ajan, ja henkilötietojen käsittelyyn syntyy jatkuvasti uusia innovaatioita. Jotta pystyisimme kaupungissa vastamaan tulevaisuuden suuriin haasteisiin, tulee tietosuojaosaston perusrakenteiden olla kunnossa. Tietosuojaosaston perusrakenteet ovat suhteellisen pysyviä, ja uutta on helpompi rakentaa vanhan päälle – ja se on myös taloudellisempaa.

Tavoitteena on, että henkilötietoja pystytään käsittelemään niin, että tiedot ovat aina mahdollisimman helposti niiden henkilöiden saatavilla, jotka tietoja työtehtävissään tarvitsevat. Tietosuojalainsäädäntö taas asettaa säännöt, miten henkilötietoja tulee käsitellä. Kun kaikessa tietojenkäsittelyn kehityksessä huomioidaan yhdessä nämä seikat heti varhaisessa vaiheessa, niin saamme rakennettua hyvin toimivan henkilötietojen käsittely-ympäristön sekä työntekijöille että kuntalaisille.

TOIMIALOJEN JA PALVELUALUEIDEN RAPORTIT

Sosiaali- ja terveydenhuollon toimiala

Tietosuoja-asioihin liittyviä prosesseja ja ohjeistuksia on työstetty paljon uuden asiakas- ja potilastietojärjestelmän käyttöönoton vuoksi. Erityisesti tietojen luovuttaminen sosiaali- ja terveydenhuollon rajojen yli on ollut esillä sekä toimialan sisällä että julkisuudessa. Tietoisuus tietosuoja-asioiden huomioimisesta on lisääntynyt, ja sekä henkilökunta että johto ovat nostaneet monia kysymyksiä esille. Tämä edesauttaa kehittämään tietosuojaa edelleen sosiaali- ja terveydenhuollon toimialalla.

Henkilökunnan koulutukseen ja tiedotukseen tietosuoja-asioissa on vuoden 2019 aikana panostettu. Tapahtuneita tietoturvaloukkauksia käydään läpi henkilökunnan kanssa, ja ne on käsitelty johtoryhmissä ja viety tiedoksi eteenpäin. Tietoturvaloukkausten käsittelystä on lisäksi tehty prosessiohje, joka on selkiyttänyt toimintaa. Esimiehillä on nyt aiempaa paremmin tietoa siitä, miten toimia, kun tietoturvaloukkaus tapahtuu. Tietoturvaloukkausten ilmoitusprosessia on kehitetty vuoden 2019 aikana, ja kehitystyö jatkuu vuonna 2020. Tavoitteena on selkiyttää prosessia ja dokumentoida tietoturvaloukkaukset entistä paremmin.

Vuoden 2019 aikana sosiaali- ja terveydenhuollon toimialalla on kokoontunut kaksi kertaa kuukaudessa tietosuojatiimi, jonka kokoonpanoon on kuulunut toimialan tiedonhallinnan ja tietosuojan asiantuntijoita. Asiantuntijat ovat laatineet ja päivittäneet tietosuojaan liittyviä dokumentteja kuten käsittelytoimiselosteita, tietotilinpäätöstä, toimialan ohjeistusta, tietosuojariskianalyysiä jne.

Sosiaali- ja terveydenhuollon toimialalla luovutetaan henkilötietoja rekisteröidylle itselleen EU:n tietosuoja-asetukseen perustuvan tarkastusoikeuden perusteella. Julkisuuslain perusteella rekisteröidyllä on oikeus saada tieto itseään koskevista asiakirjoista ja oikeus saada tietoa asianosaisaseman perusteella erityisesti lastensuojeluasioissa. Tietoja pyydetään pääsääntöisesti kirjallisesti. Tietojen pyytäjän tulee perustella tietopyyntö, ja tietopyyntö tulee toimittaa Vantaan kaupungin kirjaimoon, Vantaa-infoon tai sosiaali- ja terveydenhuollon toimipisteeseen. Vuoden 2019 aikana sosiaali- ja terveydenhuollon toimialalla on laadittu ohje tietojen luovuttamiseen sosiaali- ja terveydenhuollossa. Lisäksi on laadittu ohje tietojen luovuttamiseen lastensuojelussa, jossa on käsitelty tarkemmin sosiaali- ja terveydenhuollon tietojen luovuttamista lapsen tietojen näkökulmasta. Sosiaali- ja terveydenhuollon toimialan

tietojen luovuttamisen prosesseja kehitetään jatkuvasti. Tietojen luovuttamiseen on vaikuttanut myös uuden asiakas- ja potilastietojärjestelmän käyttöönotto.

Sosiaali- ja terveydenhuollon toimialalla on vuoden 2019 aikana siirrytty käyttämään uutta asiakas- ja potilastietojärjestelmä Apottia. Apotti-järjestelmän tietosuojan vaikutustenarviointi on aloitettu vuoden 2018 puolella ja työtä on jatkettu vuoden 2019 ajan. Apottiin liittyviä tietosuoja-asioita käsitellään yhteistyössä järjestelmän-toimittajan ja muiden samaa järjestelmää käyttävien rekisterinpitäjien toiminnassa.

Sosiaali- ja terveydenhuollon toimialalla toimii tutkimuksen koordinaatioryhmä, jossa käsitellään tutkimuslupahakemuksiin liittyviä kysymyksiä. Tietosuojalakimies on osallistunut tutkimuksen koordinaatioryhmän toimintaan elokuusta 2019 lähtien.

Lokakuussa 2019 hyväksyttiin Vantaan kaupungin alkukartoitusta ja vaikutusten-arviointia koskeva ohjeistus ja työkalut näiden tekemiseen. Asia esiteltiin tällöin myös Vantaan kaupungin johtoryhmässä. Vaikutustenarviointeja on tehty myös ennen tätä siihen asti käytettävissä olleilla työkaluilla. Velvollisuus vaikutustenarvioinnin tekemiseen tulee EU:n yleisestä tietosuoja-asetuksesta ja se on pakollista, jos asetuksessa määritellyt edellytykset täyttyvät. Jokainen sosiaali- ja terveydenhuollon toimialalla tehty alkukartoitus on osoittanut, että vaikutustenarviointi tulee tehdä.

Sosiaali- ja terveydenhuollon toimialalla raportoitiin vuoden 2019 aikana 115 tietoturvaloukkausta. Suuri osa tietoturvaloukkauksista liittyi uuden asiakas- ja potilastietojärjestelmän käyttöönottoon. Vuoden 2019 aikana on sosiaali- ja terveydenhuollon toimialalla laadittu prosessiohje tietoturvaloukkauksista ilmoittamiseen.

Sosiaali- ja terveydenhuollon toimialan yhteiset tietosuojaan liittyvät ohjeistukset löytyvät sosiaali- ja terveydenhuollon intra-sivustolta. Sivustolle on koottu ohjeistus, lomakkeet ja muut tiedostot. Ohjeistusta on päivitetty vuoden 2019 aikana ja uusia ohjeistuksia on laadittu. Ohjeistusta tarvitaan myös lisää ja ne vaativat jatkuvaa päivittämistä. Kun ohje on valmisteltu, viedään se sosiaali- ja terveydenhuollon toimialan johtoryhmään käsiteltäväksi. Johtoryhmä voi esittää muutoksia ohjeeseen tai hyväksyä sen sellaisenaan. Johtoryhmän hyväksyttyä ohjeen viedään se tietosuojasivustolle, jossa se on kaikkien saatavilla. Ohjeistuksista pyritään myös tekemään uutinen intraan, jotta se huomattaisiin. Lisäksi ohjeistuksesta tiedotetaan koulutusten ja konsultaatioihin vastaamisten yhteydessä.

Sivistystoimen toimiala

Vuonna 2019 toimialan tietosuojatyössä painottuivat kaupunkitasoisten ohjeiden, sopimusmallien ja asiakirjapohjien käyttöönotto, henkilötietojen tarkastuspyyntö-

prosessissa havaitut haasteet sekä täydentävien ohjeistusten tarpeellisuus. Lisäksi toimialalle perustettiin toimialan johtoryhmän päätöksellä tietosuojatyöryhmä, jonka tehtävänä on arvioida kasvatuksessa, opetuksessa ja koulutuksessa käytettävien sovellusten tietosuojaa. Työryhmä kokoontuu kerran kuukaudessa, ja sen työ jatkuu myös vuonna 2020.

Kaupunkitasoisten ohjeiden, sopimusmallien ja asiakirjapohjien käyttöönotto toimialalla on onnistunut hyvin. Tietosuojalainsäädännön muuttuneet vaatimukset ovat tosin lisänneet hallinnollista työtä, mikä on pidentänyt toimialalla toteuttavien pienhankintojen käsittelyaikaa sekä siten myös viivytännyt erilaisten palveluiden ottamista käyttöön.

Vuoden 2019 tietotilinpäätös on sivistystoimen toimialan viimeinen. Vantaan kaupungin 1.1.2020 voimaan tulleen organisaatiouudistuksen jälkeen sivistystoimen alaiset toiminnot jatkavat opetuslautakunnan alaisella kasvatuksen ja oppimisen toimialalla sekä vapaa-ajan lautakunnan alaisella kaupunkikulttuurin toimialalla. Jatkossa toimialat vastaavat tietotilinpäätöksen laatimisesta omalta osaltaan.

Organisaatiouudistuksen myötä Vantaan kaupungin ohjeistus vaikutustenarviointien laatimisesta ja vaikutustenarviointityökalut on esitelty uusien toimialojen johdolle alkuvuodesta 2020. Kaupunkitasoinen ohjeistus ja työkalut on kuitenkin otettu toimialalla käyttöön heti materiaalien valmistuttua lokakuussa 2019.

Toimialan palvelutuotannon järjestäminen edellyttää merkittävien henkilötietomäärien laajamittaista käsittelyä, ja suurinta osaa henkilötiedoista käsitellään toimialan tietojärjestelmissä. Toimialojen keskeisten tietojärjestelmien jo sovittuja vaikutustenarviointeja jatketaan vuonna 2020, ja uusien vaikutustenarviointien tarpeellisuudesta sovitaan yhteistyössä Tietohallinnon kanssa. Tietojenkäsittelyn laajuuden vuoksi vaikutustenarvioinnin kriteerit täyttyvät tietojärjestelmien lisäksi usein toimialan vastuulla olevien pienhankintojen, palveluiden käyttöönottojen tai vanhojen prosessien uudistamisien yhteydessä. Näiltä osin toimialalla arvioitiin vuoden 2019 aikana vaikutustenarvioinnin tarpeellisuutta 5 tapauksessa, joista 4 tapauksessa alkukartoitus johti vaikutustenarvioinnin laatimiseen.

Toimialan tietoturvaloukkaukset ilmoitetaan ja selvitetään kaupungin yleisohjeen mukaisesti. Kunkin yksikön esimies vastaa ohjeen noudattamisesta sekä ilmoitusten tekemisestä oman yksikkönsä osalta. Mikäli yksikössä tapahtuu tietoturvaloukkaus, esimies ilmoittaa loukkauksesta kaupungin tietosuojavastaavalle sitä varten laaditulla lomakkeella. Lisäksi esimies tiedottaa toimialan/tulosalueen johtoa tapahtuneesta tarvittaessa loukkauksen vakavuudesta riippuen. Vuoden 2019 aikana

toimialalta ilmoitettiin tietosuojavastaavalle 23 tietoturvaloukkausta. Näistä loukkauksista 11 johti ilmoitukseen rekisteröidyille ja 2 tietosuojavaltuutetulle. Tietoturvaloukkaukset ovat pääasiassa olleet vähäisiä, ja niihin on reagoitu nopeasti ja ohjeistuksen mukaisesti. Tietoturvaloukkausten ehkäisemiseksi yksiköissä on mm. kerrattu tarvittavat ohjeistukset sähköpostin käytöstä ja laitteiden valvomisesta, minkä lisäksi henkilökunnalle on painotettu huolellisuutta henkilötietojen käsittelyssä.

Toimialan tietojen käsittelyssä noudatetaan Vantaan kaupungin yleisiä tietoturva- ja tietosujoaohjeita. Yleisohjeita täydennetään tarvittaessa toimiala- tai tulosaluekohtaisella ohjeistuksella. Ohjeistusten ajantasaisuutta seurataan ja niitä päivitetään lainsäädännön tai kaupungin yleisohjeistusten muuttuessa. Uudet ohjeet käsitellään tarvittaessa toimialan tai tulosalueen johtoryhmässä ja niistä tiedotetaan henkilöstöä. Kukin esimies vastaa vastuualueellaan sekä alaistensa perehdyttämisestä ohjeisiin esimiesohjeen mukaisesti että ohjeiden noudattamisen valvonnasta.

Maankäytön, ympäristön ja rakentamisen toimiala

Lokakuussa 2019 hyväksyttiin alkukartoitusta ja vaikutustenarviointia koskeva ohjeistus sekä työkalut näiden tekemiseen. Toimialalla tehtiin kaksi alkukartoitusta vuonna 2019, ja alkukartoitus eteni vaikutustenarviointiin yhdessä tapauksessa.

Vuoden 2019 aikana maankäytön, rakentamisen ja ympäristön toimialalta ilmoitettiin yksi tietoturvaloukkaus, joka käsiteltiin toimialan johtoryhmässä.

Maankäytön, rakentamisen ja ympäristön toimialalla ei ole erillisiä tietosuojaa koskevia ohjeistuksia. Toimiala noudattaa kaupunkiyhteisiä ohjeita. Tietosuojaselosteita on päivitetty ja niitä on tehty lisää.

Kaupunginjohtajan toimiala

Taloussuunnittelu

Taloussuunnittelun tulosalueen johtoryhmässä ei ole erikseen käsitelty EU:n tietosuojasetuksen mukaista alkukartoitusta ja vaikutustenarviointia, vaan vaikutustenarvioinnin prosessia on käsitelty projektien ohjausryhmissä ja taloussuunnittelun sisäisissä yksikköpalavereissa. Taloussuunnittelun johtoryhmä on pieni, jolloin tiedotuksen voi hoitaa myös muun työskentelyn yhteydessä. Taloussuunnittelun tulosalueella alkukartoituksia on tehty neljälle järjestelmälle. Alkukartoitusten perusteella kolmelle järjestelmälle piti tehdä myös vaikutustenarviointi. Vuonna 2020 talouden ja strategian -palvelualueen (aikaisemmin taloussuunnittelu) pitää tehdä vaikutustenarviointi uudessa hankkeessa toteutettavalle pääkaupunki-

seudun yhteiselle väestöennusteelle sekä viimeistellä keskeneräiset vaikutustenarvioinnit.

Taloussuunnittelun tulosalueella tehtiin vuoden 2019 aikana kolme tietoturvaloukkausilmoitusta, joista yhden ilmoituksen tekeminen ei olisikaan kuulunut taloussuunnittelun tulosalueelle ja yksi ilmoitus osoittautui turhaksi. Kaikista tietoturvaloukkauksista on tehty ilmoitus tutkimuspäällikölle, tarvetta johtoryhmäkäsittelyyn ei ole ollut. Koska tietoturvailmoitukset on toimitettu kirjaamoon, niin niistä on mennyt tieto myös tietoturvapäällikölle ja tietosuojavastaavalle.

Taloussuunnittelun tulosalueella on hyödynnetty Vantaan kaupungin tietosuoja- ja tietoturvasivuston ohjeita, joista löytyy yksi erillinen ohje tietopalvelun käsittelemistä henkilötiedoista. Taloussuunnittelu on pitänyt kaikki dokumentit ajan tasalla.

Elinkeinopalvelut

Elinkeinopalveluissa käytössä oleva CRM-järjestelmä on havaittu hyvin toimivaksi. Yksikössä ei lähtökohtaisesti käsitellä sensitiivistä henkilödataa, asiakkaat ja sidosryhmät ovat pääasiassa yrityksiä ja oppilaitoksia. CV:t rekrytoinnin yhteydessä luovat näihin poikkeuksen. Kehittämiskohde on tilatut oppilastyöt ja näissä ilmenneet GDPR-haasteelliset luettelot. Oppilaitoksia on huomautettu ja ohjeistettu puuttumaan asiaan aktiivisemmin.

Vuonna 2019 ei elinkeinopalveluissa ole tehty alkukartoituksia. Alkukartoitusta ja vaikutustenarviointia on käyty läpi elinkeinopäällikön ja elinkeinojohtajan kanssa ja tarkennettu ohjeistusta uutiskirjeen ja webropolin käytön suhteen. Elinkeinopalveluissa ei ole johtoryhmää, jossa käsitellä vaikutustenarviointiprosessia. Uudessa kasvupalveluiden organisaatiossa tilanne muuttuu, ja onkin ehdotettu, että kasvupalveluilla olisi yhteinen tietoturvavastaava.

Elinkeinopalveluissa ei ole tietoon tulleita tietoturvaloukkauksia.

Ohjeistukset ovat kaupungin intranetissä.

Kaupunginkanslia

Vuonna 2019 Vantaan kaupungin tietoturva- ja tietosuojatyöryhmän kokouksia järjestettiin säännöllisesti. Kaupunginkansliasta kokouksiin osallistuivat tietosuojavastaava (puheenjohtaja) ja hallintosihteeri. Koulutuksen ja uudistetun tietosuojaohjeistuksen ansiosta kaupunginkanslian henkilöstön yleinen tietoturvatietoisuus on lisääntynyt, mutta tietoturva-asioiden viestintää ja markkinointia henkilöstölle tulisi tehostaa

edelleen. Marraskuussa 2019 tietosuojavastaava organisoï koko kaupungin henkilös-
tölle tarkoitettun tietosuojakoulutuksen, joka käsitti neljä kokonaisuutta: työntekijöiden
henkilötietojen käsittely ja yksityisyyden suoja, tietoturvaloukkaukset Vantaan
kaupungissa 2019, tietosuojan vaikutustenarviointi sekä tietojen kalastelu. Osallis-
tujamäärän rajoituksen vuoksi kaupunginkansliasta koulutustilaisuuteen osallistui
kolme henkilöä. Kaupungin intrasta löytyvä koulutusvideotallenne on tarkoitus katsoa
myöhemmin yhdessä.

Vuoden 2019 lopussa käyttöön otettu kaksivaiheinen tunnistautuminen on otettu
positiivisesti vastaan ja koettu toimivaksi. Kaupunginkanslian tiloihin viikoittain
toimitettava lukittu tietoturvapaperilaatikko on tehostanut hävitettävien asiakirjojen
tuhoamista. Kehittämistoimenpiteenä vuodelle 2020 tulisi Kuntademokratian (Laki-
asiat ja päätösvalmistelu sekä Hallintopalvelut) tietotilinpäätöksessä tuoda esille 10
keskeisintä prosessia tai järjestelmää, joista tehdään vaikutustenarviointi. Priori-
sointikriteereinä ovat käsiteltävien henkilötietojen määrä, arkaluonteisuus tai epäily
prosessin tai järjestelmän toimivuudesta, jos lainmukainen henkilötietojen käsittely
voi mahdollisesti vaarantua.

Tulosalueella ei ole tehty alkukartoituksia tai vaikutustenarviointeja vuonna 2019.

Kaupunginkanslian tulosalueella tehtiin vuonna 2019 yksi tietoturvaloukkausilmoitus.

Kaupunginkansliassa noudatetaan intranetissä olevia kaupungin yleisiä tietoturva- ja
tietosuojaohteita. Kaupunginkanslian työntekijöille jaettiin ohje henkilötiedon määri-
telmästä, jonka perusteella alkuvuodesta 2019 tehtiin kartoitus henkilötietojen käsit-
telystä kaupunginkansliassa.

Sisäinen tarkastus

Tulosalueella ei ole tehty alkukartoituksia eikä vaikutustenarviointeja vuonna 2019.
Vuoden 2020 aikana tehdään tarkastusprosessin ja parhaillaan kehitteillä olevan
vihjelinjan alkukartoitukset ja vaikutustenarvioinnit.

Tulosalueella ei ole tapahtunut vuoden 2019 aikana tietoturvaloukkauksia eikä
aikaisemminkaan. Tietoturvaloukkauksiin liittyviä asioita ei ole juurikaan käsitelty
edellä mainitusta syystä tulosalueen henkilöstön kanssa.

Tulosalueella ei ole omaa tietosuojaa/tietoturvaa koskevaa ohjeistusta. Tulosalueella
noudatetaan kaupunkitasoisia ohjeistuksia.

Viestintä

Viestinnän tulosalue on laatinut omistamiinsa palveluprosesseihin liittyvät henkilötietojen sisäiseen käyttöön tarkoitetut käsittelyselosteet sekä julkiset informointiasiakirjat. Asiakirjat on julkaistu vantaa.fi-sivustolla. Tietoisuus henkilötietojen ja yksityisyyden suojaamisesta on vahvistunut viestinnän tehtävissä. Kuva- ja videomateriaalien julkaisun yhteydessä on tullut esille kysymys kuvattavien suostuksesta kuvan luovuttamisesta kolmannelle osapuolelle. Uusien järjestelmien hankintaprosessin käynnistyessä viestintä on tehnyt vaikutusten alkukartoituksen. Viestintä on tuonut tietosuojaan liittyvät kysymykset esille toimialojen yhteisissä toimintaprosesseissa, kuten vantaa.fi -sivuston sisällöntuotanto, sosiaalisen median alustat ja uutiskirjeiden toimitus sekä tarkastellut käyttäjille suunnattuja ohjeita tietosuojan näkökulmasta.

Viestintä on tehnyt kaksi alkukartoitusta vuonna 2019, joista toinen johti vaikutustenarvioinnin tekemiseen. Alkukartoituksen esille nostamien kysymysten perusteella vaikutustenarvioinnissa pitää erityisesti selvittää käyttäjien ohjeistusta tietosuojan noudattamiseen. Järjestelmän automaatiotoiminnallisuuksien käyttöönotto velvoittaa arvioimaan tietosuojan uudelleen. Korkeita riskejä ei ole havaittu. Järjestelmän toimittajan kanssa yhteistyö on sujunut hyvin. Toimittajat ovat tietoisia tietosuojasäännöksistä.

Vuoden 2019 aikana ei ole tehty tietoturvaloukkausilmoituksia.

Yleiset ohjeet ovat luettavissa intrassa. Viestinnän omat ohjeet pitää kartoittaa, päivittää, koota ja raportoida. Tarkoitus on koota ohjeistukset tietosuojan intrasivustolle, jotta ne ovat kaikkien saatavilla, kun ne on tehty.

Henkilöstökeskus

Henkilöstökeskuksen tulosalueella ei havaittu erityisiä puutteita tai ongelmia tietosuojassa. Erilaisten muutosten yhteydessä ja erityisesti uusien järjestelmien käyttöönoton yhteydessä ei ole kuitenkaan aina muistettu tai ehditty oikea-aikaisesti huolehtia tietosuojaan liittyvien alkukartoitusten ja vaikutustenarviointien käynnistämisestä. Tässä on siis vielä parantamisen varaa, jotta toiminta olisi tietosuojaasetuksen vaatimalla tasolla.

Vuoden alussa otettiin käyttöön uusi rekrytointijärjestelmä, ja vanha poistui käytöstä. Tulosalueella valmisteltiin kolmen uuden järjestelmän käyttöönottoa. Tulosalueella otettiin myös käyttöön robotiikkaa rekrytointi- ja palkanlaskentaprosesseissa sekä

käyttöoikeuksien hallinnassa. Tietosuojaan liittyen tulosalueella toimittiin kaupungin tietosuojalinjausten mukaisesti.

Tietosuojaan liittyviä omia koulutuksia ei järjestetty vuonna 2019 Henkilöstökeskuksen tulosalueella. Henkilöstöä osallistui kuitenkin tietoturva- ja tietosuoja-työryhmän järjestämään kaupunkitasoiseen koulutukseen. Havaittuna puutteena voidaan todeta, että tietosuojaosaamiseen ei ole pystytty riittävästi resursoimaan henkilöstökeskuksen tulosalueella. Kehittämiskohteeksi nostetaan jatkossa, että osaamista tietosuojavastaavan tehtävissä keskitetään koko kaupunginjohtajan toimialalla ja että keskitettyä osaamista saadaan erityisesti toimialan henkilökunnan ohjeistamiseen ja osaamisen ylläpitämiseen sekä ohjaamaan ja tukemaan eri tulosalueilla tapahtuvaan vaikutustenarviointia.

Työvuorosuunnittelujärjestelmän tietoturva-auditointi suoritettiin loka-marraskuussa 2019, eikä avoimia asioita jäänyt. Henkilöstöhallinnon tietojärjestelmän uuden ohjelmistoversion vaikutustenarvioinnin aloituspalaveri pidettiin joulukuussa 2019. Varsinainen alkukartoitus ja vaikutustenarviointi siirtyi vuoden 2020 puolelle. Robotiikan käyttöönotosta on Vantaalla sovittu yhteisesti noudatettavat tietoturvalinjaukset, mutta alkukartoitusta tai varsinaista vaikutusten arviointia ei henkilöstökeskuksen tulosalueella käyttöön otettujen robottitehtävien osalta vielä tehty. Alkukartoitusta ja vaikutustenarviointia ei myöskään ole tehty rekrytointijärjestelmästä. Kehittämistoimenpiteenä vuodelle 2020 tulisi tehdä alkukartoitus ja vaikutustenarviointi edellä mainittujen järjestelmien lisäksi työturvallisuusjärjestelmästä ja koulutusten hallintajärjestelmästä.

Henkilöstökeskuksen tulosalueella ilmoitettiin vuoden 2019 aikana neljä tietoturvaloukkausta. Kaikki tietoturvaloukkaukset liittyivät HR-järjestelmiin. Tietoturvaloukkauksista tehtiin Vantaan ohjeistuksen mukainen ilmoitus, joka toimitettiin sähköpostilla tulosalueen johdolle, tietosuojavastaavalle ja tietoturvapäällikölle.

Henkilöstökeskuksen tulosalueella noudatetaan kaupungin yhteisiä tietosuoja- ja -turvaa koskevia ohjeita, jotka löytyvät intrasta.

Konserni- ja asukaspalveluiden toimiala

Asukaspalvelut

Asukaspalvelut osallistui kaupungin yhteiseen tietosuojakoulutukseen 20. marraskuuta.

Vaikutustenarviointi tehtiin joulukuussa asianhallintajärjestelmälle. Vuoden aikana henkilötietojen tarkastuspyyntöjä ei kohdistunut konserni- ja asukaspalveluihin eikä yhtään tietoturvaloukkausta ole kirjattu. Tietoturvaohjeistuksia on päivitetty ja lisätty intraan. Nyt konserni- ja asukaspalveluilla on yhteensä 6 informointiasiakirjaa ja 10 selostetta käsittelytoimista.

Hankintakeskus

Hankintakeskus otti loppuvuodesta 2019 käyttöönsä kaupungin tietoturva- ja tietosuojatyöryhmän laatimat lomakkeet vaikutustenarvioinnin ja vaikutustenarvioinnin alkukartoituksen tekemiseksi. Alkukartoitus ja vaikutusarviointi pyritään tekemään mahdollisimman aikaisessa vaiheessa hankintaprosessia siten, että tehdyt arvioinnit tulevat huomioiduksi hankinnan kohdetta ja sopimusehtoja määriteltäessä. Vaikutustenarvioinnin tulee olla valmis ennen kuin hankintasopimus allekirjoitetaan. Hankintakeskuksella on käytössään ns. hankintojen arviointilomake, joka sisältää myös tietosuoja- ja henkilötietojen käsittelyä koskevat osiot. Tällä tavoin tietosuoja-asiat tulevat huomioiduksi osana hankintaprosessia.

Vuoden 2019 aikana alkukartoituksia tehtiin yhteensä 11, joista kolme johti vaikutustenarvioinnin tekemiseen. Tehdyissä vaikutustenarvioinneissa ei ole löytynyt korkeita riskejä. Vaikutustenarviointien perustella voitiin todeta, että nykyiset prosessit ovat pääpiirteittäin kunnossa tietosuojan näkökulmasta, mutta yksittäisiä kehittämisen paikkojakin löytyi.

Tietohallinto

Tietohallinto on luonteensa mukaisesti ollut vahvassa roolissa muiden toimialojen tietosuoja-asioissa. Vuonna 2019 saatiin loppuun vuodesta 2016 käynnissä ollut tietosuojaprojekti EUAS. Projektin alkuperäisenä tavoitteena oli, että Vantaan kaupunki pystyy toiminnassaan vastaamaan EU:n yleisen tietosuoja-asetuksen vaatimuksiin. Yksittäisiksi kehittämiskohteiksi projektissa listattiin tietosuojaselosteet, tarpeelliset politiikat ja ohjeet, henkilötietojen riskienarviointi (vaikutustenarviointi), sopimukseen tietosuojaliitteet (DPA), tietosuojan hallintamalli, tietosuojakoulutus ja tietosuojan huomioiminen ohjelmisto- ja palveluhankkeissa. Projekti päätettiin toteamuksella, että tavoite on saavutettu ja kehittämiskohteet ovat joko valmiita tai muodostuneet osaksi päivittäistoimintaa.

Tietohallinnossa kehittämiskohteita on tunnistettu etenkin pilvipalveluiden tietoturvan alueella. Asiassa saatiin huomattava edistysaskel, kun marraskuussa 2019 Office 365 - palvelussa siirryttiin vahvan autentikoinnin käyttöön.

Vuoden 2018 tietotilin päätöksen linjauksen mukaan Tietohallinnon vastuulla olevissa järjestelmissä ei käsitellä arkaluontoisia henkilötietoja, joten niihin ei ole tehty vaikutustenarviointeja. Tietohallinto on ollut vahvassa roolissa toimialojen vaikutustenarvioinneissa sekä luomassa ja kehittämässä vaikutustenarviointiprosessia että auttamassa sen pohjalta itse vaikutustenarviointien tekemisessä. Tietohallinnon näkökulmasta suurin vaikutustenarviointiin liittyvä kehityskohde on itse vaikutustenarviointiprosessin kehittäminen sujuvammaksi. Vaikutustenarviointiprosessi ja sen työkalut on kehitetty vuoden 2019 aikana, ja se on päässyt käyntiin hyvin. Käyttökokemusten perusteella prosessissa alkaa nousta näkyviin kehityskohteita, jotka näkyvät ehkä selkeimmin Tietohallinnolle, joka osallistuu useimpiin vaikutustenarviointeihin.

Henkilötietojen tietoturvaloukkauksia ei ole ollut vuoden 2019 aikana Tietohallinnossa. Tietohallinto on usein mukana toimialojen vastuulla olevien järjestelmien ja prosessien henkilötietojen tietoturvaloukkausten käsittelyssä. Tämän myötä Tietohallinnon henkilöstön ymmärrys henkilötietojen tietoturvaloukkauksista ja niiden vaatimista toimenpiteistä on suhteellisen hyvä.

Tietohallinnolla ei ole omaa erillistä sisäistä ohjeistusta tietosuojasta, vaan se tukeutuu kaupungin tietosuojaohjeistukseen. Tietohallinto myös osallistuu aktiivisesti kyseisen ohjeistuksen kehittämiseen. Tietoturvaohjeistus Vantaan kaupungilla puolestaan on Tietohallinnon vastuulla. Vantaan kaupungin tietoturvaohjeistus on ollut pitkään suhteellisen hajanaista ja paikoin kaivannut tarkennuksia. Ohjeiden ajantasaistaminen ja yhteen kokoaminen ovat vuoden 2020 tärkeimpiä tavoitteita Tietohallinnossa tietoturvan osalta. Työ on aloitettu, ja tammikuussa 2020 ohjeiden kokoaminen yhteen keskitettyyn julkaisusijaintiin intrassa on aloitettu.

Vantaan työterveys liikelaitos

Vantaan Työterveys liikelaitos oli Vantaan kaupungin organisaatiossa kunnallinen liikelaitos, jonka toiminta ja henkilöstö siirtyivät yhtiöittämisen myötä Vantaan Työterveys Oy:lle 1.8.2019 alkaen. Kaupunginvaltuusto päätti 16.12.2019, että Vantaan Työterveys liikelaitos lakkautetaan 31.12.2019.

Vantaan Työterveys liikelaitoksen tietosuojavastaava on osallistunut kaupungin tietosuojatyöryhmän kokouksiin ja tuonut kaupungin uudet ja päivitetty tietosuojan ja tietoturvan ohjeistukset tiedoksi ja käytäntöön liikelaitokselle. Vantaan Työterveys liikelaitoksessa on päivitetty myös liikelaitoksen omia täydentäviä tietosuojaohjeistuksia. Tietosuoja-asioita on pidetty säännöllisesti esillä Vantaan Työterveys

liikelaitoksessa ja käsitelty johtoryhmän kokouksissa sekä toimipiste- ja ammattiryhmäkokouksissa. Henkilöstön koulutus tietoturvaan ja tietosuojaan liittyviin asioihin on toteutettu perehdytyksen yhteydessä. Osaaminen on tarkastettu vuosittain kehityskeskustelun yhteydessä.

Vaikutustenarviointi on käynnistynyt jo Vantaan Työterveys liikelaitoksen aikana. Vantaan Työterveys liikelaitoksessa vaikutustenarviointi on tehty työterveyshuollon yleisen toiminnan, extranetin ja potilastietojärjestelmän osalta marraskuussa 2018. Vaikutustenarviointi on jatkunut Vantaan Työterveys Oy:ssä syksyllä 2019 kaupungin uuden ohjeistuksen mukaisesti

Vuonna 2019 Vantaan Työterveys liikelaitoksessa tapahtui kaksi tietoturvaloukkausta. Esimies/tietosuojaavastaava on käynyt tietoturvaloukkauksen läpi työntekijän kanssa. Vantaan Työterveys liikelaitoksessa tapahtuneita tietoturvaloukkauksia on käsitelty johtoryhmän kokouksissa sekä toimipiste- ja ammattiryhmäkokouksissa.

Vantaan Työterveys liikelaitos on noudattanut Vantaan kaupungin tietoturvapoliitikan mukaisesti laadittuja Intranetissä olevia yleisiä ohjeita. Vantaan Työterveys liikelaitoksella on lisäksi ollut omat täydentävät tietosuojaohjeistukset. Tietojen käytön valvonnan pääasiallinen vastuu ja toteuttaminen ovat tapahtuneet tulosyksiköissä esimiesten toimesta. Tietosuojaavastaava on tarkistanut ohjeiden mukaisesti lokitiedot kerran vuodessa. Jos väärinkäytöksiä on ilmennyt, on niihin tullut puuttua välittömästi. Jokainen uusi työntekijä on perehdytetty asiakas- ja/tai potilastietojärjestelmien tietoturvalliseen käyttöön sekä tietoturvalliseen toimintatapaan suullisesti ja kirjallisen materiaalin avulla.

TIETOTILINPÄÄTÖKSEN LIITTEET

Liite 1: Vuoden 2019 tietotilinpäätöksen rakenne

Vuoden 2019 tietotilinpäätöksessä keskitytään seuraaviin asiakokonaisuuksiin:

- Tietosuoja toimialalla/tulosalueella vuonna 2019
- Alkukartoitus ja vaikutustenarvioinnit
- Tietoturvaloukkaukset
- Ohjeistukset

Tietosuoja toimialalla/tulosalueella vuonna 2019

- Havaitut positiiviset asiat, puutteet ja ongelmat sekä kehittämiskohteet
- Yleinen kuvaus mitä toimialalla/tulosalueella on tietosuojan osalta tapahtunut

Alkukartoitus ja vaikutustenarvioinnit

Lokakuussa 2019 hyväksyttiin alkukartoitusta ja vaikutustenarviointia koskeva ohjeistus ja työkalut näiden tekemiseen. Asia esiteltiin tällöin myös kaupungin johtoryhmässä. Vaikutustenarviointeja on tehty myös ennen tätä siihen asti käytettävissä olleilla työkaluilla. Velvollisuus vaikutustenarvioinnin tekemiseen tulee EU:n yleisestä tietosuoja-asetuksesta ja se on pakollista, jos asetuksessa määritellyt edellytykset täyttyvät.

Tietosuojavastuuhenkilöiden tehtävänä oli viedä työkalut ja prosessi tiedoksi omilla toimialoilla/tulosalueilla sekä jalkauttaa prosessi alulle ja opastaa sen tekemisessä.

- Miten asia on viety johdolle tiedoksi?
- Onko vaikutustenarviointiprosessia käsitelty johtoryhmissä?
- Kuinka monta alkukartoitusta on vuonna 2019 tehty?
- Prosessit tai järjestelmät, joista alkukartoitus on tehty?
- Kuinka monessa tapauksessa alkukartoitus osoitti, että vaikutustenarviointi tulee tehdä?
- Alkukartoituslomakkeen täyttämiseen käytetty aika?
- Kuinka monessa tapauksessa alkukartoitus osoitti, että varsinaista vaikutustenarviointia ei tarvitse tehdä?
- Prosessit tai järjestelmät, joista vaikutustenarviointi on tehty tai aloitettu?
- Lyhyet kuvaukset tehdyistä tai aloitetuista vaikutustenarvioinneista ja minkälaisia asioita niissä on noussut esille?
- Onko löytynyt korkeita riskejä?

- Kuinka paljon henkilöitä on osallistunut vaikutustenarvioinnin tekemiseen?
- Onko järjestetty työpajoja?
- Yhteistyön sujuminen järjestelmien toimittajien kanssa?
- Kuinka paljon vaikutustenarvioinnin tekeminen on vienyt aikaa?

Tietoturvaloukkaukset

Vuoden 2019 aikana tapahtuneet tietoturvaloukkaukset

- Lukumäärä?
- Miten esimiesten kanssa on tietoturvaloukkauksia käyty läpi?
- Miten esimiehet ovat käyneet tietoturvaloukkauksia läpi alaistensa kanssa?
- Onko tietoturvaloukkauksia käsitelty johtoryhmissä?
- Miten tieto kulkee johdolle tietoturvaloukkauksista?
- Kuinka perillä työntekijät ovat siitä mikä on tietoturvaloukkaus?

Ohjeistukset

Kartoitus toimialalla/tulosalueella olevasta tietosuojaa/tietoturvaa koskevasta ohjeistuksesta

- Mistä ohjeet löytyvät?
- Kuinka suuri osa ohjeistuksesta kaipaa päivittämistä?
- Milloin ohjeistukset tuodaan tietosuoja/tietoturvasivustolle, jotta ne ovat kaikkien saatavilla?

Liite 2: Vantaan kaupungin henkilötietojen tietoturvaloukkaukset 2019 toimialoittain

TOIMIALA	LOUKKAUKSIEN LUKUMÄÄRÄ
Sosiaali- ja terveydenhuollon toimiala	75
-Apottiin liittyvät tietoturvaloukkaukset	40
Sivistystoimen toimiala	23
Kaupunginjohtajan toimiala	8
Konserni- ja asukaspalvelujen toimiala	4
Maankäytön, ympäristö ja rakentamisen toimiala	1
Työterveys liikelaitos	2

