

Toimenpiteet, joihin tarkastuksen perusteella ryhdytään (3.4.2025)

Tarkastus: Tietosuojan toteutuminen VAV-konsernissa

Alla olevassa taulukossa esitetään olennaiset tarkastushavainnot, annetut suositukset sekä tietosuojavastaavan ja IT-päällikön päällikön vastaukset siihen, millaisiin toimenpiteisiin tarkastusraportissa annettujen suositusten osalta ryhdytään.

Selvitys on käsitelty seuraavasti VAV-konsernissa.

- VAV Yhtymä Oy:n hallituksessa 6.5.,
- VAV Asunnot Oy:n hallituksessa 30.4.,
- VAV Palvelukodit Oy:n hallituksessa 30.4. ja
- VAV Hoiva-asunnot Oy:n hallituksessa 30.4.

Vastauksen antaja näkyy vastauksen yhteydessä.

1. Vaikutustenarviointien tekeminen

VAV:n mukaan yhtiöllä on 19 tietojärjestelmää, joissa käsitellään henkilötietoja. Tarkastushavaintojen mukaan vaikutustenarviointi on tehty ainoastaan kolmeen niistä. Tarkastuksessa kävi myös ilmi, että vaikutustenarviointien tekemiseen on käytetty VAV:n Excel-pohjaista työkalua, joka keskittyy pääosin riskien arvioimiseen. Sisäisen tarkastuksen näkemyksen mukaan kyseinen työkalu ei kata kaikkia tietosuojalainsäädännön vaikutustenarvioinnille asetettuja vaatimuksia (vrt. esim. kaupungin vaikutustenarviointityökalu), jotka tulisi huomioida niiden tekemisessä.

a)

Suositus

VAV kartoittaa tietosuojavastaavan johdolla, mitkä tietojärjestelmät ja henkilötietojen käsittelykokonaisuudet edellyttävät tietosuojalainsäädännön mukaista vaikutustenarviointia, laatii suunnitelman vaikutustenarviointien toteuttamisesta ja aikataulusta sekä toteuttaa vaikutustenarvioinnit kaikkiin tietojärjestelmiin, joihin niitä ei ole tehty.

Toimenpiteet ja aikataulu (tietosuojavastaava)

- Osallistujat: tietosuojavastaava, it-päällikkö, järjestelmätoimittajat ja järjestelmien omistajat/pääkäyttäjät
- Selvitetään kaupungin työkalut ja tapa tehdä vaikutustenarviointeja (kesä 2025)
- Arvioidaan VAV:n nykyisten vaikutustenarviointityökalujen soveltuvuus jatkokehitykseen (kesä 2025)
- Päivitetään vaikutustenarvioinnit VAV:n järjestelmistä (aloitus syksy 2025 – viimeistely 2026)
- Vaikutustenarvioinnit viedään hyväksyttäväksi johtoryhmälle osana tietosuojan vuosiraportointia (aloitus syksy 2025 – viimeistely 2026)

b)	Suositus VAV täydentää tietosuojavastaavan johdolla jo tehtyjä vaikutustenarviointeja siten, että ne sisältävät tietosuojaperiaatteiden kattavan tarkastelun (esim. lain-mukaisuus, käyttötarkoitussidonnaisuus, tietojen minimointi ja säilytyksen rajoittaminen), rekisteröidyn oikeuksien arvioinnin (esim. tietojen oikaisu, poistaminen, siirrettävyys ja automaattinen päätöksenteko), tietojen käsittelijöiden ja siirtojen arvioinnin (esim. sopimukset, suojatoimet ja ETA-alueen ulkopuoliset siirrot), käsittelyn tarpeellisuuden ja oikeasuhteisuuden selvityksen (esim. vaihtoehtoiset, vähemmän tietosuojaan puuttuvat menetelmät) sekä tehdyn vaikutustenarvioinnin dokumentoidun hyväksymisprosessin, jossa arviointi hyväksytään virallisesti. Toimenpiteet ja aikataulu (tietosuojavastaava) • Kts. kohdan 1a vastaus, nämä sisällytetään päivitykseen
c)	Suositus Tietosuojavastaava selvittää, onko VAV:n mahdollista hyödyntää vaikutustenarvioinneissaan Vantaan kaupungin valmiita käytössä olevia työkaluja. On suositeltavaa, että VAV hyödyntää niitä mahdollisuuksien mukaan. Jos kaupungin työkalujen hyödyntäminen ei ole mahdollista, sisäinen tarkastus suosittelee, että VAV kehittää omia työkalujaan siten, että ne täyttävät tietosuojalainsäädännön vaikutustenarvioinneille asettamat vaatimukset. Toimenpiteet ja aikataulu (tietosuojavastaava) • Kts. kohdan 1a vastaus, nämä sisällytetään päivitykseen

2. Vantaan kaupungin tietosuojapolitiikan ja tietoturvapoliitiikan huomioiminen	
Vantaan kaupungin tietosuojapolitiikan mukaan politiikka on otettava huomioon kaupungin tytäryhteisöjen toiminnassa. Tarkastuksessa ilmeni, että VAV ei ole varmistanut, että sen toteuttamassa tietosuojatyössä noudatetaan kaupunginhallituksen 18.11.2024 hyväksymän tietosuojapolitiikan linjauksia. VAV:n mukaan se ei ole saanut tietoa uudesta tietosuojapolitiikasta konsernipalveluista. Tarkastuksessa kävi myös ilmi, että Vantaan kaupunki on valmistelemassa tarkastuksen käynnissä ollessa myös uutta tietoturvapoliitiikkaa, joka tullee politiikan luonnosversion mukaan niin ikään huomioida jatkossa tytäryhteisöjen toiminnassa.	
a)	Suositus Tietosuojavastaava varmistaa, että VAV:n tietosuojakäytännöt vastaavat Vantaan kaupungin 18.11.2024 hyväksyttyä tietosuojapolitiikkaa. Tämän tulee käydä selkeästi ilmi intranetistä sekä tietosuojaan ja tietoturvaan liittyvistä olennaisista asiakirjoista. Jos käy ilmi, että VAV:n toiminta ei ole kaupungin tietosuojapolitiikan mukaista, tulee yhtiön ryhtyä korjaaviin toimenpiteisiin. Lisäksi on suositeltavaa, että VAV arvioi, onko kaupungilla käyttökelpoisia tietosuojatyökaluja, joita se voisi hyödyntää toiminnassaan. Toimenpiteet ja aikataulu (tietosuojavastaava) • Osallistujat: tietosuojavastaava, it-päällikkö • VAV sai kaupungilta raportin valmistuttua tiedon kaupungin hyväksymästä tietosuojapolitiikasta 8.4.2025 • VAV perehtyy kaupungin tietosuojapolitiikan sisältöön ja varmistaa, että VAV:n tietosuojakäytännöt ja -ohjeistus mukailevat kaupungin tietosuojapolitiikkaa (kevät 2025-syksy 2026)

b)	Suositus IT-päällikkö seuraa aktiivisesti Vantaan kaupungin tietoturvapolitiikan valmistelua ja varmistaa, että VAV soveltaa sen linjauksia toiminnassaan, kun politiikka valmistuu. Lisäksi on suositeltavaa, että IT-päällikkö arvioi, onko kaupungilla VAV:n tietoturvatyötä tukevia käytäntöjä, työkaluja tai ohjeita, joita yhtiö voisi hyödyntää tietoturvakäytännöissään. Toimenpiteet ja aikataulu (IT-päällikkö) • Osallistujat: it-päällikkö • It-päällikkö ottaa yhteyttä kaupungin tietoturvapolitiikkaa valmisteleviin henkilöihin (kesä 2025) • Saadun tiedon mukaisesti it-päällikkö tekee tässä suositellut arvioinnit (alkuvuosi 2026) • Tietoturvapolitiikan linjaukset huomioon ottava katsaus VAV:n tietoturvaan viedään hyväksyttäväksi johtoryhmälle osana tietoturvan vuosiraportointia (kevät 2026)
3. Tietosuojaa koskeva ohjeistus ja menettelyt	
Tarkastuksessa arvioitiin VAV:n tietosuojatyön organisointia, ohjeistusta ja menettelyitä. VAV:n tietosuojatyö perustuu vuosikelloon, joka sisältää keskeiset tietosuojatoimenpiteet, kuten koulutukset, raportoinnit ja riskien arvioinnit. VAV:n tietosuojakäytännöt ovat hajautettuina intranetissä eri osioihin, mutta yhtenäistä, kattavaa tietosuojaohjetta ei ole. Tarkastuksessa havaittiin, että VAV:n käytännöt eivät kaikilta osin vastaa Vantaan kaupungin tietosuojoinen politiikan mukaisia linjauksia. Tarkastuksessa kiinnitettiin huomiota mm. seuraaviin asiakokonaisuuksiin, jotka mainitaan tietosuojoinen politiikassa osana osoitusvelvollisuutta. • VAV:n käsittelee tietoturvaloukkaukset tapauskohtaisesti, eikä sillä ole niiden käsittelyyn dokumentoitua prosessia. Kaupungin tietosuojoinen politiikassa tietoturvaloukkauksia koskeva prosessi on kytketty osaksi rekisterinpitäjän osoitusvelvollisuutta. • VAV:n tietosuojakoulutukset ja testit eivät ole yhdenmukaiset kaupungin tietosuojoinen politiikan vaatimusten kanssa, joiden mukaan työntekijöille tulee olla pakolliset tietosuojakoulutukset ja testit.	

a)	Suositus Tietosuojavastaava varmistaa, että henkilötietojen tietoturvaloukkausten käsittely- ja raportointimenettelyt ovat linjassa Vantaan kaupungin tietosuojapolitiikan toimintamallien kanssa, ja että prosessi on asianmukaisesti dokumentoitu. Toimenpiteet ja aikataulu (tietosuojavastaava) • Osallistujat: tietosuojavastaava, it-päällikkö • Käydään VAV:n olemassa oleva ohjeistus läpi ja päivitetään sitä tarvittaessa (kesä 2025) • Varmistetaan että henkilökunnan saatavilla on ohjeistus tietoturvaloukkaustilanteisiin (kesä 2025)
b)	Suositus Tietosuojavastaava varmistaa, että VAV:n nykyiset koulutuskäytännöt vastaavat kaupungin tietosuojapolitiikan pakollisten tietosuojakoulutusten ja testien vaatimuksia, ja päivittää käytännöt tarvittaessa. Toimenpiteet ja aikataulu (tietosuojavastaava) • Osallistujat: tietosuojavastaava, it-päällikkö • VAV:n tietosuojavastaava selvittää kaupungin tietosuojakoulutusten – ja testien vaatimukset ja käytännöt (kesä 2025) • VAV arvioi VAV:n toimintaan ja tarpeisiin soveltuvimman tietosuojakoulutusten- ja testien kokonaisuuden ja päivittää käytäntöjään tarpeen mukaan (syksy 2025 – kevät 2026)

c)

Suositus

Tietosuojavastaava varmistaa, että VAV:lla on kattava ja selkeästi jäsennelty tietosuojatyöhön liittyvä ohjeistus, joka on saatavilla yhtiön intranetissä yhtenä kokonaisuutena.

Toimenpiteet ja aikataulu (tietosuojavastaava)

- Osallistujat: tietosuojavastaava, it-päällikkö
- Käydään VAV:n olemassa oleva ohjeistus läpi ja päivitetään sitä tarvittaessa (kesä 2025)
- Pyritään varmistamaan intran ohjekokonaisuuden havainnollisuus ja opastavuus (syksy 2025)