

JAKELU:

Kaupunginhallitus
Pekka Timonen
KH:n konsernijaosto
Riikka Kiljander-Kiiskinen

Jussi Särkelä
Mirka Saarholma
Maria Lukkarinen

TIETOSUOJAN TOTEUTUMINEN VAV-KONSERNISSA

1

Tarkastuksen kohde, tavoite ja tausta

Tarkastuksen kohteena oli Vantaan kaupunkikonserniin kuuluva VAV-konserni.

Tarkastuksen tavoitteena oli varmistaa, että VAV-konsernissa noudatetaan tietosuojaan liittyvää lainsäädäntöä ja ohjeistusta, mukaan lukien Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, yleinen tietosuoja-asetus, kansallinen tietosuoja-lainsäädäntö sekä Vantaan kaupungin tietosuojapolitiikka.

Tarkastuksessa arvioitiin myös yleisellä tasolla tietoturvakäytänteitä siltä osin, kuin ne voivat vaarantaa tietosuojan toteutumista.

2

Tarkastuksen toteutus

Tarkastus toteutettiin helmi–maaliskuussa 2025, ja siinä arvioitiin erityisesti, miten VAV-konserni noudattaa Vantaan kaupungin tietosuojapolitiikkaa, joka on hyväksytty kaupunginhallituksessa 18.11.2024. Tietosuojapolitiikka koskee myös Vantaan kaupungin tytäryhteisöjä. Tarkastuksessa keskityttiin siihen, miten VAV toteuttaa osoitusvelvollisuuttaan Vantaan kaupungin tietosuojapolitiikassa esiin nostettujen keskeisten toimenpiteiden osalta (tietosuojapolitiikka: ”3.1. Osoitusvelvollisuus”).

Tarkastus kuuluu sisäisen tarkastuksen vuoden 2025 vuosisuunnitelmaan.

3**Olennaiset tarkastushavainnot ja toimenpidesuosituks**

VAV ei ole tehnyt kattavasti tietosuojalainsäädännön mukaisia vaikutustenarviointeja tietojärjestelmiinsä, joissa käsitellään henkilötietoja. Yhtiön mukaan sillä on 19 tietojärjestelmää, joissa käsitellään henkilötietoja. Tarkastushavaintojen mukaan niistä ainoastaan kolmeen on tehty vaikutustenarviointi.

VAV on käyttänyt vaikutustenarviointien tekemiseen Excel-pohjaista arviointityökalua, joka ei sisäisen tarkastuksen näkemyksen mukaan kata kattavasti tietosuojalainsäädännön vaatimuksia. Työkalusta puuttuvat keskeiset osiot, kuten tietosuojaperiaatteiden ja rekisteröidyn oikeuksien arviointi.

VAV:lla on kymmenen tietosuojaselostetta, joista yhdeksän on julkaistu VAV:n verkkosivuilla. Sisäinen tarkastus ei havainnut selosteissa olennaisia puutteita.

VAV ei ole varmistanut, että se on *huomioinut* tietosuojatyössään kaupunginhallituksen 18.11.2024 hyväksymän uuden **tietosuojapolitiikan** vaatimukset. VAV:n mukaan yhtiö ei ole saanut ilmoitusta uudesta politiikasta konsernipalveluista.

Vantaan kaupunki valmistelee tarkastushetkellä uutta **tietoturvapoliitikkaa**. Ko. politiikkaluonnoksen mukaan se tulee myös huomioida tytäryhteisöjen toiminnassa. Uusi tietoturvapoliitikka tulee täten vaikuttamaan myös VAV:n toimintaan.

VAV:lla ei ole dokumentoitua prosessia henkilötietojen tietoturvaloukkauksille. VAV:n mukaan tietoturvaloukkaukset käsitellään tapauskohtaisesti tietosuojavastaavan ja johtoryhmän toimesta.

VAV:n tietosuojakoulutukset eivät ole linjassa kaupungin tietosuojapolitiikan kanssa, joiden mukaan työntekijöille tulee olla pakolliset tietosuojakoulutukset ja testit.

Tarkastusraportissa on annettu 8 toimenpidesuositusta.

Tarkastushavaintojen perusteella voidaan todeta, että tietosuoja koskevan hallinnoinnin ja sisäisen valvonnan taso on tyydyttävä / hyvä, huomioiden, että merkittävä osa vaikutustenarvioinneista on tekemättä.

Seuraavassa on esitetty olennaiset tarkastushavainnot tiivistetysti sekä niiden perusteella tehty toimenpidesuosituksset.

1. Vaikutustenarviointien tekeminen

VAV:n mukaan yhtiöllä on 19 tietojärjestelmää, joissa käsitellään henkilötietoja. Tarkastushavaintojen mukaan vaikutustenarviointi on tehty ainoastaan kahteen 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.

Sisäinen tarkastus suosittelee tarkastuksen perusteella seuraavaa:

- a) 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.
- b) VAV täydentää tietosuojavastaavan johdolla jo tehtyjä vaikutustenarviointeja siten, että ne sisältävät tietosuojaperiaatteiden kattavan tarkastelun (esim. lainmukaisuus, 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.
- c) 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.

2. Vantaan kaupungin tietosuojapolitiikan ja tietoturvapoliitiikan huomioiminen

Vantaan kaupungin tietosuojapolitiikan mukaan politiikka on otettava huomioon kaupungin tytäryhteisöjen toiminnassa. Tarkastuksessa ilmeni, että VAV ei ole var-

mistanut, 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 tietoturvapoliittikkaa, joka tulee politiikan luonnosversion mukaan niin ikään huomioida jatkossa tytäryhteisöjen toiminnassa.

Sisäinen tarkastus suosittelee tarkastuksen perusteella seuraavaa:

- a) 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.
- b) IT-päällikkö seuraa aktiivisesti Vantaan kaupungin tietoturvapoliitiikan 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.

3. Tietosuoja 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 tietosuojapolitiikan mukaisia linjauksia. Tarkastuksessa kiinnitettiin huomiota mm. seuraaviin asiakokonaisuuksiin, jotka mainitaan tietosuojapolitiikassa osana osoitusvelvollisuutta.

- VAV:n käsittelee tietoturvaloukkaukset tapauskohtaisesti, eikä sillä ole niiden käsittelyyn dokumentoitua prosessia. Kaupungin tietosuojapolitiikassa tietoturvaloukkauksia koskeva prosessi on kytketty osaksi rekisterinpitäjän osoitusvelvollisuutta.
 - VAV:n tietosuojakoulutukset ja testit eivät ole yhdenmukaiset kaupungin tietosuojapolitiikan vaatimusten kanssa, joiden mukaan työntekijöille tulee olla pakolliset tietosuojakoulutukset ja testit.
-

Sisäinen tarkastus suosittelee tarkastuksen perusteella seuraavaa:

- a) Tietosuojavastaava varmistaa, että henkilötietojen tietoturvaloukkausten käsittely- ja raportointimenettelyt ovat linjassa Vantaan kaupungin tietosuojapolitiikan toimintamallien kanssa, ja että prosessi on asianmukaisesti dokumentoitu
- b) Tietosuojavastaava varmistaa, että VAV:n nykyiset koulutuskäytännöt vastaavat kaupungin tietosuojapolitiikan pakollisten tietosuojakoulutusten ja testien vaatimuksia, ja päivittää käytännöt tarvittaessa.
- c) Tietosuojavastaava varmistaa, että VAV:lla on kattava ja selkeästi jäsennelty tietosuojatyöhön liittyvä ohjeistus, joka on saatavilla yhtiön intranetissä yhtenä kokonaisuutena

4**Tarkastushavainnot**

Tarkastuksessa arvioitiin erityisesti, onko VAV huomioinut toiminnassaan kaupungin tietosuojapolitiikassa esiin nostetut rekisterinpitäjän osoitusvelvollisuuteen liittyvät asiakokonaisuudet. Tarkastuksessa kiinnitettiin huomiota muun muassa seuraaviin kokonaisuuksiin:

- Onko asianmukaiset tietosuojaohjeet tai muu vastaava kokonaisuus, josta tietosuoja-käytännöt käyvät ilmi.
- Tehdäänkö vuosittain tietotilinpäätös.
- Onko tietosuojavastaava nimetty ja onko hänellä varahenkilö.
- Onko tietosuojan vaikutustenarviointiprosessi toteutettu asianmukaisesti, mukaan lukien käytössä olevat työkalut.
- Ovatko henkilötietojen tietoturvaloukkauksille ja asiakirjapyyntöille määritellyt prosessit käytössä.
- Toteutuvatko työntekijöille määrätyt pakolliset tietosuojakoulutukset ja testit.
- Onko rekisteröityjen informointiin ja tietopyyntöihin yhtenäinen malli.
- Laaditaanko selosteet käsittelytoimista prosessien mukaisesti.
- Onko tietosuoja koskeva ohjeistus työntekijöiden saatavilla.
- Onko laadittu sopimusmallit ja ohjeet henkilötietojen käsittelijöille.
- Siirretäänkö henkilötietoja EU:n ja ETA:n ulkopuolelle ainoastaan tietosuoja-asetuksessa määritellyin perustein.

4.1.**VAV:n tietosuojatyön yleinen organisointi**

VAV:n tietosuojatyö on organisoitu vuosikellon mukaisesti, jossa määritellään kuukausittaiset tietosuojatoimenpiteet, kuten koulutukset, raportoinnit ja ohjeistusten päivitykset. Vuosikelloon sisältyy myös riskien arviointi, tietosuojaohjeistusten kartoitus, lainsäädännön muutosten seuranta sekä puolivuotisraportoinnit ja niiden käsittely johtoryhmässä. Lisäksi tietosuojatyöhön kuuluu jatkuvia tehtäviä, kuten sisäinen käytönvalvonta, tietoturvaloukkausten käsittely ja rekisteröityjen tietopyyntöihin vastaaminen. Tarkastuksessa arvioitiin erityisesti, onko VAV:n tietosuojatyön organisoinnissa huomioitu Vantaan kaupungin tietosuojapolitiikan keskeiset osoitusvelvollisuuteen liittyvät asiakokonaisuudet (huom. vaikutustenarvioinnit ja tietosuojaselosteet käsitelty omissa kappaleissaan).

Tarkastushavainnot:

- *Tietosuojavastaavaa koskevat järjestelyt.* VAV:lla on tietosuojavastaava. Hänen ollessaan vanhempainvapaalla tammikuusta 2025 alkaen, tehtävät ovat siirtyneet yhtiön lakimiehelle, joka toimii väliaikaisena tietosuojavastaavana. Hänen varahenkilönänsä toimii hallintopäällikkö. VAV:n käytäntönä on, että tietosuojavastaava raportoi tietosuojatyön edistymisestä johtoryhmälle kahdesti vuodessa vuosikellon mukaisesti. Johtoryhmä hyväksyy vuosikellon ja tarkastelee puolivuotisraportit.
- *Tietotilinpäätöksen puuttuminen.* VAV ei laadi tietotilinpäätöstä, joka tukisi kaupungin tietosuojapolitiikassa esiin nostettua osoitusvelvollisuutta. Tietotilinpäätös mainitaan kaupungin tietosuojapolitiikassa osoitusvelvollisuuden välineenä, mutta sen laatiminen ei ole tietosuojalainsäädännön mukaan pakollista.
- *Henkilötietojen siirrot.* VAV ei siirrä henkilötietoja EU:n tai ETA-alueen ulkopuolelle, mutta tiettyjen palveluntarjoajien osalta dataa saatetaan siirtää Yhdysvaltoihin EU:n hyväksymän Data Privacy Framework (DPF) -mekanismin mukaisesti.
- *Sopimusmallit ulkopuolisille toimijoille.* VAV on laatinut ulkopuolisille toimijoille, kuten IT-palveluntarjoajille, jotka käsittelevät VAV:n henkilötietoja valmiit sopimusmallit. VAV:lla on käytössä laaja tietoturvaluottamus sopimus sekä suppeampi sitoumus, joka kattaa salassapidon, henkilötietojen käsittelyn ja tietoturvan. Lisäksi tapauskohtaisesti voidaan laatia yksilölliset olosuhteet huomioiva sopimus näiden kahden mallin välimaastosta. Tarkastuksessa ei erikseen arvioitu sopimusmallien asianmukaisuutta.
- *Rekisteröityjen informointikäytännöt.* Rekisteröityjen informointi tapahtuu verkkosivujen tietosuojaosion, tietosuojaselosteiden ja työntekijöille tarkoitettun intranet-sivuston kautta. Verkkosivut kuvaavat yleiset tietosuojakäytännöt, tietosuojaselosteet tarjoavat tarkempaa tietoa henkilötietojen käsittelystä, ja työntekijät saavat ohjeistusta Tietosuoja ja tietoturva -intrasivustolta.

4.2.

Tietosuojaa koskeva ohjeistus

VAV:lla ei ole erillistä tietosuojapolitiikkaa tai -ohjetta, mutta siihen liittyvät ohjeistukset on koottu intranetin Tietosuoja ja tietoturva -sivustolle.

Tarkastushavainnot:

- **Tietosuojaohjeistus.** Intrasivuilla on kuvattu organisaation tietosuojaperiaatteet, henkilötietojen käsittelykäytännöt, tietosuojan merkitys sekä keskeiset säädökset, kuten EU:n yleinen tietosuoja-asetus ja kansallinen tietosuojalaki. Intrasivuilla on myös tietosuojaselosteet eri rekistereille, kuten asukkaiden, työnhakijoiden ja yhteistyökumppaneiden tietosujakäytännöt, jotka ovat saatavilla myös yhtiön julkisilla verkkosivuilla. Intrasivujen liitteenä on seuraavat ohjeet:
 - 1) Tietosuoja ja -turva etätyössä
 - 2) Tietopyyntöjen käsittelyohje
 - 3) Asiakkaiden henkilötietojen käsittely ja kirjauskäytännöt (Asukkaiden henkilötietojen kirjauskäytännöt Tampuurissa)
 - 4) VAV tietoturvaohje henkilökunnalle
 - 5) Säilytysaikadokumentti
 - 6) Ohjeet henkilötietojen siivoamiseksi tietokoneelta, ja
 - 7) Täydennetyt ohjeet henkilötietojen siivoamiseksi.
- **Tietoturvaloukkaukset.** Vantaan kaupungin tietosuojapolitiikassa on linjattu, että tietoturvaloukkauksille on oma prosessinsa; joka on tunnistettu osaksi rekisterinpitäjän osoitusvelvollisuutta. Tarkastushavaintojen mukaan VAV:lla ei ole erillisesti dokumentoitua prosessia henkilötietojen tietoturvaloukkauksille. Tietoturvaloukkaukset käsitellään tapauskohtaisesti tietosuojavastaavan ja johtoryhmän toimesta. VAV dokumentoi kaikki loukkaukset erilliseen Exceliin. Tarkastuksessa ilmeni, että viimeisen 7 vuoden aikana on tapahtunut 16 tietoturvaloukkausta.
- **Henkilötietojen säilytys ja poistaminen.** Intrasivuilla löytyy liitetiedostona "Säilytysaikadokumentti", jossa on tiedot henkilötietojen säilytysajoista, tietoryhmistä ja säilytysajan perusteista. Tietojen poistoprosessia ei kuitenkaan ole dokumentoitu. Ei ole kuvattu, poistetaanko tiedot automaattisesti vai manuaalisesti, kuka vastaa poistamisesta tai miten varmistetaan, että tiedot poistetaan määräajan umpeuduttua.
- **Rekisteröityjen asiakirjapyynnöt ja niiden käsittely.** Vantaan kaupungin tietosuojapolitiikassa on linjattu, että osana rekisterinpitäjän osoitusvelvollisuutta henkilötietoja koskeville asiakirjapyynnöille on oma prosessinsa. Tarkastushavaintojen mukaan VAV:lla on dokumentoitu ohjeistus tietopyyntöjen käsittelyyn, jossa kuvataan, miten tietopyyntöihin vastataan, kenelle pyynnöt ohjataan sekä mitä määräaikoja noudatetaan. VAV:n mukaan viimeisen vuoden aikana on vastaanotettu yksi

asiakirjapyyntö, joka sisälsi sekä tietojen tarkastuspyynnön että poistopyynnön, ja siihen vastattiin dokumentoidun prosessin mukaisesti.

- **Henkilöstön tietosuojakoulutus ja testit.** Vantaan kaupungin tietosuojapolitiikassa linjataan osana rekisterinpitäjän osoittamisvelvollisuutta, että työntekijöille on *pakolliset* tietosuojakoulutukset ja testit. Tarkastushavaintojen mukaan tietosuoja-koulutukset on mainittu intrasivuilla, mutta niiden toteutustapaa, aikataulua ja seurannan vastuuta ei ole selkeästi esitetty. VAV:n mukaan yhtiöllä ei ole pakollisia tietosuojakoulutuksia tai testejä. VAV järjestää vuosittain vähintään yhden tietosuojakoulutuksen, joista viimeisin pidettiin 19.11.2024, sekä alkuvuoden tiimivierailut osana tietosuojatyön vuosikelloa. Näissä käsitellään henkilötietojen käsittelyjärjestelmät, mahdolliset ongelmakohdat ja päivitystarpeet. Uudet työntekijät perehdytetään tietosuojavastaavan toimesta.
- **Vantaan kaupungin tietosuojapolitiikan huomioiminen.** Vantaan kaupungin 18.11.2024 hyväksytyn tietosuojapolitiikan mukaan se koskee myös kaupunkikonsernin tytäryhteisöjä, ja se on otettava huomioon niiden toiminnassa. VAV:n mukaan sen nykyisissä tietosuoja- ja tietoturvakäytännöissä on huomioitu Vantaan kaupungin 28.5.2018 hyväksymä tietosuoja- ja tietoturvapoliittikka, mutta tarkastuksessa ei voitu todentaa, miten kyseinen politiikka on konkreettisesti huomioitu, sillä VAV:n tietosuojakäytäntöjä koskevissa asiakirjoissa ei ollut siitä erillisiä mainintoja. Tarkastushavaintojen perusteella VAV ei ole suorittanut erillistä arviointia siitä, miten uusi, 18.11.2024 hyväksytty tietosuojapolitiikka vaikuttaa sen toimintaan, eikä tarkastuksessa havaittu näyttöä siitä, että sen sisältöä olisi sovellettu tietosuojakäytännöissä.
- **Vantaan kaupungin tietoturvapoliittikan huomioiminen.** VAV:n tietoturvapoliittikka ja henkilökunnan tietoturvaohje on uusittu keväällä 2024. VAV:n mukaan politiikan laatimisessa on huomioitu Vantaan kaupungin 28.5.2018 hyväksymä tietosuoja- ja tietoturvapoliittikka, mutta asiakirjoissa ei ole mainintoja siitä, että kaupungin ohjeistukset olisi suoraan huomioitu yhtiön toiminnassa. Tarkastushetkellä kaupunki valmistelee uutta tietoturvapoliittikkaa, joka tulee koskemaan myös tytäryhteisöjä ja jonka huomioiminen niiden toiminnassa on edellytetty.

4.3.

Henkilötietojen käsittelijän seloste käsittelytoimista (tietosuojaseloste)

VAV:lla on kymmenen tietosuojaselostetta, joista yhdeksän on julkaistu VAV:n verkkosivuilla.

- Vuokra-asuntojen hakijarekisterin tietosuojaseloste
 - Asuntojen vuokralaisia koskeva tietosuojaseloste
 - Taloyhtiön asukasrekisterin/talonkirjan tietosuojaseloste
 - Puhelu-, chat- ja WhatsApp-tallenteiden tietosuojaseloste
-

- Käyttäjähallinta- ja lokirekistereiden tietosuojaseloste
- Yritysassiakas-, toimittaja- ja yhteistyökumppanirekisterin tietosuojaseloste
- Rakennushankkeiden tietosuojaseloste
- Työnhakijarekisterin tietosuojaseloste
- Tallentavan kameravalvonnan tietosuojaseloste
- Henkilöstöhallinnon tietosuojaseloste

Tarkastuksessa arvioitiin, sisältävätkö selosteet asianmukaiset tietosisällöt, kuten rekisterinpitäjän ja tietosuojavastaavan tiedot eli onko selosteessa selkeästi mainittu, kuka vastaa rekisteristä ja miten tietosuojavastaavaan saa yhteyden; rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät eli onko määritelty, mitä henkilötietoja kerätään ja mihin tarkoitukseen niitä käytetään; tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle eli onko mainittu, siirretäänkö tietoja EU-/ETA-alueen ulkopuolelle ja millä perusteilla; sekä tekniset ja organisatoriset turvatoimet eli onko selostettu, miten tiedot suojataan ja millaisia tietoturvakäytäntöjä noudatetaan.

Tarkastushavainnot:

- **Selosteiden kattavuus.** Tarkastetut selosteet sisälsivät tietoja, kuten rekisterinpitäjän ja tietosuojavastaavan yhteystiedot; henkilötietojen käsittelyn oikeusperusteet ja tarkoitukset; kenelle tietoja luovutetaan tai siirretään; rekisterin suojauksen periaatteet ja tietojen säilytysaika.
- **Päiväyksen puuttuminen.** Useista tietosuojaselosteista puuttui päiväys, mikä vaikeuttaa niiden ajantasaisuuden arviointia ja seuranta.

4.4.

Tietosuojalainsäädännön mukaiset vaikutustenarvioinnit

Sisäinen tarkastus arvioi, onko VAV tehnyt asianmukaiset vaikutustenarvioinnit tietojärjestelmiinsä, joissa käsitellään henkilötietoja. Tämän lisäksi tarkastuksessa arvioitiin, onko VAV:n vaikutustenarviointeihin käyttämä työkalu asianmukainen, ja täyttää tietosuojalainsäädännön vaatimukset.

Tarkastushavainnot:

- VAV:n mukaan sillä on 19 tietojärjestelmää, joissa käsitellään henkilötietoja. Tarkastuksessa ilmeni, että vaikutustenarviointi on tehty ainoastaan niistä kolmeen järjestelmään.

- VAV on kaupungin tytäryhteisönä toteuttanut vaikutustenarviointeja Excel-pohjaisella työkalulla, joka keskittyy riskien kuvauksiin, seurauksiin, hallintatoimenpiteisiin ja jäännösriskeihin. Sisäisen tarkastuksen näkemykseen mukaan VAV:n vaikutustenarviointityökalu ei kata kaikkia olennaisia vaikutustenarviointien osa-alueita, jotka arvioinneissa tulisi huomioida (vrt. esim. Vantaan kaupungin työkalu):
 - **Tietosuojaperiaatteet:** Vaikutustenarvioinnista puuttuu tietosuojaperiaatteiden arviointi ja keskeisten menettelyjen kuvaus seuraavilta osin: lainmukaisuus ja kohtuullisuus (mm. käsittelyperusteiden määrittely), läpinäkyvyys (mm. rekisteröityjen informointi), käyttötarkoitussidonnaisuus (mm. käyttötarkoituksen tekninen ja organisatorinen varmistaminen), tietojen minimointi (mm. tarpeettomien tietojen välttäminen ja anonymisointi), säilytyksen rajoittaminen (mm. säilytysajat ja tietojen hävittämismenettely), täsmällisyys (mm. tietojen ajantasaisuuden seuranta) sekä luottamuksellisuus, eheys ja käytettävyys (mm. tietoturvaloukkauksiin reagointi).
 - **Rekisteröidyn oikeudet:** Vaikutustenarvioinnista puuttuu rekisteröidyn oikeuksien arviointi sekä keskeisten menettelyjen kuvaus liittyen oikeuteen saada pääsy tietoihin (esim. tietojen toimitustavat, tietolähteet ja mahdolliset rajoitukset), oikeuteen tietojen oikaisemiseen (esim. oikaisupyyntöjen käsittely ja erimielisyyksien ratkaisu), oikeuteen tietojen poistamiseen (esim. poistamisprosessit ja ilmoitukset vastaanottajille), oikeuteen tietojen käsittelyn väliaikaiseen rajoittamiseen (esim. rajoitusten käytännön toteutus ja tekniset keinot), oikeuteen tietojen siirtämiseen (esim. tekniset edellytykset ja käytännön toteutus), oikeuteen vastustaa käsittelyä (esim. vastustamisoikeuden prosessi ja soveltuminen käsittelyyn) sekä automaattiseen päätöksentekoon ja profilointiin (esim. perusteiden määrittely, rekisteröityjen informointi ja tietosuojan varmistaminen).
 - **Tietojen siirrot:** Vaikutustenarvioinnista puuttuu arviointi henkilötietojen käsittelijöistä (esim. tunnistetut käsittelijät, heidän asettamiensa kriteerien täyttyminen ja sopimukset) sekä henkilötietojen siirroista ETA-alueen ulkopuolelle (esim. siirtojen kohdemaat, palvelimien fyysinen sijainti, etäyhteydet, vakiosopimuslausekkeiden soveltaminen ja suojatoimenpiteiden riittävyys)
 - **Käsittelyn tarpeellisuus ja oikeasuhteisuus:** Vaikutustenarvioinnista puuttuu arvio suunnitellun käsittelyn tarpeellisuudesta (esim. käsiteltävien tietojen määrä ja laajuus) sekä selvitys siitä, onko olemassa vähemmän henkilötietojen suojaan puuttuvia keinoja, joilla voidaan saavuttaa sama tavoite (esim. tietojen anonymisointi tai suppeampi tiedonkeruu).
 - **Hyväksymisprosessi:** Vaikutustenarvioinnista puuttuu dokumentoitu hyväksymisprosessi, jonka vuoksi arviointeja (ml. jäännösriskit) ei hyväksytä virallisesti.
-

3.4.2025

Sisäinen tarkastus / Mikko Paananen

Sisäisen tarkastuksen näkemyksen mukaan VAV:n työkalu ei täytä tietosuojalainsäädännön vaatimuksia puuttuvien osioiden vuoksi.

5**Jälkitarkastus**

Jälkitarkastus tehdään noin vuoden kuluttua.



Mikko Paananen
sisäinen tarkastaja



Pentti Asumus
tarkastusjohtaja