

# Tietotilinpäättös

## 2021

Julkinen



# Sisällysluettelo

---

|                                                                                      |           |                                                                  |           |
|--------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------|-----------|
| <b>Esipuhe .....</b>                                                                 | <b>3</b>  | <b>6 Arviointi ja mittarit .....</b>                             | <b>22</b> |
| <b>1 Johdanto.....</b>                                                               | <b>4</b>  | 6.1 Rekisteröityjen oikeuksien toteutuminen.....                 | 22        |
| <b>2 Yleiskatsaus ja tilannearvio.....</b>                                           | <b>6</b>  | 6.2 Tietoturvapoikkeamat ja häiriöt.....                         | 24        |
| 2.1 Tietotilinpäätöksen tarkoitus.....                                               | 6         | 6.3 Henkilötietojen tietoturvaloukkaukset.....                   | 25        |
| 2.2 Muutokset Espoon kaupungin sisäisessä ja ulkoisessa<br>toimintaympäristössä..... | 6         | <b>7 Kyberturvallisuuden tiedotus, koulutus ja valvonta.....</b> | <b>28</b> |
| 2.3 Megatrendit.....                                                                 | 7         | <b>8 Tietoriskien hallinta.....</b>                              | <b>29</b> |
| <b>3 Tiedonhallinta.....</b>                                                         | <b>9</b>  | <b>9 Auditoinnit .....</b>                                       | <b>30</b> |
| 3.1 Kokonaisarkkitehtuurityö.....                                                    | 10        | <b>10 Todennetut kehittämiskohteet vuodelle 2022 .....</b>       | <b>31</b> |
| 3.2 Toiminta-arkkitehtuurityö.....                                                   | 11        |                                                                  |           |
| 3.3 Tietoarkkitehtuurityö .....                                                      | 12        |                                                                  |           |
| 3.4 ICT-arkkitehtuurityö .....                                                       | 12        |                                                                  |           |
| 3.5 Espoon kaupungin tietohallinto TIHA.....                                         | 13        |                                                                  |           |
| <b>4 Tiedolla johtaminen.....</b>                                                    | <b>14</b> |                                                                  |           |
| <b>5 Tietosuoja ja tietoturvallisuuden toteutuminen.....</b>                         | <b>15</b> |                                                                  |           |
| 5.1 Konsernihallinto KOHA .....                                                      | 15        |                                                                  |           |
| 5.2 Hyvinvoinnin ja terveyden toimiala HYTET .....                                   | 16        |                                                                  |           |
| 5.3 Kasvun ja oppimisen toimiala KOTO.....                                           | 17        |                                                                  |           |
| 5.4 Kaupunkiympäristön toimiala KYT .....                                            | 17        |                                                                  |           |
| 5.5 Tietosuojaryhmät ja tietosuojayhteistyö<br>kaupunkiorganisaatiossa .....         | 18        |                                                                  |           |
| 5.6 Tietoturvaryhmä ja tietoturvatoimet .....                                        | 19        |                                                                  |           |
| 5.7 Yhteistyöverkostot .....                                                         | 21        |                                                                  |           |

# Esipuhe

---

Vuosi 2021 oli Espoon kaupungin tietoturvalle ja henkilötietosuojalle kiireinen; sitä leimasi valmistautuminen tiedonhallintalain velvoitteisiin, kiristyshaittaohjelmien muuttuminen tavanomaiseksi osaksi hyökkääjien työkalupakkia, haasteet turvallisen viestinnän ja koulutuksen järjestämisessä, sekä loppuvuodesta ilmestynyt Log4j-haavoittuvuus, joka aiheutti laajan ja välittömän päivitystarpeen usealle järjestelmälle.

Samanaikaisesti haittaohjelmia tehtailevat tahot jatkoivat jalkautumista eri viestintäkanaviin, joista tekstiviestit näkivät erityistä, ulkomailta tulevien viestien lukumäärän kasvua. Nämä trendit eivät koskeneet pelkästään Espoota, mutta ne osoittivat Espoon sisäisen ja ulkoisen toimintaympäristön jälleen muuttuneet ja tarpeen reagoida muutoksiin.

Reagointi edellyttää resursseja, joita käytetään kunnan kyberturvallisuuden jatkuvaan valvontaan, kehittämiseen ja ylläpitoon. Keskusteluissa muiden kuntien kanssa nousi esille yhteinen tarve lisäkäsille, jonka Espoo havaitsi myös TAISTO'21 -harjoituksessa: tietoturva ja henkilötietosuojat ovat liian harvojen käsissä. Myös tämä on riski, sillä avainhenkilöstön poissaolot ja siirtymät voivat väliaikaisesti rampauttaa kunnan kyberturvallisuuden hoidon.

Oman haasteensa kyberturvallisuuden ylläpidolle tulee aiheuttamaan 2023–2024 tapahtuva hyvinvointialueiden perustaminen, jonka johdosta suosittelemme panostamaan hyvään lähtötilanteeseen jo nyt. Sijoittamalla lisähenkilökuntaa tietoturvan ja henkilötietosuojan kohentamiseen sallitaan tulevien hyvinvointialueiden periaatetta turvallisuutta kohentavia käytäntöjä, ohjeita, koulutuksia ja tekniikkaa, joilla kunta edesauttaa siirtymän onnistumista.

Sijoitus kyberturvallisuuteen onkin sijoitus tulevaisuuteen, joka edellyttää tulevaisuuden tekijöitä.

Espoossa 21.04.2022

**Harri Säkkinen**

Espoon kaupungin  
tietoturvapäällikkö

**Paula Pernilä**

Espoon kaupungin  
tietosuojavastaava

# 1 Johdanto

---

2020 aikana uutisoinnissa olivat Huawei ja Kiinan suorittama vakoilu. 2021 huomio siirtyi enemmän systemaattiseen informaatiovaikuttamiseen. Informaatiovaikuttami-sella pyritään muokkaamaan kohdeyleisön mielipidettä omille pitkän ajan tavoitteille suotuisammaksi eikä se ole totuuteen pyrkivää. Suoraan Espoon kaupunkiin ei ole toistaiseksi kohdistunut laajempia informaatiovaikuttamisen kampanjoita.

Keskustelu pilvipalveluiden ympärillä jatkui koko vuoden ajan. Uutta ohjeistusta saatiin ja Espoo päätyi käymään läpi kaikki hallinnolliset ja juridiset keinot, joilla pilvipalveluihin liittyvään sääntelyyn voidaan vastata. Mikäli nämä eivät riitä, niin myös teknisiä suojauskeinoja harkitaan. Näistä voi syntyä merkittäviä lisäkustannuksia.

Koronaepidemia kääntyi trendinä kohti päättymistään, mutta koronan aikana käyttöön otetut etäkäytännöt olivat edelleen voimassa ja etä-asiointin merkitys kasvoi. Espoon asiointipalveluissa kokeiltiin liikkuvaa neuvontapalvelua, sähköistä allekirjoitusta sujuvoitettiin ja konekäännöksiä testattiin osana asiakaspalvelua. Turvapostia ei kaupungille saatu käyttöön ja se siirtyi osaksi tulevaa kilpailutusta. Muitakin ratkaisuja selvitettiin, joista Suomi.fi-viestit osoittautui realistisimmaksi vaihtoehdoksi ja sen käyttöä suositeltiin.

2021 Espoota eniten koetelleet ulkoiset uhkatekijät koostuivat kiristämällä rahaa hakevista petostehtailijoista ja ulkomaisista rikollisista. Siirtymä hyvinvointialueisiin vaikutti organisaation sisäisesti ja jo nyt hyvinvoinnin ja terveyden toimialue painottaa toteutuksessaan siirtymän edellyttämiä toimia. Muulla kaupungilla lainmukaisuuden toteuttaminen tiedonhallintalain osalta on edennyt.

Muutosvaikutusten arviointia toteutetaan osana kokonaisarkkitehtuuri-ryhmän työtä, ja vastuita kirjattiin hallintosääntöön ja toimintaohjeisiin. Tietoaaineistojen digitalisointi jatkuu ja viranomaisten katseluyhteyksiä eri tietovarantoihin kehitetään 2023 asti, mutta huomioidaan jo hankinnoissa. Vuoden aikana tehtiin noin 90 kokonaisarkkitehtuurikäsittelyä ja 2022 keskeiseksi teemaksi valittiin tiedonhallintalain tietoturva vaatimusten toteuttaminen.

Merkittäviä toiminnallisia kehittämistöitä olivat HR- ja talousprosessien, sekä OmaEspoo-asiointin uudistaminen. Kansallisesti merkittävää varhaiskasvatuksen toiminnanohjausta ja toiminnanohjausjärjestelmä eVakaa kehitettiin. Kaupungin keräämiä ydintietoja pyritään jatkossa tuomaan laajemmin eri yksiköiden saataville, kuten asiakas- ja toimipistetiedot. Kaupungin henkilöstö-, palkanhallinta- ja talouden johtamisjärjestelmän, sekä Espoo.fi -verkkosivuja uudistettiin merkittävästi. Kansallisesti merkittäviä kehitysprojekteista Espoo osallistui muun muassa DigiOne-oppimisolustan työhön.

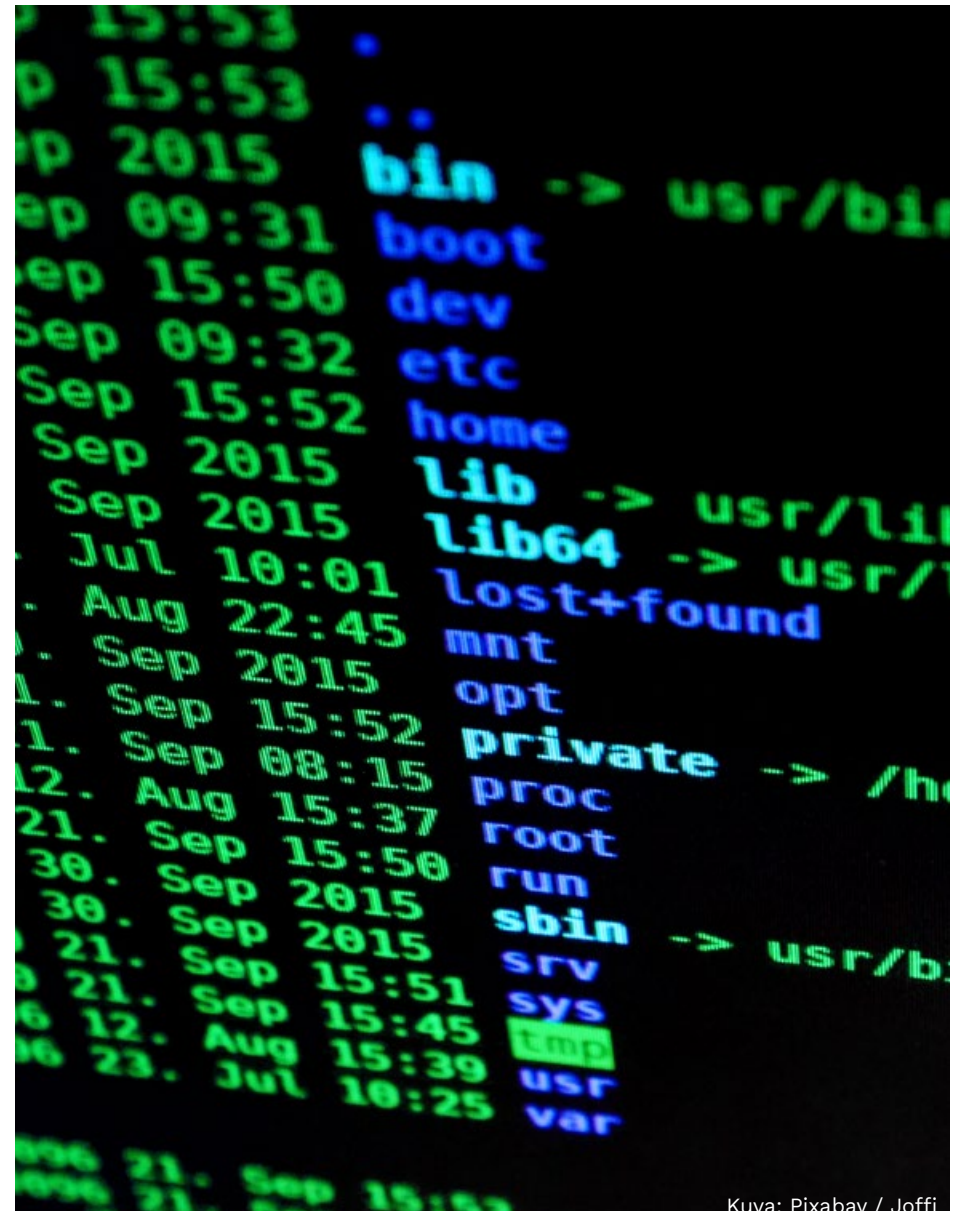
Kaupungin teknistä tietoturvaa kehitettiin uudella verkon valvontapalvelulla ja siirtämällä oppilaat erilliseen verkkoon, joka oli aiemmin yhteinen oppilaiden ja työntekijöiden kesken. Sivistyksen eVaka-järjestelmän ansiosta paperisten lomakkeiden käytöstä voidaan luopua ja tehdä kännykällä läsnäolokirjaukset. Paperittomuuden odotetaan lisääntyvän toiminnan siirtyessä järjestelmään.

Kaikilla toimialoilla on osallistuttu henkilöstön tietoturva- ja henkilötietosuoja-koulutukseen. Näiden suoritusasteet olivat 2021 aikana kuitenkin liian matalat ja koulutusta kehitetään edelleen. Mahdollisia pakkokeinoja harkitaan, kuten verkkotunnuksien lukkiutuminen mikäli kurssia ei ole suoritettu.

Kaupungin tietosuoja- ja tietoturvaryhmät kokoontuivat vuoden aikana yhteensä 22 kertaa. Tietosuoja on omaksuttu osaksi uusien toimintojen

tai hankintojen kehitystyötä, joissa tietosuojan vaatimukset on huomioitu hyvin. Ryhmissä käsitellyt aiheet koskettivat laajaa kirjoa kysymyksiä, kuten:

- Tietojen siirto kolmansiin maihin ja brittien erkaantuminen EU:sta
- Tietoriskien ja vaikutustenarviointityökalujen uudistaminen
- Esitys kyberturvallisuusasiantuntijan rekrytoimiseksi
- Hankintojen turvallisuus- ja tietosuojaliitteiden päivittäminen
- Eri ohjeiden päivitys, laajennus ja koonti Essiin
- Tietosuojavaltuutetun päätökset ja Espooseen kohdistuneet vaatimukset
- Turvallisuuskävelyjen tulokset
- Puutteet kameravalvonnassa
- Osallistuminen kansallisiin kyberturvallisuusharjoituksiin
- Kyberturvallisuuteen vaikuttavien häiriöiden seuranta, kuten laaja Log4j-haavoittuvuus, laittomat puhelutallenteet ja kaapatut verkkotilit



Kuva: Pixabay / Joffi

## 2 Yleiskatsaus ja tilannearvio

Yleiskatsauksessa tarkastellaan ensin tietotilinpäätöksen tarkoitusta ja muutoksia Espoon ulkoisessa toimintaympäristössä. Kaupunkien ja kuntien ulkoiseen toimintaympäristöön vaikuttavat paitsi kansainväliset trendit, mutta myös EU:n velvoittavat asetukset, Suomen oma lainsäädäntö ja toimialakohtaiset määräykset esimerkiksi Terveiden ja Hyvinvoinnin Laitokselta (THL).

### 2.1 Tietotilinpäätöksen tarkoitus

Espoon kaupunki laatii vuosittain tietotilinpäätöksen tietosuojavastaavan ja tietoturvapäällikön johdolla. Tietotilinpäätöksen tiedot perustuvat toimialojen ja käyttäjien toimittamiin tietoihin omasta toiminnastaan, sekä kyberturvallisuudesta vastaaville henkilöille itselleen kertyneistä tiedoista. Ensimmäinen tietotilinpäätös julkaistiin 2018 ja tämä koonti on sarjassaan neljäs, josta on tehty kaksi painosta: yleisölle julkinen, Espoon kaupungin verkkosivuilla julkaistava versio ja kaupungin sisäinen, joka sisältää johdolle tarkoitetun yhteenvedon ja tietoja, jotka paljastuessaan saattaisivat vaarantaa kaupungin edut.

Tietotilinpäätöksen laatiminen ei ole lakisääteinen tehtävä, mutta sen avulla Espoon kaupunki ja muut tietotilinpäätöksiä tuottavat kunnat pyrkivät kirjallisesti osoittamaan kuinka tietoturva ja tietosuoja toteutuvat kaupungilla. Sillä rakennetaan luottamusta kertomalla henkilötietojen käsittelystä ylätasolla, ja osoitetaan kunnan huolehtivan kuntalaistensa tietojen suojelusta. Tietotilinpäätöksiä vertailemalla on myös mahdollista havaita eroavaisuuksia kaupunkien painotuksissa, mikä voi luoda pohjaa laajemmalle vertailulle.

Tämän dokumentin kohdalla painotetaan tietosuojan ja tietoturvan toteutumista, sekä arvioidaan vuoden aikana tapahtuneita toimintaympäristön

muutoksia suhteessa Espoon toimintaan, havaittuja riskejä, onnistumisia sekä kyberturvallisuuden kehityksen suuntia. Kehittyminen tapahtuu sekä kaupungin ulkopuolella, eli ulkoisten toimijoiden välillä, että kaupungin sisällä tekniikan, käytäntöjen ja henkilökunnan muuttuessa.

Tästä tietotilinpäätöksestä laaditaan sekä sisäinen, kaupungin johtoryhmälle esiteltävä versio, että kaupungin verkkosivuilla julkaistava julkinen versio. Julkinen versio tietotilinpäätöksestä on tarkoitettu kuntalasilta, sidosryhmille ja kaupungin omille työntekijöille.

### 2.2 Muutokset Espoon kaupungin sisäisessä ja ulkoisessa toimintaympäristössä

Kunnan vastuiden lisääntyminen lakien konkretisoituessa johti vuoden aikana kasvaneisiin työmääriin vastuiden valvomisessa ja toteuttamisessa. Seuraukset ovat kumulatiivisia, eli kunnan ulkopuolelta tulevat uudet lait, ohjeet, suositukset, huomautukset ja määräykset astuvat vanhojen rinnalle näitä poistamatta tai korvaamatta, jolloin työmäärä kasvaa. On siis ennustettavissa, että uusia Espoota koskevia velvoitteita syntyy myös tulevien vuosien aikana.

2021 osoitti, että Espoolla on vielä tehtävää EU:n yleisen tietosuojasetuksen, eli GDPR:n, vaatimusten varmistamisessa, kuten esimerkiksi kuntalaisten tarkastusoikeudesta omiin tietoihinsa ja henkilötietojen käsittelystä informoinnissa. Näihin liittyvät tietosuojaselosteet ja prosessit ovat olemassa, mutta näiden tarkkuus ja tehokkuus eivät vuoden aikana joutuneet monella toimialalla laajempaan testiin. Mikäli kuntalaiset alkavat tarkastamaan omia tietojaan laajemmin ja useammin, eli aktivoimaan tarkastusprosesseja, niin myös lainmukaisuuden voidaan ennustaa kohe-nevan käytön myötä.

Kaupunki onnistui informoimaan tietosuojavaltuutettua ja muita viranomaisia, kuten Valviraa, heitä koskevista asioista siltä osin kuin tapaukset tulivat kaupungin tietoturvasta ja tietosuojasta vastaavien tietoon. Valviran

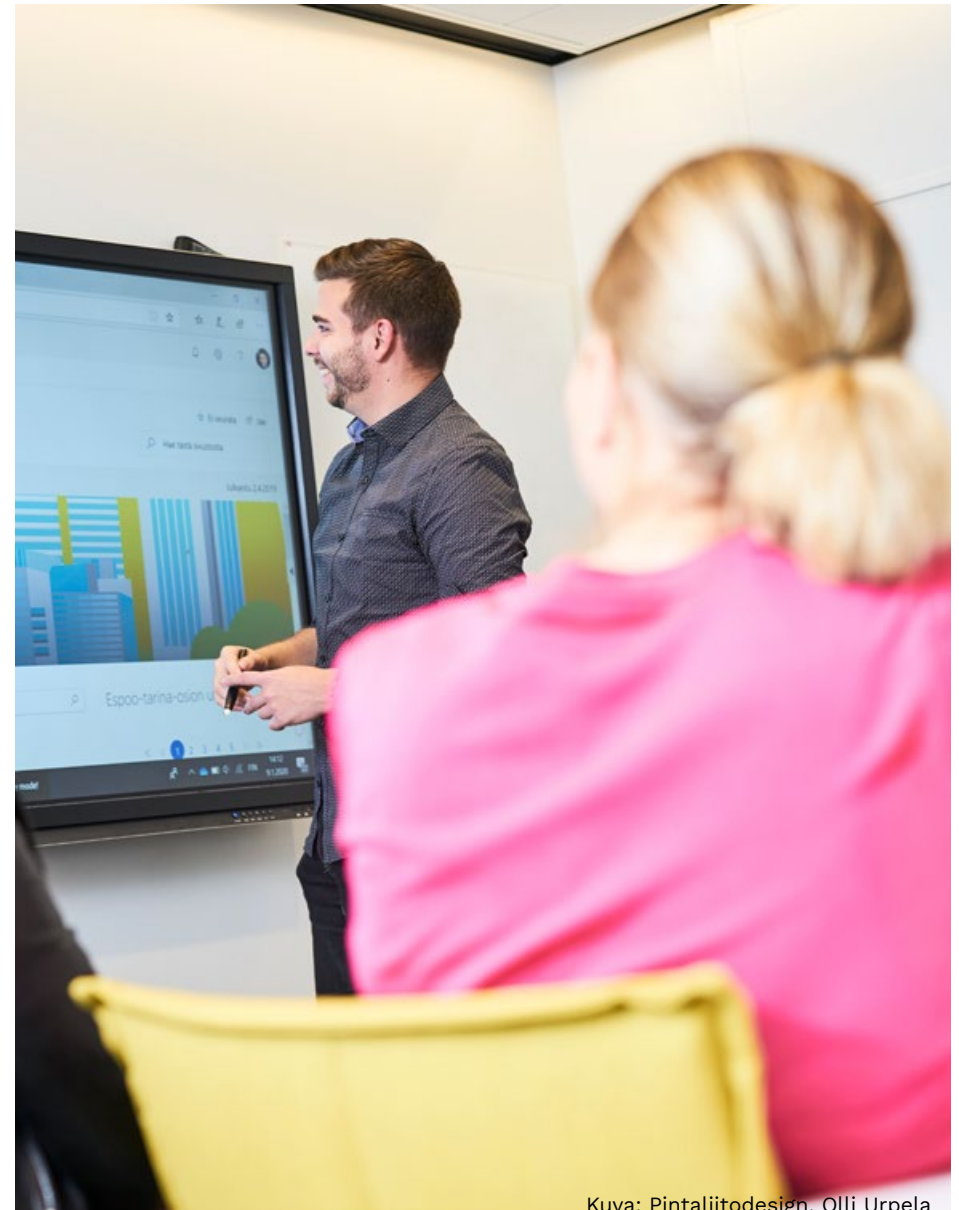
ja Kyberturvallisuuskeskuksen roolien korostuminen kuluvan vuoden aikana tulee johtamaan suurempaan määrään ilmoituksia näille viranomaisille sikäli kuin häiriöitä tapahtuu.

Vuoden aikana Espooseen kohdistuvat kyberturvallisuutta koettelevat ulkoiset uhkatekijät koostuivat pääosin ammattimaistuneesta, ulkomaisesta petostehtailusta ja haittaohjelmien jakelusta. Motiivina toimi ja toimii jatkossakin rahojen kiristäminen, joka nojaa toiminnan lukumäärälliseen volyymiin. Petostehtailijoiden jakelukanavat laajenivat ja vahvistuivat tekstiviesteissä ja ajoittaisissa puhelinsoitoissa, mutta vuosi näki myös muutamia yrityksiä toimitusjohtajapetoksissa. Kokonaisuutena ulkoisessa toimintaympäristössä ei ole havaittu erityisesti Espooseen kohdistuvaa uhkaa.

Hyvinvointialueiden muodostaminen on jo aiheuttanut selkeän muutoksen kaupungin sisäisessä toimintaympäristössä hyvinvointi-, terveys- ja pelastuspalveluiden suunnatessa voimavarat tulevaan siirtymään. Muutoksien ennakoita konkretisoituvan 2023–2024 välisenä aikana ja jatkuvuudelle on oleellista, että kyberturvallisuus huomioidaan jo nyt, ja Espoon tehtäviä jatkava turvallisuushenkilöstö saa tarvitsemansa perehdytyksen tällä hetkellä tehtäviä hoitavalta henkilöstöltä, sekä perii nykyisen tietopääoman ja ohjeet.

## 2.3 Megatrendit

Espoon kaupunki seuraa maailmalla vallitsevia megatrendejä ennakoitakseen tulevia kansallisia ja alueellisia muutoksia tuotteissa, ihmisissä, prosesseissa ja yhteistyökumppaneissa. Megatrendien seuraaminen ja ymmärtäminen luo kokonaiskuvaa kaupungin kannalta merkittävistä yhteiskunnallisista muutoksista, esimerkiksi Euroopan sotilaallisen turvallisuustilanteen kiristyminen ja pilvipalveluiden suojaamiseen liittyvä keskustelu.



Kuva: Pintaliitodesign, Olli Urpela



Edellisen vuoden tietotilinpäätöksessä Kiinan tekemä vakoilu ja Huawei olivat uutisissa, mutta 2021 aikana informaatiovaikuttaminen erityisesti Venäjän suunnalta sai enemmän jalansijaa, josta suojelupoliisi varoitti julkisesti eri tiedotusvälineissä. 2022 aikana informaatiovaikuttamisen syyt paljastuivatkin Ukrainan sodan syttymisenä. Informaatiovaikuttamisella tarkoitetaan sosiaalisen median alustoilla, kuten Facebook, Twitter ja TikTok, tapahtuvaa valheellisen tai yksipuolisen tiedon jakamista pitkänkin aikavälin strategisten tavoitteiden saavuttamiseksi. Esimerkiksi tyytymättömyyden herättäminen henkilöstössä myöhempää hyödyntämistä varten tai yleisen epäluottamuksen herättäminen turvallisuuskäytäntöjä kohtaan, joilla kuntaorganisaation toimintakykyä heikennetään asteittain.

Aktiivista ja tavoitehakuista informaatiovaikuttamista ei ole toistaiseksi havaittu Espoolla, mutta mahdollisiin kampanjoihin on hyvä varautua esimerkiksi harjaannuttamalla asiakaspalveluhenkilökunta kovaakin painostusta vastaan. Tietojen hankkiminen henkilökuntaa painostamalla tai päätöksentekoon vaikuttaminen uhkailun keinoin ovat näkyneet yksittäisinä tapauksina muun muassa korona-ilmiantojen kohdalla, mutta painostus ja uhkailu eivät ole olleet systemaattista. Tämän hetken tilanteessa ensisijainen varautumiskeino on koulutus.

Pilvipalveluiden suojaamiseen liittyvä keskustelu on ollut laajaa EU:ssa ja Suomessa, mutta ilman selkeitä, yhtenäisiä linjauksia. Ongelman ytimessä on pilvipalvelun toimittajaa velvoittavan lainsäädännön nojalla tapahtuva asiakkaan salassa pidettävien tietojen luovuttaminen ulkomaiselle viranomaiselle, vaikkakin tämä on toistaiseksi vielä toteutumaton riski. Muun muassa Microsoft esittää yhtenä ratkaisuna digitaalisten maarajojen ("EU Data Boundary") luomista, mutta edelleen on epäselvää onko tämä tarpeeksi vastaamaan huoleen Microsoftin laillisen ja Yhdysvaltojen lain pakottaman pääsyn estämisestä kunnan tietovarantoihin. Terveiden ja hyvinvointin laitos puolestaan asetti lausuntokierrokselle luonnoksen määräyksestä THL/4309/5.09.00/2021 (s.9), joka suoraan velvoittaisi kuvaamaan kuinka salassa pidettävät tiedot on suojattu kolmansien maiden viranomaisilta -ja johtopäätöksensä: olemaan sijoittamatta näitä tietoja pilveen mikäli niitä

ei ole suojattu. Tuolla ajanhetkellä luonnos vei keskustelua kohti teknisiä suojauskeinoja, kun pääosa keskusteluista liittyi ensisijaisesti hallinnollisiin ja juridisiin keinoihin.

Näitä juridiikan keinoja kommentoi Yhdysvaltain kongressin palvelu, joka julkaisi dokumentin Euroopan ja Yhdysvaltojen välisistä tietovirroista ja niiden suojaamisesta ("U.S.-EU Privacy Shield and Transatlantic Data Flows 09-2021"), päätyen ainoastaan siihen lopputulokseen, että ongelmaa ei voida ratkaista pelkästään juridiikan keinoin vaan tarvitaan myös teknisiä estotoimia. 2021 aikana keskustelun edetessä odotuksena oli, että vaatimukset tulevat konkretisoitumaan sekä teknisinä suojaustoimenpiteinä ja tietojen kryptauksena, mutta myös hallinnollisina toimintaan velvoittavina määräyksinä. 2022 alussa keskustelu ja toiminta kuitenkin kääntyi kohti tietojen minimointia ja pseudonymisointia johtuen teknisten ratkaisuiden hinnasta.

Muina megatrendeinä koronaviruspandemian jatkuminen, verkkoasioinnin vahvistuminen ja sähköautoistumisen vahvistuminen olivat uutisissa. Näistä kaksi ensimmäistä olivat vahvassa yhteydessä toisiinsa, sillä suosituksien kontaktien välttämiseksi ja asiakaspalvelupisteiden rajoitukset johtivat suoraan asioinnin siirtymiseen verkkoon. Esimerkiksi oirearvioinnit puhelimessa ja lähihoitajan tapaamiset Teams:ssä nousivat aikaisempaa tavallisemmiksi. Tietoturvan näkökulmasta tämä korostaa viestintävälineiden turvallisuuden takaamista aikaisempaa enemmän, koska pitkällä aikajänteellä valittuihin viestintäkanaviin kertyy laaja määrä asiakastietoa ja tietoa, joka on erityisen suojeluvelvoitteen alaisista.

Espoolla trendi johti kysymyksiin sähköpostien suojaamisesta ja Teamsin käytöstä viestimänä. Myös pikaviestimiä, kuten Whatsappia, Signalia ja Threemaa, arvioitiin asiakaspalvelun näkökulmasta, mutta joita ei vuoden aikana otettu laajasti käyttöön. Laajempänä trendinä on kuitenkin tietoturvallisten, digitaalisen viestinnän alustan saaminen Espoon kaupungin tai yleisesti kuntien käyttöön, jossa viestinnän kaikki osapuolet on aina tunnistettu vähintään kahdella eri metodilla.



### 3 Tiedonhallinta

Laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki 906/2019) astui voimaan 1.1.2020. Laissa säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. Laissa säädetään myös tietojärjestelmien yhteentoimivuudesta ja tietoturvallisuuden toteuttamisesta.

Espoon kaupungin tiedonhallinta kuvattiin prosessiperustaiseksi **tiedonhallintamalliksi** vuoden 2020 aikana modulaarisena toteutuksena. Tiedonhallintamalli julkaistiin sisäisessä intranetissä kokonaisarkkitehtuurityövälineessä, joka on nähtävillä koko kaupungin henkilöstölle ja hyödynnettävissä esim. kehittämistehtävissä. Tiedonhallintamallin sisältö koostetaan useaan eri työvälineeseen kertaalleen tallennetuista tiedoista ja sitä ylläpidetään jatkuvasti.

Tiedonhallintaan liittyviä info- ja koulutustilaisuuksia järjestettiin kevään 2021 aikana. Lisäksi tiedonhallinnan koulutuskokonaisuutta suunniteltiin osaksi tietoturvan ja tietosuojan koulutusta, toteutus vuoden 2022 koulutustarjonnan uusimisen yhteydessä.

Tiedonhallintamallin sisältöön perustuva **asiakirjajulkisuuskuvaus** on asiakaslähtöinen kuvaus kaupungin tiedonhallinnasta ja se on julkaistu Espoon kaupungin internetsivuilla. Asiakirjajulkisuuskuvaus tuo näkymän viranomaisen asiankäsittelyssä ja palvelujen tuotannossa hyödynnettävistä tietoa-aineistoista. Kuvauksen tavoitteena on auttaa asiakkaita tietopyynnön sisällön yksilöinnissä ja tietopyynnön kohdistamisessa oikealle taholle.

Lain velvoittamaa **muutosvaikutusten arviointia** toteutetaan osana kokonaisarkkitehtuurityötä. Muutosvaikutusten arvioinnin tarkoituksena on tunnistaa kaupungin kehitystoimenpiteiden ja muiden toimintaympäris-

tömuutosten vaikutuksia tiedonhallintaan, arvioida niitä riskiperusteisesti sekä tunnistaa tiedonhallintamallin sisältöihin kohdistuvat päivitystarpeet.

Laissa asetetaan myös vaatimuksia tietoa-aineistojen digitalisoimiseksi siirtymäajalla, teknisten rajapintojen ja katseluyhteyksien avaamiseksi sekä tietoturvaluustoimenpiteiden kehittämiseksi siirtymäajoin aina vuoden 2023 loppuun asti, mutta joita tulee jo huomioida muun muassa järjestelmien toiminnallisissa ja teknisissä määrittelyissä sekä julkisten hankintojen ehtojen määrittelyissä kilpailutusten yhteydessä.



Tiedonhallinta on koko organisaation yhteinen tehtävä, johon liittyy vastuu oman toiminnan tiedonhallinnan ajantasaisuudesta sekä tietoturvallisuudesta huolehtimisesta ja tietosuojasäädösten noudattamisesta omassa toiminnassa. Tiedonhallinnan järjestämistehtäviin liittyvät johdon vastuut kirjattiin hallintosääntöön ja toimintaohjeisiin organisaatiouudistuksen yhteydessä. Kaupunkitasoinen tiedonhallinnan järjestämistehtävä on Konsernihallinnon Palvelukehitysyksikön tietojohdamisen vastuualueella.

Tiedonhallinnan **valvontaprosessi** kuvattiin ja laadittiin seurantatyökalu valvonnan kohteille. Tiedonkeruu toteutettiin tietotilinpäätöskyselyn yhteydessä. Valvontatyökalu perustuu valvontakohteiden kypsyystason pisteytykseen. Vuoden 2021 tiedonhallinnan valvonnan kypsyystaso oli 3.63 / 5.00, joka osoittaa, että tiedonhallinta on kaupungin toiminnassa määriteltä ja johdettua. Vuoden 2021 seurannassa suurimmat tiedonhallinnan kehittämistoimenpiteet kohdistuivat ohjeiden päivitystarpeisiin ja koulutusten järjestämiseen.

### 3.1 Kokonaisarkkitehtuurityö

Kokonaisarkkitehtuurityö mahdollistaa tiedonhallinnan ja tiedon hyödyntämisen strategisen kehittämisen, luo yhteentoimivuutta toimintamallien, tietojärjestelmien ja organisaation osien välille, auttaa varmistamaan tietoturvan ja tietosuojan toteutumista, sekä tukee kaupungin toimialoja ja yksiköitä heidän omassa kehittämistyössään. Kaupungin tiedonhallinnassa kokonaisarkkitehtuurityö luo näkyvyyttä nykytilaan, asettaa tavoitearkkitehtuurin ja tarjoaa muutosvaikutusten arvioinnin kautta ymmärrystä siihen, mitä tietoturvan, asioiden käsittelyn ja tietosuojan osalta ratkaisujen suunnittelussa tulisi ottaa huomioon. Kokonaisarkkitehtuurin avulla luodaan edellytykset järjestelmien ja tietojen yhteentoimivuudelle omassa organisaatiossa ja suhteessa muihin kansallisiin organisaatioihin.

Tiedonhallintalain edellyttämän tiedonhallintamallin laatiminen nosti kaupungin kokonaisarkkitehtuurityön kyvykkyyksiä ja kypsyystasoa, kun



Kuva: Taru Turpeinen

organisaation prosessit, tietovarannot, tietoaineistot ja järjestelmät kuvattiin yhtenäiseksi kokonaisuudeksi ja näin nykytilasta saatiin kattava näkymä kehittämisen ja hankintojen tueksi.

Lain edellyttämä muutosvaikutusten arviointimenettely otettiin osaksi kokonaisarkkitehtuurityötä. Dokumentoinnin osalta muutosarviointi tarkoit-

taa jo käytössä olevan kokonaisarkkitehtuuridokumentaation laajentamista tietoaaineistojen käsittelyjen osalta aiempaa laajemmaksi ja huomion kiinnittämistä teknisten rajapintojen kuvauksiin sekä tietoturvatarkoituksiin. Muutosvaikutusten arvioinnin avulla voidaan tunnistaa tiedonhallinnan suunnitteluun liittyviä kohtia toiminnan, tietoaaineistojen ja niiden käsittelyjen, digitaalisten aineistojen ja rajapintojen hyödyntämisen sekä tietoturvan näkökulmista. Muutosvaikutusten arvioinnin yhteydessä hyödynnetään olemassa olevaa tiedonhallintamallin sisältöä nykytilasta ja tunnistetaan muutostarpeet tiedonhallintamallin sisältöön tavoitetilassa, kun kehitysprojekti on viety läpi ja toimintaympäristö on projektin myötä muuttunut. Huomioitavaa on, että muutosvaikutusten arviointi ei koske vain digitalisointiprojekteja tai järjestelmien kehittämistä, vaan tarkastelu ulottuu arvioimaan myös toiminnallisia ja hallinnollisia vaikutuksia esimerkiksi kaupungin toimintaan kohdistuneesta uudesta lakisääteisestä tehtävästä tai organisaatiouudistuksen johdosta.

Vuoden 2021 aikana vahvistettiin kokonaisarkkitehtuurityön rakenteita, laajennettiin työskentely verkostomaiseksi yhteistyöryhmäksi ja kehitettiin yhteistyötä tietohallinnon ICT-arkkitehtuuriprosessin kanssa.

Vuoden 2021 aikana toteutettiin 92 kokonaisarkkitehtuurikäsittelyä, mukaan lukien tiedonhallinnan muutosvaikutusten arvioinnit, joita oli yhteensä 19. Vuonna 2021 käsittelyjen painopisteinä olivat toiminta- ja tietoarkkitehtuurin kehittäminen, jossa onnistuttiin hyvin. Vuoden 2022 painopistealueiksi otetaan tietoturvan toimenpiteiden kehittäminen tiedonhallintalain raameissa sekä toiminnallisen muutosvaikutusten arvioinnin ja hyötyjen seurannan kehittäminen (toiminta-arkkitehtuuri ja muutosjohtaminen). Jälkimmäisellä toimenpiteellä on vaikutuksia pidemmällä tähtäimellä myös **Taloudellisesti kestävä Espoo** -ohjelman hyötyjen seurannalle.

Tiedonhallinnan muutosvaikutusten arvioinnin osalta suurin tehtävä vuonna 2021 oli laatia arviointi organisaatiomuutoksesta, johdon vastuista, sekä tiedonhallintamallin päivitys tältä osin.

Vuoden 2022 suurin muutosvaikutusten arviointi tulee olemaan hyvinvointialueeseen liittyvä uudistus ja sen myötä muutokset palvelujen järjestämiseen, johdon vastuisiin sekä poistuviin tehtäviin, prosesseihin, tietovarantoihin, tietoaaineistoihin ja järjestelmiin Hyvinvoinnin ja terveyden toimialan sekä Länsi-Uudenmaan pelastuslaitoksen tehtäviin liittyen.

Kaupungilla on edustus Kuntaliiton kuntien kokonaisarkkitehtuuriverkostossa ja valtiovarainministeriön tiedonhallintalautakunnan alaisessa julkisen hallinnon toiminnan kehittämisen arkkitehtuuriyhteistyöryhmässä.

## 3.2 Toiminta-arkkitehtuurityö

Tiedonhallintalain edellyttämä kuvaus organisaation tiedonhallinnasta vauhditti kaupunkitasoisten toiminta-arkkitehtuurikuvausten laatintaa. Vuoden aikana jatkettiin edellisen vuoden aikana kootun toimintaprosessit, tietovarannot, tietojärjestelmät ja tietoaaineistokuvaukset yhteen tuovan tiedonhallintamallin jatkokehittämistä ja ylläpitoa. Näiden kuvausten ylläpito on keskitettynä tietojohdamisen vastuualueelle ja tiedonhallintamallin päivitystyöhön käynnistettiin prosessi osana kokonaisarkkitehtuurityötä.

Operatiivisen toiminnan kuvaustaso on tiedonhallintamalliin sisältyvää ylätasen prosessikarttaa tarkemmalla tasolla sisältäen yksityiskohtaisempia palvelu- ja prosessikuvauksia. Näiden kuvausten laatimista jatketaan edelleen eri kehittämistoimenpiteiden yhteydessä. Kaupunki on tarjonnut vuonna 2021 henkilöstölle koulutusta prosessien kuvaamiseen ja prosessien laatutyöhön sisäisenä konsultaationa ja prosessikoulutuksina ulkoisen kumppanin kanssa. Kaupungin prosesseissa tapahtuvilla muutoksilla on usein vaikutuksia toiminnassa hyödynnettäviin tietoihin, tietovarantoihin ja tietojärjestelmiin. Kokonaisarkkitehtuurikuvauksien avulla kehitysprojektien yhteydessä on mahdollista tunnistaa toimintaan vaikuttavia muutoksia ja riippuvuuksia verrattaessa tilannetta nykytilasta tavoitelaan. Usein toiminnassa tapahtuvilla muutoksilla on vahva riippuvuus niin kustannushyötyjen realisoitumiseen kuin myös tietoturvaan ja tietosuojaan liittyviin toimiin.

Merkittäviä toiminnallisia kehittämistöitä vuonna 2021 olivat HR- ja talousprosessien uudistamistyö, varhaiskasvatuksen toiminnanohjauksen kehittäminen sekä kaupunkitasoisten asioinnin prosessien yhtenäistämisen ja uudistamistyö OmaEspoo-projektissa.

Toiminta-arkkitehtuurin tavoitteet vuodelle 2022 ovat toiminnallisen muutoksen tunnistaminen digitalisoinnin yhteydessä, kokonaishyötyjen arvioiminen ja muutosjohtamisen kehittämisen tukeminen.

### 3.3 Tietoarkkitehtuurityö

Tietoarkkitehtuurityö on kokonaisarkkitehtuurityön osa-alue, jossa tarkastellaan erityisesti tietosisältöjä ja niiden tallentamista, tietojen siirtymistä tehtävien ja niitä tukevien tietojärjestelmien välillä, sekä eri tehtävissä käytettävien tietojen yhteentoimivuutta ja laatua. Tietoarkkitehtuurityön keskeisenä tavoitteena on, että kukin tieto kirjattaisiin vain kerran, jonka jälkeen se olisi luotettavasti hyödynnettävissä kaikkialla, missä sitä tarvitaan.

Tietoarkkitehtuurityön tavoitteiden saavuttaminen vaatii riittävää kokonaisuuden suunnittelua ja erityisesti eri näkökulmien ja toisistaan eroavien tiedon hyödyntämisen tarpeiden huomiointia.

Kun tiedonhallinnan kehittämistä tehdään erillisinä hankkeina ja projekteina eri toimijoiden toimesta, sisältyy tähän aina riskinä, ettei yksittäisen kehittämistyön lopputulos ole yhteentoimiva muualla toteutettavien ratkaisujen kanssa. Tietoarkkitehtuurityön tehtävänä on luoda näkymää yli eri kehittämistoimien niin kaupungin sisäisessä kehittämisessä kuin kansallisen tason kehittämiseen kytkeytyen, jotta toteutetut ratkaisut olisivat yhteensopivia ja tukevat tiedon laadun ylläpitoa ja nostoa.

Eräs merkittävä tietoarkkitehtuurityön huomion kohde on ydintietojen hallinta. Ydintiedoilla tarkoitetaan kaupungin toiminnan keskeisiä kohteita kuvaavia tietoja, kuten asiakastiedot ja toimipistetiedot, jota hyödynnetään useissa toiminnoissa ja eri tietojärjestelmissä läpi kaupungin toiminnan.



Kuva: Heidi-Hanna Karhu

Hyvä ydintietojen hallinta näkyy niin parempana palveluna asiakasrajapinnassa kuin kaupungin organisaation toiminnan tehostumisena. Laadukas, jäsennelty, käyttökelpoinen, ajantasainen ja saatavilla oleva tieto mahdollistaa tiedon hyödyntämisen niin kaupungin palveluiden tuottamisessa kuin toimintojen johtamisessa ja kehittämisessä.

### 3.4 ICT-arkkitehtuurityö

Espoon ICT-arkkitehtuuri pitää sisällään kokonaisarkkitehtuurin tietojärjestelmä- ja teknologianäkökulmat strategisella, taktisella ja operatiivisella tasolla. Yhdessä toiminta- ja tietoarkkitehtuurinäkökulmien kanssa ICT-arkkitehtuuri muodostaa kokonaisnäkymän Espoon tietojärjestelmäkokonaisuuteen tietojärjestelmien ja teknologian näkökulmasta. Tietojärjestelmäarkkitehtuuria tuotiin osaksi tiedonhallintamallia vuoden 2021 aikana.

Tietojärjestelmäarkkitehtuurin kuvaaminen laajentaa tiedonhallintamallia tavoitetilan kuvauksiin ja tarkempiin teknisiin kuvauksiin esimerkiksi järjestelmäintegraatioiden ja infrastruktuurin osalta, joissa on myös huomioitu tiedon julkisuus ja tietoturvallisuus. Käytännön seurauksena osa tiedonhallintamallista on rajoitettujen ryhmien käytössä.

Arkkitehtuurityö on luonteeltaan jatkuvaa Espoon toimintaympäristön ja ympäröivän maailman seuraamista, jossa Espoon tulevaisuuden perustaa rakennetaan jo nyt varautumalla tuleviin tiedossa oleviin muutoksiin ja suunnittelemalla skaalautuvia, tietoturvallisia ja moderneja palvelupohjaisia ratkaisuja. Keskeisinä teemoina on ollut digikehityksen kiihdyttäminen ja tukeminen, uudet ketterät toimintamallit ja ICT-kyvykkyyksien yhteiskehittäminen sekä kaupunkitasoisen ICT-kehityksen ohjaus.

Tietohallinto on yhdessä toimialojen kanssa käynyt läpi ICT-kehitystarpeita, joiden pohjalta on koostettu toimialakohtaiset kehitystiekartat, jota operatiivisella tasolla kehitysprojektit toteuttavat Espoon kokonaisarkkitehtuuri-periaatteiden ja ICT-arkkitehtuurilinjausten mukaisesti. ICT-arkkitehtuuritoiminnolla on keskeinen rooli ohjata projekteja kohti tavoitetilaa.

ICT-arkkitehtuurityön keskeisiä vuoden 2021 kohteita Espoolla olivat henkilöstö- ja palkkahallintajärjestelmän ja talouden johtamisjärjestelmän, Espoo.fi-verkkosivujen sekä OmaEspoo-asiointipalvelun uudistamis- ja kehittämistyöt. Kansallisesti merkittäviä kehitysprojekteja ovat olleet varhaiskasvatuksen toiminnanohjausjärjestelmän sekä opetuksen ja oppimisen DigiOne-alustan kehittäminen.

Espoon ICT-arkkitehtuurihallinnan toimintamalliin sisältyvät viikoittaiset katselmointitapaamiset, eli niin sanotut ICTA-klinikat, joissa ICT-kilpailutuksia ja -projekteja tuetaan ICT-arkkitehtien toimesta esimerkiksi teknisiin rajapintoihin liittyvissä ja muissa teknistä asiantuntijuutta edellyttävissä kysymyksissä. Espoon ICTA-klinikoiden tukikäynneillä vierailee keskimäärin 2–6 kilpailutusta tai projektia kuukaudessa. Varsinaisia katselmointeja toteutetaan keskimäärin 30 kappaletta vuodessa.

### 3.5 Espoon kaupungin tietohallinto TIHA

Espoon tietohallinto hankki vuoden aikana kaupungin toiminnan tueksi erillisiä asiantuntijapalveluita muun muassa teknisten auditointien suorittamiseksi ja tietosuojaan liittyvien lainsäädännöllisten muutostarpeiden tunnistamiseksi. Kaupungin hankintasopimuksissa ei toistaiseksi oteta erikseen kantaa tiedonhallintalain vaatimuksiin muun muassa järjestelmien lokituksen, käyttäjähallinnan ja tietoliikenneyhteyksien suojaamisen kannalta. Kaikissa ICT-hankinnoissa käytetään kuitenkin erillisiä liitteitä, jossa tarkempia kyberturvallisuuteen liittyviä määrittelyitä on tehty.

2021 aikana tietohallinto suoritti yhteistyössä kaupungin toimialojen kanssa kahdeksan tietoturva-auditointia haavoittuvuustestauksina, kuten varhaiskasvatusjärjestelmän, potilastietojärjestelmän ja Espoon uusittujen www-sivujen haavoittuvuustestaukset. Näistä saatujen tuloksien avulla järjestelmissä päädyttiin turvallisempiin ratkaisuihin, kuten lisävahvistuksien käyttöön sisäänkirjautumisissa, ja havaitut tekniset puutteet korjattiin. Lopputuloksena kaikista auditoiduista järjestelmistä tuli tietoturvalisempia.

Tietohallinnon kautta kulki yhteensä 80 ICT-hankintasopimusta, joiden lisäksi solmittiin kansallisen hankintakynnyksen ylittäviä sopimuksia yhteensä 12 kappaletta. Kaupungin hankintakeskus solmi noin 1800 hankintasopimusta eri yritysten kanssa, joka osoittaa kaupungin käyttämien toimitusketjujen laajuuden. Näiden turvaamista myös alihankkijoiden osalta tullaan tarkastelemaan 2022 aikana esimerkiksi tietoturvasitoumuk-sien, viestinnän ja erityisen luotettavuuden osalta sikäli kuin palveluissa, hankinnoissa tai järjestelmissä käsitellään salassa pidettävää tietoa.



## 4 Tiedolla johtaminen

Tiedolla johtaminen tarkoittaa kaupungin palveluntuotannossa syntyvien tietojen hyödyntämistä päätöksenteon tueksi. Tiedon hyödyntämisellä nähdään olevan rooli erityisesti päätöksenteon valmistelun tukena ja kehittämistoiminnassa sen lisäksi, että tietoja hyödynnetään palveluja tuottaessa.

Kaupungin johtaminen on asiakkuuksien hallinnan, palvelujen järjestämisen ja palvelujen tuottamisen muodostamana kokonaisuus. Johtamisen tavoitteena on kuntalain mukaisesti edistää asukkaiden hyvinvointia ja alueen elinvoimaa sekä järjestää asukkaille palvelut taloudellisesti, sosiaalisesti, kulttuurillisesti ja ekologisesti kestäväällä tavalla. Tiedolla johtamisessa ja sen kehittämisessä on oleellista tunnistaa toiminnan kannalta tärkeät tiedot, analysoida niitä ja jakaa ne kaupungin eri organisaatioyksiköiden päätöksenteon kannalta keskeisille valmistelijoille ja päätöksentekijöille oikeaan aikaan.

Espoossa kaupunkitasoista tiedolla johtamista kehitetään muun muassa johtamisen ja talousohjauksen järjestelmäuudistuksen yhteydessä. Uudistuva järjestelmä tarjoaa analytiikkakyvykkyksiä, joiden avulla voidaan tukea asukas- ja asiakaslähtöisen Espoo-tarinan tavoitteiden toimeenpanoa uudistaen johtamisen ja talousohjauksen tiedonhallintaa ja toimintamalleja, prosesseja sekä toiminnan ohjauksen tietojärjestelmäkokonaisuutta. Vuoden 2022 kehittämistavoitteissa on tarkoitus huomioida tulevan Länsi-Uudenmaan hyvinvointialueen ja peruskaupungin välinen tiedon hyödyntäminen sekä yleisesti tietojohdamisen kyvykkyudet.

Espoon kaupungin tietohallinnon Saaga-analytiikka-alusta mahdollistaa analytiikan lisäksi muun muassa koneoppimisen ja tekoälyn hyödyntämisen toiminnan kehittämisessä sekä palvelutuotannossa. Vuonna 2021

analytiikka-alustalla toteutettiin mm. ”Varhaiskasvatuksen vaikutuksista oppilaiden lukutaitoon -raporttiin” perustuva datapohjainen Proof of Concept.

Kaupunki on toteuttanut tiedolla johtamisen kehittämistyötä myös organisaation kehittäjäkumppanien kanssa. Erityisesti VTT:n kanssa on tehty tiivistä yhteistyötä vaikuttavuuden johtamisen kehittämiseksi. Vaikuttavuuden johtaminen on Espoo-tarinaa toteuttava kehittämisohjelma, jonka tuloksena vahvistetaan vaikuttavuuden johtamista kestäväan kasvuun, hyvinvoinnin edistämiseen ja koronan jälkeiseen taloudelliseen elpymiseen valtuustokaudella 2021–2025. Kaupungissa on synnytetty uutta ymmärrystä tiedon hyödyntämisen mahdollisuuksista sekä opittu datan yhdistelemisestä tietoturvallisesti ja tietosuoja huomioiden. Kehittämisohjelman kolme kärkeä ovat kaupunkiorganisaation johtaminen, tietojohdaminen sekä kaupunkiyhteisön ja ekosysteemien johtaminen.



Kuva: Heidi-Hanna Karhu

## 5 Tietosuojan ja tietoturvallisuuden toteutuminen

---

Tässä kappaleessa tarkastellaan tietoturvan ja henkilötietosuojan toteutusta vuonna 2021 Espoon kaupunkiorganisaatiossa. Espoon kaupungissa toteutettiin syksyllä 2021 organisaatiouudistus, jonka johdosta organisaatio koostuu nyt neljästä toimialueesta ja yhdestä tulosalueesta. Nämä ovat: konsernihallinto KOHA, hyvinvointi ja terveys HYTET, kasvu ja oppiminen KOTO, kaupunkiympäristö KYT sekä elinvoiman tulosalue.

Näiden lisäksi Länsi-Uudenmaan pelastuslaitos LUP toimii toistaiseksi osana Espoon kaupunkia, mutta siirtyy HYTET:in mukana uudelle hyvinvointialueelle 2023-2024 aikana. On todennäköistä, että vuoden 2022 tietotilinpäätös on sekä HYTET:n, että LUP:n osalta viimeinen osana Espoon kaupunkia.

### 5.1 Konsernihallinto KOHA

Espoon kaupungissa konsernihallinto johtaa, ohjaa ja valvoo koko kaupunkikonsernia sekä vastaa kaupungin tukipalveluista kaupunginjohtajan johdolla. Konsernihallinnon yksiköt ovat:

- Rahoitus ja talous
- Henkilöstö
- Hallinto ja kehittäminen

Lisäksi kaupunginjohtajan johdolla toimivat elinvoiman tulosalue, sisäinen tarkastus, sekä vielä toistaiseksi myös Länsi-Uudenmaan pelastuslaitos. Nämä eivät kuitenkaan kuulu konsernihallintoon.

Koronapandemian aiheuttamat haasteet ja toiminnan turvaaminen pysyivät edelleen konsernihallinnon tyolistalla myös vuonna 2021. Läsäntöyöhön yritettiin palata asteittain syksyllä 2021, mutta pahentunut koronatilanne pakotti työntekijät jälleen etätyöhön. Konsernihallinnossa panostettiin vuonna 2021 joustavan asiakaspalvelun kehittämiseen. Espoon asiointipalveluissa kokeiltiin liikkuvaa neuvontapalvelua, jonka tarkoituksena on viedä neuvontapalveluja ja digitukea kohderyhmille, jotka näitä eniten tarvitsevat ja alueille, joissa ei ole kiinteää asiointipistettä. Sähköistä allekirjoitusta kehitettiin sujuvammaksi, kun kaupungin ulkopuolisille allekirjoittajille otettiin käyttöön rekisteröitymispalvelu. Käännössovellus-kokeilussa selvitettiin, voisiko käännössovelluksella tehostaa asiakaspalvelua ja tuoda kustannusvaikuttavuutta usein toistuvissa kaupungin palvelutilanteissa. Lisäksi kaupungin nettisivut uudistuivat syksyllä 2021.

Vuoden 2021 aikana tietohallinnon tekniseen tietoturvaan liittyvät kohdat olivat: uusien tietoturvakäytäntöjen käyttöönotto, tietoturvan valvontapalveluiden uudistaminen ja Espoon laajuisen identiteetin- ja käyttöoikeushallinnon uudistavan kilpailutuksen valmistuminen. Yksi olennaisesti tietoturvaa ja tietosuojaa parantava onnistuminen oli oppilaiden toimintaympäristön (EDU) eriyttäminen hallinnon toimintaympäristöstä.

Sote-uudistuksen toimeenpano muuttaa kaupungin toimintaa vuoden 2023 alusta. Myös konsernihallinnossa valmistauduttiin siihen, että osa hallinto- ja tukipalveluista siirtyy vuoden 2023 alussa Länsi-Uudenmaan hyvinvointialueelle. Ensijainen tavoite muutoksessa on varmistaa kaupungin palveluiden toimintakyky.





Kuva: Heidi-Hanna Karhu

## 5.2 Hyvinvoinnin ja terveyden toimiala HYTET

Hyvinvoinnin ja terveyden toimiala HYTET järjestää lakisääteisiä sosiaalihuollon ja terveydenhuollon palveluita kuntalaisille, jonka vuoksi hyvinvoinnin ja terveyden toimialalla käsitellään merkittäviä määriä salassa pidettäviä potilastietoja ja sosiaalihuollon asiakastietoja.

Hyvinvoinnin ja terveyden toimialalla on vuonna 2021 kehitetty tietosuojaa etenkin etätyön, sähköisten palveluiden sekä henkilökunnan tietosuojasaamisen ajantasaisuuden osalta. Koronaepidemian jatkuminen on vaikuttanut hyvinvoinnin ja terveyden toimialan toimintaan muun muassa niin, että etätyön määrä on kasvanut entisestään ja pandemian jatkumiseen on reagoitu lisäämällä etänä annettavia sosiaali- ja terveydenhuollon palveluita.

Toimialan toimintaympäristö on muutostilassa, koska hallituksen esitys hyvinvointialueiden perustamisesta sekä sosiaali- ja terveydenhuollon ja pelastustoimen järjestämisen uudistamisesta hyväksyttiin eduskunnassa 23.6.2021. Suomeen muodostettiin 21 hyvinvointialuetta, joille siirtyvät kuntien ja kuntayhtymien vastuulla nykyisin olevat sosiaali- ja terveydenhuollon sekä pelastustoimen tehtävät. Näin ollen kaikki Länsi-Uudenmaan hyvinvointialueen keskeiset toiminnot ja palvelut tulevat toimimaan asiakkaiden ja henkilöstön kannalta häiriöttä uudistuksen tullessa voimaan 1.1.2023.

Uudistus tuo muutoksia hyvinvoinnin ja terveyden tietosuojan kenttään. Asiakas - ja potilastietojen sekä hyvinvointialueen työntekijätietojen rekisterinpitäjäksi tulee Länsi-Uudenmaan hyvinvointialue, kun palveluiden järjestämisvastuu siirtyy.

Uusi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä eli asiakastietolaki tuli voimaan 1.11.2021. Uudella lailla kumottiin voimassa oleva laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Uusi asiakastietolaki velvoittaa sosiaalihuollon palvelunantajat

liittymään valtakunnallisiin Kanta-palveluihin. Lisäksi laki mahdollistaa sosiaalihuollon asiakastietojen luovuttamisen muille sosiaalihuollon palvelunantajille Kanta-palvelujen välityksellä. Laajan liittymisvelvoitteen ansiosta tiedot ovat saatavilla palvelunantajien välillä silloin kun tietoja tarvitaan ja niitä on oikeus käsitellä.

Uudistuvassakin toimintaympäristössä hyvinvoinnin ja terveyden toimialan tärkeänä tehtävänä on turvata potilaiden ja asiakkaiden oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä.

### 5.3 Kasvun ja oppimisen toimiala KOTO

Kasvun ja oppimisen toimialalla henkilötietojen käsittelyn isoimmat henkilötietoryhmät liittyvät opetuksen ja varhaiskasvatuksen järjestämiseen.

Toimialalla on pyritty sähköistämään erilaisia manuaalisia prosesseja ja näin vähentämään paperilomakkeiden käsittelyä. Esimerkiksi varhaiskasvatuksen toiminnanohjausjärjestelmä eVakaan on siirretty palvelusetelien käsittely, kännykällä tapahtuvat läsnäolokirjaukset ja viestintä huoltajien kanssa. Näiden johdosta paperisia lomakkeita ei enää tarvita ja työprosessit toimivat aikaisempaa luotettavammin.

Lapsen ja huoltajien osallisuutta on lisätty sähköistämällä lapsen varhaiskasvatus- ja esiopetuksen suunnitelma, sekä pedagoginen dokumentointi. Kouluilla oli syksyllä pilotoinnissa erityisen tuen kuulemislomake ja sähköinen allekirjoitus. Tarkoituksena on siirtyä erityisen tuen hakuprosessissa kokonaan sähköiseen käsittelyyn. Jatkossa Wilmassa laaditaan pedagoginen selvitys huoltajan ja oppilaan kanssa laadittavan sähköisen asiakirjan avulla.

Kehittämiskohteiksi vuodelle 2022 on tunnistettu edelleen esimerkiksi asiakirjojen sähköisen käsittelyn ratkaisujen kehittäminen ja käyttöönotto. Henkilöstön tietosuojan osaamisen ylläpitämiseen ja lisäämiseen panostetaan edelleen sekä tietosuojaprosessien kehittämiseen.

### 5.4 Kaupunkiympäristön toimiala KYT

Espoon kaupungin sisäisen organisaatiouudistuksen seurauksena entinen tekninen ja ympäristötoimi uudelleennimettiin kaupunkiympäristön toimialaksi ja ympäristöterveydenhuollon tehtävät siirtyivät toimialalle. Pääpiirteissään tietosuojan ja tietoturvan osalta KYT:in tuottamat palvelut ovat säilyneet ennallaan, mutta hallinnollisia käytäntöjä ja ohjeistuksia on tarkennettu. Henkilötietojen käsittely toimialalla perustuu lakisääteisten tehtävien lisäksi rekisteröidyn suostumukseen tai sopimukseen. Erityisiä henkilötietoryhmiä käsitellään vähän. Tietosuoja pyritään huomioimaan kaikissa tilanteissa, joissa henkilötietoja käsitellään, ja tietosuojan ja tietoturvan osalta seurataan kaupungin ohjeistuksia.

Vuoden 2021 aikana henkilöstöä on edelleen kannustettu kehittämään omaa tietosuojaosaamistaan muun muassa kaikille työntekijöille saatavilla olevan tietoturvan ja henkilötietosuojan peruskurssin avulla. Yhteistyötä kaupungin tietosuojavastaavan kanssa on lisätty ja jatkossa tavoitteena on yhä laajempi tiedonjakaminen eri tietosuoja- ja tietoturva-asiantuntijoiden kesken. Julkisuuslain sekä henkilötietoja koskevan lainsäädännön soveltaminen on useissa tilanteissa koettu hanakalaksi ja sen osalta on toivottu parempaa ohjeistusta ja koulutusta.

KYT otti käyttöön sähköisen allekirjoittamisen useissa asiakirjanhallinnon prosesseissa ja edisti tietojen sähköistä arkistointia. Virheetöntä tiedonkäsittelyä ja -hallintaa kehitettiin robotiikan avulla ympäristö- ja rakennusvalvonnan rakennuslupaprosesseissa. Kaupunkisuunnittelukeskus muutti toimintatapojaan kaavoituksen hallinnointiprosessissa sähköisten toimintatapojen edistämiseksi. Asuntoyksikössä uudistettiin asumiskeushakemusmenettely ja KYT:in päivitetyt tietosuojaselosteet julkaistiin kaupungin www-sivuilla.

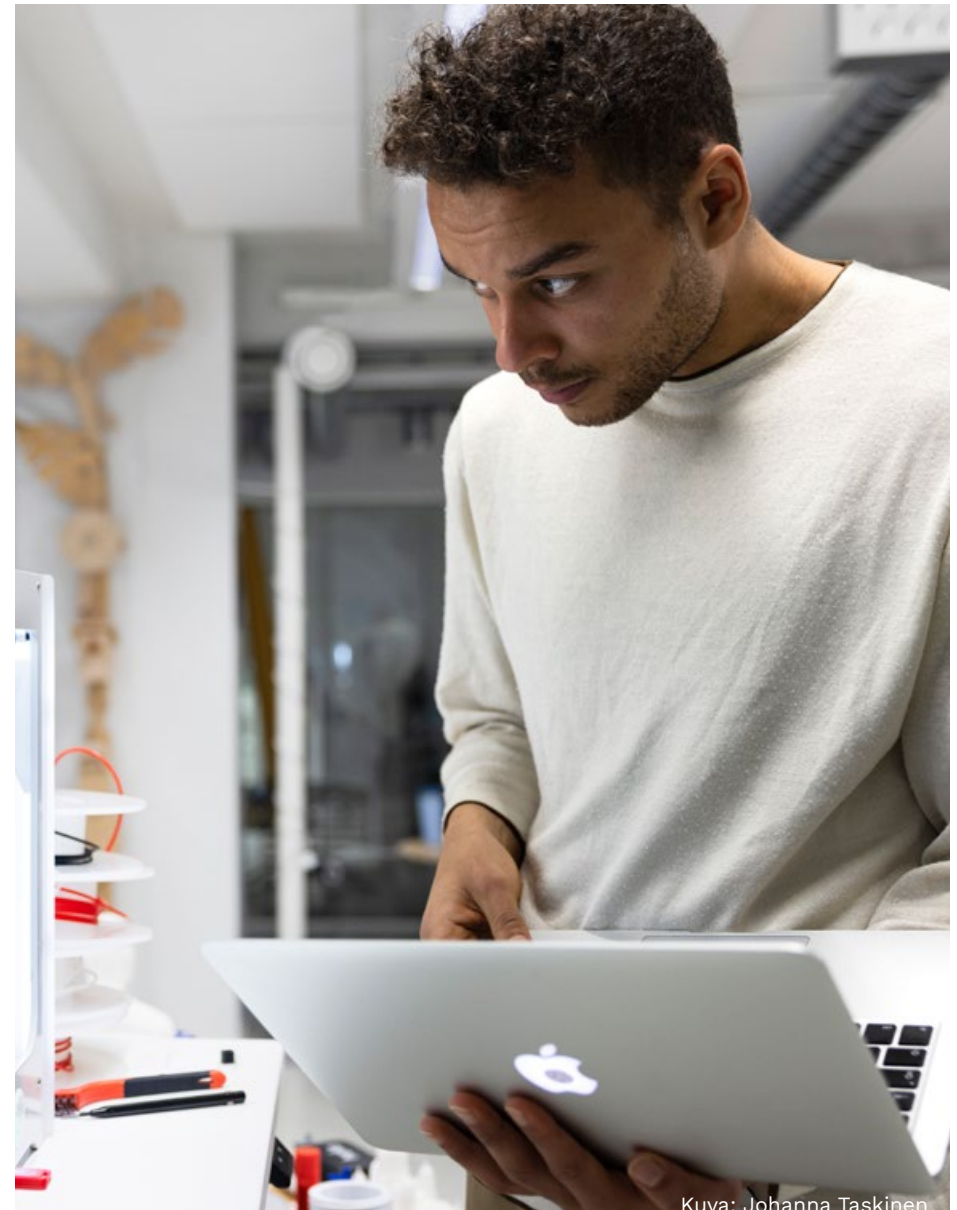
2022 aikana KYT pyrkii saamaan tarkempaa ohjeistusta muun muassa potentiaalisesti haitallisen eli rajoitetun käytön tiedon jakamiseen, sekä toimialan sisällä ohjeistusta henkilötietojen käsittelystä tietojen luo-

vuttamistarkoituksissa. Myös tietosuojaan liittyvien riskien arviointia ja tietosuojan huomioimista sopimuksissa on tavoitteena kehittää edelleen. Pääkäyttäjien ja muun avainhenkilöstön täsmäkoulutus voi olla tarpeen, jotta kuntalaisten tietoja voidaan suojata aikaisempaa paremmin.

## 5.5 Tietosuojaryhmät ja tietosuojayhteistyö kaupunkiorganisaatiossa

Espoon kaupungissa tietosuojan toteutumisesta kaupunkiorganisaatiossa huolehtii omalta osaltaan kaupungin tietosuojaryhmä. Tietosuojaryhmä koostuu toimialojen ja konsernihallinnon eri toimintojen tietosuojan vastuutahoista. Kaupunginjohtajan päätöksellä nimetyn tietosuojaryhmän tehtävä on määriteltä Espoon kaupungin tietoturva- ja tietosuojapolitiikassa: **”Tietosuojaryhmä seuraa tietosuojan toteutumista kaupungissa. Ryhmä tekee kaupunkitasoisia linjauksia ja tulkintoja tietosuojan toteuttamiseksi ohjeiden, toimintatapojen, koulutusten ja raporttien muodossa, analysoi toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietosuojariskejä. Ryhmä toimii koko kaupunkiorganisaation tukena tietosuoja-asioissa.”**

Vuonna 2021 tietosuojaryhmä kokoontui tietosuojavastaavan johdolla yhteensä 11 kertaa (heinäkuussa lomaillaan, eikä kokousta järjestetty). Osallistuminen on jatkunut aiempiin vuosiin nähden aktiivisena, ja ryhmän koko kasvoikin uusilla jäsenillä vuoden lopulla. Tietosuojan merkitys ja näkyvyys arjen työssä ja yhteistyön tärkeys korostuu edelleen jatkuvasti, mikä näkyy osaltaan ryhmän aktiivisuutena ja jäsenmäärän kasvuna: toimialat haluavat olla mukana tietosuojaan liittyvässä kehitystyössä, sekä kuulemassa tietosuojan ajankohtaisista asioista. Tietosuoja on GDPR:n voimaantulon jälkeen jalkautunut tehokkaasti toimialoille ja sen merkitys on selvästi noussut myös henkilöstön keskuudessa, mikä näkyy tietosuojaryhmän osallistumisaktiivisuuden lisäksi myös lisääntyneinä yhteydenottoina kaupungin tietosuojavastaavalle. Tietosuoja on Espoossa omaksuttu osaksi esimerkiksi uusien toimintojen tai hankintojen kehitystyötä, ja tietosuoja



Kuva: Johanna Taskinen

otetaankin hyvin näissä huomioon. Yksi osoitus tietosuojan merkityksen korostumisesta on kaupungin Hankintakeskuksen perustama oma tietosuojaryhmä, jossa käsitellään hankintojen tietosuojakysymyksiä, esimerkiksi rekisterinpitovastuun määräytymistä tai tietosuojan vaikutustenarvioinnin laatimista. Kaupungin tietosuojavastaava kuuluu Hankintakeskuksen tietosuojaryhmään.

Kaupunkitasoisen ja Hankintakeskuksen tietosuojaryhmien lisäksi HYTET:n toimialalla on oma tietosuojaryhmänsä. Siihen kuuluu kaupungin tietosuojavastaavan lisäksi myös kaupungin tietoturvapääallikkö. Kokouksissa käsitellään erityisesti sote-toimialan tietosuojakysymyksiä, mutta myös kaupunkitasoisia tietosuojaan ja tietoturvaan liittyviä ajankohtaisia asioita.

Tietosuojaryhmien lisäksi yhteistyötä on tiivistetty KYT:n ja kaupungin tietosuojavastaavan kesken, kuten edellä kappaleessa 4.3. todettiin.

Kaupunkitasoisen tietosuojaryhmän käsittelyssä vuonna 2021 olivat esimerkiksi seuraavat asiat:

- Edellisen vuoden tietotilinpäätöksen laatiminen
- Tietojen siirto kolmansiin maihin (Privacy Shieldin kumoutuminen)
- Tietosuojaselosteiden saavutettavuus
- Brexit ja tiedonsiirto Iso-Britanniaan
- Turvallinen tiedonvälitys (turvaposti, Suomi.fi ja muu tiedonvälitys)
- Kaupungin henkilötietojen tietoturvaloukkusprosessin kehittäminen
- Vaikutustenarvioinnin työkalun ja toimintamallin uudistus (mm. keskitetty säilyttäminen)
- Tietosuojatyön resursointi
- Sähköisen asiointin kehittäminen erityisesti tietopyyntöjen osalta (OmaEspoo-asiointikanava)
- Hankintojen tietosuojaliitteiden päivittäminen
- Tietosuojavaltuutetun päätökset ja kansallinen ohjaus
- Toteutuneet henkilötietojen tietoturvaloukkaukset ja toimenpiteet

## 5.6 Tietoturvaryhmä ja tietoturvatoimet

Tietoturvaryhmä kokoontui 10 kertaa vuoden 2021 aikana, johon vaikutti tietoturvapääallikön vaihtuminen. Siirtymällä oli selkeä vaikutus ryhmän toimintaan, koska rekrytoinnin aikana seurantakokouksia ei järjestetty. Espoon tietoturvaryhmä koostuu kaupungin toimialoja ja tulosalueita edustavista tahoista, joiden tehtävänä on välittää tietoturvaan liittyviä tapahtuma- ja kehitystietoja omalle vastuualueelleen ja takaisin. Tietoturvaryhmää vetää tietoturvapääallikkö, joka yhdessä toimialojen kanssa seuraa Espoon sisäisen ja ulkoisen toimintaympäristön kehittymistä. Seurannalla toteutetaan tiedonhallintalain velvoitteita ja siitä jää kirjallinen jälki kaupungin arkistoihin.

Vuoden ensimmäisellä neljänneksellä käsiteltiin petostehtailijoiden teemoja, joita olivat veronpalautukset ja teknisen tuen puhelut. Teema osoitti, että teknisen tuen tulee kyetä tunnistamaan itsensä ja asiakkaat riittävän luotettavasti, johon käy puhelinnumeron ja sähköpostiosoitteen haltijuuteen perustuva tunnistus, jota täydennetään tietoon perustuvalla kyselyllä. Teknisen tuen edustajan tunnistaminen on vaikeampaa, koska asiakkailla ei ole samanlaista pääsyä rekisteritietoihin ja siksi pelkästään puhelimella tai sähköpostilla tapahtuvaan viestintään on vaikea luottaa.

TietoEVERY ja Eilakaisla joutuivat saman vuosineljänneksen aikana kiristys-haittaohjelman kohteeksi, jonka perusteella myös Espoo kehotti organisaatiotaan testaamaan varmuuskopioidensa toimivuus ja riittävä säilytysaika myös pitkäaikaisia soluttautumisia vastaan. Rikolliset toimivat myös aktiivisesti eri sosiaalisen median alustoilla, joilla Espoon organisaatio järjesti arpajaisia ja muuta toimintaa. Arpajaistoiminta kuitenkin herätti rikollisten huomion ja arpajaisten päättymispäiviin kohdennettiin petosviestejä, joissa rikolliset esiintyivät Espoon julkisilla tiedoilla. Eli tekivät identiteettivarkauden, mutta jonka selvittämiseen ja toistumisen estämiseen kyseinen SOME-alusta ei reagoinut mitenkään.

Seuraajien näkeminen on nyt estetty. Vuosineljänneksen aikana Espoo havaitsi, että netissä jaetaan vuotaneita tunnuksia laajassa COMB-ko-





Kuva: Heidi-Hanna Karhu

koelmassa (Combination of Many Breaches), jonka johdosta vuotaneita tunnuksia verrattiin Espoolla käytössä oleviin. Lopputuloksena useita käyttäjiä pakotettiin vaihtamaan salasanasensa. Joukossa oli muutama yhteiskäyttötunnus, joiden paljastuminen olisi saattanut vaarantaa henkilötietoja. Tarkastus osoitti, että käyttäjätunnuksien säännöllinen vertaaminen julkiseen vuotaneiden tunnuksien tietokantaan auttaa poistamaan uinuvia, murrettuja tilejä verkosta.

Toisen vuosineljänneksen aikana Kyberturvallisuuskeskus varoitti kouluihin kohdistuvasta PYSÄ-lunnaskampanjasta. Henkilökuntaa tiedotettiin varovaisuudesta tuntemattomien viestien avaamisessa ja lähettäjän riittävästä tunnistamisesta, jossa pelkän sähköpostiosoitteen omistajuus ei ole riittävästi. Varmuuskopioiden testaamista kehoitettiin uudestaan. Kyberturvallisuuskeskus varoitti myös valvontakameroiden väärinkäytöstä, erityisesti jos ne ovat avoimena julkiseen verkkoon. Varoitus käynnisti pitkällisen selvityksen Espoon valvontakameroiden tilasta, joiden perusteella Espoo pyrkii luomaan valvontakameroille hallitun elinkaaren, jonka perusteella laitekantaa uudistetaan ennustettavalla aikavälillä. Muutos tulee näkymään hitaasti, mutta uudistuksien myötä tallenteiden hallinta keskittyy ja kameroiden laatu kasvaa. Yleiset alueet, joissa käsitellään salassa pidettävää tietoa tai kaupungille kriittistä omaisuutta, otetaan tarkemmin mukaan valvontaan.

Toisen vuosineljänneksen aikana petostehtailijoiden trendeinä olivat tekaistut tekijänoikeusrikkomukset ja viestien levittäminen organisaatioiden omien verkkolomakkeiden kautta. Espooseen kohdistui ainoastaan vähäinen määrä näitä tapauksia, mutta kaupunkien tulee yleisesti suosia CAPTCHA-tyyppisiä lisävahvistuksia omissa verkkolomakkeissaan. Näillä estetään verkkolomakkeiden väärinkäyttö roskapostin jakelussa. Roskaposti ja jatkuvat huijausyritykset kuitenkin vahvistavat tarvetta turvallisen digitaalisen viestinnän alustoille, joissa jokaisen viestin lähettäjä ja vastaanottaja on aina vahvasti tunnistettu. Toistaiseksi Espoo ei ole laajasti ottanut käyttöön Suomi.fi-viestit kaltaisia viestintäalustoja.

Vuosineljänneksen aikana Espoo päivitti tietoturva- ja henkilötietosuojaohjeistustaan. Erityisesti sähköpostin salaamiseen liittyvää ohjeistusta tarvittiin laajalti, koska ilman muita turvallisen asiakasviestinnän alustoja sähköpostista on muodostunut oletusarvoinen viestintäalusta. Salassa pidettävien tietojen suojaaminen koskettaa myös sähköpostia, joka vaarantuu mikäli tili murretaan. Lisävahvistus kännykkänumeroon on toiminut näiden estämisessä luotettavasti.

Kolmannella vuosineljänneksellä Espoolla otettiin kantaa pikaviestimien käyttöön, TAISTO'21 harjoitukseen osallistumiseen, Jyvsectecin kyberturvalisuusharjoitukseen (KYHA) ja pilvipalveluiden tietoturvaan. Pikaviestimistä Whatsapp -sovelluksen käyttöä kaupungin palveluissa puntaroitiin, mutta tätä ei puollettu Facebookin käyttöehtojen johdosta. Tämän tilalle ehdotettiin turvallisempaa Signal -sovellusta, mutta ilman kaupallista sopimusta tätä ei voitu käyttää. Sopimuksella sovellukselle saadaan juridinen vastinpari, joka vastaa sovelluksen tietosuojasta ja lainmukaisuudesta. Toistaiseksi Espoo ei käytä pikaviestimiä kuin erityistapauksissa.

Neljännellä vuosineljänneksellä Espoon kaupunki osallistui Digi- ja väestötietoviraston TAISTO 2021 -harjoitukseen, aloitti toimet uutisissa laajasti tiedotetun Log4j-haavoittuvuuden paikkaamiseksi ja selvitti mahdollisuuksia osallistua laajempaan Kyberturvallisuusharjoitus KYHA'21 -harjoitukseen.

TAISTO-harjoituksessa havaittiin, että kaupungin riippuvuus Microsoftin tarjoamasta Azure-alustasta on varsin merkittävä ja mikäli Azure ei ole käytettävissä mistä tahansa syystä, niin arkisetkin tehtävät monimutkaistuvat. Näitä ovat esimerkiksi puhelinluettelon käyttö ja tietokoneille sisäänkirjautuminen. Tällä voi olla merkitystä laajoissa, kansallisissa poikkeustilanteissa tai ulkomaanyhteyksien heikentyessä, jolloin palautuminen voi kestää pitkään. Näissä tilanteissa avainhenkilöiden saavutettavuus ja valmius kriisityöskentelyyn on oleellista, sekä tärkeimpien tietojen saatavuus esimerkiksi omista kopioista tai paperisista asiakirjoista.

## 5.7 Yhteistyöverkostot

Tietosuoja- ja tietoturvatyössä erilaiset yhteistyöverkostot olivat vuoden aikana hyödyllisiä tiedonjakamisen ja käynnissä olevien toimien vertailulle, antaen näkymää niihin asioihin ja toimenpiteisiin, joihin kukin kaupunki panostaa. Espoo tekee tiivistä yhteistyötä pääkaupunkiseudun kaupunkien kanssa, sekä suurten kaupunkien verkostoissa. Lisäksi kaupungin tietosuojavastaava kuuluu Kuntaliiton tietosuojavastaavien verkostoon. Yhteistyöryhmissä käsiteltiin muun muassa seuraavia aiheita:

- Pilvipalveluiden tietoturva ja henkilötietosuoja, sekä uudet kehitykset
- Yhteisrekisterinpitäjyys
- Tietosuojan vaikutustenarvioinnit
- Erilaiset tietopyynnöt ja niihin vastaaminen

Näiden lisäksi yhteistyötä käynnisteltiin Helsingin ja Vantaan yhteisessä foorumissa, DVV:n järjestämässä kokouksessa ja Jyvsectecin järjestämän kyberturvallisuusharjoituksen kautta. Näiden toistuminen on kuitenkin vielä epävarmaa, mutta voi vakiintua 2022–2023 aikana.



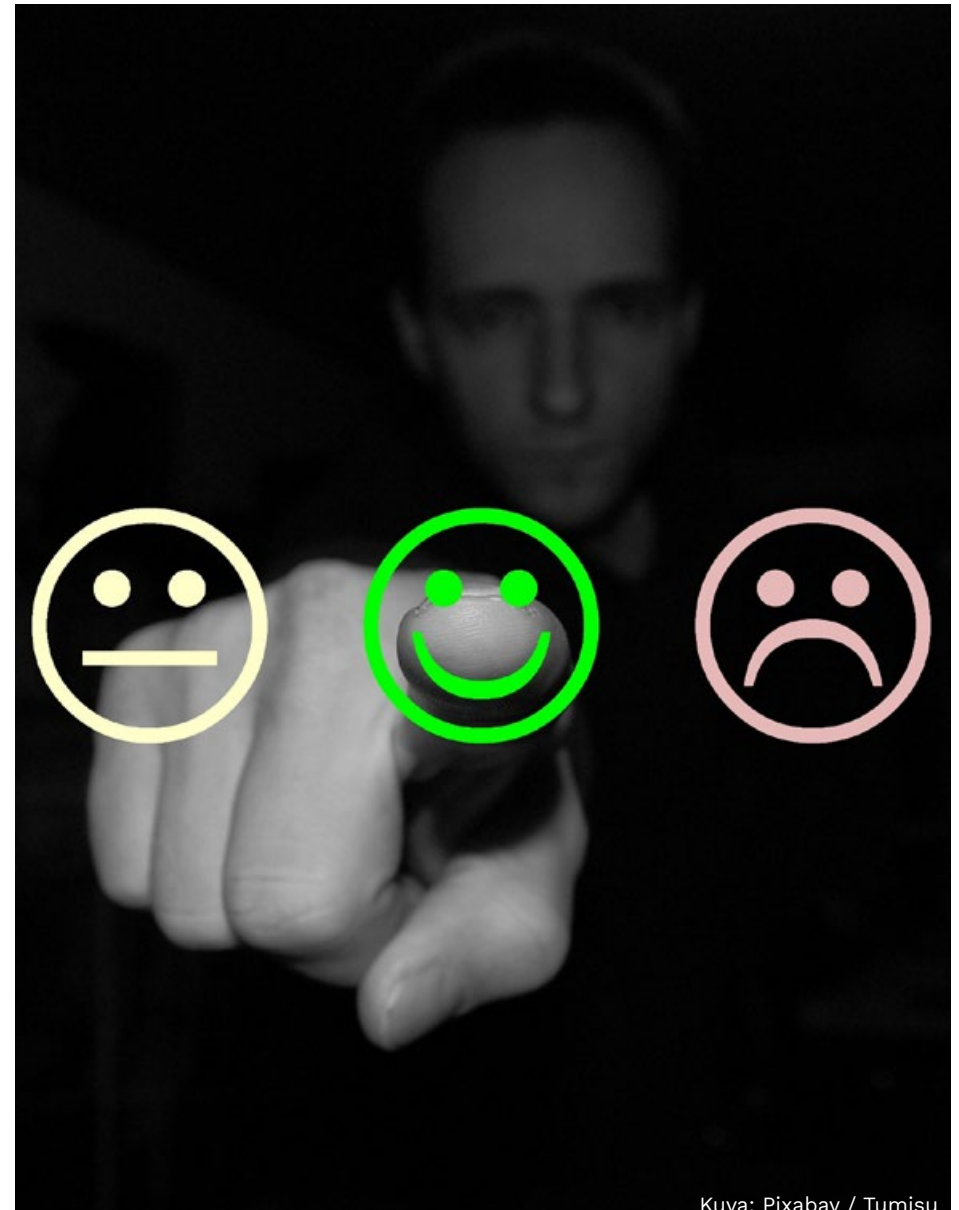
## 6 Arviointi ja mittarit

Tässä kappaleessa tarkastellaan rekisteröityjen oikeuksien toteutumista, tukipyyntöjen yleistä tilaa, Helpdeskiin saapuneita tietoturvailmoituksia ja näiden volyymejä, sekä näiden käsittelyn yleisiä periaatteita.

### 6.1 Rekisteröityjen oikeuksien toteutuminen

Tietosuoja-asetuksen yksi keskeisimmistä tavoitteista on vahvistaa asiakkaiden oikeuksia suhteessa omiin henkilötietoihinsa. Tietosuoja-asetuksen kolmas luku keskittyy kokonaan rekisteröityjen oikeuksiin, ja viime vuosina valvojan viranomaisen päätöksissä on erityisesti keskitetty rekisteröidyn oikeuksien puutteelliseen toteuttamiseen rekisterinpitäjän toimesta. Tietosuojan keskiössä on yksilö ja hänen henkilötietojensa suoja, joten rekisteröidyn oikeuksien toteutuminen ja toteuttaminen on myös Espoon kaupungin näkökulmasta keskeistä.

Ensimmäinen tietosuoja-asetuksen listaama asiakkaan oikeus on oikeus läpinäkyvään informointiin. Espoossa asiakkaiden informoinnissa käytetään tietosuojaselosteita. Tietosuojaseloste ei ole laissa säädetty informointimuoto, mutta selosteet ovat vakiintuneet laajasti informointimuodoksi niin kuntakentällä kuin yksityissektorillakin, niin Suomessa kuin myös ulkomailla. Tietosuojaselosteet ovat julkisia ja ne ovat asiakkaiden helposti saatavilla Espoon verkkosivuilla. Selosteissa kerrotaan läpinäkyvästi henkilötietojen käsittelystä: mitä tietoja asiakkaasta kerätään, kenen toimesta, mihin käyttötarkoitukseen, luovutetaanko tietoja jonnekin ja miten tietoja suojellaan. Lisäksi selosteesta löytyvät yhteystiedot, jotta asiakas voi käyttää selosteessa kuvattuja oikeuksiaan mahdollisimman helposti. Selosteet pyritään laatimaan niin, että asiakas ei joudu etsimään tietoja monesta



Kuva: Pixabay / Tumisu

eri selosteesta, vaan yhden palvelukokonaisuuden tiedot löytyvät yhdestä selosteesta. Espoon verkkosivut uudistuivat syksyllä 2021, ja uudistuksen yhteydessä luovuttiin pdf-muotoisista selosteista. Selosteet rakennetaan verkkosivuille sisältösivuina samoin kuin muukin verkkosivujen sisältö, jolloin selosteet ovat helpommin asiakkaiden saatavilla riippumatta käytössä olevasta välineestä. Asiakas ei siis esim. tarvitse erillistä lukuohjelmaa pdf-tiedostoille, vaan selosteet ovat helposti luettavissa myös matkapuhelimella. Lisäksi selosteet ovat varmasti saavutettavia.

Alla oleva taulukko näyttää tietosuojaselosteiden lukumäärän tietotilinpäätöksen kirjoittamisen aikaan, maaliskuussa 2022. Selvityksen yhteydessä huomattiin, että joitain tietosuojaselosteita on edelleen viemättä kaupungin uusille verkkosivuille, joten selosteita tullaan vielä lisäämään uusille verkkosivuille.

**Tietosuojaselosteiden lukumäärä**

| Toimiala                       | Lukumäärä |
|--------------------------------|-----------|
| Espoo yhteensä                 | 171       |
| Konsernihallinto               | 23        |
| Kasvu- ja oppiminen            | 30        |
| Hyvinvointi ja terveys         | 24        |
| Kaupunkiympäristö              | 53        |
| Länsi-Uudenmaan pelastuslaitos | 12        |
| Elinvoiman tulosalue           | 29        |

Tietosuojaselosteiden lisäksi Espoon kaupungin verkkosivuilla kerrotaan tarkemmin siitä, miten kaupunkilaiset voivat käyttää oikeuksiaan omiin tietoihinsa, mutta tiedot ovat saatavilla myös tietosuojaselosteista.

Espoon kaupunki kerää ja käsittelee asiakkaidensa henkilötietoja vain siinä määrin kuin se on tarpeellista palvelun tuottamiseksi. Henkilötietoja käsitellään henkilötietojen käsittelyn käyttötarkoituksen mukaan. Jos tiedonkeruu perustuu suostumukseen, asiakas voi milloin tahansa peruuttaa antamansa suostumuksen ja vaatia tietojensa poistamista. Kaupungin palveluista suurin osa perustuu kuitenkin lakisääteisen velvoitteen noudattamiseen tai julkisen vallan käyttämiseen, eikä asiakas voi niihin liittyvissä tapauksissa vaatia tietojensa poistamista. Asiakkaalla on oikeus tietää, mitä tietoja hänestä kerätään. Jos tiedoissa on virheitä, asiakas voi vaatia tietojen oikaisemista. Tietopyynnön voi toimittaa joko 1) postitse tietosuojaselosteessa mainitulle yhteyshenkilölle osoitettuna, tai 2) asioimalla henkilökohtaisesti asiointipisteessä tai kirjaamossa, missä tarkistetaan asiakkaan henkilöllisyys. Sosiaali- ja terveystoimen toimialalla tietopyynnön voi jättää myös henkilökohtaisesti sosiaali- ja terveydenhuollon toimintayksikössä asiointin yhteydessä. Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin kirjaamosta tai asiointipisteestä. Tiedot voidaan toimittaa hänelle myös postitse tietyin edellytyksin. Espoon kaupungin tietopyyntöprosessi on ensimmäisten pilotoitavien kohteiden joukossa, kun kaupunki ottaa käyttöön sähköisen OmaEspoo-asiointikanavan. Asiointikanava ja sähköinen tietopyyntöprosessi on asiakaskäytössä tavoitteiden mukaan viimeistään vuonna 2024, jolloin tietopyyntöprosessi tulee olennaisesti helpottumaan asiakkaiden näkökulmasta.

Alla olevasta taulukosta käy ilmi Espoon toimialoille vuonna 2021 tehdyt tietosuojasetuksen mukaiset tietopyynnot. Toimialojen selvityksistä selviää, että välillä tietosuojasetuksen nojalla tehtävä tietopyyntö on vaikeaa erottaa julkisuuslain nojalla tehtävästä tietopyynnöstä, mikä voi aiheuttaa vaihtelua toimintojen ilmoittamisissa lukumäärissä. Lisäksi osa kaupunginarkiston kautta kulkevista pyynnöistä ohjataan edelleen toimialoille, joten osa pyynnöistä saatetaan raportoida kahteen kertaan. Lukumäärät ovat näistä haasteista johtuen ainoastaan suuntaa antavia.

#### GDPR:n mukaisten tietopyyntöjen lukumäärä 2021

| Toimiala                       | Lukumäärä |
|--------------------------------|-----------|
| Espoo yhteensä                 | 1988      |
| Konsernihallinto               | 4         |
| Kasvu ja oppiminen             | 16        |
| Sosiaali- ja terveystoimi      | 1654      |
| Tekninen ja ympäristötoimi     | 0         |
| Länsi-Uudenmaan pelastuslaitos | 0         |
| Kaupunginarkisto               | 314       |

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä antaa asiakkaalle oikeuden tarkistaa omat lokitietonsa. Lokitiedoilla tarkoitetaan kirjauksia asiakkaan henkilötietojen käsittelystä: kuka on käsitellyt henkilötietoja ja mihin tarkoitukseen tietoja on käsitelty. Lain perusteella asiakkaalla on oikeus saada tietää, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste. Vastaavaa oikeutta ei muilla toimialoilla ole, koska erityislainsäädäntöä ei ole. Kansallinen valvova viranomainen, tietosuojavaltuutetun toimisto, on linjannut päätöksissään että lokitiedot ovat asiakkaan henkilötietoja käsittelevän työntekijän henkilötietoja, ja näihin ei asiakkaan tiedonsaantioikeus ylety. Ainoastaan poikkeustilanteissa (esimerkiksi rikostutkinnan yhteydessä) asiakkaalla on oikeus muihin kuin sote-toimialan lokitietoihin. Alla olevassa taulukossa kerrotaan vuosittain Espoon kaupungissa tehdyt lokiselvitykset 2015 vuodesta lähtien.

#### Lokiselvitykset vuosittain

| Vuosi | Tehdyt lokiselvitykset |
|-------|------------------------|
| 2015  | 72                     |
| 2016  | 84                     |
| 2017  | 78                     |
| 2018  | 125                    |
| 2019  | 83                     |
| 2020  | 91                     |
| 2021  | 101                    |

Taulukko, Hyvinvoinnin ja terveyden toimialan lokiselvitykset 2015–2021

## 6.2 Tietoturvapoikkeamat ja häiriöt

Jokaisen häiriöihin liittyvän tukipyynnön kohdalla Espoon kaupunki noudattaa samaa työprosessia, jossa havainnot siirtyvät HelpDeskin kautta eri tahojen työjonoon ja tarvittaessa eskaloituvat tietoturvapäällikölle. Prosessia tarkennettiin vuoden aikana huomioimaan johto ja Valviralle tehtävät ilmoitukset, sekä pääkäyttäjien tiedonsaanti. Prosessia on vertailtu Oulun ja Kuopion malleihin ja niiden on todettu olevan pääosin yhteneviä, jonka johdosta prosessiin ei kohdistu merkittäviä muutostarpeita. Uudet muutostarpeet voivat tulla lainsäädännöstä tai viranomaisilta tulevista suosituksista tai määräyksistä.

Espoon kaupunki ei kohdannut tietotilinpäätöskauden aikana merkittäviä ja laajoja kyberturvallisuuteen kohdistuneita kriisejä, jotka olisivat huomattavassa määrin vaarantaneet useiden tai yksittäisten palveluiden tuottamisen. Useimmat tietoturvapoikkeamat olivat luonteeltaan yksittäisiin virheisiin pohjautuneita tapahtumia, jotka korjautuivat virheen poistamisen myötä.

#### **Huomionarvoisia tapahtumia ja oppeja olivat:**

1. Log4j-haavoittuvuuden julkaisu, joka pakotti päivittämään noin 80 järjestelmää tavallisesta poikkeavalla aikataululla. Tapaus osoitti, että järjestelmistä vastaaville tahoille on suotavaa olla yksi keskitetty koordinoitintaho tai ryhmä, joka kykenee viestimään lukuisten yksittäisten vastuuhenkilöiden kanssa
2. Huijaustekstiviestien lukumäärän kasvu ja laaja jakelu myös käyttämättömiin numeroihin, joka pakotti teleoperaattorit toimiin ja osoitti tekstiviestien olevan alttiita vastaavalle roskaviestinnälle kuin sähköpostin
3. Asiakaspalvelu henkilö kertoi painostuksen alaisena salassa pidettävän tiedon ulkopuoliselle, joka saattoi johtaa vainoamiseen. Asiakaspalveluhenkilökunnan tulee tunnistaa mitkä tiedot saattavat aiheuttaa vahinkoa ja ennakolta varautua painostamiseen
4. Kaupungeille saapuu harvakseltaan kohdennettuja toimitusjohtajahyökkäyksiä ja tekaistuja laskuja tyypillisesti sähköpostilla. Laskutuksen siirtäminen vahvan tunnistautumisen viestintäalustalle ehkäisisi näitä tehokkaasti
5. Eräessä julkisen palvelun toimipisteessä havaittiin heikosti lukittua omaisuutta, kuten tabletti ja tietokone, sekä runsaasti läheisestä koulusta kumpuavaa rauhattomuutta. Isojen organisaatioiden on suositeltavaa suorittaa pistokoeluonteisia turvallisuuskävelyjä näiden ongelmien havaitsemiseksi

6. Muutamassa tapauksessa työntekijät vuotivat rajoitetun käytön tietoa, eli tietoa josta on potentiaalista haittaa, kuvakaappauksilla sosiaaliseen mediaan. Henkilökuntaa on hyvä säännöllisesti muistuttaa sosiaalisen median julkisesta luonteesta myös yksityisissä keskusteluryhmissä
7. Kaupungin vierailijaverkkoa käytettiin muutamassa tapauksessa huijaus- ja uhkailuviestien lähettämiseen, joista kahta tutkittiin rikoksena. Tapaukset ovat toistaiseksi määrältään vähäisiä, mutta vierailijaverkkoihin liitettävää pakollista tunnistautumista saatetaan joutua harkitsemaan mikäli tapauksia tulee lisää tai niiden vakavuus kasvaa
8. Eräissä kaupungin puhelinpalveluissa puheluita tallennettiin ilman asianmukaista ilmoitusta soittajalle, jossa tulee myös ilmoittaa mikä on tallentamisen lakisääteinen perustelu
9. Kahdessa järjestelmässä oli epäilty tietomurto, joista kumpikaan ei johtanut tietojen paljastumiseen. Kummassakin tapauksessa toimittajat reagoivat tapahtumiin kiitettävästi, sekä suorittivat asianmukaiset järjestelmän käyttöönpalautuksen hyväksynnät ja testaukset

Kokonaisuutena Espoon kaupungin kyberturvallisuuden tila oli 2021 aikana vakaa, mutta ennakkoivaa valvontaa, tarkastuksia ja koulutusta lisätään.

### **6.3 Henkilötietojen tietoturvaloukkaukset**

Tietosuoja-asetus velvoittaa rekisterinpitäjän (eli käytännössä Espoon kaupungin tai sen toimialan) ilmoittamaan valvovalle viranomaiselle 72 tunnin kuluessa tietoturvaloukkauksista, jotka aiheuttavat riskin asiakkaan oikeuksille ja vapauksille. Valvovan viranomaisen lisäksi loukkauksista tulee ilmoittaa myös asiakkaalle silloin, kun aiheutuva riski on korkea. Arvion tekee kaupungin tietosuojavastaava yhdessä loukkauksen kohteeksi joutuneen toimialan vastuutahon kanssa. Kaupungin tulee siis myös lainsäädännön näkökulmasta reagoida loukkauksiin nopeasti, mutta ensisijaisesti

nopea reagointi on olennaista, jotta pystytään suojaamaan asiakasta ja hänen henkilötietojaan. Myös organisaatioon kohdistuvat riskit pyritään minimoimaan nopealla reagoinnilla.

Tietosuojavastaavalla on olennainen rooli loukkausprosessissa. Tietosuojavastaava osallistuu tilanteen selvittämiseen yhdessä muiden loukkauksen kannalta olennaisten osapuolten kanssa (toimiala, tietoturvapääällikkö, tietohallinto), ja selvityksen jälkeen tietosuojavastaava päättää riskiarvion johdosta jatkotoimenpiteistä. Ilmoitus valvovalle viranomaiselle tehdään käyttäen tietosuojavaltuutetun toimiston verkkosivujen tietoturvaloukkausten ilmoituslomaketta. Kaikki loukkaukset dokumentoidaan riippumatta siitä, tehdäänkö ilmoitusta viranomaiselle vai ei. Lisäksi tietoturvapääällikkö arvioi jatkoilmoitusten tekemistä Valviralle, mikäli kyseessä on terveydenhoitoa koskeva tapahtuma, ja Kyberturvallisuuskeskukselle. 2021 aikana Valvira-ilmoituksia tehtiin kaksi kappaletta. Ilmoituksia Kyberturvallisuuskeskukselle ei yhtään. Kaikissa tapauksissa häiriöt ratkottiin Espoon ja Espoon sopimuskumppanien kesken.

Espoossa ryhdyttiin tilastoimaan tietoturvaloukkauksia systemaattisesti vuoden 2018 alusta. Vuosi 2018 ilmoitusten tekemistä vielä harjoiteltiin Espoossa kuten muissakin kaupungeissa, mutta vuodesta 2019 lähtien tehtyjä ilmoituksia voidaan jo vertailla keskenään käytäntöjen vakiinnuttua. Loppuvuodesta 2021 tietosuojavaltuutetun toimisto julkaisi tarkennetun ohjeistuksen sote-toimialan tietoturvaloukkausten ilmoituskäytännöistä. Tämä tulee osaltaan jatkossa helpottamaan tietosuojavastaavan arviointiyötä ilmoitusvelvollisuuden täyttymisestä, koska ohjeistuksessa on selkeät ja hyvät esimerkit siitä milloin ilmoitus tulee tehdä. Tämä tulee jatkossa myös yhtenäistämään ilmoitusten tekemistä sote-toimialalla.

Seuraavissa taulukoissa vertaillaan henkilötietojen tietoturvaloukkausten määriä toimialoittain sekä loukkausten syitä vuosina 2019, 2020 ja 2021. Taulukointi on tehty vielä vanhalla organisaatorakenteella. Jatkossa elinvoiman tulosalue tullaan huomioimaan omana kokonaisuutenaan loukkausten raportoinnissa.



Kuva: Heidi-Hanna Karhu

Taulukoista selviää, että henkilötietoihin kohdistuneiden tietoturvaloukkausten lukumäärä on pysynyt samoissa lukemissa vuoden 2020 kanssa. Tietosuojavaltuutetulle ja rekisteröidylle on kuitenkin ilmoitettu vähemmän loukkauksia kuin edellisellä vuonna, mikä tarkoittaa että loukkauksista ei ole aiheutunut korkeaa riskiä rekisteröidylle. Yleisin juurisyy henkilö-tietojen tietoturvaloukkauksille on inhimillinen virhe. Kentältä saadun palautteen perusteella virheen syynä on useimmiten kiire, joka johtaa huolimattomuuteen ja sitä kautta loukkauksiin. Työnjohdolla on merkittävä rooli resursoinnissa ja työkuorman hallinnassa, näistä huolehtiminen auttaa myös vähentämään kiireessä tehtyjä virheitä. Myös koulutuksella on tärkeä rooli loukkausten vähentämisessä. Koulutusta tullaankin lisäämään tulevana vuosina jo muun lainsäädännön vaatimuksistakin johtuen.

#### Henkilötietojen tietoturvaloukkaukset

| Toimiala        | Yhteensä  |           |           | Tietosuojavaltuutetulle ilmoitettu |           |           | Rekisteröidylle ilmoitettu |           |           |
|-----------------|-----------|-----------|-----------|------------------------------------|-----------|-----------|----------------------------|-----------|-----------|
|                 | 2019      | 2020      | 2021      | 2019                               | 2020      | 2021      | 2019                       | 2020      | 2021      |
| KOHA            | 11        | 7         | 14        | 2                                  | 2         | 3         | 2                          | 4         | 4         |
| KOTO            | 9         | 21        | 15        | 6                                  | 14        | 10        | 6                          | 10        | 11        |
| HYTET           | 35        | 59        | 63        | 15                                 | 37        | 25        | 15                         | 39        | 21        |
| KYT             | 5         | 3         | 2         | 2                                  | 1         | 0         | 2                          | 0         | 1         |
| <b>Yhteensä</b> | <b>60</b> | <b>90</b> | <b>94</b> | <b>25</b>                          | <b>54</b> | <b>38</b> | <b>25</b>                  | <b>53</b> | <b>37</b> |

Taulukko: Henkilötietojen tietoturvaloukkaukset Espoossa 2019–2021

#### Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019 - 2021

| Loukkauksen juurisyy                       | Loukkausten määrä kpl |           |           | Loukkausten määrä % |            |            |
|--------------------------------------------|-----------------------|-----------|-----------|---------------------|------------|------------|
|                                            | 2019                  | 2020      | 2021      | 2019                | 2020       | 2021       |
| Työntekijän erehdys tai väärä toimintatapa | 32                    | 61        | 64        | 53                  | 68         | 68         |
| Palveluntuottajan virhe                    | 12                    | 11        | 16        | 20                  | 12         | 16         |
| Tietomurto tai muu tahallinen teko         | 6                     | 9         | 6         | 10                  | 10         | 8          |
| Tekninen virhe                             | 5                     | 6         | 7         | 8,5                 | 6,7        | 7          |
| Prosessivirhe                              | 5                     | 3         | 1         | 8,5                 | 3,3        | 1          |
| <b>Espoo yhteensä</b>                      | <b>60</b>             | <b>90</b> | <b>94</b> | <b>100</b>          | <b>100</b> | <b>100</b> |

Taulukko: Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019–2021



## 7 Kyberturvallisuuden tiedotus, koulutus ja valvonta

Espoon kaupunki kouluttaa henkilöstöään verkkokursseilla. Tietoturvan ja tietosuojan osalta henkilöstölle on tarjolla pakollinen kurssi, jonka suoritusaste vuoden aikana jäi kuitenkin alhaiseksi. Tämän johdosta kurssin suorittamista tullaan tulevana vuosina vaatimaan myös teknisin keinoin ja tarjontaa laajentamaan myös pääkäyttäjille. Tavoitteena on kouluttaa henkilöstö perusteisiin ja pääkäyttäjät vastuullaan olevien järjestelmiensä erityispiirteisiin siten, että koulutuksesta jää kirjallinen jälki.

Koulutusta parantamalla Espoon kaupunki pyrkii puuttumaan inhimillisistä syistä ja erehdyksistä johtuviin tietosuojaloukkauksiin, sekä tietoturva-häiriöihin vaikuttaviin tekijöihin, näistä esimerkkinä haittaohjelmalinkkien klikkaaminen ja salassa pidettävien tietojen paljastaminen henkilöstön erehdyksen kautta. Koulutusalueita kehitetään tänäkin vuonna ja 2023 aikana alustan odotetaan sisältävän nykyisen peruskurssin lisäksi tärkeimpien järjestelmien pääkäyttäjäkoulutukset, joilla tavoitellaan seuraavia hyötyjä:

- Ensimmäisen ja myöhemmin päivitettyjen koulutuksien suorittamisen osoittaminen, jolloin osaamisen kasvattaminen ei nojaa yksin tiedottamiseen
- Henkilöstön tekemien henkilötietopoikkeamien määrän vähentäminen ainakin puoleen nykyisestä
- Avainhenkilöstön työmäärän vähentäminen siirtämällä ohjausta verkkoalustalle
- Koulutusten laadullinen ja määrällinen yhtenäistäminen, eli koulutuksien toistaminen aina samanlaisina ja samantasoisina

Verkkokoulutusten lisäksi kirjallista ohjeistusta pyritään tuomaan kentälle osaksi varsinaista toimintaa lisäämällä pistokoe -luonteisia tarkastuksia. Tällä hetkellä tarkastuksia, eli niin sanottuja turvallisuuskävelyitä, tehdään kaupungin omana toimintana noin kolme kappaletta vuodessa. Tavoitteellisesti näitä tulisi tehdä vähintään 24 kpl/v, sekä näiden toteutumisen jälkiseuranta. Verkkokurssien suoritusprosentti pyritään nostamaan noin 40%:sta 80%:iin, joka tulee edellyttämään teknisiä pakkotoimia. Esimerkiksi verkko- tai järjestelmätunnusten salasanan uusimisen epäämistä tai käytöstä poistoa eräpäivään mennessä, mikäli kurssia ei ole suoritettu. Näiden saavuttaminen tulee edellyttämään myös laajempaa keskustelua ja päätöksentekoa, jota ei vielä 2021 aikana ole aloitettu.



Kuva: Pintaliitodesign, Olli Urpela

## 8 Tietoriskien hallinta

---

Tietosuojan vaikutustenarvioinnit nostettiin kehittämiskohteeksi jo 2018 ja arvioinnit aloitettiin ensimmäisellä Excel-pohjaisella vaikutustenarvioinnin työkalulla 2019. Toiminta jatkui 2020 pienin parannuksin ja sama asteittainen kehityspolku jatkui Espoossa myös vuoden 2021 aikana, jolloin työkalu päivitettiin enemmän kohti Kyberturvallisuuskeskuksen kybermittarin osoittamaa mallia. Kybermittari kuitenkin todettiin liian laajaksi ja erityistä asiantuntijuutta edellyttäväksi työkaluksi, jotta sitä olisi voinut ottaa Espoolla vakinaiseen käyttöön.

Vaikutustenarvioinnissa rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyys ja vakavuus määritellään tietojenkäsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan. Vaikutustenarviointi toteuttaa osaltaan Espoossa osoitusvelvollisuutta ja riskiperusteista lähestymistapaa esimerkiksi silloin, kun hankittavassa tietojärjestelmässä käsitellään laajasti terveystietoa. Vaikutustenarvioinneilla kerätään ennen kaikkea oleellista tietoa päätöksenteon tueksi, sekä pyritään pienentämään havaittuja rekisteröidylle aiheutuvia riskejä hyväksyttävälle tasolle.

Espoon vaikutustenarviointiprosessin mukaisesti prosessiin osallistuvat ensimmäisessä vaiheessa:

- Projektipäällikkö tai toiminnasta vastaava (omistaja)
- IT-projektipäällikkö
- Tarvittaessa palveluntuottajan edustaja
- Toimialan lakimies

Tämän jälkeen dokumentin tarkastavat:

- Tietosuojavastaava
- Tietoturvapäällikkö
- Teknisestä tietoturvasta vastaava it-päällikkö

Tarkastusten jälkeen tietosuojan vaikutustenarviointi ja tietoriskien vaikutusarvio toimitetaan hyväksyttäväksi palvelusta tai järjestelmästä vastuussa olevalle virkamiehelle, joka voi tarvittaessa palauttaa käsittelyyn.

Tiedonhallintalakiin liittyvien selvitysten aikana havaittiin, että tietoriskien hallintaa ja henkilötietojen käsittelyn vaikutustenarviointeja tulee jatkokehittää huomioimaan lain vaatimukset ja Valtiovarainministeriön ohjeet aikaisempaa tarkemmin. Erityisenä nostona VM:n ohje 65/2021, jossa havaittiin olevan selkeitä neuvoja tietoriskien arviointien avuksi.

Kansallinen tietosuojaviranomainen, tietosuojavaltuutetun toimisto, julkaisi loppukeväästä 2021 luonnoksen tietosuojan vaikutustenarvioinnin työkalusta. Espoossa työkalua testattiin syksyllä 2021 muutamassa kaupungin vaikutustenarvioinnin projektissa. Työkalusta saatiin kriittistä palautetta sen haastavuuden vuoksi. Vaikutustenarvioinnin työkalun on oltava ensisijaisesti työkalu substanssin henkilöstölle, eikä ole riskien arvioinnin näkökulmasta tarkoituksenmukaista, että työkalun käyttö edellyttää vähintään tietosuojajuristin koulutusta. Lisäksi tietosuojavaltuutetun toimiston työkalun rinnalla tulee lukea laajaa erillistä ohjetta, eikä itse työkalu ohjaa käyttäjää mitenkään. Saadun palautteen perusteella ohjeistus olisi pitänyt siirtää kokonaan itse työkaluun, mikä olisi edellyttänyt mittavaa työkalun jatkotyöstöä. Näistä kokemuksista, ja havaituista puutteista ja haasteista johtuen Espoon kaupunki päätti vuoden lopulla ottaa käyttöön Helsingin kaupungin laatiman vaikutustenarvioinnin työkalun. Tietosuojaryhmä katselmoi työkalun yhdessä Helsingin tietosuoja-asiantuntijoiden kanssa, ja hyvin ja selkeästi laadittu ja ohjeistettu työkalu sai ryhmältä kiitosta ja johti käyttöönottoon tietosuojavaltuutetun toimiston työkalun sijaan. Helsingin työkalun käyttöönoton myötä vaikutustenarviointien tulisi olla jatkossa melko samanlaisia ja vertailukelpoisia Helsingin ja Espoon välillä. Työkalut eivät vielä salli keskitetyn riskirekisterin luomista kuin enintään kertaluonteisena työnä, mutta riskien ja vaikutustenarviointi samoista järjestelmistä eri kuntien kesken saattaisi olla perusteltua.

Vaikutustenarvioinnit on koettu Espoossa yleisesti hyödyllisiksi, mutta aikaa vieviksi. Edelleen toimialoille on haasteellista tunnistaa, koska vaikutustenarviointi on pakko laatia. Vaikutustenarviointien laatimiseen tullaan jatkossa edelleen panostamaan suorittamista yksinkertaistamalla sekä viemällä suorittamiseen liittyvää ohjeistusta verkkokoulutuslavalle.



Kuva: Pintaliitodesign, Olli Urpela

## 9 Auditoinnit

Espoon kaupungin tietoturva-auditoinnit kohdistuivat pääsääntöisesti tietojärjestelmiin, ja koostuivat keskitetysti tilatuista haavoittuvuustestauksista, sekä näiden kautta paljastuneiden heikkouksien korjaamisesta. Haavoittuvuustestauksia ei tehty vuoden aikana riittävästi ja osa tarkoitukseen varatuista varoista jäi käyttämättä, minkä johdosta kaupunki pyrkii jatkossa suorittamaan kaikille kriittisille palveluille ja salassa pidettävää tietoa sisältäville järjestelmille vähintään seuraavat auditoinnit:

- Haavoittuvuustestaus, joka on tekninen testi järjestelmän tietoturvallisuuden ja vikasietoisuuden osoittamiseksi
- Hallinnollinen auditointi, jolla varmistetaan toimittajien ja oman henkilökunnan noudattavan sovittuja käytäntöjä, sekä tarvittavien ohjeiden ja koulutuksien olemassaolo
- Toiminnallinen itsearviointi, jossa pääkäyttäjät tarkastavat vastuullaan olevan järjestelmän toimivuuden, käyttöoikeudet, lokit ja asetukset

Yhtenä keskeisenä tuloksena auditoinneista oli saatu päätöksenteon tuki: auditoinnin tuella johdon on helpompi perustella pakollisia lisävaatimuksia ja muutoksia jo olemassa oleviin käytäntöihin, joita muuten ei muutettaisi. Tämä koskee erityisesti muutoksia, joilla on taloudellisia vaikutuksia tai jotka koskevat laajaa joukkoa henkilöstöä. Esimerkiksi tietoaltaiden lisäautentikaatio (Multi-Factor Authentication, MFA) kännykkään, jota jatkossakin Espoolla edellytetään pakollisena ominaisuutena salassa pidettävää tietoa käsittelevissä järjestelmissä.

# 10 Todennetut kehittämiskohteet vuodelle 2022

---

Tietotilinpäätöksen tehtävänä on nostaa johdon, tietosuojavastaavan ja tietoturvapäällikön tietoisuuteen keskeisimmät ongelmakohdat ja ponnistelut kyberturvallisuuden parantamiseksi. Näistä ongelmakohdista ja ponnisteluista voidaan johtaa seuraavalle vuodelle tärkeimmät kehittämiskohteet ja tukea näin kyberturvallisuuden toteutumista kaupungilla. Tietotilinpäätöksen yhteydessä näissä onnistumista voidaan arvioida.

Toimialat nostivat tietosuojan keskeisimmäksi kehittämiskohteeksi ohjeistuksen ja koulutuksen, jota varten turvallisuus- ja valmiusryhmä julkaisi uudistetun tietoturvan ja tietosuojan peruskurssin, päivitti ohjeita ja keskitti niitä tietoturvan Essi-sivuille. Vuoden 2022 aikana tarkoituksena on jatkaa tätä toimintaa luomalla uusia verkkokursseja, joilla pääkäyttäjät koulutetaan vastuullaan olevien järjestelmien käyttöön, sekä laajentamalla ohjeistusta, jonka tulisi olla aina saatavilla kaupungin intrasta. Näillä muutoksilla vastataan tiedonhallintalain vaatimuksiin ja parannetaan tiedon saatavuutta, sekä ohjeistuksen yleistä laatua.

Sekä tietoturvan että tietosuojan kannalta yhteinen kehityskohde vuodelle 2021 oli tietoturvaloukkausprosessin sähköistäminen. 2021 aikana siirtymää Forms-lomakkeisiin harkittiin ja tämä toteutui ainoastaan tietoturvan valvontailmoitusten osalta - tietosuojaan liittyvät ilmoitukset tapahtuvat edelleen sähköpostilla. Näiden rinnalla toimii kuitenkin kaksi erillistä ilmoituskanavaa: WhistleB kokonaan anonyymejä ilmoituksia varten ja Espoon oma palautekanava. 2022 tarkoituksena on tarkastella WhistleB:n

käyttömahdollisuuksia toimittajilta ja toimittajien henkilökunnalta tulevien anonyymien ilmoitusten vastaanottamiseen.

2021 Espoo osallistui eri kuntien ja valtion tahojen järjestämiin yhteisiin kokoontumisiin. Käytäntö on osoittanut, että kuntien tietosuoja- ja tietoturvatarpeet ovat varsin samanlaiset ja siksi yhteistyön tiivistäminen on käytännöllinen tapa vähentää työtaakkaa ja edistää muun muassa tietoturva- ja tietosuojaohjeistuksen laatua. 2022 Espoo tulee osallistumaan kaikkiin niihin yhteistyöfoorumeihin, joissa (a) työstetään yhteisiä asioita ja (b) käytetyllä työajalla saavutetaan samoja lopputuotoksia, joita muutenkin päädyttäisiin tuottamaan Espoolla, tai (c) osallistuminen on välttämätöntä Espoolla käynnissä olevan projektin edistämiseksi ja turvaamiseksi, tästä esimerkkinä tiedonhallintalain edellyttämät linjaukset ja ohjeet henkilöstölle. Mikäli näistä vähintään kaksi ehtoa ei täyty, uusiin osallistumisiin suhtaudutaan lähtökohtaisesti varauksella.

Hankintojen tietoturvaliitteet havaittiin vanhentuneiksi jo 2020. Näitä päivitettiin 2021 aikana ja 2022 Espoon käyttämä turvallisuusliite valmistuu. Turvallisuusliitteen käyttöä joko osittain tai kokonaan tullaan suosittelemaan kaupungin toimialoille myös niiden hankintojen osalta, joita ei tehdä tietohallinnon kautta ICT-hankintoina. Suosituksella pyritään poistamaan kyberturvallisuuteen liittyviä eroja eri hankintojen välillä. Myös hankintojen turvallisuusliite tulee osaksi Espoon verkkokoulutuksia.

Vuoden aikana turvaposti otettiin käyttöön Espoon työllisyyspalveluissa, mutta sitä ei saatu laajempaan käyttöön lisenssihankintoihin ja kilpailutukseen liittyvistä syistä. Turvapostin ei myöskään koettu vastaavan kaikkiin turvallisen, digitaalisen viestinnän tarpeisiin, koska turvaposti toimii edelleen kaikille avoimen sähköpostijärjestelmän päällä. Ilman jokaisen lähettäjän ja vastaanottajan riittävän vahvaa tunnistamista riski ulkopuolisten toimijoiden väliintulosta on olemassa ja siksi 2022 aikana kaupungin toimintaa pyritään ohjaamaan Suomi.fi -palveluiden kaltaisiin vahvan tunnistamisen ympäristöihin.

Espoon kaupunki tulee vuoden 2022 aikana panostamaan erityisesti tiedonhallintalain vaatimusten huomioimiseen. Tavoitteellisesti Espoo pyrkii toimimaan vähintään lain edellyttämällä minimitasolla ja tuomaan lain tarkoittamat ja Valtiovarainministeriön ohjeistamat hyvät käytännöt konkreetian tasolle vuoden loppuun mennessä. Järjestelmissä ja palveluissa voidaan kuitenkin jo ennakoida olevan muutosviiveitä, minkä johdosta esimerkiksi lokituksiin tehtävät muutokset saattavat näkyä osalla toimittajista vasta 2023 puolella.



Kuva: Pintaliitodesign, Olli Urpela

