

Tietotilinpäättös 2024





Kuva: Antti Kangassalo

Johdanto

Espoon kaupunki on laatinut vuodesta 2018 lähtien vuosittaisia tietotilinpäätöksiä kaupungin tietosuojavastaavan ja tietoturvapäällikön johdolla.

Tietotilinpäätöksen tarkoituksena on arvioida tietosuojan ja tietoturvan toteutumista kaupungilla ja kuinka kaupungin sisäinen ja ulkoinen kyberturvallisuuden toimintaympäristö on muuttunut vuoden aikana, sekä mitä haasteita ja onnistumisia kaupungin eri toiminnot kohtasivat. Toimintoja ovat esimerkiksi varhaiskasvatus, kirjastot, tietohallinto ja kaupunkitekniikka.

Tämä tietotilinpäätös on julkinen asiakirja, jolla kaupunki tuo läpinäkyvyyttä sen toimintaan julkisena organisaationa. Espoon kaupunki ei ole ainoa tietotilinpäätöksiä laativa organisaatio vaan 2023 näitä laativat myös esimerkiksi Helsingin ja Kotkan kaupungit, sekä Traficom ja Väylävirasto. Sen kohdelukijakuntaa ovat muiden kuntien ja valtion edustajat, joille Espoon havainnoista saattaa olla hyötyä omassa toiminnassaan.

Osassa muista kunnista tietotilinpäätös on sisällytetty osaksi varsinaista tilinpäätöskertomusta.

Me olemme joukkue

Olen usein todennut - ja kokemuksen kautta todeksi oppinut - että onnistumme parhaiten silloin, kun teemme asioita yhdessä. Se on espoolainen tapa toimia ja meidän tekemisemme kivijalka. Tällainen toimintakulttuuri johdatti meidät myös tänä vuonna Euroopan innovaatiopääkaupunkikisan finaaliin.

Yhdessä tekeminen edellyttää toimivaa vuorovaikutusta ja aktiivisuutta. Se tarkoittaa yhteisten tavoitteiden ymmärtämistä ja toistemme kuulemistä ja kuuntelemista. Parhaita tuloksia syntyy silloin, kun aidosti yritämme ymmärtää toisiamme ja oppia uutta.

Meidän on tärkeää kehittää oman työyhteisön vuorovaikutusta. Kun kommunikaatio toimii omassa työyhteisössä, toimii se hyvin myös ulospäin. Tämä näkyy toimivana kumppaniyhteistyönä, mutta myös esimerkiksi asiakaspalvelun laatuna tai sujuvana työskentelynä, jossa aikaa ei kulu turhaan työhön tai päällekkäisten asioiden tekemiseen.

Avainasia on se, että me olemme yhteisö. Kukaan meistä ei onnistu yksin, vaan työtä tehdään joukkueena, joka puhalttaa yhteen hiileen. (Jukka Mäkelä, kaupunginjohtaja 2011-2024, *Espressi* 03/2024.)

Kirjoitus koskee hyvin myös tietoturvaa: tietoturva on osiensa summa, johon vaikuttaa paitsi sisäinen yhteistyö, mutta myös näiden vuorovaikutus ulkoisten tekijöiden ja kehittyvän teknologian kanssa. Siksi myös tietoturvan toteutumiselle on tärkeää, että sen turvallisuuden eri osat toimivat hyvin yhteen yli organisaatorajojen.



Kuva: Elias Metsämaa, Fimbutik

Sisällysluettelo

Johdanto	2
Me olemme joukkue	3
1 Muutokset ulkoisessa toimintaympäristössä ja megatrendit..	5
2 Tiedolla johtamisen kehittäminen -tiedolla parempaa tietoturva.....	6
3 Konsernihallinto	7
3.1 Tietosuojaryhmä ja henkilötietojen suojaaminen	7
3.2 Tietoturvaryhmä ja kaupungin toimintaympäristön seuranta..	7
4 Kasvun ja oppimisen toimiala.....	9
5 Elinvoiman tulosalue	10
6 Kaupunkiympäristön toimiala	11
7 Arviointi ja mittarit.....	12
7.1 Rekisteröityjen oikeuksien toteutuminen	12
7.2 Tietoturvapoikkeamat ja niiden ennaltaehkäisy.....	13
7.3 Henkilötietojen tietoturva- ja tietosuojaloukkaukset.....	14
8 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen.....	15
9 Kokonaistilanne	16



Kuva: Heidi-Hanna Karhu

1 Muutokset ulkoisessa toimintaympäristössä ja megatrendit

Megatrendeilla tarkoitetaan laajoja, yleisiä kehityssuuntia, jotka tapahtuvat usein maailmanlaajuisesti. Espoon toimintaympäristössä näitä kehityssuuntia on seurattu kolmella tasolla: maailmanlaajuiset, kansalliset ja paikalliset, sekä näiden vaikutusta Espoon kaupungin etujen näkökulmasta.

Tekoälyn käyttö, erityisesti ChatGPT-4:n kehittyminen, toi uusia käyttömahdollisuuksia. Espoon kaupungille tämä näkyi 2024 ensin käännöspalveluissa ja työllisyyspalveluissa, joissa määrämuotoista ja samanlaisena toistuvaa työtä suunniteltiin tekoälyn tehtäväksi Espoon julkisen www-sivun käännöksissä ja työnhakijoiden kielitason arvioinnissa, sekä työhakemuspohjien laadullisissa ensiarvioinneissa. Vuoden loppupuolella oli nähtävissä, että tekoälyn käyttö tulee lisääntymään, joka tuo tarvetta arvioida tietojenkäsittelyä kokonaan uudella tavalla riskien, henkilötietosuojan ja tietojensiirron näkökulmista vuoden 2025 aikana. Arviointitarve korostuu pilvipalveluissa, joiden toimittajilla voi olla tarve käyttää pilveen tallennettuja tietoja tekoälyn eduksi, eli toissijaiseen käyttötarkoitukseen.

Kansallisessa toimintaympäristössä havaittiin muutos tietoliikenneyhteyksien häiritsemisessä, kun merenalaisia tietoliikenne- ja energiakaapeleita katkaistiin. Globaalissa pilvipalveluympäristössä kaapelien katkeamiset näkyivät Espoolla hetkellisenä häiriönä

sähköpostin ja verkkopalveluiden saatavuudessa. Lisäksi eri kuntien verkkosivujen saatavuutta pyrittiin häiritsemään samanlaisina toistuvilla palvelunestohyökkäyksillä ja käyttäjiltä kalasteltiin tunnuksia eri teemoilla, kuten poliisin rikostutkinta tai rahalahjotukset.

Odotettavissa on, että myös tulevana vuosina Espoon julkiseen tietoverkkoon näkyviä verkkopalveluita pyritään häiritsemään lyhyillä jaksoilla kunnes hyökkääjä siirtyy seuraavaan kohteeseen tai havaitsee hyökkäyksen tehon hiipuneen. Vastaavasti tunnuskalastelijoiden on odotettavissa siirtyvän käyttämään tekoälyä aikaisempaa enemmän osana sähköpostikampanjoitaan, joka edellyttää käyttäjiltä jatkuvaa valppautta.

Drone -laitteiden käyttö ja epäilykset niiden avulla tehtävästä tiedustelusta ovat olleet uutisissa ja TikTok-videoissa esillä Ukrainan sodan jatkuessa. Uutisoinnissa on kiinnitetty huomiota myös perinteisempään kriittisen infran tiedusteluun: YLE uutisoi 04.07.2024 ”Imatran tärkeisiin laitoksiin on pyrkinyt tuntemattomia, jotka ”etsivät olematonta Penaa.” Epäilyksien johdosta julkisesti saatavilla olevaan tietoon ja sen merkitykseen varautumiselle on tarpeen kiinnittää aikaisempaa enemmän huomiota.

Espoon paikallisessa toimintaympäristössä tietoturvaa ja tietosuojaa koskevat muutokset koskivat eniten tekoälyä, jonka ensimmäisiä käyttökohteita olivat työllisyyspalveluissa tapahtuva työhakemusten vapaaehtoinen oikoluku ja kielitasotestit. Näitä ennen tekoälyn käytännöllisiä hyötyjä oli ollut vaikea hahmottaa.

2 Tiedolla johtamisen kehittäminen -tiedolla parempaa tietoturvaa

Kaupunkitasoinen kokonaisarkkitehtuurityö on tiedonhallinnan strateginen suunnittelumenetelmä, joka huomioi muutosvaikutukset toiminnan, tietojen, tietojärjestelmien ja teknologioiden näkökulmasta. Tämä edistää digitalisaation hallittua hyödyntämistä ja tukee kaupungin toimialoja tiedonhallinnan lakisääteisten tietoturva- ja tietosuojavelvoitteiden täyttämässä.

Kokonaisarkkitehtuurityössä tarkasteltiin loppuvuodesta eri lainsäädännöllisten muutosvaikutusten arviointimalleja ja niiden asemoitumista toisiinsa. Työssä pyrittiin pureutumaan ennakoivasti kansallisiin ja eurooppalaisiin tekoälysäädöksiin, sekä näiden yhteensovittamiseen jo olemassa olevien prosessien kanssa. Yhteensovittaminen tarkoitti puutteiden havaitsemista ja niiden korjaamista ilman mahdollisia lisäkustannuksia.

Vuoden 2024 aikana tarkasteltiin tiedonhallinnan kaupunkitasoisia vastuita ja velvoitteita tiedonhallintalain, tietosuojasääntelyn, arkitolain ja julkisuuslain velvoitteiden pohjalta. Tätä kokonaisuutta selkeytettiin vastuisiin liittyvällä ohjeella, joka nimettiin tiedonhallintamallin kansilehdeksi. Yhtenä kansilehden tavoitteena oli luoda tuloksikkokohtaiset yhteyshenkilöroolit tiedonhallintaan, tietosuojaan ja tietoturvaan, sekä roolinhaltijoiden kouluttaminen tehtävään. Koulutukset etenevät tulevan vuoden aikana.



Kuva luotu tekoälyllä.

Tiedolla johtamisessa Espoo ylsi marraskuussa 2024 kansainvälisen World Smart City Awards -älykaupunkikilpailun finaaliin ainoana pohjoismaisena kaupunkina. Espoo oli ehdolla kilpailun pääkategoriassa vaikuttavuudella johtamisen kehittämisohjelmalla, jota on toteutettu kaupungilla vuodesta 2019 lähtien. Espoon kaupunki on toteuttanut vuodesta 2019 vaikuttavuudella johtamisen ohjelmaa yhteistyössä Teknologian Tutkimuskeskus VTT Oy:n kanssa, jossa syksyllä 2024 käynnistyi uusi vaikuttavuuden arvioinnin koulutuskonaisuus.

Creatido Oy:n kypsyysanalyysi arvioi Espoon tiedolla johtamisen kypsyystasoksi 3,40, joka on korkein arvioitavista suomalaisista kaupungeista ja valtionhallinnosta sekä kahdeksan prosenttia korkeampi kuin vuoden 2022 mittauksessa. Tulosta nostivat vahvuudet ihmisten ja organisaation johtamisessa, tiedon muuttamisessa toiminnaksi sekä johdon roolissa tiedolla johtamisessa. Tiedon hyödyntämisen merkitys korostuu Espoossa, sillä 96 % selvityksen vastaajista uskoo tiedolla johtamisen tuottavan merkittävää lisäarvoa tulevaisuudessa.

3 Konsernihallinto

Espoon kaupungin hallintosäännön mukaisesti konsernihallinnon tehtävänä on johtaa, ohjata, valvoa ja kehittää koko kaupunkikonsernia sekä vastata kaupungin tukipalveluista ja niiden kehittämisestä kaupunginjohtajan johdolla. Konsernihallinto vastaa kaupunkitasoisesta tietoturvasta, tietosuojasta ja niiden ohjauksesta.

3.1 Tietosuojaryhmä ja henkilötietojen suojaaminen

Espoossa tietosuojan tilannetta ja toteutumista seuraa kaupunkitasoinen tietosuojaryhmä. Tietosuojaryhmään kuuluvat muun muassa toimialojen tietosuojan yhteyshenkilöt, jotka osaltaan seuraavat toimialansa erityislainsäädännön huomioimista tietosuojatyössä.

Vuonna 2024 ryhmässä käsiteltiin muun muassa tekoälyasetusta, kameravalvonnan ohjeistusta ja tietosuojadokumentaation uudistamista.

Euroopan unionin tekoälyasetus tuli voimaan 1.8.2024 ja sen soveltaminen käynnistyy portaittain kahden vuoden siirtymäajalla. Tekoälyä hyödyntävän järjestelmän, joka otetaan käyttöön 2.8.2026 tai sen jälkeen, on vastattava asetusta. Asetuksen tarkoituksena on suojella luonnollisten henkilöiden perusoikeuksia ja niiden toteutumista tekoälyjärjestelmissä.

Poikkeuksellista tekoällysäädöksessä on, että tekoälyjärjestelmien käyttöönottajia veloitetaan suorittamaan muun muassa perusoi-

keuksien vaikutustenarviointi FRIA (*Fundamental Rights Impact Assessment*) ja tarkistamaan tietosuojan vaikutustenarviointi DPIA ennen käyttöönottoa. Suurin osa sääntelystä koskee korkeariskisten tekoälymallien kehittäjiä -rajoitetun riskin tekoälyjärjestelmiä koskevat suppeammat velvollisuudet.

Espoon kaupungille perustettiin syksyllä 2024 poikkihallinnollinen tekoälytyöryhmä, jonka tarkoituksena on muun muassa selkeyttää vastuunjakoa, tuottaa kaupunkitasoisia ohjeita ja koulutusmateriaaleja, sekä varmistaa, että tekoälyjärjestelmien käyttöönotossa noudatetaan olemassa olevia prosesseja.

Vuonna 2024 valmistui uusi kaupunkitasoinen tietosuojaselosteiden mallipohja. Mallipohjaa hyödynnetään uusissa ja päivitettävissä tietosuojaselosteissa, jotta niiden laatu ja niille asetetut vaatimukset voidaan varmistaa kaupunkitasoisesti. Mallipohjan lisäksi luotiin ohje, jonka tarkoitus on auttaa tietosuojaselostepohjan täyttämisessä, sekä päättelypuu oikean henkilötietojen käsittelyperusteen valinnan helpottamiseksi.

Espoon kaupunki jatkaa tulevanakin vuonna tietosuojadokumenttien uudistamista vastaamaan uusia lakisääteisiä vaatimuksia, sekä parantamaan aiemmin laadittujen sisällöllistä laatua.

3.2 Tietoturvaryhmä ja kaupungin toimintaympäristön seuranta

Espoon kaupungin tietoturvaryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä arvioi edellä mainittua kokonaisuutta ja tekee siihen perustuen suosituksia ja ohjeita kaupungin tietoturvallisuuden parantamiseksi.

Vuoden aikana ryhmässä käsiteltiin tekoälyn ensimmäisten käyttötapauksien lisäksi tiedonhallintalaista kumpuavia vaatimuksia tietoturvan vastuunjaolle ja riittävälle kouluttamiselle, sekä missä määrin lakisääteisistä vastuista kerrotaan henkilöstölle. Kunnilla, kuten Espoolla, on ollut käytössä erillisiä tietoturvasitoumuksia, mutta sitoumuksien kerääminen ei kuitenkaan ole tarpeellista, koska laki ja sen rikkomisen seuraamukset pätevät ilman hyväksyntääkin.

Kirjallisista koko henkilöstölle tarkoitetuista sitoumuksista luovutaan, koska allekirjoitusten keräämistä ja sitoumuksien jakamista riittävän kattavasti ei voitu seurata tehokkaasti ilman uusia työkaluja ja rekrytointiprosessin täydentämistä. Jatkossa vastuista, kuten työkäyttöön luovutetusta puhelimesta ja vaitiolovelvollisuuden tiedostamisesta, kerrotaan erillisellä yhden sivun tiedoksiannolla. Vastuiden tuntemus on kaikkien osapuolien yhteinen etu.

Tietoturvakoulutuksien osalta Espoon kaupunki on tarjonnut työntekijöilleen jo pitkään erillistä tietoturva-, tietosuoja- ja tilaturvallisuuden opintopolkua. Tästä kerättiin ensimmäistä kertaa tyytyväisyystuloksia, joiden perusteella opintopolun suorittaneet kokivat opetusmateriaalin liian pitkäksi ja teoreettiseksi. Tämän johdosta opintopolun suoritusprosentti on ollut matala ja materiaalit on tarkoitettu uusien kokonaan jo 2025 niiden kiinnostavuuden ja hyödyllisyyden lisäämiseksi. Kaikkien henkilöstöryhmien kokonaissuoritusprosentti oli noin 34% vuoden lopussa.

Tietoriskien etukäteispainotteisesta hallinnasta keskusteltiin ryhmässä, joka on tiedonhallintalain vaatimus kaikille kunnille. Espoolla tätä on toteutettu jo kahden vuoden ajan toimintokohtaisilla tietoriskiarvioinneilla, joita tuetaan järjestelmä- ja palvelukohtaisilla selvityksillä muun muassa pääsynhallinnassa ja tietojenkäsittelyn lokittamisessa. Muualla vastaavanlaiset selvitykset

ovat aikaisemmin paljastaneet väärinkäytöksiä esimerkiksi Helsingin kotihoidon ja HUS:in palveluissa joulukuussa 2024, joista uutisoitiin laajasti. Espoolla selvitykset tulevat jatkumaan 2025.

Espoon verkkosivuja häirittiin lyhyesti ulkomailta tulevilla palvelunestohyökkäyksillä. Ne todettiin yleiseksi verkossa tapahtuvaksi häiriköinniksi, jotka torjutaan niin sanotuilla DDoS-pesureilla. Palvelunestohyökkäyksien ennustetaan toistuvan vuosittain samasta lähteestä vastaavalla tavalla kuin tietojenkalastelukin. Keskustelun yhteydessä harkittiin tarkempia sähköpostiestoja, kuten erillistä varoitussivua siirryttäessä kaupungin ulkopuolisille verkkosivuille pikalinkistä, mutta näille ei koettu toistaiseksi olevan tarvetta. Automaattisen suodatuksen todettiin olevan riittävää ja myös Espoo.fi-verkkosivuilla olevia osoitteita ei koettu tarpeelliseksi peittää, jotta ne säilyvät riittävän helposti kuntalaisten saatavilla.

Helsingin kasvatuksen ja koulutuksen toimialan tietomurto aiheutti kysymyksiä sekä ryhmässä että kaupungin johdossa. Tapauksen piirteet käytiin läpi ja Espoo kertasi VPN-käytännöt, sekä keskusteli edellä mainituista sähköpostikäytännöistä käyttäjätunnuskalastelun estämiseksi. Tapauksen johdosta kaupungin verkkoasemia siivottiin, jonka yhteydessä ainakin yksi merkittävä tietovaranto paljastui olevan potentiaalinen kohde vastaavalle tietomurrolle. Se poistettiin.

Verkkoasemien tietoturvallisuudesta keskusteltaessa **todettiin pilvipalveluiden yleistilanne**, eli pilven olevan lähtökohtaisesti tietoturvallinen paikka tallentaa tietoja, mutta salassa pidettävillä tiedoilla suositellaan käytettäväksi kryptauskerrosta, jolla toimittajan pääsy tietoihin voidaan estää. Ilman kryptauskerrosta esimerkiksi Sharepointin käyttöä ei ole voitu edistää, jolloin paikalliselle tallennuskapasiteetille on jatkossakin tarvetta. Tilanteen korjaamiseksi toimittajilta toivotaan oma-aloitteisuutta kryptauskeroksen saamiseksi sisäänrakennetuksi vakio-ominaisuudeksi.

4 Kasvun ja oppimisen toimiala

Kasvun ja oppimisen toimialalla lukumääräisesti eniten henkilötietojen käsittelyä tapahtuu kouluissa ja päiväkodeissa. Tietosuojajoikeamisissa suurin yksittäinen syy on viestin lähettäminen väärälle vastaanottajalle tai ryhmälle.

Toimialan tietoturva- ja tietosuojatyötä vahvistettiin 2024 perustamalla toimialalle oma tietoturvan ja tietosuojan työryhmä, jossa on laaja edustus toimialan eri yksiköitä, suunnittelijoita ja asianajaja käsittelemään tietoturvan tilannetta kouluissa, päiväkodeissa ja muissa sivistyksen yksiköissä.

Painopisteinä vuoden aikana olivat toimialalla tärkeimmät tietoturvan ja tietosuojan tehtäväkokonaisuudet, niiden priorisointi ja toteuttamisaikataulut. Esimerkiksi toimialan tietosuojaselosteiden läpikäynti ja päivittäminen, jotta ne ovat helpommin löydettävissä, tietojenkäsittelyn lakiperusteiden tarkistamiseksi ja rekisteröityjen oikeuksien toteuttamiseksi.

Tiedon löydettävyyttä parannettiin huolehtimalla selosteiden saatavuudesta ruotsiksi ja englanniksi, sekä jakamalla kohdennettuja tietosuojajooppaita koulujen henkilökunnalle ja jatkossa päiväkodeille.

Helsingin kaupungilla 2024 aikana tapahtuneen tietomurron seurauksena, jossa hyödynnettiin käyttäjältä kalasteltua tunnusta ja VPN-tuotteen haavoittuvuutta, ryhmä esitti toimenpiteitä tarpeet-



Kuva: Taru Turpeinen

tomien sähköpostiviestien, verkkolevytiedostojen ja paperisten asiakirjojen siivoamiseksi. Vuosittaista siivousta laajennettiin Espoolaisten oppijoiden käyttämään **Google Workspace for Education** -oppimisympäristöön, johon muodostuu säännöllisesti tarpeettomia ryhmiä ja työtiloja.

Varhaiskasvatuksen toiminnanohjausjärjestelmä eVaka:ssa toteutettiin syksyllä tietoturvatestaus ja -auditointi ulkopuolisen toimijan toimesta. Tietoturva-auditoinnissa löytyi yksi haavoittuvuus käyttövaltuuksien tarkistamiseen liittyen ja se korjattiin. Varhaiskasvatukseen kuuluvat muun muassa Espoon päiväkodit, joissa käsitellään lasten ja näiden huoltajien tietoja.

Tekoälyn hyödyntämisen ensimmäinen pilottihanke aloitettiin toimialalla. Sitä jatketaan vuoden 2025 aikana. Toimiala myös jatkaa henkilöstön tietosuojaosaamisen kehittämistä uuden verkkokoulutus- ja ohjemateriaalin keinoin. Turvasähköpostilisenssien määrää on tarve kasvattaa ja varmistaa niiden käyttäminen kaikille sitä tarvitseville.

5 Elinvoiman tulosalue

Elinvoiman tulosalue vastaa kaupungin elinvoiman, kilpailukyvyyn ja vetovoiman vahvistamisesta sekä edistää kuntalaisten ja asiakkaiden hyvinvointia, yhteisöllisyyttä ja osallisuutta yhteistyössä toimialojen ja kumppaneiden kanssa.

Elinvoiman tulosalueen tulosityksiköt vastaavat muun muassa kaupungin liikunta- ja kulttuuritoiminnoista, kirjastoista, museoista sekä laajasti elinkeinon ja työllisyyden tehtävistä. Tulosalueella toimii hyvinvoinnin, terveyden ja osallisuuden edistämisen tiimi.

Tulosityksikoilla on monipuolinen tehtäväkenttä ja muuttuva toimintaympäristö. Tietosuoja- ja tietoturva-asioiden vahvistamiseksi tulosalueella on vuoden 2024 aikana tiedotettu henkilökuntaa koulutuksista ja opastettu muun muassa tiedostojen ja asiakirjojen säännölliseen siivoamiseen.

Elinkeinon ja työllisyyden tulosityksikössä jatkettiin työllisyyspalveluiden siirtoon valmistautumista. Kansallisen uudistuksen myötä TE-palvelut ja näiden työntekijät siirtyvät kuntien vastuulle 1.1.2025. Järjestämisvastuun siirron valmistelun yhteydessä henkilöstön ja järjestelmien siirto on vaatinut myös laaja-alaisesti tietoturva- ja tietosuojariskien arviointia ja hallintatoimenpiteiden luomista. Tehtävien siirtyminen ja toimintatapojen uudelleen muodostaminen tulevat olemaan myös vuoden 2025 aikana keskeisiä asioita. Työvoimapaalveluiden tarjoamisessa nojaututaan myös KEHA-keskuksen tarjoamiin järjestelmiin, joka osaltaan vaikuttaa mahdollisuuksiin hallita riskejä.

Kulttuurin tulosityksikössä aloitettiin uuden kirjastojärjestelmän hankinta yhteistyössä muiden Helmet-kirjastojen kanssa ja uusittu Helmet-verkkosivusto avattiin. Kaupunginmuseon kulttuuriperintötietojärjestelmä KUHA, joka on kaiken museon tietopalvelutyön, museon kokoelmien ja kulttuuriympäristötiedon keskitetty tietopankki, otettiin tuotantokäyttöön joulukuussa. Espoon kaupunginmuseon digitaalisia museopalveluita kehittävä ja museoalan valtakunnallista toimintamallia valmisteleva projekti on päättynyt, jonka seurauksena valtakunnallinen museoiden digipolitiikan toimintamalli julkaistiin.

Liikunta ja urheilu- tulosityksikössä tehtiin vuoden 2024 aikana monipuolisesti toimia kuntalaisten liikuntapalveluiden ja harrastusmahdollisuuksien parantamiseksi, ja jatkettiin digitaalisten ratkaisujen hyödyntämistä käyttäjämäärien seurannan, liikunta- paikkojen ylläpidon ja seurayhteistyön kehittämisen saralla. Henkilöstön osaamisen kehittämiseen kiinnitettiin erityistä huomiota, ja kehitettiin muun muassa henkilötietojen käsittelyn lainmukaisuutta. Vuonna 2024 käynnistettiin kehitys- ja käyttöönottoprojekti käytössä olevan resurssivarausjärjestelmän korvaamiseksi uudella järjestelmällä, ja projekti rajattiin koskettamaan vain venepaikkojen varausta. Vuonna 2025 käyttöönotettavalle venepaikkojen varausjärjestelmälle tehdään sekä tietoturva- että saavutettavuusauditoinnit ja luodaan henkilötietojen käsittelystä tietosuojaseloste uudelle pohjalle. Vuonna 2025 käynnistetään uusi projekti, jonka tavoitteena on korvata tilavaraus- ja ohjatun liikunnan kurssi-ilmoittautumisjärjestelmä nykyaikaisemmalla järjestelmällä.

6 Kaupunkiympäristön toimiala

Kaupunkiympäristön toimialalla luodaan edellytykset asumiselle ja yrittämiselle Espoossa. Toimiala vastaa kaupungin tiloista muun muassa kouluissa ja päiväkodeissa, sekä rakentaa ja ylläpitää liikenneväyliä ja viheralueita. Kaavoitus ja ympäristöstä huolehtiminen ovat osa toimialan tehtävää.

2024 aikana toimiala valmistautui eri hakemusten toimittamiseen Maanmittauslaitokselle tietoturvalaisia viestinvaihtokanavia pitkin, kuten Suomi.fi-palvelu, joka samalla edellyttää Espoon kasvattavan asiointivaltuuksiaan näillä kanavilla. Toiminnan tarkoituksena on varmistaa ettei Espoon kirjaamis- ja hakemuspalveluista tuotettu tieto vuoda julkisuuteen esimerkiksi tunnuskalastelukampanjoiden seurauksena. Tietoja on tarkoitus käsitellä vähenevässä määrin sähköpostilla ja enemmän vahvan tunnistautumisen kanavilla, joihin anonyymeillä käyttäjillä ei ole pääsyä. Anonyymien käyttäjien lähettämien huijausviestien laadun on havaittu kasvaneen tekoälyn käytön seurauksena.

Henkilöstön perehdytystä tietoturvan ja tietosuojan perusteisiin jatkettiin ohjaamalla henkilökuntaa kaupungin videokoulutusallalle. Alustalla tarjottavan kurssin suoritusprosenttia, joka on tällä hetkellä kaupunkitasoisesti 34%, on tarkoitus nostaa tulevan vuoden aikana. Vastavoimana suoritusprosenttia madaltaa vuosittainen henkilöstön vaihtuvuus mikäli uutta henkilöstöä ei heti perehdytetä tietoturvalisiin käytäntöihin. Tämän johdosta yleisenä suosituksena



Kuva: Elias Metsämaa, Filmbutik Oy

myös muille kunnille on tiedottaa perehdytysmateriaalin saatavuudesta jo työntekijän tunnuksien luonnin yhteydessä esimerkiksi erillisellä tietoturvallisuuden tervetuloa -viestillä.

Pysäköinninvalvonnassa käytetty järjestelmä auditoitiin kaupallisen auditointiyrityksen toimesta, jonka pohjalta järjestelmän tietoturvaa on kohennettu. Samanaikaisesti kaupungin palautejärjestelmän käyttövaltuushallintaa tiukennettiin siten, että sen sisältöä ei ole mahdollista katsella

7 Arviointi ja mittarit



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

7.1 Rekisteröityjen oikeuksien toteutuminen

Keskeisenä rekisteröidyn oikeutena on oikeus tietää, miten ja kenen toimesta hänen henkilötietojaan käsitellään. Rekisterinpitäjä informoi rekisteröityä suorittamastaan henkilötietojen käsittelystä riittävällä ja selkeällä tavalla. Tätä toteutetaan Espoo.fi:stä löytyvien tietosuojaselosteiden avulla.

Vuonna 2024 kartoitettiin tietosuojaselosteiden laatua ja ryhdyttiin tarvittaviin toimenpiteisiin kaupungin tietosuojaselosteiden yhtenäistämiseksi sekä informoinnin parantamiseksi. Toimenpiteet tietosuojaselosteiden yhtenäistämiseksi sekä rekisteröityjen informoinnin parantamiseksi jatkuu vuonna 2025.

Tietosuojaselosteiden lukumäärä 31.12.2024

Toimiala	Lukumäärä
Espoo yhteensä	152
Konsernihallinto	31
Elinvoima	34
Kasvu ja oppiminen	28
Tekninen ja ympäristötoimi	57
Yleinen	2

Taulukko: Tietosuojaselosteita oli vuoden lopussa yhteensä 152 kappaletta.

Vuonna 2024 Espoo vastaanotti viisi GDPR:n mukaista tietopyyntöä sekä kolme tietojen poistopyyntöä. Tietopyynnöt on voinut toimittaa postitse tietosuojaselosteessa mainitulle yhteyshenkilölle tai vierailamalla asiointipisteessä, missä myös henkilöllisyys voidaan tarkistaa. Tapauksissa, joissa henkilö pyytää tuntemattomasta sähköpostiosoitteesta laajasti kaikkia henkilötietojaan, hänet täytyy ensin tunnistaa. Yksittäisen palvelun kohdalla ensirekisteröinnin yhteydessä kerättyjä tietoja, kuten yhteystiedot, voidaan käyttää tunnistamisen apuna.

Nykyisillä kaupungin prosesseilla pelkkää sähköpostiosoitetta ei voida pitää lain julkisen hallinnon tiedonhallinnasta 906/2019 14 § mukaisena riittävän tietoturvallisena vastaanottajan tunnistamistapana, koska laaja tiedonkeruu todennäköisesti johtaa salassa pidettävän tiedon muodostumiseen. Vuonna 2024 aloitettiin tietopyyntöprosessin sähköistämiseen liittyvää valmistelua. Sähköinen tietopyyntöjärjestelmä pyritään saamaan käyttöön vuonna 2025. Myöhempi tietopyyntöjä käsittelevän prosessin sähköistäminen tulee helpottamaan tunnistamiseen ja pyynnön etenemisen seurantaan liittyviä haasteita.

7.2 Tietoturvapoikkeamat ja niiden ennaltaehkäisy

Espoon kaupunki selvittää sisäistä tietoturvallisuuttaan ja tietosuojakäytäntöjä vuosittain tietoturvakävelyillä, joiden aikana toimipisteistä etsitään ennalta erilaisia haavoittuvuuksia. Näiden avulla 2022-2024 on jo havaittu merkittäviä puutteita asiakirjojen käsittelyssä, kameravalvonnan katvealueissa, tietojen säilytyksessä, tunnushallinnassa ja omaisuuden suojelussa. Ne ovat tapa osoittaa kaupungin tietoriskien hallintaa konkreettisesti.



Kuva: Taru Turpeinen

Tietoturvakävelyitä tehtiin kouluihin, kaupungille siirtyneisiin TE-palveluihin ja ruokapalveluihin. Selvitys oli ensimmäinen laatuaan kaupungille siirtyneiden TE-palveluiden kohdalla, jolla Espoo ja TE varmistivat palveluidensa tietoturvan ja tietosuojan todellista tilannetta.

Selvityksien perusteella suosittelemme kaikille kaupungeille kiinnittämään huomiota henkilökohtaisten lokeroiden lukituksiin, yhteisissä tiloissa olevien henkilö- ja tiimikohtaisten postilokeroiden asettamista lukittaviksi, kameravalvonnan kehittämistä kaikilla pysäköinti- ja saattoalueilla, vartija -kutsujen testaamista erityisesti yksin toimivien vartijoiden kohdalla, sekä vanhentuneen tietoteknisen omaisuuden asiallista poistamista tiloista riittävän lyhyellä viiveellä. Myös sähkökaappien lukitukset on suositeltavaa tarkistaa asiatonta pääsyä vastaan.

Koko vuoden aikana Espoon kaupungilla käsiteltiin vähintään 779 tietoturvaa tai tietosuoja koskevaa poikkeamailmoitusta. Näistä suurin osa oli automaattisia ilmoituksia, joihin myös reagoitiin automaattisesti esimerkiksi käyttäjätilejä sulkemalla tai poistamalla saastuneita tiedostoja. Espoo käsitteli laajan määrän myös muita automaattisia tietoturvailmoituksia.

Vähäinen osa tapahtumista johtui käyttäjien tahallisista toimista, kuten opiskelijoiden lataamista tiedostoista. Pääasiallinen ilmoitusten lähde olivat sähköpostissa vastaanotetut huijausryitykset, joka edelleen korostaa sähköpostin merkitystä huijareiden ensisijaisena työkaluna ja suurimpana tietomurtojen osatekijänä.

Tietoturvapoikkeamia voidaan edelleen ennaltaehkäistä kiristämällä sähköpostiin liittyviä käytäntöjä ja poistamalla julkisessa verkossa saatavilla olevaa tiedustelutietoa, kuten esihenkilösuhteita,

sähköpostiosoitteita ja kaikki rahankäsittelyyn liittyvä tieto. Samat tiedot tulisi peittää myös eri alustojen some-profiileista.

7.3 Henkilötietojen tietoturva- ja tietosuojaloukkaukset

Rekisterinpitäjillä on velvollisuus ilmoittaa valvovalle viranomaiselle ja rekisteröidyille tietosuojaloukkauksista, jotka aiheuttavat riskin asiakkaan oikeuksille. Tietosuojavastaava tekee viranomaisilmoitukset, mutta asiakkaalle tietoturvaloukkauksesta ilmoittaa rekisterin omistaja.

Tietosuojaloukkausten määrä vuonna 2024 oli 46 kappaletta. Eniten henkilötietojen tietosuojaloukkauksia tapahtui kasvun ja oppimisen toimialalla, joita oli 25 kappaletta. Myös elinvoiman tulosalueella tapahtui useampia tietosuojaloukkauksia, näitä oli 11 kappaletta. Muiden toimialojen kohdalla tietosuojaloukkauspaukset olivat yksittäisiä.

Tapahtuneista tietosuojaloukkauksista laadittiin ilmoitus tietosuojavaikuttetulle 30:ssä tapauksessa. Rekisteröidyille ilmoitettiin 35:ssä tapauksessa. Tietosuojaloukkausten keskimääräinen lukumäärä on pysynyt samana vuodesta 2020 alkaen eikä suuria muutoksia ole nähty.

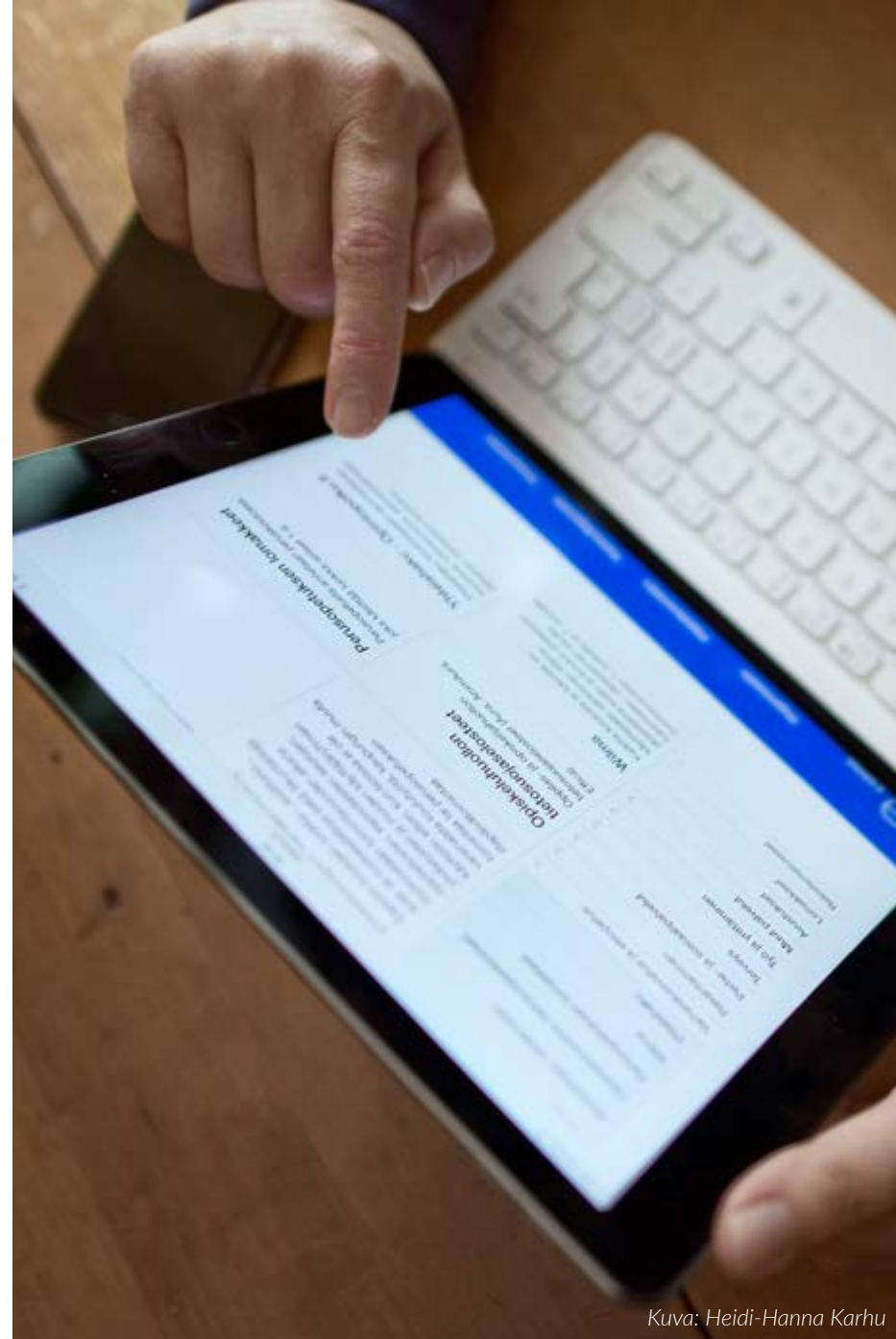
Suurin yksittäinen syy tietosuojaloukkauksille on ollut vuonna 2024 aiempien vuosien tapaan inhimillinen erehdys. Inhimilliset erehdykset muodostavat suurimman osan kaupungilla raportoiduista tietosuojaloukkaustapauksista. Yleisimpänä yksittäisenä syynä voidaan nostaa esiin väärän vastaanottajan tai vastaanottajaryhmän valinta, tai viestin lähettäminen niin, että kaikki vastaanottajat näkevät vastaanottajaketjun.

8 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen

Espoolla on noin 11 000 työntekijää, jotka hoitavat laajaa kirjoa kaupungin lakisääteisiä tehtäviä. Tehtävien hoitamisen edellyttää tiedon tuottamista ja käsittelyä, josta osa on salassa pidettäviä tai paljastuessaan potentiaalisesti vahingollista kunnan tai rekisteröityjen eduille.

Lain julkisen hallinnon tiedonhallinnasta 906/2019 4§ mukaan tiedonhallintayksikössä on oltava tarjolla koulutusta, jolla varmistetaan henkilöstön riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista.

Kaupungin kaikille työntekijöille tarjoaman tietoturvan ja tietosuojan peruskurssin suoritti noin 34%, eli 3746 työntekijää. Osallistuneita oli 70% jos mukaan lasketaan vähintään 40% kurssin sisällöstä katsoneet. Suoritusastetta pyritään nostamaan 2025-2026 uusimalla peruskurssi, jolloin myöskään osasuorituksia ei huomioida raportoinnissa. Uusi kurssi sisältää enintään 20 videota, joiden enimmäispituudet ovat 3 minuuttia kustakin aiheesta ja täten sisällöltään helpompia omaksua.



Kuva: Heidi-Hanna Karhu

9 Kokonaistilanne

Espoon kaupungilla ei 2024 aikana ollut merkittäviä tietomurtoja tai tietovuotoja, jotka olisivat vaarantaneet vähäistä merkittävämmän määrän kaupungin tietoja tai omaisuutta. Pääosa tietovuodoista tapahtui yksittäisten käsittelyvirheiden seurauksena.

Vertailuotoksena YLE:n uutiset aikaväliltä 01.01.2024-31.12.2024 näyttää aiheita HSL:n järjestelmäviasta, verkkosivujen palvelunestohyökkäyksistä, turvallisuusselvityksien aloittamisesta ja tulipaloista, mutta tänä aikana ei yhtään tietoturvaa tai tietosuojaa koskettavaa tapahtumaa.

Espoon kaupunki pyrkii strategiansa mukaisesti jatkossakin parantamaan arjen turvallisuutta monialaisella yhteistyöllä siten, että Espoo on Suomen turvallisin kaupunki. Espoo profiloituu Suomen turvallisimpana ja elinvoimaisimpana sivistyksen, osaamisen, innovaatioiden ja yritystoiminnan kansainvälisenä edelläkävijäkaupunkina. Tämän saavuttamiseksi kaupungin tietoja säilytetään tietoturvallisesti ja hyviä käytäntöjä noudattaen kaikissa sen palveluissa.



Kuva: freepik.com



Espoon kaupunki
Y-tunnus 0101263-6
Turvallisuus ja valmius -vastuualue
Virastopiha 2 C, 3.krs
PL 12, 02070 ESPOON KAUPUNKI