

Tietotilinpäättös 2022

Julkinen



Sisällysluettelo

Esipuhe	3	10 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen	22
1 Muutokset Espoon ulkoisessa toimintaympäristössä ja megatrendit	4	11 Tietoriskien hallinta osana Espoon palveluita.....	23
2 Tiedonhallinta ja kokonaisarkkitehtuurityö, tiedon hyödyntämisen kehittäminen	5	12 Todennetut kehittämiskohteet tulevalle vuodelle	24
3 Hankinnat.....	6		
4 Konsernihallinto	7		
4.1 Henkilöstöyksikkö	7		
4.2 Tietohallinto.....	8		
4.3 Asiakirjahallinto	9		
4.4 Tietosuojaryhmä	9		
4.5 Tietoturvaryhmä ja toimintaympäristön seuranta.....	10		
5 Kasvun ja oppimisen toimiala	12		
6 Elinvoiman tulosalue	14		
7 Kaupunkiympäristön toimiala.....	15		
8 Yhteistyöverkostot	16		
9 Arviointi ja mittarit	17		
9.1 Rekisteröityjen oikeuksien toteutuminen	17		
9.2 Tietoturvapoikkeamat	19		
9.3 Henkilötietojen tietoturvaloukkaukset	20		



Kuva: Roope Permanto, Otavamedia

Esipuhe

Tietotilinpäätöksellä rakennetaan luottamusta ja hyvää tiedolla johtamisen tapaa. Tietotilinpäätös on julkishallinnon organisaation vuosittainen kertomus henkilötietojen käsittelystä Espoon kaupungilla ja toimenpiteistä, joilla turvataan kuntalaisten, kaupungin työntekijöiden ja sidosryhmien kriittiset tiedot.

Tietotilinpäätöksen laatiminen ja julkaisu on linjassa tietosuojavaltuutetun suositusten kanssa, joiden mukaan tietotilinpäätöksen laatiminen on yksi tapa toteuttaa tietosuojalainsäädännön edellyttämää rekisterinpitäjän osoitusvelvollisuutta. Kyse ei ole kuitenkaan pelkästään lainmukaisuuden edistämisestä, vaan kunnan toiminnan läpinäkyvyydestä ja yhteisten ponnisteluiden esille tuomisesta.

Tämä vuoden 2022 tietotilinpäätös laadittiin aikana, jolloin Ukrainan kriisi ja tästä seuranneet muutokset toimintaympäristössä olivat tuoreita. Informaatiovaikuttamisen, vakoilun, varautumisen ja sisäisen turvallisuuden merkitys on kasvanut, sekä näihin liittyvä keskustelu resurssoinnista on siirtynyt valtamediaan. Kysymykset poikkeusoloihin varautumisesta ovat jälleen ajankohtaisia ja myös Espoossa esimerkiksi tietojen saatavuutta sähkökatkojen aikana on suunniteltu.

Megatrendit vaikuttavatkin laajasti Espoon ja muiden Suomen kuntien turvallisuussuunnitteluun. Palveluita digitalisoidaan ja tietoja siirretään pilveen, minkä seurauksena näihin liittyviä riskejä on syytä kartoittaa ja vaikutuksia tietosujoaan arvioida aiempaa tarkemmin. Kyseessä on kuitenkin vaiheissa tapahtuva muutos, jonka lopulliset vaikutukset nähdään vasta tulevana vuosina. Mahdollisesti aikana, jolloin kriisin tulokset ovat jo tiedossa.

Tätä kirjoittaessa on kuitenkin selvää, että Espoon täytyy jatkaa omaa varautumistaan tietojenkalastelua laajempiin ilmiöihin, kuten informaatiovaikuttaminen, tilaturvallisuus, salassa pidettävien tietojen tunnistaminen ja näiden aikaisempaa huolellisempi suojaaminen. Erityisesti jos turvallisuusuhat syvenevät vuosien 2023–2025 aikana.

Espoossa 28.03.2023

Harri Säkkinen
Tietoturvapäällikkö

Paula Pernilä
Tietosuojavastaava

1 Muutokset Espoon ulkoisessa toimintaympäristössä ja megatrendit

Espoon kaupunki laatii vuosittain tietotilinpäätöksen tietosuojavastaavan ja tietoturvapäällikön johdolla. Ensimmäinen tietotilinpäätös julkaistiin 2018, ja käsissäsi on sarjassaan viides tietotilinpäätös. Tietotilinpäätöksen keskiössä on vahvasti tietosuojan ja tietoturvan toteutuminen vuoden aikana ja siinä arvioidaan toimintaympäristön muutoksia, Espoon kaupungin ja sen toimialojen omaa toimintaa, havaittuja riskejä, onnistumisia sekä kehityksen suuntaa.

2022 megatrendejä, eli kansainvälisiä useita maita koskevia ilmiöitä, olivat Ukrainan kriisi ja vuoden aikana jatkunut keskustelu pilvipalveluiden riskeistä. Ukrainan kriisin seurauksista muun muassa Suojelupoliisi julkaisi uutisen (YLE 29.03.2022), jossa Suojelupoliisi varoitti Venäjän hybridivaikutamisen ja tiedustelun olevan suurimpia kansallisia uhkia. Ei vain uhkina, vaan suurimpina uhkina joihin täytyy reagoida ja varautua. Esimerkiksi väärennetyt sosiaalisen median videot ja uutiset, vaalivaikuttaminen, palvelunestohyökkäykset ja muu verkossa tapahtuva häiriköinti, sekä ihmisten rekrytointi tiedustelutoimintaa varten erityisesti ääriaineistojen ryhmistä.

Espoon paikallisessa toimintaympäristössä suurin muutos tapahtui hyvinvointialueiden (HVA) perustamisen yhteydessä, jota edelsi henkilökunnan ja suuren tietomäärän siirtyminen kunnalta hyvinvointialueelle. Valmistelu vei myös joiltakin Espoon työntekijöiltä merkittävän määrän työaika, jotta pystyttiin takaamaan turvallinen siirtymä henkilöstön lisäksi myös asiakkaiden henkilötiedoille ja muille hyvinvointialueen toiminnan aloittamisen

kannalta välttämättömille tiedoille. Samassa yhteydessä ei kuitenkaan kaikkia järjestelmiä tai niiden pääsynhallintaa voitu välittömästi siirtää HVA:lle, minkä johdosta esimerkiksi pääsynhallinta ja tietoverkkojen väliset yhteydet vaativat edelleen 2023 aikana yhteistyötä kahden eri organisaation välillä. Osana siirtymää selviää myös mitkä palvelut jäävät pysyvästi Espoon kaupungin ja Länsi-Uudenmaan Hyvinvointialueen yhteisiksi, jos yhtään.

Suomessa laki julkisen hallinnon tiedonhallinnasta 906/2019 astui voimaan 2019. Lain siirtymäaikaisten puitteissa kaupungeilla on ollut mahdollisuus toteuttaa tarvittavat tietoturvallisuuteen vaikuttavat muutokset. Lain edellyttämät muutokset ja tulkinnot kohdistuvat tietojenkäytön lokitukseen, pääsynhallintaan, koulutukseen, kunnan lukuun toimivien ohjeistuksiin ja muihin tietoturvaan liittyviin kokonaisuuksiin, jotka voivat olla laajoja. Useimpiin vaatimuksiin kyetään Espoon organisaatiossa vastaamaan jo olemassa olevin käytännöin, mutta esimerkiksi vastuukysymyksien selvittäminen osoittautui haastavaksi ja käytännöt muutosten tilaamiseen riippuvaiseksi vuosibudjetoinnista.

Tiedonhallintalain osalta on odotettavissa että keskustelu ja vaatimusten toimeenpano jatkuu laajemmin kunnilla, kuntayhtymillä ja hyvinvointialueilla myös 2023 aikana. Mahdollisesti jatkuen 2025 asti, jolloin näihin liittyvien hankintojen ja muutostöiden voidaan olettaa valmistuvan.

2 Tiedonhallinta ja kokonaisarkkitehtuurityö, tiedon hyödyntämisen kehittäminen

Espoo-tarinan mukaan Espoo kehittää tiedolla, data-analyysillä ja vaikutavuudella johtamista. Espoo yhdessä kumppaniensa kanssa on aktiivinen digitalisaation, robotiikan, tekoälyn ja muun teknologian hyödyntäjä läpi toimintaprosessien. Strategisten tavoitteidensa ohella kaupungin on otettava digitaalisessa kehittämisessä huomioon kansallinen ja EU-tason digilainsäädäntö.

Tietojen käsittelyä kaupungin toiminnassa ohjaa laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki 906/2019), jolla varmistetaan viranomaisen tietoaaineistojen laadukas hallinta ja tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi, mahdollistetaan tietoaaineistojen turvallinen ja tehokas hyödyntäminen sekä edistetään tietojärjestelmien yhteentoimivuutta. Muuta kaupunkia velvoittavaa digilainsäädäntöä ovat mm. tietosuojasääntely, digitaalisia palveluita ja sähköistä asiointia koskeva lainsäädäntö sekä EU:n data-asetukset. Tiedonhallintaa kaupungin eri toiminnoissa ohjaa lisäksi näitä toimintoja koskeva erityislainsäädäntö.

Kaupunkitasoisella kokonaisarkkitehtuurityöllä mahdollistetaan tiedonhallinnan ja tiedon hyödyntämisen strateginen kehittäminen, luodaan yhteentoimivuutta toimintamallien, tietojärjestelmien ja organisaation osien välille, autetaan varmistamaan tietoturvan ja tietosuojan toteutumista, sekä tuetaan kaupungin toimialoja ja yksiköitä heidän omassa kehittämistyössään. Tiedonhallintalain mukainen muutosvaikutusten arviointi ja tiedonhallintamallin ylläpito on kytketty kaupungin kokonaisarkkitehtuurityöhön.

Vuoden 2022 aikana kokonaisarkkitehtuurityön toimintamalleja on kehitetty, tavoitteena tuoda arkkitehtuurin suunnittelun tukea ja ohjausta yhä enemmän digitaalisen kehittämisen alkuvaiheisiin ja varmistaa siten eri arkkitehtuuri-näkökulmien riittävä tarkastelu alusta alkaen. Kokonaisarkkitehtuurityössä kehitettäviä kokonaisuuksia tarkastellaan muun muassa toiminnan muutoksen, tietojen, tietojärjestelmien, teknologian, tietoturvallisuuden, tietosuojan, käyttäjälähtöisyyden, lainmukaisuuden, yhteentoimivuuden ja hyvien suunnitteluperiaatteiden toteutumisen näkökulmista.

Tiedon hyödyntämisen kehittämiseen panostettiin vuonna 2022 arvioimalla kaupungin tiedon hyödyntämisen kypsyystasoa ja tunnistamalla tämän arvion perusteella kehittämistoimia. Jo edeltävänä vuonna aloitettua vaikuttavuudella johtamisen kehittämistä jatkettiin muun muassa tulossikkipilotein. Vaikuttavuuksia ymmärtämällä on tarkoitus tunnistaa keskeisiä tietotarpeita ja tämän kautta pyrkiä tavoitteelliseen tiedon hyödyntämiseen. Samaan aikaan kaupungin tiedon hyödyntämisen kyvykkyyksiä on kehitetty mm. vuoden 2023 alussa käyttöönottovaiheeseen tulleessa johtamisen ja talousohjauksen järjestelmäuudistuksessa. Lisäksi keskeistä on tiedon hyödyntämisen jatkuva kehittäminen kaupungin kunkin tulossyksikön omassa toiminnassa.

Tiedon turvallista hyödyntämistä sekä organisaatorajat ylittävää hyvinvointitiedon hyödyntämistä on vuonna 2022 kehitetty Valtiovarainministeriön digikannustinrahoitusta saaneissa yhteistyöprojekteissa.

3 Hankinnat

Espoon kaupungin hankintakeskus vastaa hankintalain soveltamisalaan kuuluvien hankintojen valmistelusta, mutta ei kuitenkaan kaupunkiympäristön toimialan rakennusurakoista ja suunnittelukilpailuista.

Hankintakeskuksen oma tietosuojaryhmä on vuoden 2022 aikana vakiinnuttanut toimintaansa kokoontuen pääsääntöisesti joka toinen viikko. Kaikki hankintakeskuksen kilpailuttamat hankinnat käsitellään hankintakeskuksen tietosuojaryhmässä. Hankintakeskuksen tietosuojaryhmä järjesti myös koulutusta jäsenilleen vuoden aikana. Kaupungin tietosuojavastaava osallistuu hankintakeskuksen tietosuojaryhmän toimintaan.

Hankintakeskuksen vastuulla olevissa hankinnoissa käytetään henkilötietojen käsittelyä koskevia sopimusliitteitä ja lisäksi ICT-hankinnoissa käytetään pääsääntöisesti liitteenä myös turvallisuuskuvasta. Hankintakeskus on vuoden 2022 aikana päivittänyt käytössään olevia tietosuojaliitteitä vastaamaan paremmin erilaisia käsittelysuhteita.

Hankinnoissa tietosuojaan liittyvät haasteet koskevat lähinnä kansainvälisiä tiedonsiirtoja ja niiden riittävää huomioimista. Kehityskohteena on huomioida tietosuoja paremmin jo hankintojen kilpailutusprosessin alkuvaiheessa.



Kuva: Pixabay / StartupStockPhotos

4 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 tietoturvasta, tietosuojasta ja niiden ohjauksesta.

Tietoturvan ja tietosuojan ohjaamisessa ja toimintaympäristön seuraamisessa tukena toimivat kaupungin tietosuojavastaava ja tietoturvapäällikkö, sekä teknisestä tietoturvasta vastaava IT-päällikkö. Tietosuojavastaava koordinoi kaupungin tietosuojaryhmää ja tietoturvapäällikkö puolestaan tietoturvaryhmää.

4.1 Henkilöstöyksikkö

Laki julkisen hallinnon tiedonhallinnasta 12§ edellyttää kuntia tunnistamaan ne tehtävät, joiden suorittaminen edellyttää työntekijöiltä tai kaupungin lukuun toimivilta erityistä luotettavuutta.

Lain vaatimuksen mukaisesti Espoolla määriteltiin vuoden 2022 aikana erityistä luotettavuutta edellyttäviä tehtäviä, joihin valittavasta henkilöstä tullaan ennen palvelussuhteen aloittamista teettämään Suojelupoliisilta tilattava suppea turvallisuus selvitys. Määrittely tehtiin kaupungin johdon ja henkilöstöhallinnon yhteistyönä, ja sitä tullaan tarkentamaan vuoden 2023 aikana.



Lisäksi Espoo tulee päivittämään erityistä luotettavuutta edellyttäviin tehtäviin liittyvää rekrytointi- ja palvelussuhteen aloitusprosessia sekä kaupungin sisäisiä käytäntöjä.

2022 aikana Espoo otti käyttöön tarkennetun päihdeohjelman, jossa käsitellään muun muassa huumausainetestien teettämistä ja joka käsittelee tältä osin henkilön luotettavuutta ja sopivuutta tehtävään.

Huumausainetestattavien tehtävänimikkeiden listaukset julkaistiin työntekijöille tarkoitetulla intranet-sivuilla. Listan tehtävänimikkeisiin teetetään tehtävään valittavasta henkilöstä huumausainetestin ennen palvelussuhteen aloittamista.

4.2 Tietohallinto

Espoossa tietoturvallisuuden kehittämisen painopiste on viimevuodet ollut tietoturvan kivijalan uudistamisessa, peruskyvykkyyksien kehittämisessä ja perustason määrittelyssä. Vuoden 2022 aikana jatkettiin teknologiauudistuksia, uusien kyvykkyyksien käyttöönottoa, tietoturvan valvonnan ja reagoinnin kehittämistä sekä identiteetinhallinnan uudistamista.

Tietohallinnossa jatkettiin edellisvuonna kilpailutetun ja käyttöönotetun Tietoturvan valvonta- ja asiantuntijapalveluiden kokonaisuuden kehittämistä. Tavoitteena on yhtenäistää Espoon käyttämiä tietoturvateknologioita, kehittää ja keskittää tietoturvatapahtumien havainnointia sekä parantaa näihin liittyviä reagointikyvykkyyksiä. Teknologiauudistusten lisäksi kokonaisuudessa kehitetään palvelukerrosta tuottamaan Espoolle sen tarvitsemia tietoturvan kokonaispalveluita sekä varmistamaan riittävä resurssointi tietoturvan kehittämisessä ja poikkeusten hallinnassa.

Espoossa toteutettiin 2022 aikana useita tietoturvatestauksia, joiden prioriteetti oli muun muassa Espoon ICT-peruspalveluiden kriittisissä kohteissa, Länsi-Uudenmaan hyvinvointialueen ja pelastustoimen palveluiden siirtymässä, toimialan kriittisten järjestelmien tarkastuksissa sekä projektikäyttöönottojen tukemisessa. Vaikka Espoossa toteutettiin vuoden aikana useita testauskokonaisuuksia, oli tietoturvatestauksien toteutuksessa myös merkittäviä resurssihaasteita, joiden vuoksi kaikkia suunniteltuja testauksia ei saatu toteutettua.

Tilanne liittyy muun muassa tietoturvan testauspalveluiden uudistamiseen sekä hyvinvointialueuudistuksen aiheuttamaan suureen ICT-asiantuntijapalvelukysyntään, jonka vuoksi sekä palvelutoimittajat että Espoon Tietohallinto ovat kärsineet resurssiongelmista. Tietohallinnon resurssihaasteen taustalla ovat erityisesti hyvinvointialueen ennakoitua pitkäkestoisemmat ja laajemmat ICT-tukitarpeet.

Espoossa uudistettiin ja käyttöönotettiin vuoden 2022 aikana keskitetty identiteetin- ja käyttövaltuushallinnan järjestelmä sekä siihen liittyvä palvelukokonaisuus muun muassa asiantuntija- ja pääkäyttäjäpalvelut. Palvelukokonaisuuden kehittäminen jatkuu Espoossa myös seuraaville vuosille huomioiden muun muassa kattavuuden laajentamisen, toimialojen kriittisten järjestelmien uudistukset ja näiden riippuvuudet Espoon identiteetin- ja käyttövaltuushallintaan. Käyttöönoton myötä saatiin yhtenäistettyä identiteetin ja käyttöoikeuksien hallintaan liittyviä prosesseja, sekä varmistettiin resurssointi kokonaisuuden kehittämiseen. Projektin yhteydessä siivottiin myös merkittävä määrä vanhentuneita käyttäjätunnuksia ja käyttöoikeuksia.

Vuoden 2022 aikana julkaistiin Espoon perus ICT-palveluita koskeva tarjouspyyntö. Kyseessä on merkittävä hankintakokonaisuus, joka koskee Espoon perustietotekniikkapalveluiden kilpailutusta. Espoon perustietotekniikkapalvelut sisältävät käyttäjätuki- ja työasemapalvelut, palvelinalustan käyttö- ja kapasiteettipalvelut sekä muita liitännäisiä palvelukokonaisuuksia, joilla on merkittävä rooli myös Espoon tietoturvan perustason toteutamisessa.

Hyvinvointialueiden uudistus aiheutti merkittäviä muutoksia Espoon toimintaympäristössä. Uudistuksessa Espoon ICT-tuotantoympäristön Hyvinvointi ja terveyspalveluiden, pelastustoimen sekä osia muiden toimialojen henkilöstöstä, tuotantojärjestelmät ja ICT-laitteet siirtyivät vaihteittain Espoolta hyvinvointialueen vastuulle.

Siirtymävaiheessa Espoon ICT-infrastruktuuriin tehtyjen toimenpiteiden tunnistettiin lisäävän siirtymävaiheessa Espoon tietoturvan ja tietosuojan riskitasoa. Muutoksia siirtymävaiheen ristiinkäytön sekä tietojen ja tietojärjestelmien siirtojen mahdollistamiseksi tehtiin riskiarviolähtöisesti huomioiden palveluiden mahdollisimman sujuva siirtyminen Espoosta hyvinvointialueen vastuulle.

Siirtymäajan muutoksien tietoturva vaikutuksia hallittiin muun muassa teknisin käyttövaltuus- ja pääsynhallinnan rajoituksin, tehostetun muutoshallinnan avulla, ICT-arkkitehtuurin arvioinneilla sekä erillisin tietoturvastrategioilla. Muutokset ja toiminnan vakiintuminen jatkuvat tulevana vuonna.

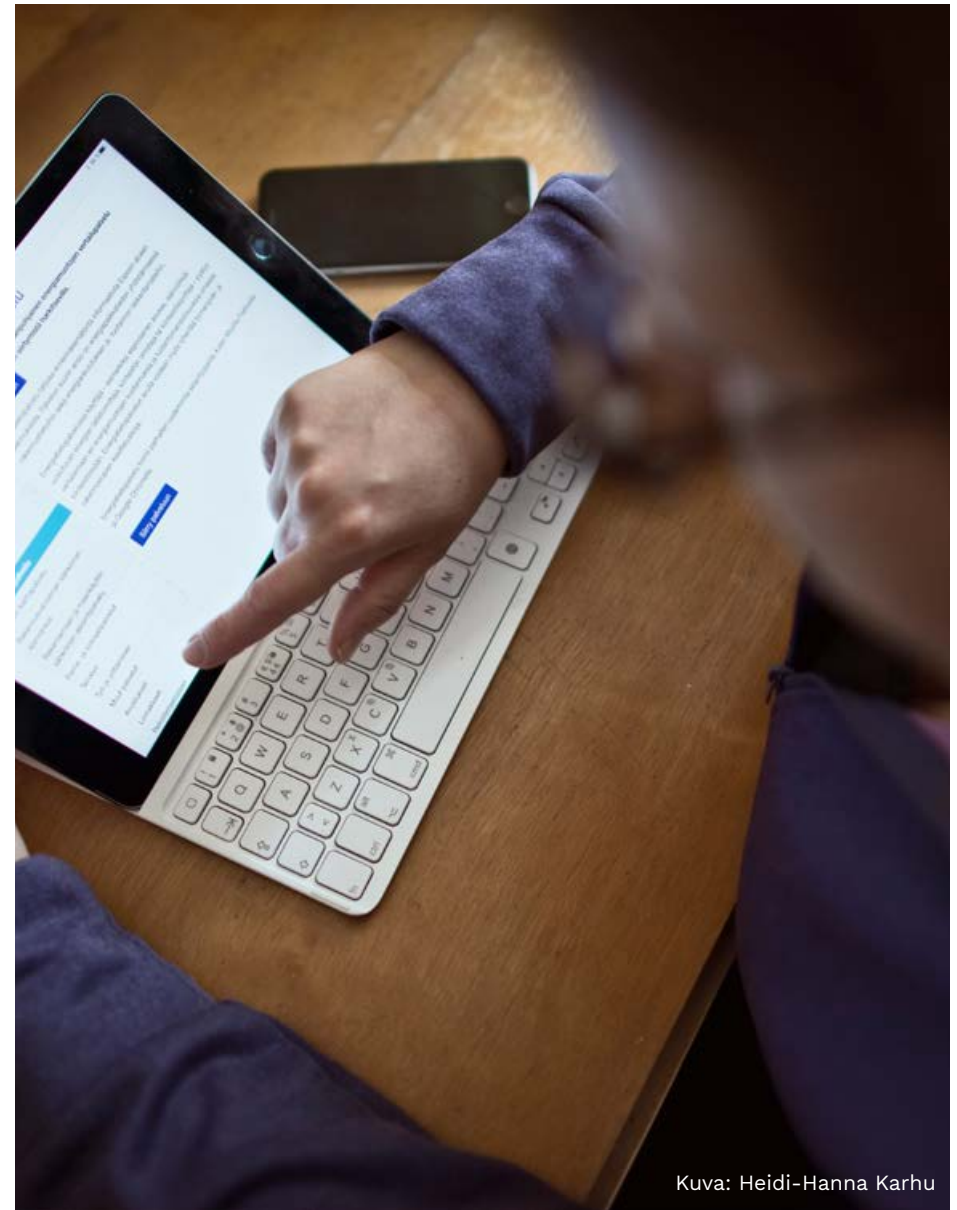
4.3 Asiakirjahallinto

Merkittävimpiä toimenpiteinä vuonna 2022 olivat voimaapanolain perusteella Länsi-Uudenmaan hyvinvointialueelle (LUVN) siirrettävien asiakirjojen siirtojen valmistelut sekä hyvinvointialueen toiminnan kannalta välttämättömien tietojen luovutukset hyvinvointialueelle. Vuoden 2023 alusta lähtien hyvinvointialueen omistukseen siirtyi paperisia asiakirjoja reilut 3800 hyllymetriä. Sähköisessä muodossa olevia asiakirjoja siirtyi useammista eri tietojärjestelmistä. Siirtyneissä asiakirjoissa olevien henkilötietojen rekisterinpitäjänä toimii LUVN 1.1.2023 alkaen.

2022 aikana jatkettiin asiakirjojen ja niissä olevien henkilötietojen elinkaarenhallinnan prosessien digitalisoimista tiedonhallintalain, arkistolain sekä tietosuojasääntelyn edellyttämällä tavalla. Keskeisinä toimenpiteinä tietojärjestelmissä, kuten Espoon entisessä henkilöstöhallinnon tietojärjestelmässä tuotettujen tietoaineistojen siirrot Espoon säilytysjärjestelmään kattaen myös siirrettävien tietoaineistojen sekä niihin sisältyvien henkilötietojen säilytysaikojen tarkistukset ja tarvittavat määritykset.

4.4 Tietosuojaryhmä

Espoossa tietosuojan tilannetta ja toteutumista seuraa kaupunkitasoinen tietosuojaryhmä. Tietosuojaryhmä on kaupunginjohtajan päätöksellä nimetty tietosuojavastaavan johtama työryhmä, johon kuuluu kattavasti jäseniä koko kaupunkiorganisaatiosta. Tietosuojaryhmään kuuluvat muun muassa toimialojen tietosuojan yhdyshenkilöt, jotka omalta osaltaan huolehtivat toimialansa erityislainsäädännön huomioimisesta tietosuo-



Kuva: Heidi-Hanna Karhu

jatyössä. Tietosuojaryhmän tehtäviin kuuluu mm. toimintaympäristön ja lainsäädännön muutosten seuraaminen ja analysointi, sekä kapunkitasoisten linjausten ja ohjeiden valmistelu.

Vuonna 2022 tietosuojaryhmä kokoontui 11 kertaa, heinäkuussa kokousta ei järjestetä lomista johtuen. Ryhmän toiminta on aktiivista ja ryhmän koko pysyy edelleen suurena, vaikka muutama jäsen siirtyikin vuoden 2022 lopulla Länsi-Uudenmaan hyvinvointialueen palvelukseen. Sosiaali- ja terveyspalvelut ovat perinteisesti olleet keskeinen toimiala kaupunkitasoisen tietosuojan näkökulmasta, koska toimialalla käsitellään pääsääntöisesti erityisiä henkilötietoja. Lisäksi sosiaali- ja terveyspalveluiden asiakkaina on edes jossain vaiheessa elämänsä suurin osa kaupunkilaisista. Jatkossa tietosuojan kannalta keskeisin toimiala tulee olemaan kasvun ja oppimisen toimiala, sosiaali- ja terveyspalveluiden järjestämistä vastuu siirryttyä hyvinvointialueelle vuoden 2023 alusta.

Tietosuojaryhmä käsitteli vuonna 2022 sekä kaupunkitasoisia tietosuojaan liittyviä prosesseja ja työkaluja, että toimintaympäristöön vaikuttavia laajempia tapahtumia. Ryhmä seuraa valvovan viranomaisen ohjeistusta ja ratkaisukäytäntöjä, ja nostaa ratkaisuihin nostetut haasteet myös kaupunkitasoiseen käsittelyyn. Tietosuojaavaltuutetun toimiston tuoreimmat ratkaisut käsitellään pääpiirteittäin jokaisessa tietosuojaryhmän kokouksessa. Vuoden 2022 keskeisimpinä nostoina olivat Google Analyticsin käyttöön liittyvät ongelmat, pilvipalveluiden ja tiedonsiirtojen haasteet sekä asiakkaiden informointiin ja oikeuksiin liittyvät ratkaisut. Tietosuojaryhmän kokouksissa käsitellään myös edellisen kokouksen jälkeen tapahtuneet henkilötietojen tietoturvaloukkaukset.

Tietosuojariskien arviointi ja erityisesti korkeiden riskien arviointi on yksi keskeinen keino huolehtia asiakkaiden oikeuksien toteutumisesta ja henkilötietojen käsittelyn turvallisuudesta. Tietosuoja-asetuksen toimeenpanon yhteydessä Espoossa otettiin käyttöön korkeiden riskien arviointiin tietosuojan vaikutustenarvioinnin työkalu. Usean vuoden kokemuksen jälkeen työkalua oli tarve päivittää, ja Espoo ottikin keväällä 2022 käyttöön uuden

vaikutustenarvioinnin työkalun. Työkalun valinnassa ja kehityksessä tietosuojaryhmällä oli keskeinen rooli. Alkuvuodesta valmistui myös Espoon kaupungin ensimmäinen tiedonsiirron riskiarvio eli Transfer Impact Assessment, lyhyemmin TIA. Ensimmäinen TIA laadittiin yhteistyössä asianajotoimisto Boreniuksen kanssa, ja tämä ensimmäinen TIA toimi pohjana muille kaupungissa vuoden aikana tehdyille tiedonsiirron riskiarvioinneille. Tiedonsiirtojen riskiarvio tulee tehdä, kun henkilötietoja siirretään EU/ETA-alueen ulkopuolelle. Riskiarvion tavoitteena on varmistua siitä, että henkilötietojen suoja pysyy EU/ETA-alueen suojaa vastaavana myös silloin, kun tietoja siirretään esimerkiksi kansainväliseen pilvipalveluun. Riskiarvion perusteella otetaan tarvittaessa käyttöön lisäsuojatoimenpiteitä, joilla varmistetaan ettei tietosuojan taso pääse laskemaan. Tiedonsiirtojen riskiarviot olivat keskeinen teema tietosuojakeskusteluissa myös yhteistyöverkostoissa ja kuntien välisessä yhteiskehittämisessä.

Edellä jo mainittujen aiheiden ja tiedonsiirtoihin ja pilvipalveluihin liittyvän keskustelun lisäksi tietosuojaryhmässä käsiteltiin kaupungin tietosuojaverkkokoulutusten siirtoa toiseen koulutusjärjestelmään, kaupungissa meneillään olevia tietoturvaan liittyviä toimenpiteitä sekä tietoturvaloukkausten ilmoitusprosessin uudistamista ja loukkausilmoitusten tekemiseen soveltuvan käyttäjäportaalin käyttöönottoa.

4.5 Tietoturvaryhmä ja toimintaympäristön seuranta

Espoon kaupungin tietoturvaryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä analysoi ja arvioi edellä mainittua kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia ja linjauksia kaupungin tietoturvallisuuden parantamiseksi. Lisäksi ryhmä toimii koko kaupunkiorganisaation tukena tietoturva-asioissa.

2022 alkoi Log4j-haavoittuvuuden jälkiarvioinnilla, johon liittyen Espoon kaupunki paikkasi noin 70 järjestelmässä olevia haavoittuvuuksia. Samaan

aikaan tunnuksia vuodettiin nettiin, joita on voinut tarkastaa eri vuotosivujen kautta. Sivuilta löytyvät tunnukset suljetaan kunnes niiden salasanat on vaihdettu ja vahva tunnistautuminen on käytössä.

Alkuvuoden aikana tietoturvaryhmässä myös päätettiin Espoon käyttämän tietoturvakoulutuksien alustan korvaamisesta eri tuotteella, joka oli jo ostettu toisen yksikön toimesta. Työntekijät ohjeistettiin käyttämään uuden alustan tietoturvakurssia, jonka suoritusprosentin tavoitellaan olevan vähintään 80%.

Espoon kaupunki ja osa ryhmän jäsenistä osallistui 2022 järjestettyyn Jyväskylän ammattikorkeakoulun (JAMK) kyberturvallisuusharjoitukseen, joka kesti viisi päivää, ja DVV:n järjestämään puolenpäivän TAISTO-harjoitukseen. Harjoitusten aikana harjoiteltiin simuloitua tietomurtoa ja kuinka siihen reagoidaan eri työntekijöiden yhteistyönä. Harjoituksessa havaittiin, että nopeasti etenevissä tilanteissa monikanavainen ja nopeisiin päätöksiin kykenevä organisaatio selviää häiriötilanteesta tehokkaammin. Samalla organisaation täytyy kyetä varautumaan palveluiden ja linjojen ruuhkautumiseen ja toimimaan vaikka osa avainhenkilöistä ei olisikaan saatavilla.

Ukrainan kriisi näkyi erityisesti ensimmäisen vuosipuoliskon aikana Espoon tietoturvallisuuden toimintaympäristössä eri tiedotteista ja varautumisessa. Haktivismin ja informaatiovaikuttamisen uhan todennäköisyys nousi hyvin realistiseksi, jonka johdosta myös Espoolla näihin on tarpeen varautua tietoriskilähtöisesti. Eri toimia tehtiinkin tunnistamalla ensin Espoon tärkeimmät järjestelmät ja tämän jälkeen arvioimalla toimien riittävyttä esimerkiksi tietomurron ja sähkökatkojen varalle.

Ryhmässä huomioitiin Espoon siirtyminen ePassin käyttöön, Aluevalvontaviraston kysely työllisyyskokeilun viestinvaihdosta, tietosuojavaltuutetun linjaus Google Analyticsin käytöstä ja pitkään jatkunut keskustelu Outlookissa laadittavien sähköpostien riittävän tietoturvallisesta lähettämisestä.

Epassiin siirtyminen herätti huolia sen käyttöehtojen johdosta, joiden perusteella toimittaja varasi oikeudet mainosviestien lähettämiseen Espoon henkilökunnalle ja esimerkiksi poliittisten sidonnaisuuksien kysymiseen. Syyksi ilmeni sovellukseen ladattavien rahojen käsittäminen pankkipalveluksi, jonka johdosta sidonnaisuuksien selvittäminen on lakisääteistä. Mainosviestien lähettäminen pyydettiin muutettavaksi opt-in -tyyppiseksi, eli niitä ei tule lähettää ilman erillistä pyyntöä.

Aluevalvontaviraston kysely työllisyyskokeilun viestinvaihdosta keskittyi sähköpostiviestien lähettämisen metodeihin. Tarkoitusta varten työllisyyspalveluille oli jo ostettu turvapostilisenssejä ja työntekijöitä ohjeistettu käyttämään puhelinnumeroon lähetettävää lisävahvistusta. Sama periaate on käytössä kaikissa Espoon palveluissa, joissa käytetään turvapostia.

Palveluissa, joissa turvaposti tai mikään muukaan turvallisen viestinnän sovellus ei ole käytössä, ainoaksi vaihtoehdoksi jää suojattavan tiedon siirtäminen erilliseen liitetiedostoon ja sen suojaaminen salasanalla, joka lähetetään tekstiviestinä vastaanottajalle. Näiden toimien on tulkittu olevan riittäviä tiedonhallintalain 14 §:n täyttämiseksi.

Tietosuojavaltuutetun linjaus Google Analyticsistä aiheutti toimia Espoon kaupungilla ja tietoturvaryhmässä. Analyticsin, Tagsin ja Fonttien käytöstä linjattiin, että näiden käyttö ei voi jatkua ja esimerkiksi espoo.fi:n tulee siirtyä käyttämään sellaisia analytiikkapalveluita jotka eivät siirrä tietoa EU/ETA-alueen ulkopuolelle.

5 Kasvun ja oppimisen toimiala

Kasvun ja Oppimisen keskeisiä arvoja ovat palvelujen ja niiden tietojärjestelmien tietoturvallisuus, skaalautuvuus ja käytettävyyden edistäminen.

Näitä arvoja edistettiin vuoden 2022 aikana myös Kasvun ja Oppimisen toimialan tärkeimmissä digitaalisissa kehityshankkeissa, jotka ovat opetuksen digitaalinen ekosysteemi DigiOne ja varhaiskasvatuksen toiminnanohjausjärjestelmä eVaka.

Edelleen käynnissä olevan DigiOne:n kehityshankkeen tavoite on luoda oppimisen ja koulutuksen palveluita yhteen kokoava kansallinen palveluportaali. Hankkeessa ovat mukana Espoon lisäksi Vantaa, Jyväskylä, Lahti, Oulu, Tampere, ja Turku sekä Kuntien Tiera. Opettajien, opiskelijoiden, rehtorien, huoltajien, sekä kaupungin henkilöstön käyttämät tiedot, järjestelmät ja palvelut kootaan palvelualustalle käyttäjäystävälliseksi ja yhteneväiseksi kokonaisuudeksi.

Hankkeessa on saatu eri palveluiden kilpailutukset päätökseen. Kehittämistyö jatkuu vuosina 2023-24 ja sen lisäksi käynnistyy peruskoulujen tuotantopilotti arviolta elokuussa 2023. DigiOne olisi kaikkien peruskoulujen osalta tuotantokäytössä arviolta elokuussa 2024, jolloin myös lukioden tuotantopilottit käynnistyvät. Lukioden tuotantokäyttö alkaisi arviolta elokuussa 2025.

eVaka on Espoon, Tampereen, Oulun ja Turun yhteinen hanke, jolla luodaan toiminnanohjausjärjestelmä päiväkodeille. Vuoden aikana eVakan tietoturvaa kiinnitettiin erityistä huomiota suorittamalla auditointi, jossa järjestelmän koodia katselmoitiin, sekä henkilötietojen suojaamiskäytäntöjä. Digi- ja Väestötietovirasto suoritti tarkastusta eVakaan digitaalisen yhteiskunnan keskeisten toimintojen suhteen ja raportissa ei tullut mitään merkittäviä kehittämiskohteita esille.

Uudeksi toiminnallisuudeksi eVakaan lisättiin henkilökunnan reaaliaikaiset läsnäolot, ryhmän toimintakalenteri, sekä hallinnon massaviestintä kuntalaisille. Tietosuoja kehitettiin tuomalla varhaiskasvatus- ja esiopetuksen opetussuunnitelmat eVakaan, jolloin näitä asiakirjoja ei enää tarvitse käsitellä paperilla.

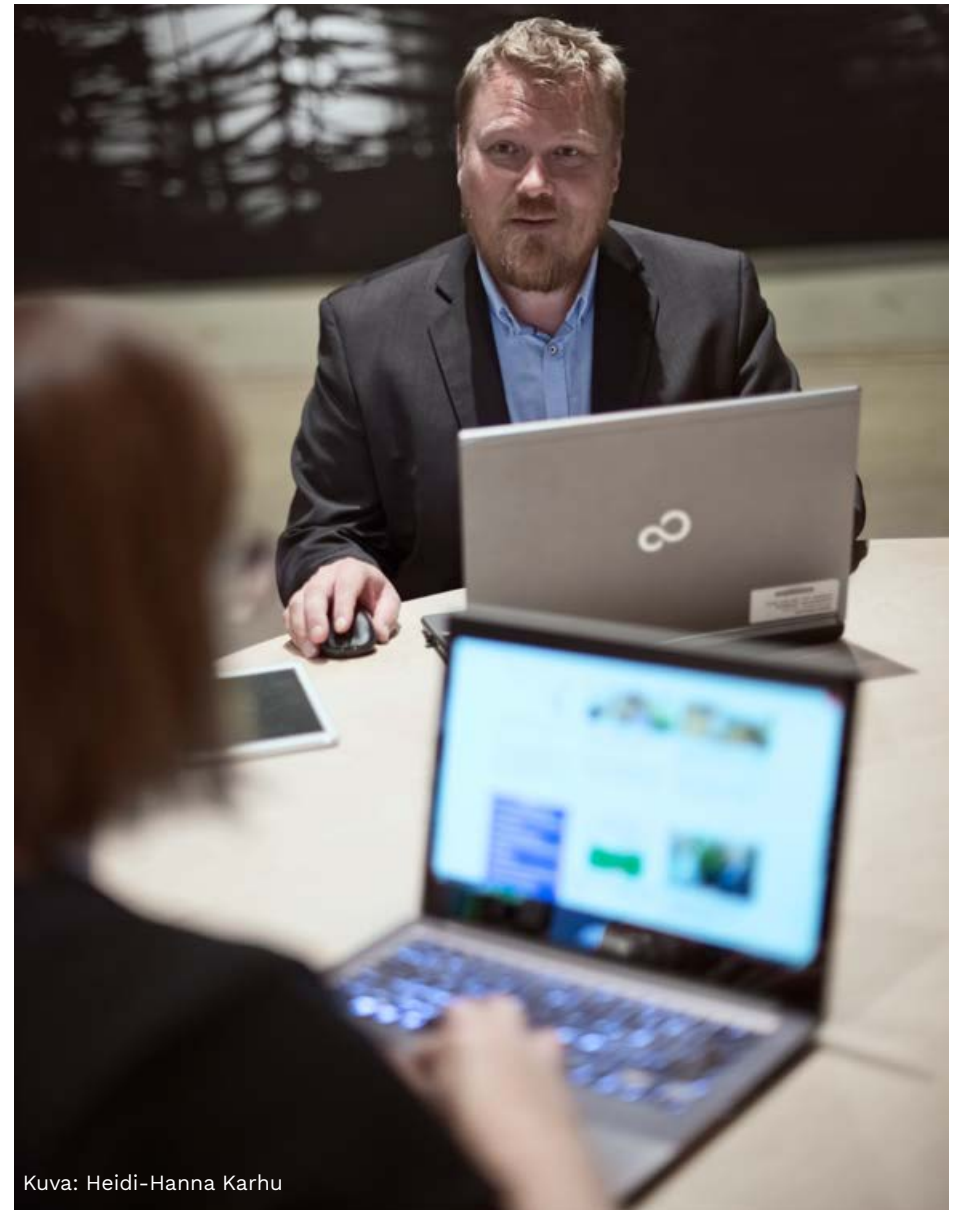
Pilvipalveluiden käyttö osana Kasvun ja Oppimisen toimialan palveluiden käyttämiä järjestelmiä asettaa erityisiä pilvipalveluita koskevia tietosuojavaatimuksia esimerkiksi henkilötietojen suojaamiseksi. Tämän johdosta esimerkiksi Google pilvipalveluihin tallennettujen tietojen käyttöä ja tarpeellisuutta arvioitiin ja joihin kohdistuvien toimien riittävyttä arvioidaan hallinto-oikeudessa tietosuojavaltuutetun antaman päätöksen johdosta.

Espoo selvittää vuoden 2023 aikana henkilötietojen pseudonymisoinnin aloittamista ja mahdollisten Google lisäpalveluiden tilaamista, missä tiedon tallennuspaikka määriteltäisiin EU/ETA alueelle. Yleisellä tasolla kansallisen

tason linjauksien puuttuminen koettiin edelleen ongelmaksi pilvipalveluiden käytössä ja niiden kehittämisessä.

Odotamme vuoden 2023 aikana pilvipalveluihin liittyvien keskusteluiden ratkeamista ja hallinto-oikeuden päätöksen valmistumista Kasvun ja Opimisen toimialalle, joilla voi olla huomattavia vaikutuksia pilvipalveluiden käytölle koulujen- ja opetuksen järjestelmissä.

Koulujen ja päiväkotien päätelaiteympäristön kehittäminen jatkui edelleen vuonna 2022. Esimerkiksi tarjoamalla maksuttomat toisen asteen opetuksessa käytettävät lukiolaisten tietokoneet.



Kuva: Heidi-Hanna Karhu

6 Elinvoiman tulosalue

Elinvoiman tulosalueeseen kuuluvat Elinkeino ja työllisyys, Kulttuuri sekä Liikunnan ja urheilun tulosityksiköt. Tulosityksiköt ylläpitävät muun muassa kaupungin museoita, nuorisotiloja ja kirjastoja, sekä näihin liittyviä tietoaineistoja. Elinvoima vastaa kaupungin kilpailukyvyyn ja vetovoiman vahvistamisesta sekä edistää kuntalaisten hyvinvointia ja yhteisöllisyyttä.

Elinvoiman tulosalueella on vuonna 2022 edistetty museon 10 vuotta käytössä olleen kokoelmanhallintajärjestelmän uudistustyötä, jossa pyritään varmistamaan aiempaa paremmin tietojen säilyvyys ja järjestelmän käytettävyys. Kokoelmanhallintajärjestelmän kilpailutuksessa hankitaan ja käyttöön otetaan uudempi ratkaisu vuosien 2023 ja 2024 aikana. Uudesta järjestelmästä tavoitellaan merkittävää parannusta paitsi toiminnallisuuksien, myös tiedonhallinnan ja tietoturvan osalta.

Elinvoiman tulosalueella kirjastopalvelut ovat käyttöönnettäneet oman Varaamo-nimisen palvelun, jolla pystytään varaamaan kirjaston ja palvelutorin kokoustiloja, varattavia laitteita ja muita resursseja. Erityisesti ilta-aikaan tapahtuvien tilavarausten kohdalla tilaturvallisuuteen ja omaisuuteen liittyvät riskit tulee huomioida 2023 aikana.

Elinvoimassa on menneen vuoden aikana arvioitu tiedonhallintalain edellyttämiä tietoturvariskejä, joka edellytti tietojärjestelmien sisältämien tietojen arkaluonteisuuden tunnistamista. Liikunnan varausjärjestelmä ja Elinkeino- ja työllisyystulosityksikön asiakashallintajärjestelmä arvioitiin



korkean tason suojatoimia edellyttäväksi järjestelmiksi, jonka johdosta niihin kohdistetaan lisätietoturvatavoimia vuosien 2023 ja 2024 aikana.

Elinvoiman tietoturvan ja tietoturvapoikkeamien vastuita selvennettiin vuoden aikana, jonka johdosta tulosityksikön voidaan odottaa selviytyvän paremmin mahdollisista tietoturvauhkien aiheuttamista poikkeamista.

Vuonna 2023 Elinvoiman tulosalue valmistautuu erityisesti tulevaan TE-palveluiden uudistukseen, jonka myötä TE-palvelut ja näiden työntekijät siirtyvät kuntien vastuulle. Tavoitteena on, että palveluiden järjestämisvastuu siirtyy kunnille 2025 alussa. Odotettavissa on, että järjestämisvastuun siirto aiheuttaa lisäkysymyksiä vastuunjaosta toimintatapojen yhteensovittamisessa, henkilökunnan kouluttamisessa ja käytettävien työkalujen valinnassa. Puutteet näissä voivat aiheuttaa uusia tietoturva- ja tietosuojariskejä, joita siirtymäaikana pyritään poistamaan. Onnistuneella ja ennen kaikkea turvallisella siirtymällä varmistetaan, että Elinvoiman ja TE-palveluiden palvelut ovat kuntalaisten käytettävissä myös tulevina vuosina.

7 Kaupunkiympäristön toimiala

Kaupunkiympäristön toimialalla luodaan edellytykset asumiselle ja yrittämiselle Espoossa. Se vastaa kaupungin tiloista muun muassa kouluissa ja päiväkodeissa, sekä rakentaa ja ylläpitää liikenneväyliä ja viheralueita. Kaavoitus ja ympäristöstä huolehtiminen ovat osa toimialan tehtävää. Tietoturva ja tietosuoja ovat keskeinen osa kaupunkiympäristön käyttämiä järjestelmiä ja palveluita.

2022 aikana kaupunkiympäristön käyttämiä tiloja katselmoitiin turvallisuuskävelyn aikana, josta kerättyjen huomioiden pohjalta tilojen turvallisuuspuutteita korjattiin. Havaintojen perusteella tiloissa säilytettäviä tietoja suojattiin tarkemmin.

Kaupunkiympäristön toimialan ylläpitämissä kaupungin työtiloissa on kehitetty kulunvalvontaa ja ohjeistusta 2022 aikana, kuten kameravalvontaa ja ovien kulkemiskäytäntöjä. Näillä toimilla toimiala pyrkii varmistamaan tilojen turvallisuuden ja niin kouluissa, terveysasemilla kuin kirjastoissa.

Toimialalla on 2022 aikana tehty tilojen omistusoikeuksiin ja vuokrasopimuksiin liittyviä järjestelyjä Länsi-Uudenmaan hyvinvointialueen tueksi. Osa kaupungin henkilöstöstä siirtyi hyvinvointialueelle, jonka yhteydessä kaupungin ja hyvinvointialueen tarvitsemia käyttöoikeuksia oli tarpeen selvittää. Toimiala on turvannut muun muassa pelastustoimen tarvitsemien tietojen saannin pelastustehtäviin.



Sopimuksien ja lupien sähköisen allekirjoittamisen käyttöönotto on edennyt, joka on tarkoitettu yritysasiakkaille ja kuntalaisille. Espoon kaupunki on samassa yhteydessä kehittänyt sopimuksienhallinta järjestelmää ja hankkinut uusia järjestelmiä, kuten 2023 uudistettava asiakkaiden käyttämä sähköinen kauppapaikka. Kauppapaikalla asiakkaat ovat voineet ostaa muun muassa rakennuspiirustuksia ja muuta viranomaisaineistoa.

2023 aikana toimiala kartoittaa tietojärjestelmiensä käyttöä ja niiden tietovarantoja, jolla niihin kohdennetaan tietoturva- ja tietosuoja-auditointeja turvallisuuden parantamiseksi.

8 Yhteistyöverkostot

Espoon kaupungin tietosuojavastaava ja tietoturvapäällikkö osallistuvat eri viranomaisten ja kaupunkien yhteistyöryhmiin. Ryhmien tarkoituksena on pääsääntöisesti jakaa tietoa kaupunkien toimista turvallisuuden parantamiseksi ja yleisen turvallisuustilanteen seuraamiseksi.

Espoon kaupunki osallistui Tampereen vetämään digitaalisen turvallisuuden seurantaryhmään, jossa käsiteltiin muun muassa pilvipalvelulinjauksia, tietosuojavaltuutetun toimintaa, kaupunkikohtaisia kuulumisia ja hyvinvointialueisiin liittyvää siirtymää. Pääkaupunkiseudun ja Kelan tietosuojayhteistyöryhmässä käsiteltiin pitkälti vastaavia aiheita erityisesti tietosuojan näkökulmasta katsoen. Verkostoitumista tehtiin myös Kauniaisen ja Helsingin kanssa, jolloin keskiössä olivat muun muassa tiedonhallintalakiin liittyvät toimenpiteet.

Näiden lisäksi kaupungin turvallisuusyksikkö osallistui kahteen ProGradu-työnä tehtyyn turvallisuuskulttuurin selvitykseen, joiden perusteella kaupungin tietoturvaosaamisen taso vaihtelee, mikä vaikuttaa edelleen motivaatioon. Kouluttamisella on myönteinen vaikutus motivaatioon, minkä johdosta tietoturvaa ja tietosuojaa on hyvä kouluttaa myös jatkossa.

Vuoden 2023 aikana kyberturvallisuuskeskuksen tiedonvaihtoverkoston, eli kunta-ISAC:in, odotetaan aktivoituvan. Myös Espoo tulee osallistumaan verkostoon. Kunta-ISAC:ssa tarkoituksena on käsitellä kuntien ja Kyberturvallisuuskeskuksen tietoon tulleita tietoturvailmiöitä ja muita ajankohdaisasioita. Ryhmä tulee keskittymään asiantuntijatasolla tapahtuvaan luottamukselliseen tietojen ja näkemysten vaihtamiseen.



Kuva: Johanna Taskinen

9 Arviointi ja mittarit

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

9.1 Rekisteröityjen oikeuksien toteutuminen

Yksi keskeisimmistä tietosuoja-asetuksen säätämistä rekisteröidyn oikeuksista on oikeus tietää, miten ja kenen toimesta henkilötietoja käsitellään. Rekisterinpitäjän velvollisuus on informoida rekisteröityä suorittamastaan henkilötietojen käsittelystä riittävällä ja selkeällä tavalla. Tietosuoja-asetuksen voimaantulon myötä informointitavaksi ovat vakiintuneet tietosuojaselosteet. Tietosuojaselosteista selviää mitä tietoja kerätään, kenen toimesta ja mihin käyttötarkoitukseen tiedot kerätään, miten tietoja suojellaan sekä mitkä asiakkaan oikeudet ovat. Espoossa tietosuojaselosteiden laadinta- ja päivitysvastuu on rekisterinpitäjällä, ja toimialan tietosuojan yhdyshenkilöt koordinoivat oman toimialansa tietosuojaselosteisiin liittyviä prosesseja. Vaikeissa tilanteissa kaupungin tietosuojavastaava ohjaa ja neuvoo selosteiden laadinnassa. Tietosuojaselosteet ovat julkisia, ja ne löytyvät keskitetysti Espoon kaupungin [verkkosivuilta](#).

Espoossa tietosuojaryhmän vuosikellon mukaisesti tietosuojaselosteet tulisi katselmoida ja tarkistaa joka syksy. Syksyllä 2022 todettiin, että tietosuojaselosteen pohja vaatii laajempaa päivittämistä, erityistä huomiota

tulisi kiinnittää säilytysaikojen yhtenäiseen ilmaisemiseen sekä tiedonluovutuksien riittävään kuvaamiseen. Erityisesti tiedonsiirrot kolmansiin maihin vaativat Espoossa tietosuojaselosteiden osalta tarkentamista. Tuoreet viranomaisratkaisut (mm. [Tietosuoja-valtuutus 13.12.2022 - FINLEX®](#)) ovat kiinnittäneet lisähuomiota asiakkaiden riittävään informointiin. Meneillään olleesta Hyvinvointialue-siirtymästä johtuen tietosuojaselosteiden uudistamistyötä lykättiin vuoden 2023 keväälle. Tästä uudistustyöstä johtuen kattavaa tietosuojaselosteiden katselmointia ei tehty syksyllä 2022, vaan uudistetaan selosteet kerralla vuoden 2023 puolella. Samassa yhteydessä on tarpeen tarkistaa myös uusien Espoon verkkosivujen tietosuojasivuston sisältö asiakaslähtöisyyden näkökulmasta.

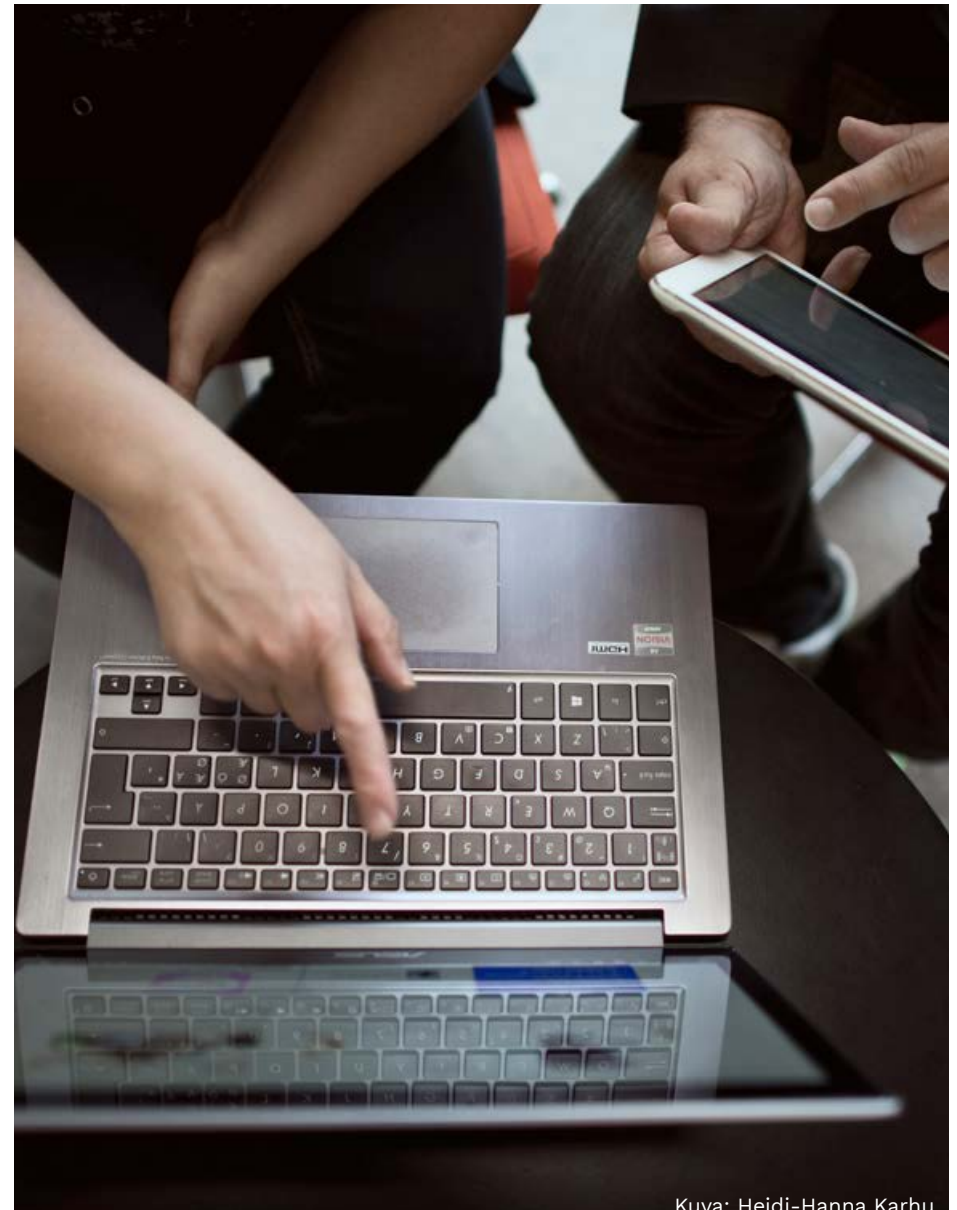
Tietosuojaselosteiden lukumäärä 29.3.2023

Toimiala	Lukumäärä
Espoo yhteensä	142
Konsernihallinto	31
Elinvoima	32
Kasvu ja oppiminen	26
Tekninen ja ympäristötoimi	53

Tietosuojaselosteiden lisäksi Espoon kaupungin [verkkosivuilla](#) kerrotaan tarkemmin siitä, miten kaupunkilaiset voivat käyttää oikeuksiaan omiin tietoihinsa. Tietosuojalainsäädäntö määrittelee tarkasti asiakkaan oikeudet ja velvoittaa rekisterinpitäjän, kaupungin, toteuttamaan nämä oikeudet.

Asiakkaan oikeus omiin tietoihinsa toteutuu usein GDPR:n mukaisen tarkastuspyynnön kautta. Asiakas voi tehdä tarkastuspyynnön tietosuojaselosteesta löytyvälle rekisterinpitäjän vastuutaholle. Tietopyynnön voi toimittaa joko 1) postitse tietosuojaselosteessa mainitulle yhteyshenkilölle osoitettuna tai 2) asioimalla henkilökohtaisesti asiointipisteessä tai kirjaamossa, missä tarkistetaan asiakkaan henkilöllisyys. Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin kirjaamosta tai asiointipisteestä. Tiedot voidaan toimittaa hänelle myös postitse tietyin edellytyksin. Valitettavasti Espoolla ei ole edelleenkään käytössä sähköistä asiointikanavaa tietopyynnöille, vaan prosessi edellyttää edelleen asiakkaan tunnistamista vahvasti, pääsääntöisesti henkilökohtaisella asiointilla. Sähköpostitse tietopyyntöjä ei voida vastaanottaa vahvan tunnistamisen ja tietoturvapuutten vuoksi.

Espoossa tietopyyntöjen käsittelyyn liittyy muitakin haasteita, kuin sähköisen asioinnin puuttuminen. Kaupungissa tietopyyntö voi tulla käytännössä minne tahansa kirjaamosta ja tietosuojavastaavasta lähtien, jolloin pyynnön kohdistaminen oikein saattaa aiheuttaa hankaluuksia, ja tietopyyntöön vastaaminen saattaa hidastua. Tietopyyntöjä ei rekisteröidä eli kirjata keskitysti, mikä aiheuttaa haasteita etenkin tietopyyntöjen määrän seurannassa. Lisäksi tietopyynnön perustetta on usein hankala tulkita, eli pyydetäänkö tietoja julkisuuslain vai tietosuoja-asetuksen nojalla. Keskeinen ero näissä eri tietopyynnöissä on vastausajan pituus: julkisuuslain nojalla tehtyihin tietopyyntöihin tulee vastata kahden viikon kuluessa, tietosuoja-asetus taas antaa kuukauden vastausajan, jota laajoissa tietopyynnöissä voidaan jatkaa jopa kahdella kuukaudella. Lopputulos on asiakkaan näkökulmasta kuitenkin sama, asiakkaalla on oikeus omiin tietoihinsa (tietyin lainsäädännössä säädettyin poikkeuksin).



Kuva: Heidi-Hanna Karhu

Tietopyyntöprosessin sähköistäminen toisi ratkaisun moneen tietopyyntöihin liittyvään haasteeseen, mutta usean vuoden selvityksistä huolimatta Espoossa ei vielä olla saatu toimivaa järjestelmää asiakaskäyttöön. Prosessin sähköistäminen on nostettu kehityskohteeksi jo kaupungin ensimmäisessä tietotilinpäätöksessä vuonna 2018. Toivottavasti seuraavan tietotilinpäätöksen kirjoittamisen aikaan tähän pitkäaikaiseen tarpeeseen on viimein saatu ratkaisu.

Alla olevasta taulukosta käy ilmi Espoon toimialoille vuonna 2022 tehdyt tietosuoja-asetuksen mukaiset omien tietojen tarkastuspyynnöt. Asiakkaat ja sen myötä toimialat eivät välttämättä erottele tietopyyntöjä julkisuuslain tai GDPR:n mukaisiin tietopyyntöihin, mikä voi aiheuttaa vaihtelua toimintojen ilmoittamisissa lukumäärissä. Esimerkiksi kasvun ja oppimisen toimialalla tietopyyntöjä oli vuonna 2022 504 kappaletta, mutta rekisterin tarkastuspyyntöjä näistä oli vain yksi. Lisäksi osa kaupunginarkiston kautta kulkevista pyynnöistä ohjataan edelleen toimialoille, joten osa pyynnöistä saatetaan raportoida kahteen kertaan. Lukumäärät ovat näistä syistä johtuen ainoastaan suuntaa antavia. Luvuista puuttuu hyvinvoinnin ja terveyden toimialan luvut, hyvinvointialueuudistuksen yhteydessä näiden raportointi siirtyi Länsi-uudenmaan hyvinvointialueelle.

GDPR:n mukaisten tietopyyntöjen lukumäärä 2022

Toimiala	Lukumäärä
Espoo yhteensä	432
Konsernihallinto	1
Kasvun ja oppimisen toimiala	1
Kaupunkiympäristön toimiala	10
Kaupunginarkisto	420

9.2 Tietoturvapoikkeamat

2022 aikana Espoon kaupunkiin ei kohdistunut yhtään merkittävää tietoturvahäiriötä, kuten esimerkiksi todennettu tietomurto, merkittävä henkilötietojen vuotaminen julkisuuteen, laajaa mediahuomiota saanut häiriö, systemaattinen vakoilu tai haittaohjelman leviäminen. Kokonaisuutena kaupungin kyberturvallisuuden tila oli vakaa.

Vähäisempiä tai torjuttuja poikkeamia oli kuitenkin runsaasti. Pääosa tapahtumista liittyi tietojenkalasteluun, joiden motiivina oli haittaohjelmien asentaminen, kiristäminen ja/tai rahojen kavaltaminen. Huijausviestien tyypillisinä aiheina olivat Poliisin ja Interpolin nimissä esiintyen lähetetyt haasteuhkaukset, arpajaisvoittoilmoitukset, laskumuistutukset ja teknisen tuen nimissä tekaistut pyynnöt.

Kaupungin teknisestä tuesta vastaava taho raportoi yhteensä 976 tietoturvaan tai tietosuojaan liittyvää tukipyyntöä, tiedustelua tai muuta potentiaalisia toimia edellyttävää yhteydenottoa. Näiden lisäksi tukipyyntöjä ja tietoturva-aiheisia tehtäviä on käsitelty sähköpostilla, joka oli 2022 aikana edelleen valitettavan yleinen kanava tiedonvaihdon ja suojattavien tietojen lähettämiseksi.

Yleisin syöte Espoon kaupungilla oli automaattinen ilmoitus epäilyttävästä tapahtumasta, joka pääosan ajasta on informatiivinen tai aiheeton. Tämän lisäksi käyttäjät usein raportoivat roskapostista, jonka aiheina olivat muun muassa virushälytykset, laskut, aikuisviihdesivustoihin viittaavat kiristys- haittaohjelmat, pankit ja Poliisi. Myös kohdennettuja hyökkäysyrityksiä nähtiin muutamia, joissa hyökkääjä lyhyellä viestillä pyrki esiintymään hoitajana, rehtorina tai johtajana ja tätä kautta selvittämään tilitietoja.

Varsinaisia toteutuneita poikkeamia oli vähän. Näitä olivat muun muassa luvaton pääsy opettajan Wilmaan, kahden Chromebookin varkaus ja yksi Espoon sopimuskumppaniin kohdistunut tietomurto, jonka johdosta Espoon asiakkuuden julkisia tietoja saattoi vuotaa hyökkääjälle.

Poikkeamien havaitseminen edellyttää toimintaympäristön jatkuvaa seuranta ja puutteellisten käytäntöjen oikaisemista, sekä teknisten alustojen ylläpitoa. Tulevina vuosina kaupungin fyysisen ja digitaalisen tilan seuranta onkin kehitettävä, jotta kaikki tunkeutumisyritykset ja potentiaalisesti rikollinen toiminta voidaan estää jo varhaisessa vaiheessa.

9.3 Henkilötietojen tietoturvaloukkaukset

Yksi keskeinen tietosuoja-asetuksen tuoma rekisterinpitäjän velvollisuus on ilmoittaa valvovalle viranomaiselle tietoturvaloukkauksista, jotka aiheutavat riskin asiakkaan oikeuksille. Ilmoitus tulee tehdä 72 tunnin sisällä, ja tähän määräaikaan on Espoossa pääsääntöisesti hyvin päästy. Rekisterinpitäjällä on myös velvollisuus ilmoittaa asiakkaalle häneen kohdistuneesta tietoturvaloukkauksesta, mikäli asiakkaalle aiheutuu loukkauksesta korkea riski. Espoossa henkilötietojen tietoturvaloukkauksia on seurattu systemaattisesti vuoden 2018 alusta lähtien. Tietoturvaloukkaukset ilmoitetaan keskitetysti tietosuojavastaavalle, joka arvioi loukkauksesta aiheutuvan riskin ja ohjaa jatkotoimenpiteet riskin perusteella. Tietosuojavastaava tekee viranomaisilmoitukset, mutta asiakkaalle tietoturvaloukkauksesta ilmoittaa henkilötietoja normaalistikin käsittelevä taho.

Espoon tietoturvaloukkauksen ilmoitusprosessi on aiempien vuosien kyselyiden perusteella koettu raskaaksi. Tästä syystä tietoturvaloukkausten ilmoittamisen prosessia uudistettiin syksyllä 2022. Loukkausten ilmoittamiselle luotiin oma kanava kaupungin palveluportaaliin ja samalla ilmoituslomaketta yksinkertaistettiin huomattavasti. Uudistuksen tavoitteena on helpottaa työntekijöiden poikkeamista ilmoittamista, ja lyhentää ilmoittamiseen käytettävää työaika. Näin toivottavasti kynnys ilmoituksen tekemiselle madaltuu ja tietoturvaloukkauksia saadaan entistä paremmin raportoitua kaupunkitasoisesti. Samalla järjestelmä mahdollistaa ilmoitusten paremman raportoinnin, helpottaen tietosuojavastaavan ja tietoturvapäällikön manuaalista työtä raportointiin liittyen. Kanavan käyttöönotolla saadaan myös parannusta tietoturvaan, kun loukkausilmoituksia ei enää lähetetä sähköpostitse tietosuojan sähköpostiin.

Seuraavissa taulukoissa vertaillaan henkilötietojen tietoturvaloukkausten määriä toimialoittain, ilmoitusten määriä viranomaiselle ja rekisteröidyille, sekä loukkausten taustalla olleita syitä vuosina 2019–2022. Tietoturvaloukkausten määrä oli vuonna 2022 selvästi pienempi kuin edellisenä kahtena vuotena. Tähän vaikuttaa hyvin todennäköisesti hyvinvointialueuudistus, kun henkilöstö siirtyi asteittain hyvinvointialueen palvelukseen jo syksystä 2022 alkaen. Toisekseen uudistuksen aiheuttama kiire varmasti vähensi osaltaan ilmoitusten laatimista, koska ilmoitusmäärä tippui aivan selkeästi erityisesti hyvinvoinnin ja terveyden toimialan osalta heti kesälomien jälkeen. Suurin osa ilmoituksista tehtiin vuoden ensimmäisellä puoliskolla. Syyskausi oli selvästi varsin hiljainen ilmoitusten osalta. Näin ollen luvut eivät ole täysin verrannollisia edellisten vuosien lukujen kanssa.

Seuraavan sivun yläosan taulukoista nähdään selvästi, että eniten henkilötietojen tietoturvaloukkauksia tapahtui hyvinvoinnin ja terveyden toimialalla, kuten myös aiempina vuosina. Vuonna 2022 HYTET-toimialalla tapahtui 75 % kaupungin kaikista henkilötietoihin kohdistuneista tietoturvaloukkauksista. Kasvun ja oppimisen toimialalla tapahtui seuraavaksi eniten tietoturvaloukkauksia, 19 % kaupungin loukkauksista. Konsernihallinnossa ja kaupunkiympäristön toimialalla sattui vain yksittäisiä henkilötietojen tietoturvaloukkauksia. Lukumäärät eivät kuitenkaan välttämättä kerro koko totuutta, pienet luvut saattavat kertoa myös siitä, että loukkauksia ei osata tunnistaa tai niitä ei raportoida kaupungin tietosuojavastaavalle. Valvovalle viranomaiselle ja rekisteröidyille tehtyjen ilmoitusten määrät tippuivat samassa suhteessa kuin ylipäätään henkilötietojen tietoturvaloukkausten ilmoitukset vuonna 2022.

Seuraavan sivun alaosan taulukoista nähdään, että henkilötietojen tietoturvaloukkausten syyt ovat pysyneet varsin samanlaisina seurantajakson aikana. Suurin juurisyy loukkauksille ovat inhimilliset erehdykset ja virheet. Palveluntuottajan virheet ovat myös olleet inhimillisiä erehdyksiä, mutta ne on kaupungin ulkopuolisina laskettu erikseen. Kaupunki vastaa kuitenkin rekisterinpitäjänä myös palveluntuottajiensa aiheuttamista virheistä suhteessa asiakkaisiin. Näin ollen inhimillisistä erehdyksistä johtua loukkauksia on noin 85 % kaikista loukkauksista. Loput noin 15 % johtuvat tahallisista teoista, teknisistä virheistä tai virheistä prosessissa.

Henkilötietojen tietoturvaloukkaukset vuosina 2019-2022

Yhteensä

Toimiala	2019	2020	2021	2022
KOHA	11	7	14	3
KOTO	9	21	15	11
HYTET	35	59	63	44
KYT	5	3	2	1
Yhteensä	60	90	94	59

Tietosuojavaltuutetulle ilmoitettu

Toimiala	2019	2020	2021	2022
KOHA	2	2	3	2
KOTO	6	14	10	3
HYTET	15	37	25	22
KYT	2	1	0	0
Yhteensä	25	54	38	27

Rekisteröidylle ilmoitettu

Toimiala	2019	2020	2021	2022
KOHA	2	4	4	1
KOTO	6	10	11	1
HYTET	15	39	21	20
KYT	2	0	1	1
Yhteensä	25	53	37	23

Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019 - 2022

Loukkausten lukumäärä

Loukkauksen juurisyy	2019	2020	2021	2022
Työntekijän erehdys tai väärä toimintatapa	32	61	64	38
Palveluntuottajan virhe	12	11	16	11
Tietomurto tai muu tahallinen teko	6	9	6	3
Tekninen virhe	5	6	7	4
Prosessivirhe	5	3	1	3
Espoo yhteensä	60	90	94	59

Loukkausten lukumäärä prosentteina

Loukkauksen juurisyy	2019	2020	2021	2022
Työntekijän erehdys tai väärä toimintatapa	53	68	68	64
Palveluntuottajan virhe	20	12	16	19
Tietomurto tai muu tahallinen teko	10	10	8	5
Tekninen virhe	8,5	7	7	7
Prosessivirhe	8,5	3	1	5
Espoo yhteensä	100	100	100	100

10 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen

Espoolla on noin 10 000 työntekijää ja satoja erilaisia tehtävänimikkeitä, jotka hoitavat kaupungin lakisääteisiä tehtäviä. Tehtävien hoitamisen ohessa työntekijät tuottavat salassa pidettäviä ja muita suojattavia tietoja. Henkilötietojen tietoturvaloukkausten juurisyy yli puolessa tapauksia työntekijän inhimillinen erehdys, minkä johdosta Espoon kaupunki panostaa henkilöstön jatkuvaan kouluttamiseen ja osaamisen kehittämiseen.

Laki julkisen hallinnon tiedonhallinnasta 906/2019 4§ toteaa, että tiedonhallintayksikössä on oltava tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista.

Espoo toteuttaa lakia ja tietoturvaosaamisen kehittämistä kilpailutuksen kautta valitun sähköisen koulutusalan avulla, jossa työntekijät suorittavat kurseja ja keräävät kurssitodistuksia. Todistuksien ja niistä kerättävän tilastoinnin avulla kaupunki osoittaa, että henkilöstöä on koulutettu riittävästi. Lähtökohtaisesti vähintään 80%:lla aktiivisesta henkilökunnasta tulee olla tietoturvan ja tietosuojan peruskurssi suoritettuna, sekä tavoitteellisesti kaupungin tärkeimpien järjestelmien vastuhenkilöillä perehdytys heidän vastuullaan olevan järjestelmän tietoturvaan.



Kuva: Pixabay / Bruno, Germany

11 Tietoriskien hallinta osana Espoon palveluita

Yleisen tietosuoja-asetuksen artikla 24:n mukaisesti tietosuojan vaikutustenarvioinneissa näkökulmana on rekisteröityjen oikeuksiin kohdistuvat riskit. Rekisterinpitäjän, eli Espoon kaupungin ja sen eri yksiköiden, yleisenä velvoitteena on huomioida toiminnassaan henkilötietojen käsittelyn riskit ja kohdistaa tarvittavat toimenpiteet niiden lieventämiseksi tai kokonaan poistamiseksi.

Tietoturvan tietoriskien arviointeja suoritettiin Espoon eri järjestelmistä vuoden aikana 22 kappaletta, joissa arvioitiin Espoon tietoriskitasoltaan korkeimmiksi tunnistettujen järjestelmien riskeihin ja uhkiin varautumista. Näitä olivat esimerkiksi tietomurto, sähkökatkot, tietojen väärentäminen ja auditoinneista kerätyt järjestelmäkohtaiset havainnot. Arviointien yhteydessä järjestelmien vastuuhenkilöt ja toimittajat harkitsivat myös kuinka riskin toteutuminen vaikuttaisi kuntalaisiin ja kuinka pitkään riskistä kestää palautua.

Tuloksien perusteella varautumista on tehty pitkälti teknisestä näkökulmasta, mutta hallinnollisissa toimissa on parannettavaa. Esimerkiksi suojattavan tiedon käsittelyä voidaan lokittaa tarkemmin ja voimassa olevien käyttöoikeuksien elinkaarenhallintaa tarkentaa. Sähkökatkoihin varautuminen nojaa pitkälti varavoimaan, jonka on usein arvioitu kestävän enintään 48 tuntia. Kuinka tämän jälkeen toimitaan ei ole aikaisemmin harkittu.



Kokonaisuutena Espoon kaupunki on varautunut poikkeusoloihin ja kyberrikollisuuteen kohtuullisesti, mutta eri toimien yksityiskohdissa ja tehokkuudessa on kehitettävää. Esimerkiksi palautumisaikoja, erityisesti kun kyseessä on kuntalaisille näkyvä palvelu, voidaan vielä 2023-2025 aikana tehostaa.

12 Todennetut kehittämiskohteet tulevalle vuodelle

Hyvinvointialueen perustaminen toi jo 2022 aikana muutoksia Espoon kaupungin organisaatioon, joista on pysyviä ja osa väliaikaisia. 2023 aikana väliaikaiset ratkaisut päättyvät ja pysyvien yhteispalveluiden määrittely tarkentuu. Ratkaisujen ja yhteispalveluiden määrittely on tärkeää, koska niissä käsitellään käyttöoikeuksia ja usein suojattavia tietoja, joiden paljastuminen sivullisille voi johtua kumman tahansa osapuolen tietoturvatointien epäonnistumisesta tai ohittamisesta.

Tiedonhallintalain johdosta tuotettujen linjausten käyttöönotto jatkuu. Pelkästään linjausten ja prosessien kirjaaminen ei riitä, vaan jo lain vaatimusten täyttämiseksi niiden tosiasiallinen toteutuminen tulee kyetä osoittamaan. Yhtenä osoituskeinona on tarkastusten ja auditointien suorittaminen, jolloin todennetaan nykytilanne suhteessa linjauksiin ja sopimuksiin. Tarkastustoiminnan käynnistäminen on uutta ja edellyttää tukea kaupungin johdolta, sekä kohdentamista tietosisällöltään Espoon tärkeimpiin järjestelmiin.

Järjestelmien salassapidon ja suojattavuuden määrittelyn tulee jatkua kuluvan vuoden aikana. Järjestelmien omistajien tulee olla tietoisia järjestelmänsä tietosisällön tärkeydestä ja niistä toimista, joilla osoitetaan niiden olevan riittävästi suojattu. Lisäksi henkilökunnan tulee olla riittävästi koulutettu tietojen turvalliseen käsittelyyn. Mikäli tietoja käsitellään Kumppanin toimesta, tulee myös Kumppanin toimintaa seurata. Kumppanuuk-

sien hallinta tulee olemaan tärkeää jatkossakin Espoon kilpailuttaessa perustietotekniikan toimittajansa. Kumppanin panostukset tietoturvallesi toimintatapoihin ja työkaluihin tulee kyetä varmentamaan.

Asiakkaiden oikeuksien varmistaminen on yksi tietosuojatyön tärkeimmistä tavoitteista. Kuluvan vuoden aikana Espoossa panostetaan erityisesti asiakkaiden informoinnin kehittämiseen. Informointi tapahtuu näkyvimmin Espoon verkkosivujen tietosuojasivuston ja tietosuojaselosteiden kautta, joten näiden uudistaminen ja selkiyttäminen tulee vaikuttamaan siihen, miten asiakas saa tietoa omien henkilötietojensa käsittelystä. Toisekseen pitkään kehityskohteena ollut tietopyyntöjen sähköistäminen on nytkähtänyt taas askeleen eteenpäin, joten on toivoa siitä että seuraavan tietotilin-päätöksen kirjoittamisen aikaan aiheesta voi kirjoittaa jo enemmän. Espoon nykyinen, pitkälti manuaalinen ja paikallakäyntiä vaativa prosessi aiheuttaa haasteita tietojen tarkastavien kaupunkilaisten lisäksi myös työntekijöille.

