

Tieto- tilinpäätös 2020



SISÄLLYSLUETTELO

ESIPUHE	3	6 TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTUMINEN.....	16
1 TIIVISTELMÄ	4	6.1 Konsernihallinto KOHA	16
2 YLEISKATSAUS JA TILANNEARVIO	6	6.2 Sosiaali- ja terveystoimi SOTET	17
2.1 Lyhyt katsaus 2020 tietotilinpäätökseen.....	6	6.3 Sivistystoimi SITO.....	18
2.2 Muutokset toimintaympäristössä.....	6	6.4 Tekninen ja ympäristötoimi TYT	18
2.3 Megatrendit	7	6.5 Länsi-Uudenmaan pelastuslaitos LUP.....	19
3 TIEDONHALLINTA.....	9	6.6 Tietosuojaryhmä	19
3.1 Kokonaisarkkitehtuurityö.....	9	6.7 Tietoturvaryhmä.....	21
3.2 Toiminta-arkkitehtuurityö	10	6.8 Yhteistyöverkostot	22
3.3 Tietoarkkitehtuurityö.....	11	7 ARVIOINTI JA MITTARIT.....	23
3.4 ICT-arkkitehtuurityö.....	12	7.1 Rekisteröityjen oikeuksien toteutuminen	23
4 TIEDOLLA JOHTAMINEN.....	13	7.2 Tietoturvapoikkeamat	25
5 VERKKOPALVELUYMPÄRISTÖN HAASTEET JA HANKINNAT.....	14	7.3 Henkilötietojen tietoturvaloukkaukset	27
5.1 Hankinnat ja palveluostot.....	14	8 OSAAMISEN SEURANTA JA KEHITTÄMINEN	29
		9 TIETORISKIEN HALLINTA	30
		10 AUDITOINNIT	31
		11 TODENNETUT KEHITTÄMISKOHTEET VUODELLE 2021.....	32
		LÄHTEET	34

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.

Tämä vuoden 2020 tietotilinpäätös on tarkoitettu kaupungin johdolle sekä julkiseen jakeluun Espoon kaupungin verkkosivuilla. Se on laadittu yhteistyössä kaupungin eri toimialojen edustajien kanssa ja koostettu turvallisuus ja valmius -ryhmän toimesta, joka tarvittaessa myös käsittelee oikaisupyynnöt ja palautteen.

Tietotilinpäätöksen avulla kuvataan tietoturvallisuuden muuttuvaa toimintaympäristöä, tunnistettuja tietoturvariskejä ja uhkia, sekä kuinka tietoturvallista toimintaa voisi kehittää.

Turvallisten toimintatapojen kehittäminen edellyttää tietoisuuden ja myönteisen kulttuurin varjelemista. Tietoturva ja -suoja eivät ole olemassa hidastaakseen työntekoa tai luodakseen esteitä, vaan suojatakseen jokaisen espoolaisen arkea, jossa jokaisen päivittäisillä valinnoilla ja riskien tunnistamisella on merkitystä. Tuomalla näkyviin kaupungin tietoturvan ja -suojan eteen tekemää työtä edistetään samalla lukijakunnan tietoisuutta arkeen kohdistuvista uhista.

Espoo tarinan, eli Espoon strategian, hengessä tärkeintä on arjen sujuvoittaminen ja asiakaslähtöisyys. Tietoturvan tai tietosuojan pettäminen voi vaikuttaa asiakkaiden palveluihin ja oikeuksiin. Näin kävi psykoterapiakeskus Vastaamo Oy:n tapauksessa, missä arkaluonteiset ja henkilöihin yhdistettävät tiedot kiristysyrityksien jälkeen vuotivat julkiseen jakeluun ja yhtiö joutui tammikuussa 2021 arvioimaan jopa konkurssin uhkaa. Pidetään Espoo siis turvallisena ja arkaluonteisiksi määritellyt tiedot suojassa.

Espoossa 14.04.2021

Harri Säkkinen

Espoon kaupungin
tietoturvapäällikkö

Paula Pernilä

Espoon kaupungin
tietosuojavastaava

1 TIIVISTELMÄ

Espoo laatii vuosittain tietotilinpäätöksen tietosuojavastaavan ja tietoturvapäällikön johdolla. Tietotilinpäätös on työkalu kaupungin johdolle. Tietotilinpäätöksellä kuvataan tietosuojan ja tietoturvan näkökulmasta: 1) Toimintaympäristön muutosten vaikutuksia Espoon toimintaan; 2) Espoon toiminnassa tunnistettuja tietoriskejä; 3) Miten toimintaa on kehitetty kuluvan vuoden aikana ja 4) Millaisia kehittämiskohteita on tunnistettu. Tietotilinpäätökseen sisältyy myös katsaus tiedonhallintaan erityisesti tiedonhallintalain täytäntöönpanon näkökulmasta.

Edellisenä vuonna käyttöön otettu tietoturvan ja tietosuojan verkkokoulutus laajennettiin kaikkien toimialojen suoritettavaksi. Verkkokoulutus on saanut kiitosta ja siitä on pidetty henkilöstön keskuudessa, mutta tietotilinpäätöksen selvitystyön perusteella henkilöstö kokee kuitenkin ettei verkkokoulutus korvaa vuorovaikutteista koulutusta. Koulutuksen ja ohjeistuksen parantaminen korostui selvityksissä, ja näihin tullaankin panostamaan vuonna 2021.

Koronapandemian aiheuttaman työn luonteen muutoksen lisäksi myös lainsäädännön muutokset tuovat painetta prosessien sähköistämiseen ja ylipäättään digitalisointiin. Koronavuoden haasteet näyttäytyvät myös tietotilinpäätöksessä: etätöihin siirtyminen aiheutti tarvetta nopeille teknisille ratkaisuille ja prosessien muutoksille (esim. laiteresurssien ja VPN-kapasiteetin lisääminen, uusien puhelinpalveluiden ja koronabotin käyttöönotto, takaisinsoittopalveluiden kapasiteetin kasvattaminen jne, lue lisää kappaleesta 2), samalla tietoturvan ja tietosuojan rooli korostui muuttuvassa toimintaympäristössä. Kaupungin on pystyttävä turvaamaan

asiakkaiden oikeudet myös etätöskentelyssä ja tietoverkon yli tapahtuvassa asiakaspalvelussa.

Tiedonhallinta on muutoksessa tiedonhallintalain astuttua voimaan vuoden 2020 alussa. Osa kuntien velvoitteista astui voimaan samaan aikaan lain kanssa, osalle velvoitteista on aikataulutettu siirtymäaika. Tiedonhallintalain velvoitteet tulevat pitämään tiedonhallinnan ammattilaiset ja muut tiedonhallinnan kannalta keskeiset asiantuntijat kiireisenä siirtymäaikojen päättymiseen eli vuoden 2023 loppuun saakka. Nyt on tehty jo paljon: tiedonhallintamallissa yhdistyvät kaupungin toimintaympäristön prosessit, tietovarannot, tietojärjestelmät ja tietoturvatoinenpiteet, asiakirjajulkisuuskuvauksella kerrotaan asiakkaille ymmärrettävästi kaupungin tietoaineistoista (vrt. tietosuojaseloste henkilötietojen käsittelyn informoinnissa), muutosvaikutusten arviointi on lisätty arkkitehtuurityöhön ja jatkuvaan toimintaan sekä hankintojen ehtoja on päivitetty vastaamaan tiedonhallintalain vaatimuksia. Tehtävää on vielä tietoaineistojen digitalisoinnissa, teknisten rajapintojen ja katseluyhteyksien rakentamisessa sekä tietoturvaan liittyvissä lain vaatimuksissa. Tiedonhallinnasta ja arkkitehtuurityöstä voi lukea lisää kappaleesta 2.

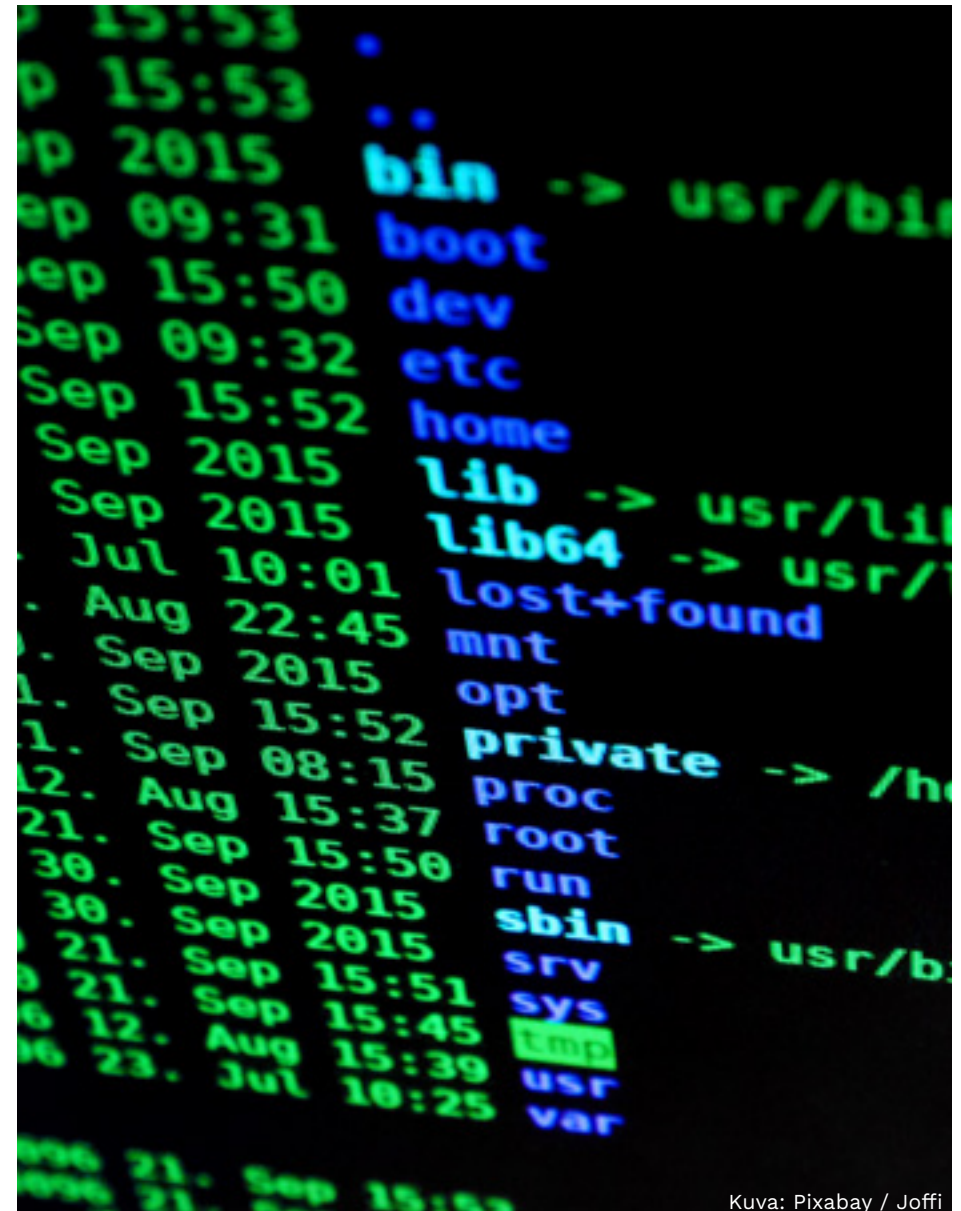
Vuoden 2019 tietotilinpäätöksen tavoin tietosuoja- ja tietoturvatyön riittämätön resursointi kävi hyvin ilmi toimialojen selvityksissä. Etenkin tietosuojaytyöhön kaivataan monella toimialalla lisää resursseja. Toimintojen erilaisuudesta ja laaja-alaisuudesta johtuen kaupungin tietosuojavastaan aika ei riitä toimialojen erityispiirteisiin tai niiden erityislainsäädännön ja toimintaympäristön asettamiin vaatimuksiin perehtymiseen tarpeellisella tasolla. Tämän takia toimialojen omaan tietosuojaytyön resursointiin on tarpeen panostaa.

Avainluvut vuodelta 2020:

- 90 dokumentoitua henkilötietojen tietoturvaloukkausta
- 63 ilmoitusta tietosuojavaltuutetulle
- 44 ilmoitusta asiakkaille
- 17 toteutettua tietosuojan vaikutustenarviointia

Luvussa 6 käydään tarkemmin läpi avainlukuja vuodelta 2020.

Kehittämiskohteiksi vuodelle 2021 tunnistettiin: 1) Sähköisen asiointi-kanavan kehittäminen; 2) Koulutuksen ja ohjeistuksen parantaminen ja parempi jalkauttaminen; 3) Tietosuojan ja tietoturvan ydinprosessien selkiyttäminen ja 4) Muuttuvan lainsäädännön edellyttämien sähköisten työvälineiden käyttöönotto



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 ja Suomen oma lainsäädäntö.

2.1 Lyhyt katsaus 2020 tietotilinpäätökseen

Espoon kaupunki laatii vuosittain tietotilinpäätöksen tietosuojavastaavan ja tietoturvapäällikön johdolla. Ensimmäinen tietotilinpäätös julkaistiin 2018, ja käsissäsi on sarjassaan kaupungin kolmas tietotilinpäätös. Tietotilinpäätöksen fokus on vahvasti tietosuojan ja tietoturvan toteutumisessa, ja siinä arvioidaan vuoden aikana tapahtuneita toimintaympäristön muutoksia suhteessa Espoon toimintaan, havaittuja riskejä, onnistumisia sekä kehityksen suuntaa.

Vuonna 2019 tietotilinpäätöksen näkökulmaa laajennettiin koskemaan tiedolla johtamista ja tiedonhallintaa. Näitä näkökulmia avattiin tarkastelemalla Espoon keskeisiä tietovarantoja, tietojen hyödyntämistä päätöksenteossa, sekä kuinka tiedon avulla voidaan tuottaa parempia palveluita. Näistä lähtökohdista aloitetaan myös vuoden 2020 tietotilinpäätös.

Tietotilinpäätös ei ole vakiintunut tai lakisääteinen tehtävä, mutta sen avulla Espoon kaupunki pyrkii kirjallisesti osoittamaan tietosuojan ja

tietoturvan toteutumista kaupungilla. Tietotilinpäätöksen sisältö riippuu kaupunkien omista painotuksista, jotka tämän dokumentin kohdalla kokoavat yhteen eräitä Espoossa tehtyjä kehitystoimia. Sillä rakennetaan luottamusta ja kerrotaan ylätasolla henkilötietojen käsittelystä ja siitä, kuinka henkilötiedot on turvattu Espoon kaupungissa.

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

2.2 Muutokset toimintaympäristössä

Vuoden 2020 aikana lainsäädäntö asetti kunnille uusia lakisääteisiä velvollisuuksia. Näitä olivat muun muassa toisiolaki, GDPR, tiedonhallintalaki ja laki digitaalisten palveluiden tarjoamisesta. Moni näistä säädettiin jo 2019, mutta velvoitteiden toteuttamiselle annettu siirtymäaika on pääosin umpeutunut 2020 aikana.

Toisiolaki, eli laki sosiaali- ja terveystietojen toissijaisesta käytöstä 552/2019 ([linkki](#)), astui voimaan jo 01.05.2019. Lain tarkoituksena on mahdollistaa sosiaali- ja terveydenhuollon ohjaus- ja tilastotarkoituksessa tallennettujen henkilötietojen tietoturallinen käsittely ja yhdistäminen eri viranomaisten keräämiin henkilötietoihin. Toisin sanoen: asiakkaasta kerättyjen hoitotietojen käyttö muuhun kuin hoitoon, toisiokäyttöön tilastoissa ja tiedolla johtamisessa. Laki asetti kunnille (”6 § sosiaali- ja terveydenhuollon julkiset palvelunjärjestäjät”) uusia palveluvaatimuksia, joiden lopputuotoksena kunnan täytyy tuottaa kerättyjen tietoaineistojen kirjalliset kuvaukset, neuvontapalvelua, yhdistämispalvelua, tunnistneiden hallintapalvelua, hallintajärjestelmä ja varmistaa näihin liittyvä tietoturva (552/2019, 10 §).

1.1.2020 voimaantullut tiedonhallintalaki vaikuttaa vahvasti myös Espoon kaupungin toimintaan. Tiedonhallintalain vastuista ja aiheuttamista toimenpiteistä kerrotaan tarkemmin kappaleessa 2 tiedonhallinta.

Käytännössä kunnan vastuut lisääntyivät ja valtion tietosuojavaltuutetun, sosiaali- ja terveysministeriön ja tietolupaviranomaisen valta kasvoivat. Samanaikaisesti jo EU:n yleisessä tietosuojasetuksessa (GDPR) vuonna 2018 voimaantulleet vaatimukset täytyy edelleen varmistaa: esim. kuntalaisen oikeudet suhteessa omiin tietoihinsa, kuntalaisen informointi henkilötietojen käsittelystä sekä kaupungin 72 tunnin ilmoitusvelvollisuus valvovalle viranomaiselle henkilötietoihin kohdistuvista tietoturvaloukkauksista. Arkityössä on myös huomioitava, että lainsäädäntö edellyttää palveluntuottajaa tarkistamaan tietopyytäjän henkilöllisyys kaikkia kohutuullisia keinoja käyttäen sekä rajoittamaan henkilötietoihin pääsy vain siihen, mikä on ehdottoman välttämätöntä.

2.3 Megatrendit

Organisaatiot seuraavat megatrendejä osana omaa ennakointityötään ja toimintaympäristön analysointia. Megatrendien seuraaminen ja ymmärtäminen luo kokonaiskuvaa kaupungin kannalta merkittävistä yhteiskunnallisista muutoksista. Esimerkiksi Suomen itsenäisyyden juhlarahasto Sitra julkaisi selvityksen vuoden 2020 megatrendeistä ([linkki](#)). Sitra nostaa selvityksessään monia megatrendejä, joista Espoon tietotilinpäätöksen kannalta tärkeä nosto on teknologinen kehitys. Teknologia sulautuu kaikkeen toimintaan, myös kaupungin palveluihin. Termillä digitalisaatio tarkoitetaan digitaalitekniikan hyödyntämistä toiminnassa, niin arkielämän kuin myös yhteiskunnan toiminnoissa. Koronapandemia osaltaan kiihdytti digitalisaatiota siirtämällä toimintoja ja palveluja sähköiseen muotoon, ja kaupungin piti pystyä vastaamaan toimintaympäristön muutokseen nopeasti. Näitä pandemian aiheuttamia toimenpiteitä tarkastellaan tulevissa kappaleissa.

Vuonna 2020 aikana yleinen trendi Android- ja iOS-pohjaisten haittaohjelmien leijumuksesta jatkui. Haittaohjelmat ovat vahvistaneet läsnäoloaan estoista huolimatta Googlen Play-kaupassa, joka on johtanut kasvaneeseen tarpeeseen valvoa ja hallita kaupungin kännyköitä ja tabletteja. Muun muassa Iltasanomat uutisoi ([linkki](#)) 20.02.2020 otsikolla **“Kasvava uhka – Ethän ladannut mitään näistä sovelluksista Google Playsta?”** haittaohjelmien systemaattisesta levittämisestä kauppapaikalla.

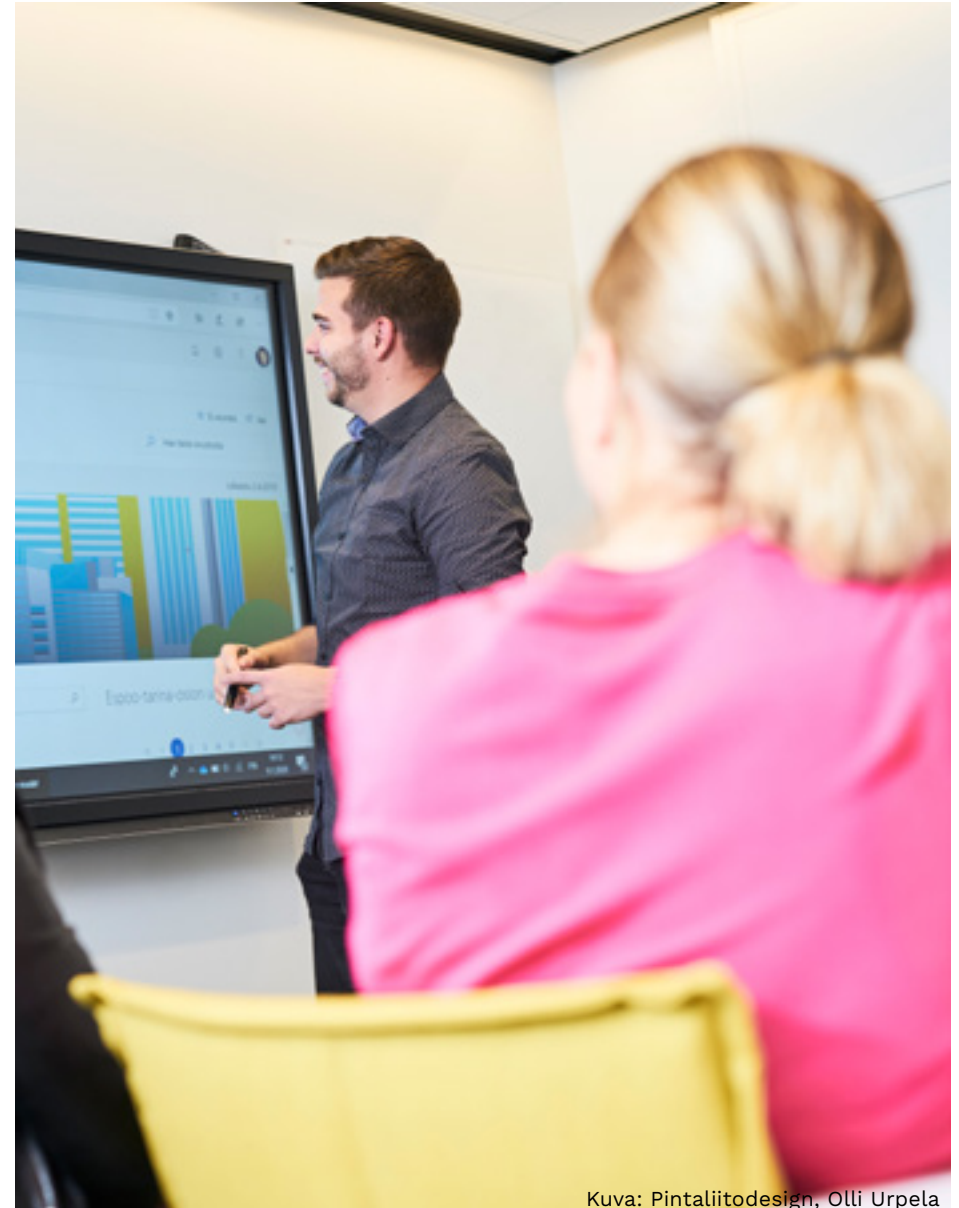
Samaan aikaan Huawei syytettiin vakoilusta Kiinan hyväksi, mikä johti pakotteisiin yhtiötä vastaan ja yrityksen markkinaosuuksien putoamiseen. YLE uutisoi ([linkki](#)) 20.10.2020 otsikolla **”Ruotsi rajaa kiinalaisyhtiöiden tekniikan pois 5G-verkostaan turvallisuuspoliisin ja puolustusvoimien suosituksesta”**, joka pohjaa epäilykseen tai salaiseen aineistoon Huaweiin käytöstä osana Kiinan suorittamaa vakoilua. Espoon kaupunkiin tämä ei vaikuttanut, koska Huawei ei ole kuulunut kaupungin vakiomallistoon, mutta osoittaa liikehdintää valtiotason vakoilussa.

Kumpikin trendi kohdistaa Espooseen kansainvälisestä ympäristöstä kumpuavia uhkia, jossa haittaohjelmilla kiristävät tahot pyrkivät hyötymään rahallisesti tietojen kaappauksesta tai tuhoamisesta, mutta toisaalta myös isojen organisaatioiden tahtotilan kerätä luvallisesti tai luvatta kaikkea heitä hyödyttävää informaatiota. Nämä tahot eivät rajoitu pelkästään Kiinaan, vaan toimijoita on useita ja osoittavat kasvanutta panostusta verkkojen yli tapahtuvaan tiedusteluun.

Urkinta ja tietojenkalastelu on saanut 2020 aikana myös todellisia piirteitä: ulkomaiset petostehtailijat ovat lisänneet toimintaansa puhelinsoittojen kautta ja vakoilun kautta saaduilla tiedoilla on järjestetty vastamielenosoituksia tai henkilötarkkailua lisätty julkisilla alueilla. (Skön 2020). Näiden kansainväliset trendit luovat painetta tarkentaa henkilötietojen käsittelyä ja suojata tiedot aikaisempaa paremmin, mutta myös lisätä panostusta fyysisten laitteiden ja tilojen turvaamiseksi vakoilua ja varastelua vastaan. Uutta ohjeistusta tarvitaan paitsi puhelimiin kohdistuvien

hyökkäysten ehkäisemiseksi, mutta myös uusien turvaominaisuuksien käyttämiseksi.

Ennustettavissa on, että nämä trendit ja jo 2019 havaitut trendit GDPR:n tuomien oikeuksien vahvistumisena jatkuvat vuonna 2021, johtaen suurempaan määrään tietokyselyitä, petosyrityksiä ja tiedustelua.



Kuva: Pintaliitodesign, Olli Urpela

3

TIEDONHALLINTA

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

Laki velvoitti julkisen sektorin tiedonhallintayksiköitä kuvaamaan organisaationsa tiedonhallinnan yhden vuoden siirtymäajalla sekä määrittelemään tiedonhallinnan vastuut. Tiedonhallinnan kaupunkitasoinen järjestämistehtävä kirjattiin konsernihallinnon toimintaohjeeseen palvelukehitys-vastuu yksikön vastuiksi. Tiedonhallinnan kuvaaminen toteutettiin vuoden 2020 aikana **tiedonhallintamalliksi**, jossa kuvattiin toimintaympäristön prosessit sekä niihin liittyvät tietoaaineistot, tietovarannot, tietojärjestelmät ja tietoturvatoinenpiteet. Tiedonhallintamallin sisältö on koostettu useaan eri työväliseen. Näitä tietoja on mahdollista saattaa yhteen kokonaisarkkitehtuurityövälineillä ja näin saada tiedonhallintamallin sisältö laajaan käyttöön mm. kehittämis- ja suunnittelutöiden tueksi.

Tiedonhallintamallin sisältöön perustuva **asiakirjajulkisuuskuvaus** on asiakaslähtöinen kuvaus kaupungin tiedonhallinnasta. Asiakirjajulkisuuskuvausten avulla kerrotaan Espoon kaupungin asiakkaille miten Espoossa hallitaan tietoaaineistoja, joita syntyy viranomaisen asiankäsittelyssä ja palvelujen tuottamisessa. 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 toimintaympäristömuutosten vaikutuksia tiedonhallintaan sekä tunnistaa tiedonhallintamallin sisältöihin kohdistuvat päivitystarpeet. *(ks. lisää seuraavissa kappaleissa).*

Laissa asetetaan myös vaatimuksia tietoaaineistojen digitalisoimiseksi siirtymäajalla, teknisten rajapintojen ja katseluyhteyksien rakentamiseksi sekä tietoturvasuustoimenpiteiden kehittämiseksi siirtymäajoin aina vuoden 2023 loppuun asti, mutta joita tulee jo huomioida mm. 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 ja tietoturvan ja tietosuojan noudattamisesta omassa toiminnassa. Tiedonhallinnan järjestämistehtäviin liittyy myös ohjeiden ja koulutusten laadinta sekä tiedonhallinnan valvonnan tehtävät. Näitä toimenpiteitä toteutetaan v. 2021 aikana yhteistyössä toimialojen, palvelukehitys-vastuuyksikön, turvallisuus ja valmius -vastuualueen ja tietohallinnon kanssa.

Kaupungilla on edustus Kuntaliiton kuntien kokonaisarkkitehtuuriverkostossa ja valtiovaraministeriön tiedonhallintalautakunnan alaisessa julkisen hallinnon toiminnan kehittämisen yhteistyöryhmässä.

3.1 Kokonaisarkkitehtuurityö

Kokonaisarkkitehtuurityö mahdollistaa tiedonhallinnan ja tiedon hyödyn-tämisen strategisen kehittämisen, luo yhteentoimivuutta toimintamallien, tietojärjestelmien ja organisaation osien välille, auttaa varmistamaan tietoturvan ja tietosuojan toteutumista, sekä tukee kaupungin toimialoja ja yksiköitä heidän omassa kehittämistyönsä. Kaupungin tiedonhallin-

nassa kokonaisarkkitehtuuri luo näkyvyyttä siihen, mitä nykytilassa on, ja siihen, mitä kaikkea tavoiteltuja uudistuksia suunnitellessa tulisi ottaa huomioon.

Tiedonhallintamallin koostaminen toteutettiin kaupunkitasoisesti kokonaisarkkitehtuuriverkoston kautta ja tiedonhallintamallin sisältö kuvattiin useisiin jo käytössä oleviin työvälineisiin. Tiedonhallintamallin sisältöä kaupungilla oli olemassa jo varsin hyvin, kyse oli yhteisten kuvaustasojen ja -paikkojen päättämisestä ja sisällön laadun harmonisoinnista.

Lain edellyttämä muutosvaikutusten arviointimenettely laadittiin osaksi kokonaisarkkitehtuurityötä. Dokumentoinnin osalta se tarkoittaa jo käytössä olevan kokonaisarkkitehtuuridokumentaation laajentamista tietoaineistojen käsittelyjen osalta aiempaa laajemmaksi ja huomion kiinnittämistä teknisten rajapintojen kuvauksiin. Muutosvaikutusten arvioinnin avulla voidaan tunnistaa tiedonhallinnan suunnitteluun liittyviä kohtia toiminnan, tietoaineistojen 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, kun kehitysprojekti on viety läpi ja toimintaympäristö on muuttunut. Huomioitavaa on, että muutosvaikutusten arviointi ei koske vain digitalisointiprojekteja tai järjestelmien kehittämistä, vaan tarkastelu ulottuu arvioimaan myös toiminnallisia ja hallinnollisia vaikutuksia esim. johtuen kaupungin toimintaan kohdistuneesta uudesta lakisäätteisestä tehtävästä tai organisaatiouudistuksen johdosta.

Vuonna 2020 toteutettiin 28 kokonaisarkkitehtuuritarkastelua. Vuoden 2020 kehittämisen painopisteet olivat toiminta- ja tietoarkkitehtuurin kehittämisessä.

3.2 Toiminta-arkkitehtuurityö

Tiedonhallintalain edellyttämä kuvaus organisaation tiedonhallinnasta vauhditti kaupunkitasoisten toiminta-arkkitehtuurikuvausten laadintaa. Käytännössä vuoden 2020 aikana toteutettiin ohjatusti prosessien ja niitä kuvaavien tietojen keruu. Näiden tietojen pohjalta toteutettiin prosessien visuaalinen kuvaus prosessikartta- ja toimintamallikuvausten muodossa, joihin on näkyvyys koko organisaatiolla. Näiden kuvausten ylläpito on keskitettynä konsernihallintoon, ja kuvausten ajantasaisuutta sekä muutostenhallintaa toteutetaan osana kokonaisarkkitehtuurityötä.

Operatiivisen toiminnan kuvaustaso on tarkemmalla tasolla sisältäen prosessikarttaa ja toimintamallikuvauksia yksityiskohtaisempia palvelu- ja prosessikuvauksia. Näiden kuvausten laatimista jatketaan edelleen eri kehittämistoimenpiteiden yhteydessä. Kaupunki on tarjonnut vuonna 2020 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 tavoitettiin. Usein toiminnassa tapahtuvilla muutoksilla on vahva riippuvuus niin kustannushyötyjen realisoitumiseen kuin myös tietoturvaan ja tietosuojaan liittyviin toimiin.

Juuri tästä on kyse tiedonhallintalain edellyttämässä muutosvaikutusten arvioinnissa: tunnistaa toimintaympäristön muutos ja niiden vaikutukset nykytilaan nähden, jotta muutos voidaan viedä hallitusti läpi ja taata jatkossakin tietoturallinen toimintaympäristö.

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 ei ole yksinkertaista. Se 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 se riski, 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 yhteentoimivia ja tukisivat tietojen laadun ylläpitoa ja parantamista.

Eräs merkittävä tietoarkkitehtuurityön huomion kohde on ydintietojen hallinta. Ydintiedoilla tarkoitetaan kaupungin toiminnan keskeisiä kohteita (esim. asiakkaat, palvelut, kustannuspaikat, tilat) kuvaavaa tietoa, jota hyödynnetään useissa toiminnoissa ja eri tietojärjestelmissä läpi kaupungin toiminnan. 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.



Kuva: Taru Turpeinen

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 on vuoden 2020 aikana kuvattu nykytilan osalta osana tiedonhallintamallia. Tietojärjestelmäarkkitehtuurin kuvaaminen laajentaa tiedonhallintamallia tavoitetilan kuvauksiin ja tarkempiin tekniisiin kuvauksiin esimerkiksi järjestelmäintegraatioiden ja infrastruktuurin osalta.



Kuva: Heidi-Hanna Karhu

Arkkitehtuurityö on luonteeltaan jatkuvaa Espoon toimintaympäristön ja ympäröivän maailman jatkuvasti muuttuessa. Espoon tulevaisuuden perustaa rakennetaan jo nyt varautumalla tuleviin tiedossa oleviin muutoksiin ja suunnittelemalla skaalautuvia ja 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 kokonaisarkkitehtuuriperiaatteiden ja ICT-arkkitehtuurilinjausten mukaisesti. ICT-arkkitehtuuritoiminnolla on keskeinen rooli ohjata projekteja kohti tavoitetilaa.

ICT-arkkitehtuurityön keskeisiä vuoden 2020 kohteita ovat olleet henkilöstö- ja palkkahallintajärjestelmän ja päätöksentekojärjestelmän uudistaminen, sekä sähköisen allekirjoituksen ja arkistoinnin käyttöönotto.

Espoon ICT-arkkitehtuurihallinnan toimintamalliin kuuluu viikoittaiset ICTA-klinikat ja -katselmoinnit, joissa ICT-kilpailutuksia ja -projekteja tuetaan ICT-arkkitehtien toimesta, esimerkiksi teknisten rajapintojen ja muiden teknistä asiantuntijuutta edellyttävissä kysymyksissä. Keskimäärin ICTA-klinikoiden tukikäynneillä vierailee 2-6 kilpailutusta tai projektia kuukaudessa. Varsinaisia ICTA-katselmointeja toteutetaan keskimäärin 30 kappaletta vuodessa.

4 TIEDOLLA JOHTAMINEN

Tiedolla johtaminen tarkoittaa kaupungin palveluntuotannossa syntyvien tietojen, tietovarantojen ja prosessien hyödyntämistä päätöksenteon tueksi. Tiedon hyödyntämisellä nähdään olevan rooli erityisesti päätöksenteon valmistelun tukena ja kehittämistoiminnassa sen lisäksi, että tietoja hyödynnetään ensisijaisesti 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 asukkailla palvelut taloudellisesti, sosiaalisesti, kulttuurillisesti ja ekologisesti kestävällä tavalla. Kaupungin toiminta on tänä päivänä monien muiden organisaatioiden tavoin tietointensiivistä. Tiedolla johtamisessa ja sen kehittämisessä on oleellista tunnistaa toiminnan kannalta tärkeät tiedot, analysoida niitä ja jakaa kaupungin eri organisaatioyksiköiden päätöksenteon kannalta keskeisille valmistelijoille ja päätöksentekijöille oikeaan aikaan. Espoossa kaupunkitasoista tiedolla johtamista kehitetään johtamisen ja talousohjauksen järjestelmä uudistuksen yhteydessä. Järjestelmä tarjoaa analytiikkakyvykkyksiä, joiden avulla voidaan tukea asukas- ja asiakaslähtöisen Espoo-tarinan tavoitteiden toimeenpanoa uudistaen johtamisen ja talousohjauksen tieto- ja toimintamalleja, prosesseja sekä toiminnan ohjauksen tietojärjestelmäkokonaisuutta.

Tiedolla johtamisen kehittämiseksi Espoossa on vuoden 2020 aikana jatkettu teknisen analytiikkaratkaisun (Saaga) ja sitä tukevan toimintamallin käyttöönottoa ja jalkauttamista. Saaga-analytiikka-alusta mahdollistaa analytiikan lisäksi mm. koneoppimisen ja tekoälyn hyö-

dyntämisen toiminnan kehittämisessä sekä palvelutuotannossa. Vuonna 2020 analytiikassa toteutettiin Proof of Concept -tyyppisiä kokeiluja, eri palautekanavista vastaanotettavien asiakaspalautteiden tietoaallastointeja sekä rekrytoinnin raportoinnin toteutus, jossa toteutettiin datan siirto organisaation ulkopuolisesta palvelusta kaupungin sisäiseen tiedon hyödyntämisen käyttötarkoitukseen.

Kaupunki on toteuttanut tiedolla johtamisen kehittämistyötä myös organisaation kehittäjäkumppanien kanssa. Erityisesti VTT:n kanssa on tehty tiivistä yhteistyötä. Heidän kanssaan on synnytetty uutta ymmärrystä ja ratkaisuja sekä opittu datan yhdistelemisestä tietoturvallisesti ja tietosuoja huomioiden. Esimerkiksi on meneillään Maahanmuuttajien osaamiskeskus -projekti yhteistyössä Omnian, VTT:n, Kelan ja muiden toimijoiden kanssa sekä keväällä 2020 aloitettu ReStart Espoo ja vaikuttavuudella johtaminen -projekti VTT:n kanssa. Jälkimmäisessä valmistaudutaan tietoa hyödyntämällä koronan jälkeiseen ”uuteen normaaliin” eli kestävään kasvuun, hyvinvoinnin edistämiseen ja koronan jälkeiseen taloudelliseen elpymiseen. ReStart Espoo vahvistaa vaikuttavuudella johtamista tulevalle valtuustokaudella 2021-2025.

5

VERKKOPALVELU- YMPÄRISTÖN HAASTEET JA HANKINNAT

Alkukeväästä vuonna 2020 koronaepidemian alku asetti kaupungin tietoliikenne- ja puhepalveluille uusia haasteita, joiden seurauksena toimintaa täytyi sopeuttaa kohti etätöitä. Työntekijöiden VPN-yhteyksien määrää ja kapasiteettia laajennettiin, jotta työntekijöiden oli mahdollista päästä kaupungin sisäverkon palveluihin myös etänä.

Myös sosiaali- ja terveystietopalveluiden puhelintietopalveluiden takaisinsoittokapasiteettia kasvatettiin vastaamaan kasvaneisiin puhelumääriin. Monikieliset Korona-palvelulinjat perustettiin ja niistä järjestettiin yhteys takaisinsoittopalveluun. Linjojen ruuhkautumisen estämiseksi saapuvat puhelut asetettiin jakautumaan kaikkien linjalla olevien asiakaspalvelijoiden kesken.

Puhelintietopalveluiden rinnalle perustettiin keskustelutyökalu esimerkiksi nuorisotieto- ja kulttuuritoimen tarpeisiin, ja koronapalveluiden äkillisiä koneita varten luotiin erillinen tietokoneiden käyttövarasto, josta muun muassa sosiaali- ja terveystietopalveluiden edustajat kykenivät noutamaan koneita asiakaspalvelua varten.

Kasvaneiden etätöitä varten vuoksi osa työntekijöistä ei välttämättä käy toimistolla ollenkaan. Etätöityskentelystä johtuen kaupungin koneita oli tarpeen päivittää riippumatta laitteen sijainnista, ja tähän tarpeeseen vastattiin teknisellä ratkaisulla. Lisäksi kaupungin yhteistyökumppanien

kanssa tehostettiin kapasiteetin valvontaa käyttökatkojen estämiseksi. Edellä mainitut toimet edellyttivät lisähankintoja.

5.1 Hankinnat ja palveluostot

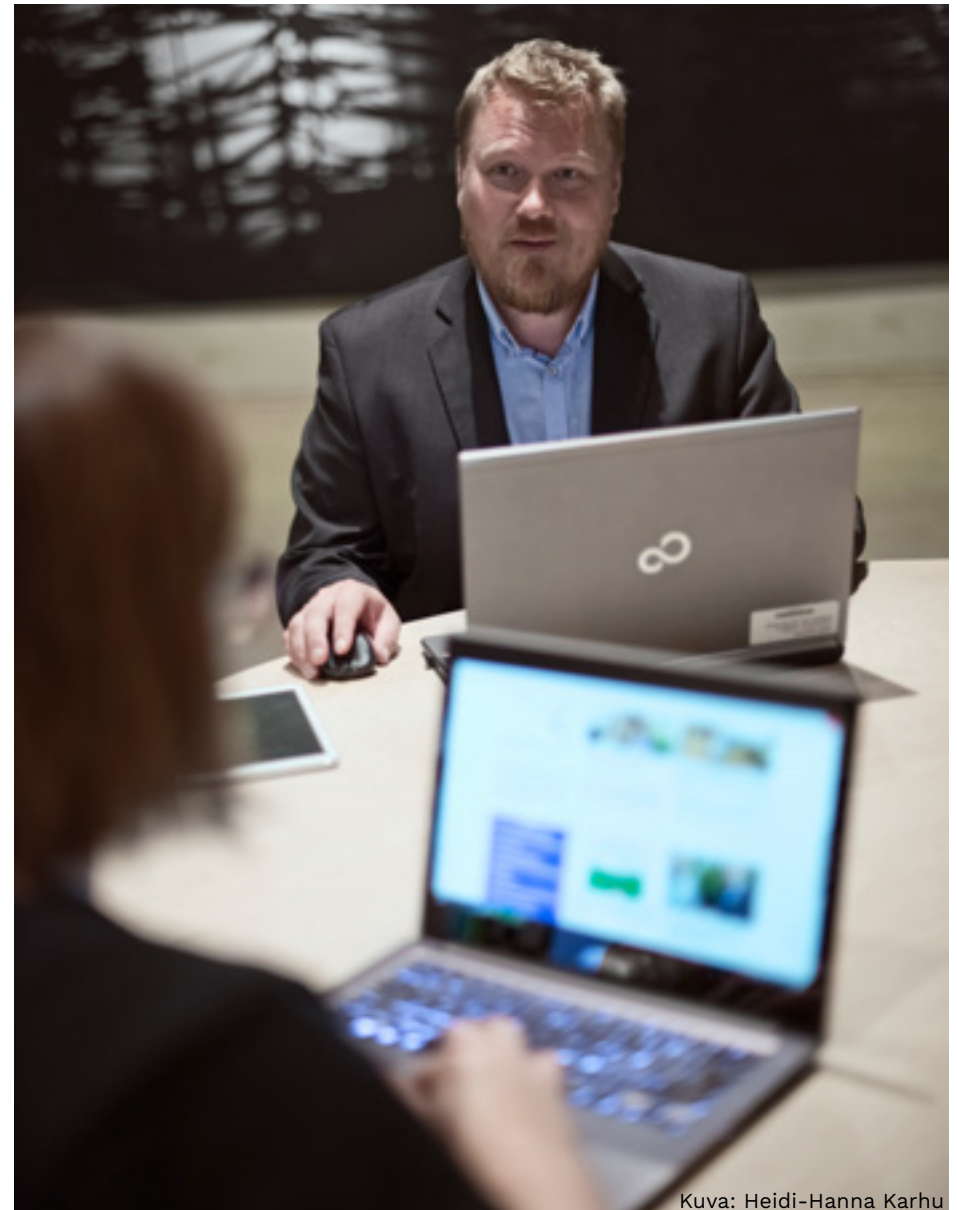
Hankinnat jakautuvat Tietohallinnossa tehtäviin tietojärjestelmähankintoihin ja kaupungin Hankintakeskuksen tehtäviin hankintoihin. Espoossa tehdään vuoden aikana useampia pien- ja suoraan hankintoja, joiden tarpeet syntyvät kaupungin eri toimialoilta. Lakisääteisen kansallisen kynnysarvon alittaville pienhankinnoille kaupungilla on hankintaohjeet, joiden mukaisesti tehdyissä hankinnoissa noudatetaan hyvää hallintotapaa ja hankinnat toteutetaan tasapuolisesti ja syrjimättömästi, unohtamatta myöskään tietosuojaan liittyvää ohjeistusta.

Kaikissa kaupungin hankinnoissa tehdään ennen hankintaa tai kilpailutusvaiheessa arvio siitä, käsitelläänkö sopimuksen mukaisissa palveluissa/tavaran toimituksissa henkilötietoja. Jos henkilötietoja käsitellään, liitetään tarjouspyynnön liitteenä oleviin sopimusasiakirjoihin tietosuojaliitteet (henkilötietojen käsittelyn ehdot, kuvaus käsittelytoimista sekä tarvittaessa turvallisuuskuvaus). Hankintakeskuksella on n. 1700 voimassa olevaa sopimusta, joista arviolta n. 50–70 %:ssa käsitellään henkilötietoja.

Riippumatta siitä tehdäänkö hankinta Hankintakeskuksen vai Tietohallinnon kautta, on vastuu tietosuojan huomioon ottamisesta hankinnan valmistelutyöryhmällä. Tietohallinnon tai hankintakeskuksen hankinnan valmistelijan vastuulla on nostaa esille kysymys henkilötietojen käsittelystä, ja työryhmän jäsenenä olevien toimialan edustajien tulisi tehdä arvio siitä, käsitelläänkö hankinnassa henkilötietoja.

Vastuu henkilötietojen käsittelyn valvonnasta ja henkilötietojen palautumisesta huolehtimisesta käsittelyn päättyessä on toimialoilla.

Tiedonhallintalain myötä on tullut huomioitavaksi velvoitteita, joihin tulee varautua julkisissa hankinnoissa. Velvoitteet kohdistuvat järjestelmähan-
kinnoissa teknisiin rajapintoihin, kansallisten yhteisten tietovarantojen
hyödyntämiseen sekä mm. lokitietojen keräämiseen liittyviin määrittelyi-
hin. Vaatimusmäärittelyjen tarpeita pyritään tunnistamaan tapauskohtai-
sesti mm. muutosvaikutusten arvioinnin kautta osana kokonaisarkkiteh-
tuuritarkastelua.



Kuva: Heidi-Hanna Karhu

6

TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTUMINEN

Tässä kappaleessa tarkastellaan tietoturvan ja henkilötietosuojan toteutumista vuonna 2020 Espoon kaupungin toimialoilla. Kaupungin organisaatio koostuu neljästä toimialueesta: konsernihallinto, sosiaali- ja terveystoimi, sivistystoimi, sekä tekninen- ja ympäristötoimi. Näiden lisäksi organisaatiossa toimii Länsi-Uudenmaan pelastuslaitos ja joukko eri toimialojen asiantuntijoista koostuvia ryhmiä, kuten aiemmin mainittu kokonaisarkkitehtuuriryhmä sekä tietoturvaryhmä ja tietosuojaryhmä.

6.1 Konsernihallinto KOHA

Konsernihallinnon keskeisimmät henkilötietovarannot ovat:

- HR-tiedot (rekrytointi ja työntekijätiedot)
- Laskutukseen ja maksatukseen liittyvät tiedot
- Työterveyshuollon potilastiedot
- Työllisyyspalvelujen asiakastiedot
- Tilastointi ja tutkimustoiminta
- Päätöksenteko ja asianhallinta
- Kaupunginarkiston arkistot

Espoon kaupungin tietoturva- ja tietosuojapolitiikan mukaan toimialat ovat vastuussa tietoturvan ja tietosuojan toteutumisesta. Toimialojen tukena ja ohjaavina tahoina toimivat tiesuojavastaava ja tietoturvapääl-

likkö, jotka sijoittuvat organisaatiossa konsernihallinnon turvallisuus ja valmiusryhmään. Tietoturvan ja tietosuojan kannalta kolmas tärkeä yhteyshenkilö, teknisen tietoturvan vastuutaho, sijoittuu konsernihallinnon tietohallinnon yksikköön. Tietosuojavastaava koordinoi kaupungin tietosuojaryhmää ja tietoturvapääallikkö puolestaan tietoturvaryhmää. Näillä ryhmillä on keskeinen rooli tietosuojan ja tietoturvan toteutumisessa kaupungissa sekä laajan organisaation tietosuoja- ja tietoturvakäytäntöjen yhtenäistämässä. Ryhmien toiminnasta voit lukea enemmän kappaleista 6.6 ja 6.7.

Vuonna 2020 konsernihallinnon suuri työllistäjä oli koronaviruspandemia. Konsernihallinnolla on tärkeä rooli muiden toimialojen toimintojen tukemisessa, myös tietosuojan ja tietoturvan käytännön toteutumisen kannalta. Tietohallinto koordinoi tietoturvallisten työvälineiden käyttöä ja tietosuojavastaava laati ja tarkensi työohjeita vaikeassa ja muuttuneessa työtilanteessa, jossa iso osa henkilöstöstä siirtyi työskentelemään etätyössä. Keskeistä koko kaupungin toiminnassa ja kaikilla toimialoilla oli pystyä takaamaan asiakkaiden asiointi ja oikeuksien toteutuminen uudessa tilanteessa ja huolehtia myös tietosuojan ja tietoturvan toteutumisesta. Tässä onnistuttiin hyvin, ja kaupunginjohtaja Jukka Mäkelä nostikin keskeiseksi syyksi onnistumiselle sen, että kriisijohtaminen noudattelee hyvin normaaliolojen organisaatiota. Lisäksi huomionarvoista on se, että konsernihallinto oli käytännössä ainoa organisaation toimiala, jossa etätyöhön siirtyminen oli mahdollista lähes kaikkien työntekijöiden kohdalla.

Kehitystyö ei kuitenkaan tauonnut konsernihallinnossa koronasta tai haastavasta taloustilanteesta huolimatta. Uuden henkilöstö- ja palkkahallinnan järjestelmän käyttöönottoa valmisteltiin täydellä teholla, ja uuden järjestelmän testauksen jälkeen tuotantoon päästiin jo alkuvuodesta 2021. Tietojärjestelmävaihdoksen lisäksi otettiin käyttöön uusi sähköinen työajanseuranta, joka osaltaan luo pohjaa myös digitaalisten palveluiden jatkokehittämiselle (digipalvelulain edellytys). Tietohallinnossa parannettiin mobiililaitteiden tietoturvaa ottamalla käyttöön mobiililaitteiden hallintaratkaisu, otettiin käyttöön uusi turvatulostuksen järjestelmä, jolla



Kuva: Heidi-Hanna Karhu

parannetaan tietosuojan ja tietoturvan toteutumista, kaupunginarkistolla laajennettiin sähköistä arkistointia toteuttamalla useita integraatioita tai migraatioita, otettiin käyttöön sähköinen allekirjoitus hankinnoissa, mobiilitulkkauksovellus otettiin kaupungin laajuisesti käyttöön ja työllisyyspalveluissa valmistauduttiin alkuvuodesta 2021 alkavaan työllisyyden kuntakokeiluun, jossa kaupungille siirtyy vastuu kokeilun kohderyhmän työllisyyspalveluista. Kaikissa kehityskohteissa tietosuojalla ja tietoturvalla on merkittävä rooli asiakkaiden tietojen turvaamisessa ja hallinnassa.

Yksi perinteisesti Suomessa laiminlyöty tietosuojan peruseriaate on **henkilötietojen säilyttäminen ainoastaan niin kauan kuin on tarpeen** tietojenkäsittelyä varten. On tavallista niin eri organisaatioissa kuin yksityisarkistoissakin, että (henkilö)tietoja säilytetään pitkään eikä niitä uskalleta hävittää, ”jos näitä vaikka joskus vielä tarvitsee”. Espoossa säilytysaikoihin on kiinnitetty erityistä huolta konsernihallinnon osalta asiakirjahallinnossa ja kaupunginarkistossa. Vuoden 2020 aikana ohjeistettiin kaupungin rekistereiden vastuuhenkilöitä tarkistamaan ja tarvittaessa määrittämään uudelleen henkilötietojen säilytysajat. Asia on huomioitu kaupungin sähköisessä säilytysjärjestelmässä niin, että säilytysajan päätyttyä aineisto hävitetään automaattisesti sille määritellyn säilytysajan mukaisesti. Asiakirjahallinto on myös ohjeistanut, että kaikissa uusissa järjestelmä-hankinnoissa pakollisena toimintona tulee olla sähköisten asiakirjojen hävittämiskyvykyys. Espoon kaupungilla ei siis jatkossakaan säilytetä asiakkaiden henkilötietoja kauempaa kuin mihin kaupungilla on oikeus.

6.2 Sosiaali- ja terveystoimi SOTET

Sosiaali- ja terveystoimi SOTET järjestää lakisääteisiä sosiaalihuollon ja terveydenhuollon palveluita kuntalaisille, jonka vuoksi sosiaali- ja terveystoimessa käsitellään merkittäviä määriä salassa pidettäviä potilastietoja ja sosiaalihuollon asiakastietoja.

Sosiaali- ja terveystoimessa on vuonna 2020 kehitetty tietosuojaa etenkin etätöön, sähköisten palveluiden sekä henkilökunnan tietosuojaosaamisen ajantasaisuuden osalta. Koronaepidemia on vaikuttanut sosiaali- ja terveystoimen toimintaan muun muassa niin, että etätö ja etänä annettavat sosiaali- ja terveydenhuollon palvelut ovat lisääntyneet.

Espoo liittyi kansalliseen sähköiseen sosiaalihuollon asiakastiedon arkistoon, mikä on edellyttänyt henkilökunnan kouluttamista. Sosiaali- ja terveystoimessa otettiin käyttöön kaupunkitasoinen tietosuoja ja tietoturvan verkkokoulutus, jossa on omat osionsa sosiaalihuollon ja terveydenhuollon tietosuojalle. Sosiaali- ja terveystoimessa on havaittu kehittämiskohteiksi muun muassa sähköinen asiointi sekä siihen liittyvät tietosuoja- ja tietoturvakysymykset, sekä henkilökunnan osaamisen ylläpitäminen.

Toimialan toimintaympäristö on muutostilassa. Tämä johtuu laajoista lainsäädäntöuudistuksista, kuten sote-uudistuksesta, vammaislainsäädäntöuudistuksesta, sosiaali- ja terveydenhuollon tiedonhallinnan uudistuksesta sekä asiakas- ja potilaslakiuudistuksesta.

6.3 Sivistystoimi SITO

Sivistystoimessa henkilötietojen käsittely perustuu pääsääntöisesti lakisääteisiin tehtäviin. Isoimmat henkilötietoryhmät liittyvät opetuksen ja varhaiskasvatuksen järjestämiseen. Tietoturva- ja tietosuojariskeistä käydään säännöllistä vuoropuhelua ja yhdessä arviointia toimialan eri yksiköiden kanssa tietoriskienhallinnan suunnittelijan johdolla.

Vuonna 2020 on otettu käyttöön kaupunkitasoinen tietosuojaan verkko-koulutustyökalu, joka on suunnattu henkilöstölle. Espoon kirjastoissa on otettu uusi tulostusratkaisu käyttöön, mikä parantaa oleellisesti asiakkaan tietosuojaan toteutumista. Lisäksi on panostettu teknisiin tietoturva-kontrolleihin, esim. kaksivaiheiseen tunnistautumiseen.

Kehittämiskohteiksi vuodelle 2021 on tunnistettu esim. asiakirjojen sähköisen käsittelyn ratkaisujen kehittäminen ja käyttöönotto. Henkilöstön tietosuojaan osaamisen ylläpitämiseen ja lisäämiseen panostetaan edelleen sekä tietosuojaprosessien kehittämiseen.

6.4 Tekninen ja ympäristötoimi TYT

Henkilötietojen käsittely teknisessä ja ympäristötoimessa perustuu lakisääteisten tehtävien lisäksi rekisteröidyn suostumukseen tai sopimukseen. Erityisiä henkilötietoryhmiä käsitellään hyvin vähän. Tietosuoja pyritään huomioimaan kattavasti kaikissa tilanteissa, joissa henkilötietoja käsitellään.

Vuonna 2020 käyttöön otettu koko kaupungin verkkokoulutustyökalu tietoturvan ja -suojaan oppimisessa on saanut hyvän vastaanoton ja koulutuksen suorittaminen on koettu tärkeäksi. Etätöihin siirtyminen on tuonut uusia haasteita, mutta kaupungin ohjeistusten avulla on tietosuoja opittu huomioimaan myös etätöissä. Vuoden 2020 aikana on kannustettu kehittämään omaa tietosuojaosaamista ja olemaan tietosuojaan liittyvisissä kysymyksissä rohkeasti yhteydessä kaupungin tietosuojavastaavaan ja toimialan yhdyshenkilöön.

Toiveena on, että vuoden 2021 aikana tietopyyntöprosessi saataisiin selkeämmäksi, jotta rekisteröityjen oikeudet voidaan turvata. Myös muihin tietosuojaan liittyviin prosesseihin kiinnitetään huomiota, mm. tietosuojaan liittyvien riskien arviointi ja henkilöstön tietosuojaosaamista kehitetään edelleen.

6.5 Länsi-Uudenmaan pelastuslaitos LUP

Osana pelastuslaitosten yhteistyötä LUP on tehnyt tietoturvallisuuden itsearviointia, jossa pelastuslaitosten toimintaa on peilattu kaupungin tietoturvaluusvaatimuksiin. Hallinnon turvallisuusverkon rakentamisessa operaattorin kanssa on arvioitu toimitila- ja kulunvalvontaratkaisujen tietoturvaa.

Pelastuslaitosten toimitiloissa on aloitettu hallinnon turvallisuusverkko TUVE:n käyttöönotto, parantaen näin toimitilojen turvallisuusjärjestelyitä. TUVE:n käyttöönotto ja työt jatkuvat tulevina vuosina. Myös ulkopuolisten toimijoiden osalta on aloitettu menettelytapojen tarkentaminen, tavoitteena on tuoda tiloissa liikkuvat ulkopuoliset tahot samojen henkilöturvallisuusmenettelyiden piiriin kuin työntekijät. Haasteena ovat kunnossapito- ja siivoushenkilöstön tietojen saaminen ja henkilöstön vaihtuvuus.

Pelastuslaitoksessa linjattiin, että LUP suorittaa kaupungin yhteisen verkkokoulutuksen lisäksi tietoturvakoulutusta ja tietoturvatenttejä, joita vuonna 2020 suoritti noin 300 henkilöä. Pelastuslaitoksissa on sovittu, että tietoturvakurssi tulee suorittaa hyväksytysti kahden vuoden välein. Muistutukset vanhenevista suoritteista on lähetetty koko henkilöstölle. Koulutusjärjestelmään aukesi oma tietosuoja koskeva koulutusosio keväällä 2020.

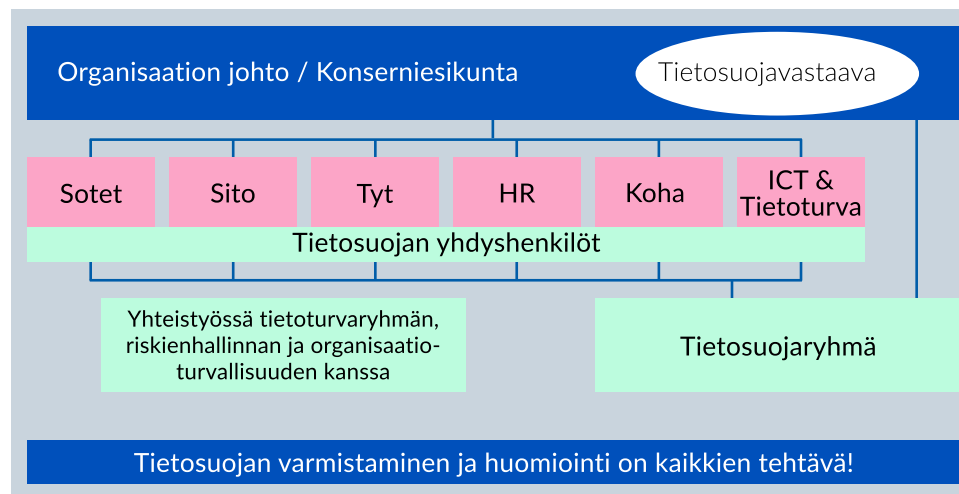
Etätyöhön siirtymisen takia etätyön ohjeistukset tarkastettiin ja jaettiin henkilöstölle. Kaupungin uusi HR-järjestelmä toi haasteita myös pelastuslaitokselle ja henkilöstö tarvitsee ohjeistusta sensitiivisen tiedon jakamisen säännöissä.

Kokonaisuutena LUP:n tietoturvaa ja henkilötietosuoja ohjaa lainsäädännön lisäksi Espoon tietoturva- ja tietosuojapolitiikka, pelastuslaitosten yhteiset periaatteet, tietoturvasuunnitelma, kumppanuusverkoston ohjeet, aluekohtaiset sopimukset sekä omat ohjeet. Näiden jatkokehitys jatkuu kussakin pelastuslaitoksessa myös 2021.

Tulevina vuosina erityisenä haasteena on sovittaa Espoon kaupungin arkkitehtuuri ja tiedonhallintamalli pelastustoimen kansallisen tiedonhallinnan kanssa saumattomaksi kokonaisuudeksi, sekä määrittää LUP:n kokonaisarkkitehtuuri.

6.6 Tietosuojaryhmä

Kaupunginjohtajan päätöksellä nimetyn tietosuojaryhmän tehtävä on määritelty 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.”*



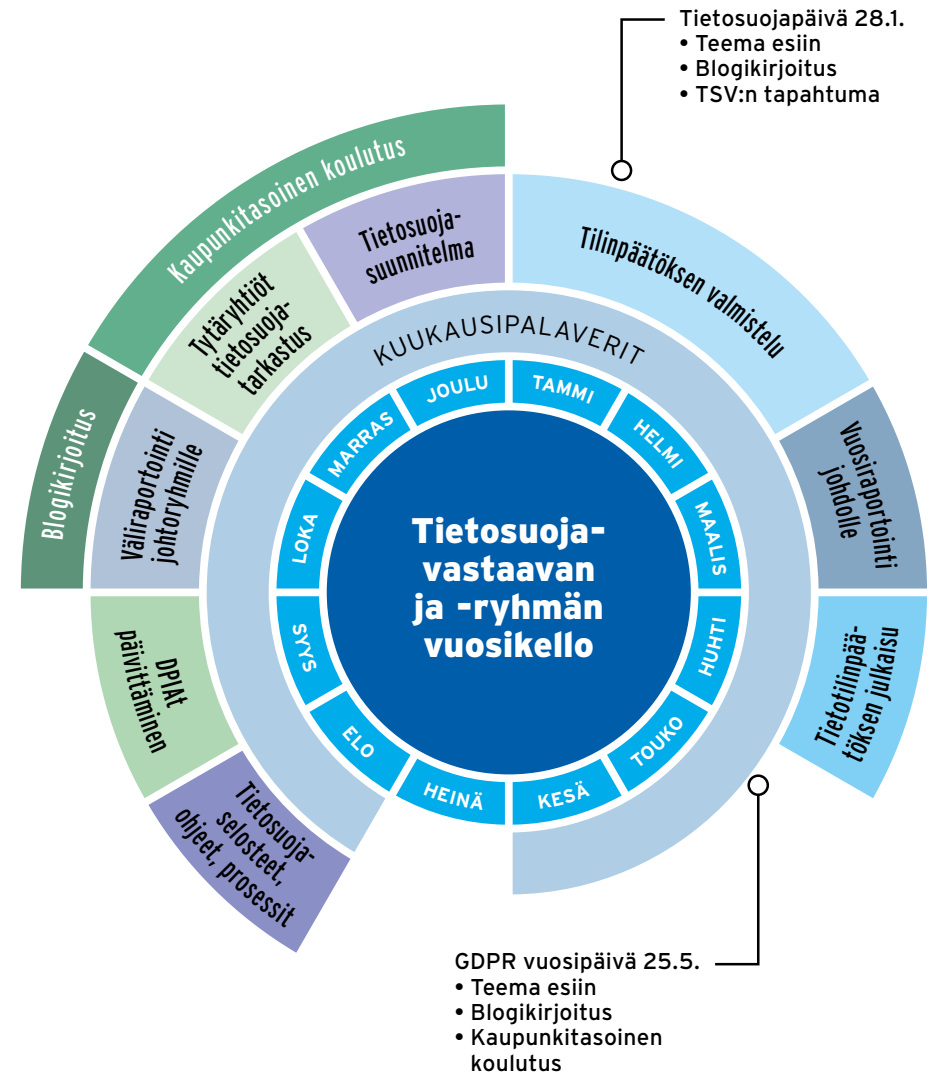
Tietosuojaryhmän kokoonpano

Vuonna 2020 kaupunkitasoinen tietosuojan, tietoturvan, riskienhallinnan, juridiikan ja asiakirjahallinnon asiantuntijoista koostuva ryhmä täytti kaksi vuotta, ja sen rooli kaupunkiorganisaatiossa oli jo vakiintunut. Ryhmä kokoontui tietosuojavastaavan johdolla vuoden 2020 aikana yhteensä 9 kertaa. Osallistuminen kokouksiin on jatkunut aktiivisena, toimialat ja avainyksiköt ovat sitoutuneet ryhmän toimintaan ja kokeneet sen hyödylliseksi.

Tietosuojaryhmän käsittelemiä asioita ja tärkeimpiä onnistumisia vuodelta 2020:

- Tiedonkeruu vuoden 2020 tietotilinpäätökseen
- WhatsAppin tietosuojaohje
- Henkilötietojen käsittely koronatilanteessa
 - Etätyöohjeistuksen parantaminen ja lisääminen
 - Ohjeistus salassa pidettävien henkilötietojen käsittelyyn koronatilanteessa
- Espoon kaupungin lokipolitiikka
- Tietosuojan vaikutustenarvionnin (DPIA) vakiinnuttaminen Espoon projektien hallintamallissa
- Tietoturvan ja tietosuojan verkkokoulutuksen jalkauttaminen
- Privacy Shieldin kaatuminen
- Henkilötietojen tietoturvaloukkaukset
- Tietoturvaparannukset
- Tietosuojan digikokeiluissa

Tietosuojatyön apuna tietosuojavastaava ja tietosuojaryhmä käyttävät tietosuojan vuosikelloa. Vuosikellossa aikataulutetaan kuukausittain tietosuojaan liittyvät vuosittain toistuvat toiminnot, esimerkiksi tietosuojaselosteiden päivittäminen tai vaikutustenarviointien katselmointi ja jäännösriskien hallinta. Myös tietotilinpäätöksen julkaisulla on paikkansa vuosikellossa.





Kuva: Heidi-Hanna Karhu

6.7 Tietoturvaryhmä

Tietoturvaryhmän toiminnassa ensimmäinen kvartaali alkoi huomioilla kalasteluviesteistä ja tiedonhallintamallista, sekä alkuvuodesta julkaistulla toimintaympäristöanalyysillä. Analyysin mukaan Espoon rakenteiden on tuettava aikaisempaa enemmän sisäänrakennettuja tietoturvallisuuden riskienarviointeja ja työrooleja sekä asialle omistettua työaikaa, jotta kasvaviin tietoturvauhkiin kyetään vastaamaan myös jatkossa. Nykyresursseilla keskushallintotasolla ei ole mahdollisuutta keskittyä toimialojen erityispiirteisiin tai vaatimuksiin, minkä vuoksi Espoon on tarpeen kehittää toimialakohtaisia tietoturvanostuksia.

Vuoden toisen kvartaalin aikana kasvanut etätyöskentelyn määrä aiheutti keskustelua, koska kannettavien tietokoneiden päivitys niiden ollessa työntekijän kotona on haastavampaa kuin tietokoneiden päivittäminen kaupungin toimitiloissa. Kaupunki hyväksyi uuden lokipolitiikan, joka ohjaa järjestelmien käytöstä syntyvien lokien käytön, tallentamisen ja luovutuksen periaatteita. Lokipolitiikan näkyvyyttä on kuitenkin tarpeen kehittää tulevina vuosina, jotta kuntalaisten tiedonsaantioikeudet toteutuvat.

Kolmannen kvartaalin aikana TAISTO-harjoitukset aiheuttivat keskustelua käyttöpalvelutoimittajan kanssa, johon osallistuivat Espoon tietohallinto ja konsernihallinto. Tulevina vuosina esitetään myös sosiaali- ja terveystoimea osallistujaksi. Osallistuminen edellyttää ajallista lisäresursointia, mutta harjoittelulla kaupunki kykenee reagoimaan esimerkiksi tietomurtoihin nopeammin ja laadukkaammin. Tämä on tärkeää paitsi tietomurron käsittelyssä, mutta myös siitä mahdollisesti kumpuavan uutisoinnin ja maineenhallinnan osalta.

Tiedonhallintalain vaatimukset olivat esillä ja siitä syntyvät tarpeet sensitiivisen aineiston tallennustiloille, joissa tiedon katselu- ja käyttöhistorioiden on oltava nykyistä tarkempia. Tallennustilojen lopullinen ratkaisu ei selvinnyt vuoden aikana, joten tehtävä siirtyi vuodelle 2021 uutena

projektina. Tarve pohjautuu lakisääteisiin vaatimuksiin muun muassa paperisten asiakirjojen siirtämisestä sähköisiksi, ja koskettaa kaikkia kuntia.

Neljännän ja viimeisen kvartaalin aikana esiteltiin uusia tietoturvahankintoja, joihin kuuluivat tietoturva- ja tietoliikennepalveluiden kilpailutus, identiteetinhallintajärjestelmän hankinta, ehdollinen pääsynhallinta O365 ympäristöissä, sähköpostien toimialueen suojaus ja Espoon palomuurin uudet ominaisuudet. Kaikilla näillä toimilla kohennetaan kaupungin ICT-infrastruktuurin teknistä tietoturvaa.

Vuoden lopulla Vastaamo Oy:n tapaus nousi uutisiin ja noteerattiin myös tietoturvaryhmässä, jossa Espoon käyttäjien mahdollista osuutta käsiteltiin. Lisäksi oman henkilöstön vaihtuvuus asetti ryhmän uuteen tilanteeseen, jossa sekä vetäjä että useampi avainhenkilö poistui kaupungin palveluksesta. Tämän takia tulevien vuosien haasteena tulee olemaan uudet rekrytoinnit, vanhojen työntekijöiden säilyttäminen ja kilpailu osajista yksityisten yritysten kanssa.

6.8 Yhteistyöverkostot

Tietosuoja- ja tietoturvytyössä erilaiset yhteistyöverkostot ovat kunnallisissa tiedon jakamisen ja vertaistuen näkökulmasta. Vaikka tietosuoja onkin sote-puolella jo ”vanha juttu”, on tietosuoja-asetuksen mukanaan tuoma tietosuojavastaavan kaupunkitasoinen rooli edelleen suhteellisen uusi, ja vakiintuneiden käytäntöjen puutteessa yhteistyöverkostojen tuki on arvokasta. Toisaalta taas tietoturvan osalta jatkuvasti muuttuva ja kehittyvä toimintaympäristö edellyttää jatkuvaa kouluttautumista ja ajan hermolla pysymistä, ja yhteistyöverkostot auttavat tässä, kun kaikessa ei tarvitse (eikä voikaan) olla itse paras asiantuntija.

Vuoden 2020 aikana sekä tietosuojavastaava ja tietoturvapäällikkö osallistuivat aktiivisesti Helsingin kaupungin vetämään tietosuojan yh-

teistyöryhmään. Ryhmä kokoontui kuukausittain, ja sen toiminta koettiin Espoossa hyödylliseksi.

Ryhmässä käsiteltiin erityisesti seuraavia aiheita:

- Profilointi ja automaattinen päätöksenteko
- Suostumuksen käyttö viranomaistoiminnassa
- Microsoftin O365 ja vaikutustenarviointi
- Toisiokäyttölaki ja asiakkaan informointi
- Tietotilinpäätöksen laatiminen
- Henkilötietojen tietoturvaloukkaukset

Tietosuojavastaava ja tietoturvapäällikkö osallistuvat lisäksi suurten kaupunkien epäviralliseen tietoturvan ja tietosuojan yhteistyöryhmään. Ryhmään osallistuu Espoon kaupungin lisäksi tietosuojavastaavia ja tietoturvapäälliköitä Helsingin, Tampereen, Oulun ja Kuopion kaupungeista. Ryhmä kokoontuu verkon välityksellä kahden viikon välein. Ryhmässä on keskusteltu seuraavista aiheista:

- Tietojenkäsittely pilvipalveluissa (mm. O365)
 - Kansalliset tulkinnot tai niiden puutteet
- DPIA-arviot
- Ulkoistussopimukset
- Tietoturvaloukkaukset

Espoon kaupungin tietosuojavastaava on aiempina vuosina osallistunut eurooppalaisten kaupunkien Eurocities-verkostoon, jonka jäsen Espoo on. Tietosuojavastaava kuuluu verkoston alajaostoon Knowledge Society Forum:iin, joka käsittelee kaikkia suuria eurooppalaisia kaupunkeja koskevia tekoälyn ja yleisesti datan hyödyntämiseen liittyviä suuria kokonaisuuksia. Lisäksi jaosto ottaa kantaa eettisiin kysymyksiin ja kansalaisten oikeuksiin datataloudessa. Koronatilanteen vuoksi tapaamiset rajoittuvat vuoden 2020 aikana verkon välityksellä pidettyihin kokouksiin.

7

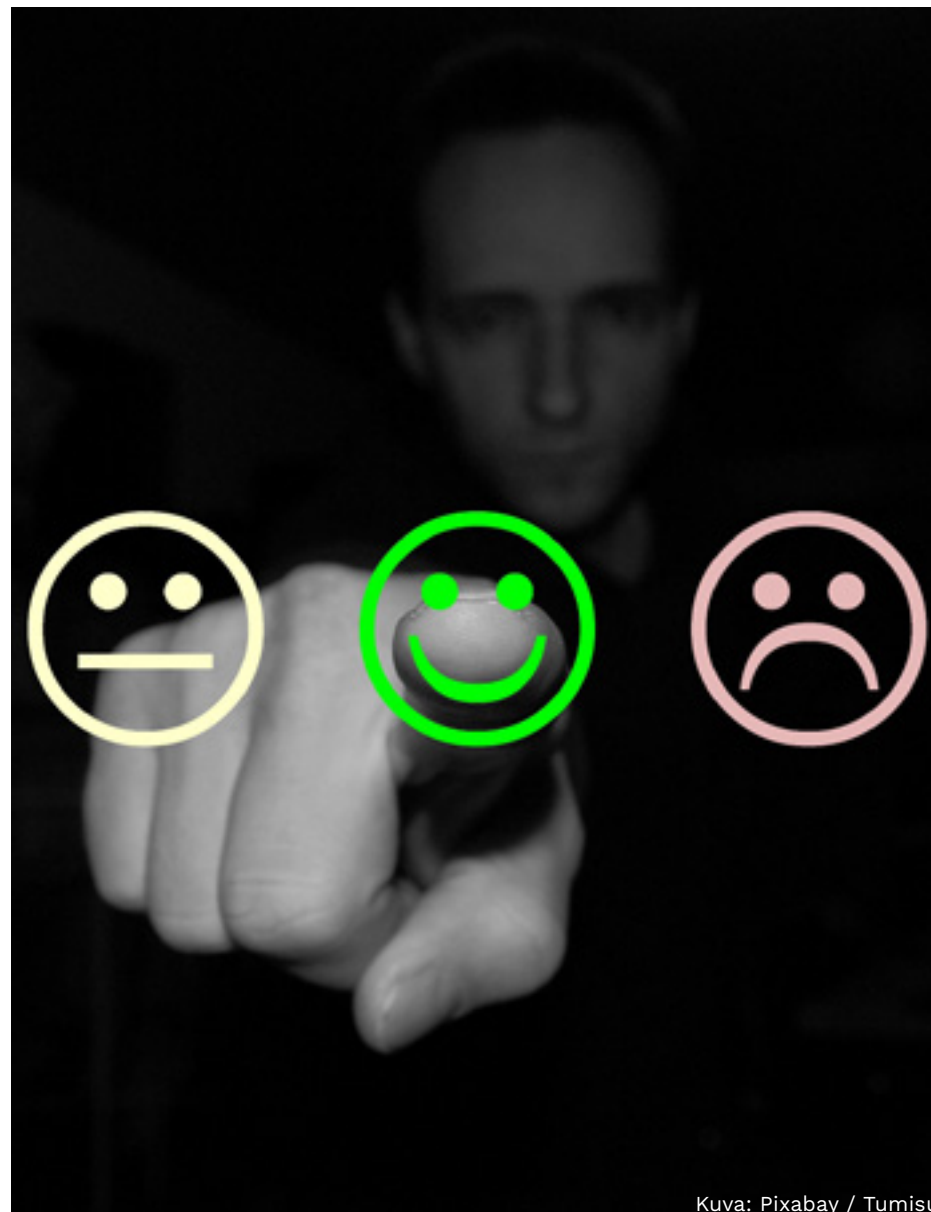
ARVIOINTI JA MITTARIT

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

7.1 Rekisteröityjen oikeuksien toteutuminen

Monen muun kaupungin ja kunnan tavoin Espoon kaupunki käyttää tietosuojaselosteita täyttämään tietosuoja-asetuksen läpinäkyvyys- ja informointivaatimukset. Tietosuojaseloste on tapa kertoa asiakkaalle mitä tietoja hänestä kerätään ja kenen toimesta, mihin käyttötarkoitukseen tiedot kerätään, miten tietoja suojellaan ja mitkä asiakkaan oikeudet ovat. Tietosuojaselosteet ovat julkisia, ja ne löytyvät keskitetysti Espoon kaupungin verkkosivuilta. Tietosuojaselosteet pyritään laatimaan siten että asiakas saa tarvitsemansa tiedon mahdollisimman helposti, eli esimerkiksi yhden toiminnon tiedot pyritään keskittämään yhteen selosteseen vanhojen yhteen tietojärjestelmään keskittyvien rekisterikohtaisten selosteiden sijaan.

Espoossa tietosuojaselosteet tarkistetaan tietosuojaryhmän vuosikellon mukaisesti joka syksy. Syksyllä 2020 normaalin tarkastuksen yhteydessä tietosuojaselosteiden pohja päivitettiin myös vastaamaan digipalvelulain saavutettavuuskriteereitä, joten tietosuojaselosteet päivitettiin pääsääntöisesti saavutettaviksi syksyn 2020 aikana. Selosteiden päivitysvastuu on rekisterin yhteyshenkilöllä, ja toimialan tietosuojan yhteyshenkilöt koordinoivat oman toimialansa tarkastusprosessia.



Kuva: Pixabay / Tumisu

Tietosuojaselosteiden lukumäärä 17.3.2021

Toimiala	Lukumäärä
Espoo yhteensä	176
Konsernihallinto	38
Sivistystoimi	53
Sosiaali- ja terveystoimi	22
Tekninen ja ympäristötoimi	51
Länsi-Uudenmaan pelastuslaitos	12

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.

Espoon kaupunki kerää ja käsittelee asiakkaidensa henkilötietoja vain siinä määrin kuin se on tarpeellista palvelun tuottamiseksi. Henkilötietoja käsitellään rekisterin käyttötarkoituksen mukaan. Jos tiedonkeruu perustuu suostumukseen, asiakas voi milloin tahansa peruuttaa antamansa suostumuksen ja vaatia tietojensa poistamista. Kaupungin palveluista suurin osa perustuu kuitenkin lakisääteisen veloitteen noudattamiseen tai julkisen vallan käyttämiseen. Asiakas ei voi niihin liittyvissä tapauksissa vaatia tietojensa poistamista. Asiakkaalla on oikeus tietää, mitä tietoja hänestä kerätään. Jos tiedoissa on virheitä, asiakas voi vaatia niiden 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.

Pääsääntöisesti kaupunki on pystynyt vastaamaan tietosuoja-asetuksen nojalla tehtyihin tietopyyntöihin lainsäädännön edellyttämässä yhden kuukauden aikataulussa koronan aiheuttamista haasteista ja lisätyöstä huolimatta, mutta valitettavasti aina tähän kuukauden määräaikaan ei olla päästy. Pyyntöjen suuri määrä aiheuttaa joillekin toimialoille haasteita, samoin asiakkaiden haaste kohdistaa pyyntönsä oikealle taholle. Joskus asiakas joutuu odottamaan vastausta siksi, että hän on pyytänyt tietoja rekisteristä, jossa hänen tietojaan ei edes ole, ja tämän takia niukkoja resursseja tuhraantuu turhiin hakuihin asiakkaan odotellessa vastausta. Lisäksi laajoissa tietopyynnöissä koetaan usein vaikeaksi tulkita, onko kyse tietosuoja-asetuksen nojalla tehtävästä tarkastuspyynnöstä vai julkisuulain mukaisesta tietopyynnöstä. Tietopyyntöprosessin sähköistäminen toisi helpotusta moneen haasteeseen, ja tämä on jo aiempina vuosina nostettu tärkeäksi kehityskohteeksi, mutta valitettavasti prosessin sähköistäminen ei onnistunut vuoden 2020 aikana ja siirtyy jälleen tulevan vuoden tavoitteisiin. Myös digipalvelulaki edellyttää palveluiden tarjoamista sähköisessä muodossa, joten painetta sähköistämislle on asiakkaiden paremman palvelun näkökulman lisäksi myös lainsäädännön taholta.

GDPR:n mukaisten tietopyyntöjen lukumäärä 2020

Toimiala	Lukumäärä
Espoo yhteensä	1906
Konsernihallinto	Ei tiedossa / 0
Sivistystoimi	12
Sosiaali- ja terveystoimi	1777
Tekninen ja ympäristötoimi	5
Länsi-Uudenmaan pelastuslaitos	0
Kaupunginarkisto	112

Lokitietojen tarkastuspyynnöt koskevat käytännössä ainoastaan sosiaali- ja terveystoimen toimialaa, koska muilla toimialoilla vastaavaa oikeutta ei lain-
säädännön perusteella ole. Lokitiedot eivät nimittäin koske sitä henkilöä,
jonka tietojen käytön yhteydessä ne syntyvät, vaan lokitietojen katsotaan
olevan tietoja käsittelevän työntekijän tietoja. Tämän tulkinnan mukaisesti
asiakkaalla ei ole oikeutta saada lokitietoja tietosuojalainsäädännön nojalla.
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
antaa kuitenkin sote-puolen asiakkaalle oikeuden pyytää lokitietoja tieto-
jensa käsittelystä, ja tätä oikeutta käytetäänkin Espoossa aktiivisesti.

Sosiaali- ja terveystoimen toimialan lokiselvitykset 2015 - 2020

Vuosi	Tehdyt lokiselvitykset, yhteensä	Sisäiset lokiselvitykset
2015	53	19
2016	67	17
2017	62	16
2018	104	21
2019	69	14
2020	87	4

7.2 Tietoturvapoikkeamat

2020 aikana uutisointiin levisi Emotet, joka lähetti viestejä myös Espoon
nimissä (Harjumaa 2021, Maailman vaarallisin haittaohjelma Emotet on
saatu kaadettua). Alustavien uutisten vastaisesti Espoon verkkoon ei ollut
murtauduttu, mutta Espoon nimissä esiinnyttiin. 2021 käyttöön tulevat
tekniset parannukset tulevat jossakin määrin näitä estämään, mutta to-
dennäköisesti toisena henkilönä esiintymistä ei saada kokonaan estettyä.

Pääosa Espoon kaupunkiin kohdistuneista tietoturvauhista ja poikkeaa-
mista liittyi tietojenkalastelupuheluihin ja viesteihin. Huijausviestien
tyypillisinä aiheina ovat rahanpalautukset, laskumuistutukset ja teknisen
tuen nimissä tekaistut pyynnot. Lukumäärällisesti tietoturvaan liittyviä
HelpDesk-tikettejä ja tiedoksiantoja saapui yhteensä 516 kappaletta:

Tietoturvailmoitusten volyymit 2020

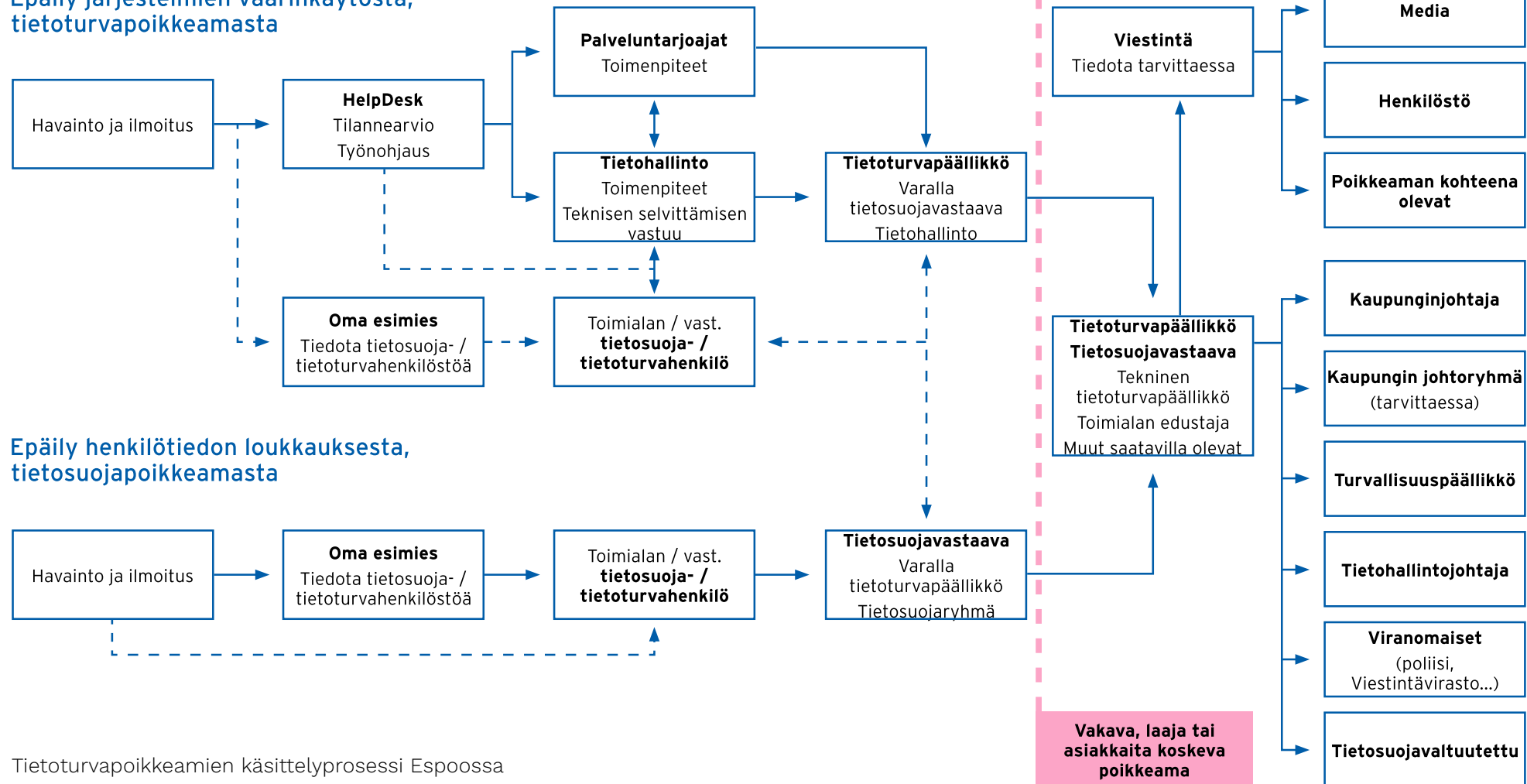
Toimiala	Lukumäärä
Espoo yhteensä	516
Konsernihallinto	88
Sivistystoimi	102
Sosiaali- ja terveystoimi	125
Tekninen ja ympäristötoimi	89
Muut/Ei kirjattu	112

Tikettien lukumäärä jakautuu tasaisesti toimialojen kesken, mutta kohta
'muut/ei kirjattu' voi kohdistua mihin tahansa niistä. Muihin tiketteihin
sisältyvät myös järjestelmistä saapuneet ilmoitukset, joita ovat esimer-
kiksi puuttuvat antiviruspäivitykset, vaarantuneet sähköpostitilit ja haitta-
ohjelmailmoitukset.

Tietoturvan osalta ylivoimaisesti suurin uhka oli kuitenkin juuri huijaus-
viestit sähköpostilla, tekstiviestein sekä huijauspuhelut. Osa puheluista
tulee myös suomalaisista numeroista, joten näiden estäminen voi olla
vaikeaa. Määrää voi kuitenkin vähentää estämällä ulkomaiset numerot ja
pyrkimällä estämään numeroiden ja osoitteiden paljastumista ulkopuoli-
sille henkilöille.

Jokaisen tukipyynnön kohdalla Espoon kaupunki noudattaa samaa työprosessia, jossa havainnot siirtyvät HelpDeskin kautta eri tahojen työjonoon ja tarvittaessa eskaloituvat:

Epäily järjestelmien väärinkäytöstä, tietoturvapoikkeamasta



Tietoturvapoikkeamien käsittelyprosessi Espoossa

Tämä prosessi ei ole muuttunut edellisestä vuodesta ja se on todettu toimivaksi myös 2020 aikana, mutta sitä voisi kehittää enemmän yhden luukun -periaatteen mukaiseksi, jossa eri palveluissa ja sähköposteissa kulkevat työpyynnöt reitittyisivät HelpDeskin kautta oikeille asianomaisille.

7.3 Henkilötietojen tietoturvaloukkaukset

Tietosuoja-asetuksen myötä rekisterinpitäjän velvollisuudeksi tuli ilmoittaa 72 tunnin sisällä valvovalle viranomaiselle tietoturvaloukkauksesta, josta aiheutuu korkea riski rekisteröidylle. Rekisterinpitäjällä on siis lain-säädännön nojalla velvollisuus reagoida loukkauksiin nopeasti. Vuosi 2018 loukkausilmoitusten tekemistä vielä harjoiteltiin, ja vuonna 2019 alkoi olla jo selkeää, milloin ilmoitus tehdään ja milloin sitä ei tarvitse tehdä. Valvova viranomainen, tietosuojavaltuutettu, tarjoaa ilmoitusta varten sähköisen lomakkeen ja ohjeistusta loukkausilmoitusten tekemiseen. Tietosuojavaltuutetun toimisto oli edelleen vuonna 2020 niin ruuhkautunut ilmoitusten takia, että toimiston vastaus loukkausilmoituksiin tuli usein kuukausien viiveellä, eikä lähes vuoden viivekään ollut tavaton.

Espoossa henkilötietojen tietoturvaloukkausprosessi kulkee tietosuoja-vastaavan kautta. Tietosuojavastaava arvioi, aiheutuuko loukkauksesta vakava riski rekisteröidyn oikeuksille ja tekee ilmoituksen tähän arvioon perustuen. Mikäli päädytään siihen, että tietoturvaloukkauksesta ei tarvitse ilmoittaa tietosuojavaltuutetulle, dokumentoidaan kuitenkin syyt siihen miksi ilmoitus on todettu tarpeettomaksi. Jos loukkaus todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille, on siitä ilmoitettava valvojan viranomaisen lisäksi myös loukkauksen kohteeksi joutuneelle henkilölle. Espoon prosessi henkilötietojen tietoturvaloukkauksille on koeponnistettu toimivaksi jo aiempina vuosina, ja 72 tunnin aikamääreeseen on kyetty pääsääntöisesti vastaamaan.

Henkilöstön tietoisuutta ilmoitusvelvollisuudesta pyritään parantamaan koulutusten ja ohjeistuksen avulla, ja parin vuoden kokemuksen perus-



teella henkilöstö ilmoittaa loukkauksista tietosuojavastaavalle matalalla kynnyksellä. Joissain yksikössä aihetta sivutaan säännöllisesti tiimikouksissa.

Espoossa ryhdyttiin tilastoimaan tietoturvaloukkauksia systemaattisesti vuoden 2018 alusta. Vuosi 2018 ilmoitusten tekemistä vielä harjoiteltiin Espoossa kuten muissakin kaupungeissa, mutta vuoden 2019 ja 2020 ilmoituksia voidaan jo vertailla keskenään käytäntöjen vakiinnuttua.

Psykoterapiakeskus Vastaamo Oy:n tapaus nousi keskeiseksi henkilötietojen tietoturvaloukkaukseksi kansallisessa uutisoinnissa. Espoon tietosuojavastaava sai tapaukseen liittyen useita kyselyitä huolestuneilta kaupunkilaisilta. Espoon kaupunki huolehti parhaansa mukaan kaupunkilaisten avustamisessa vaikeassa tilanteessa. Tapaus nosti entisestään tietoisuutta tietosuojan ja tietoturvan merkityksestä niin kaupungin johdon kuin myös kaupungin työntekijöiden keskuudessa ja auttaa jatkossa tietosuojavastavaan ja tietoturvapäällikön työssä lisäten merkityksellisen työn painoarvoa. Seuraavissa taulukoissa vertaillaan henkilötietojen tietoturvaloukkausten määriä toimialoittain sekä loukkausten syitä vuosina 2019 ja 2020.

Henkilötietojen tietoturvaloukkaukset Espoossa 2019 ja 2020

Toimiala	Yhteensä		Tietosuojavaltuutettu		Rekisteröity	
	2019	2020	2019	2020	2019	2020
Espoo yhteensä	60	90	25	63	25	44
Konsernihallinto	11	7	2	2	2	4
Sivistystoimi	9	21	6	14	6	10
Sosiaali- ja terveystoimi	35	59	15	37	15	30
Tekninen ja ympäristötoimi	5	3	2	1	2	0

Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019 ja 2020

Toimiala	Yhteensä 2019	Yhteensä 2020	% 2019	% 2020
Espoo yhteensä	60	90	100	100
Työntekijän erehdys tai väärä toimintatapa	32	61	53	68
Palveluntuottajan virhe	12	11	20	12
Tietomurto tai muu tahallinen teko	6	9	10	10
Tekninen virhe	5	6	8,5	6,7
Prosessivirhe	5	3	8,5	3,3

8 OSAAMISEN SEURANTA JA KEHITTÄMINEN

Vuoden 2020 globaali koronapandemia johti siihen, että henkilöstö joutui nopealla aikataululla ottamaan käyttöön uusia työvälineitä ja omaksumaan uusia toimintatapoja. Pakotettu digiloikka johti siihen, että perinteiset kouluttajan vetämät lähikoulutukset siirtyivät verkkoon.

On tunnettu tosiasia, että ihminen on tietoturvan ja tietosuojan heikoin lenkki. Tämä näkyy siinä, että henkilötietojen tietoturvaloukkausten juurisyy on yli puolessa tapauksia työntekijän inhimillinen erehdys. Tästä syystä Espoossa pyritään panostamaan henkilöstön jatkuvaan kouluttamiseen, osaamisen parantamiseen ja tietoisuuden lisäämiseen. Espoossa on työntekijöitä noin 14 500 ja satoja erilaisia tehtävänimikkeitä, kaupungilla on myös satoja erilaisia lakisääteisiä tehtäviä. Toimialojen ja erilaisten tehtävien erityispiirteet on otettava huomioon osaamisen kehittämisessä, joten yksi perusmalli ei sovi kaikille.

Nämä toimialojen erityisvaatimukset on otettu huomioon kaupungissa vuonna 2019 käyttöönotetussa tietosuojan ja tietoturvan verkkokoulutusjärjestelmässä, jossa yleisen tietosuoja- ja tietoturvakoulutuksen lisäksi on myös toimialoille räätälöityjä, kohdennettuja koulutuksia. Koulutuspaketti on kattava, sisältö päivitetään vuosittain ja henkilöstö myös uusii koulutuksen vuosittain, eli osaamista pidetään jatkuvasti yllä ja sitä päivitetään. Koulutusjärjestelmän käyttö laajennettiin vuoden 2020 aikana koko kaupungin laajuiseksi. Koulutuksen jalkauttamisessa on kuitenkin tekemistä edelleen, vain reilu puolet Espoon työntekijöistä oli suorittanut verkkokurssin vuoden 2020 loppuun mennessä.

Verkkokoulutuksella tavoitellaan seuraavia hyötyjä:

- Työntekijöiden perehdyttäminen
- Osaamisen parantaminen ja riskien pienentäminen
- Aika- ja kustannussäästöt
- Esimies kykenee seuraamaan ja varmistamaan, että alaiset ovat suorittaneet koulutuksen
- Verkkokoulutuksen tilastodatan avulla kyetään tunnistamaan koulutustarpeita

Espoossa pyritään siihen, että havaituista poikkeamista ilmoitetaan matalalla kynnyksellä, ja ennemmin ilmoitetaan kuin jätetään ilmoittamatta. Jatko-toimenpiteiden harkinta jää asiantuntijoiden vastuulle, yksittäisen työntekijän ei odoteta itse osaavan ratkaista ja hoitaa tietosuojaan ja tietoturvaan liittyviä poikkeamia. Ilmapiiri on kannustava, ja tietosuojavastaavan rooliin kuuluu osaltaan myös työntekijän mielen rauhoittaminen, kun saadaan asia hoidettua kunnialla. Ilmoitusten tekeminen on tietosuojavastaavan ja tietoturvapäällikön työn kannalta äärimmäisen tärkeää, koska asiantuntijoiden näkyvyys koko organisaation ongelmakohtiin on muutoin aika heikko, ja poikkeamailmoitukset tuovat vastuutahojen tietoon korjattavia prosesseja tai muita puutteita.

Vaikka verkkokoulutus olikin vuoden 2020 pääasiallinen tietosuojan ja tietoturvan koulutustapa, panostettiin kaupungissa myös muuhun koulutukseen etenkin sote-toimialalla. Myös kaupungin Hankintakeskuksessa järjestettiin tietosuojakoulutusta, eikä koronasta huolimatta uuden työntekijän ”Missä mennään Espoo” -perehdytyspäivääkään unohdettu, jonka ohjelmaan kuuluu tietosuojan ja tietoturvan perusteiden kokonaisuus.

9 TIETORISKIEN HALLINTA

Tietosuojan vaikutustenarvioinnit nostettiin kehittämiskohteeksi jo Espoon vuoden 2018 tietotilinpäätöksessä, ja tietoriskien hallinta painottui vuoden 2019 aikana erityisesti vaikutustenarviointeihin. Tietosuojan vaikutustenarvioinneissa näkökulma on rekisteröityjen oikeuksiin kohdistuvissa riskeissä. Tietoturva taas tarkastelee riskejä organisaation näkökulmasta. Rekisterinpitäjän yleisenä veloitteenä on huomioida toiminnassaan henkilötietojen käsittelyn riskit ja kohdistaa tarvittavat toimenpiteet niiden minimoimiseksi (GDPR 24 artikla).

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. Tietosuojan vaikutustenarvioinnin prosessia hiottiin pitkällisesti jo vuonna 2019, ja vuonna 2020 siihen tehtiin enää muutamia parannuksia. Espoon kaupungin pohja on koettu myös yhteistyöpiireissä hyväksi, ja sitä on pyydetty pohjaksi muiden kuntien käyttöön. Vuoden 2020 aikana vaikutustenarvioinnit otettiin osaksi sähköistä projektinhallinnan työkalua, missä niitä voidaan myös jatkossa seurata paremmin. Voidaan siis perustellusti todeta, että Espoo on onnistunut hyvin tietosuojan vaikutustenarviointiprosessin kehittämisessä.

Espoon vaikutustenarviointiprosessin mukaisesti prosessiin osallistuvat seuraavat henkilöt:

- Projektipäällikkö tai toiminnasta vastaava (omistaja)
- IT-projektipäällikkö
- Tarvittaessa palveluntuottajan edustaja
- Toimialan lakimies
- Tietosuojavastaava
- Tietoturvapäällikkö tai teknisestä tietoturvasta vastaava it-päällikkö

Espoossa vaikutustenarvioinnit on koettu hyödyllisiksi, vaikka ne vaativatkin runsaasti monen asiantuntijan ja mahdollisen toimittajan / palveluntuottajan työpanosta. Vaikutustenarviointia on myös päivitettävä jatkuvasti prosessin muuttuessa, ja muutoinkin ylläpidettävä. Myöskään havaittujen jäännösriskien seurantaa ei saa unohtaa, ja tämän vuoksi vaikutustenarviointien tarkastus sisältyy tietosuojaryhmän vuosikelloon. Näin riskienhallinta saadaan osaksi tietosuojan hallintaa, mikä onkin seuraavassa auditointeihin keskittyvässä kappaleessa yksi aikaisemmissa auditoinneissa havaittu keskeinen tietosuoja- ja tietoturvatyön kehittämiskohde.

Tietosuojan vaikutustenarvioinnit 2020

Toimiala	Lukumäärä
Espoo yhteensä	17
Konsernihallinto	5
Sivistystoimi	8
Sosiaali- ja terveystoimi	3
Tekninen ja ympäristötoimi	1
Länsi-Uudenmaan pelastuslaitos	0

10

AUDITOINNIT

Tietosuojaan toteutumisen kannalta tietoturva on keskeinen rooli. Espoon kaupungissa tietoturvaan liittyvät auditoinnit kohdistuvat pääsääntöisesti tietojärjestelmiin. Tekniset auditoinnit suorittaa keskitetysti tietohallinto yhteistyökumppaneineen. Vuonna 2020 toimialoilla ei toteutettu tietosuojaan tai tietoturvaan liittyviä auditointeja. Sisäinen tarkastus toteutti tietosuojaan liittyviä auditointeja vuonna 2019, joten vuonna 2020 näitä ei sisäisen tarkastuksen toimesta toteutettu. Vuonna 2019 toteutettiin kaupunkitasoinen ulkoinen tietosuojaan auditointi, jonka nostamat huomiot kuitenkin pätevät vuoden 2020 osaltakin, koska kaikkia korjaavia toimenpiteitä ei saatu suoritettua vuonna 2019.

Keskeiset nostot vuoden 2019 auditoinnista kehittämistarpeiden osalta:

- Tietosuojariskien hallinta näkyvämmiin osaksi prosesseja ja toimintaa
- Henkilötietojen elinkaaren hallinta ja sisäänrakennettu tietosuoja
- Sopimusten ja ulkoistusten hallinta
- Tietosuojaan ja tietoturvan hallinta



Kuva: Pintaliitodesign, Olli Urpela

11

TODENNETUT KEHITTÄMISKOHTEET VUODELLE 2021

Tietotilinpäätöksen tehtävänä on nostaa johdon, tietosuojavastaavan ja tietoturvapäällikön tietoisuuteen keskeisimmät tietosuojatyön ongelmakohdat eri toimialoilla. Näistä ongelmakohdista voidaan johtaa seuraavalle vuodelle tärkeimmät kehittämiskohteet ja tukea näin tietosuojatyön toteutumista kaupungilla.

Toimialojen selvityksissä nousi seuraavan vuoden kehittämiskohteeksi yksi vuonna 2020 toteuttamatta jäänyt kohde: tietopyyntöprosessin sähköistäminen. Toimialoilla koetaan haastavaksi seurata tietopyyntöjä ja niiden toteutumista, eikä yhtenäistä seurantatapaa tai järjestelmää ole käytössä. Asiakkaan kannalta nykyinen prosessi on myös hankala, koska tietopyynnön jättäminen vaatii joko henkilökohtaisen käynnin kaupungin asiakaspisteellä tai kirjeen lähettämisen. Prosessin sähköistäminen auttaisi asiakkaan lisäksi myös kaupungin työntekijöitä ja yhtenäistäisi toimintatapoja. Myös tunnistamiseen liittyvät haasteet ratkaistaisiin sähköisellä asiointikanavalla, johon liittyisi asiakkaan vahva tunnistaminen.

Asiakkaiden informointi tapahtuu tällä hetkellä tietosuojaoselosteiden kautta. Vuonna 2021 verkkosivu-uudistuksen yhteydessä tullaan selvittämään, voidaanko ottaa käyttöön joku asiakkaiden kannalta selkeämpi ja ymmärrettävämpi informointitapa.

Tietotilinpäätöksen selvitystyössä toimialat nostavat edelleen tietosuojan keskeisimmäksi kehittämiskohteeksi ohjeistuksen ja koulutuksen. Kaupungissa on käytössä laaja, toimialojen erityistarpeet huomioiva verkkokoulutusjärjestelmä, mutta tästäkin huolimatta juuri koulutus nostettiin vastauksissa keskeisimmäksi kehittämiskohteeksi. Toimialoilla kaivataan kouluttujaa kouluttamaan henkilöstöä ja vastaamaan kysymyksiin, verkkokoulutuksen ei koeta vastaavan henkilöstön tarpeisiin. Uusi vuodenvaihteessa aloittanut tietosuojavastaava tulee ottamaan tämän toiveen huomioon vuonna 2021 ja jalkautumaan paremmin toimialoille. Myös ohjeiden päivitystyöhön tullaan panostamaan vuoden 2021 aikana.

Sekä tietoturvan että tietosuojan kannalta yhteinen kehityskohde vuodelle on tietoturvaloukkausprosessin sähköistäminen. Nykyinen prosessi koetaan raskaaksi ja työllistäväksi niin henkilöstön kuin vastuutahojen tietosuojavastaavan ja tietoturvapäällikön puolelta, joten prosessia tullaan kehittämään ja helpottamaan vuoden 2021 aikana.

Tietoturvan osalta haittaohjelmien trendit ovat osoittaneet, että ulkomailta tulevien huijauspuheluiden, sähköpostien ja tekstiviestien volyymit jatkavat kasvuaan. Tämän takia näihin liittyvää ohjeistusta ja ohjeistuksen tiedostamista pyritään kasvattamaan koulutuksellisin keinoin. Samanlaisesti myös teknisiä valmiuksia tullaan kasvattamaan ottamalla käyttöön O365:n uusia tietoturvaominaisuuksia ja turvallisen viestinvälityksen palveluita. Tavoitteena on paitsi tehostaa ja turvata kaupungin toimintaa, mutta myös vastata kasvaviin lainsäädännöstä kumpuaviin vaatimuksiin.

Lisäksi aikaisempina vuosina luotuja ohjeistoja ajantasaistetaan ja linjataan yhdessä muiden kuntien kanssa. 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.

Osana tätä ohjeistusta ja kirjallisia linjauksia ovat hankintojen tietoturvaliitteet, jotka on havaittu vanhentuneiksi. Aikaisemmat ohjeistukset

on laadittu aikana, jolloin pilvipalvelut, palveluna tuotetut ohjelmat ja alihankkijoiden hallinta eivät olleet yhtä keskeisessä roolissa kuin vuonna 2020, mutta joilla on oleellinen rooli palveluiden tietoturvassa. Esimerkkinä tästä suomalaisen tuottama järjestelmä, joka nojaa Microsoftin pilvipalveluihin tai verkkosivulle erikseen ostettu asiakaspalvelu-chat.

Kuntien tietoaineistojen ja viestinnän työkalujen tietoturvaan kohdistuvat lakisääteiset velvollisuudet konkretisoituvat vuonna 2021, johtaan tarpeeseen ottaa käyttöön turvapostiin, turvalliseen tietojen säilytykseen, käyttäjien tunnistamiseen ja salattuun tiedostojensiirtoon liittyviä käytäntöjä ja työkaluja. Nykyiset verkkoasemat ja Outlookin viestin salaus-toiminnallisuus eivät riitä, vaan tarvitaan aikaisempaa kattavampia työkaluja. Näissä Espoolla, kuten muillakin kunnilla, tietohallinnon ja eri toimialojen välinen yhteistyö on tärkeää.



Kuva: Pintaliitodesign, Olli Urpela

LÄHTEET

Skön, K. 2020. Kiinan valvovan silmän alla. Ylen julkaisu 21.05.2020.

URL: <https://yle.fi/aihe/artikkeli/2020/05/21/uhkaavassa-puhelinsoitossa-harria-vaadittiin-lopettamaan-kiinan-arvostelu-tai>

Harjumaa, M. 2021. Maailman vaarallisin haittaohjelma Emotet on saatu kaadettua 27.01.2021.

URL: <https://yle.fi/uutiset/3-11759178>



Espoon kaupunki
Y-tunnus 0101263-6
Turvallisuus ja valmius
Käyntiosoite: Virastopiha 2 B
Postiosoite: PL 12, 02070 ESPOON KAUPUNKI