ESPOO
ESBO

Miten tietosuojaa ja tietoturvaa on toteutettu?

2018

Espoon kaupungin tietotilinpäätös

Sisällysluettelo

1 Esipuhe

Espoon kaupunki kuvaa tässä tietotilinpäätöksessä, miten se hallitsee, hyödyntää ja johtaa tietoa erityisesti tietosuojan ja tietoturvan näkökulmasta. Tämä on kuntasektorin ensimmäisiä tietotilinpäätöksiä Suomessa. Sisällön pääpaino on tietoturvan ja tietosuojan toteutumisen kuvaamisessa sekä EU:n tietosuoja-asetuksen toimeenpanossa. Isossa kuvassa puhutaan digitaalisesta turvallisuudesta. Käsitteen alle kuuluvat 1) riskienhallinta, 2) toiminnan jatkuvuus ja varautuminen, 3) kyberturvallisuus, 4) tietoturva ja 5) tietosuoja.

Espoon keskeisin arvo on asukas- ja asiakaslähtöisyys, joka on läpileikkaava teema kaupungin strategiassa, Espoo-tarinassa. Tietotilinpäätös korostaa vastuullisuutta tiedon käsittelemisessä. Monessakaan organisaatiossa Suomessa ei käsitellä niin paljoa erilaista sensitiivistä henkilödataa kuin suuressa kaupungissa. Kaupungin toiminnassa luottamus on elinehto. Kuntalaista, työntekijää ja yhteistyökumppania koskevaa tietoa on käsiteltävä turvallisesti ja vastuullisesti. Kyse on välittämisestä, empatiasta.

Digitalisoinnilla ja datan turvallisella hyödyntämisellä pyritään rakentamaan kuntalaisille asiakaslähtöiset, luotettavat ja kustannustehokkaat palvelut. Tämä kaikki edellyttää, että tietosuojasta ja tietoturvasta huolehditaan riittävällä tasolla. Tietosuoja- ja tietoturvaperiaatteet tulee siis konkretisoida käytännön tasolle ja istuttaa osaksi organisaation toimintaa.

Tämä on Espoon ensimmäinen kokonaisvaltainen tietotilinpäätös. Ensimmäinen, ns. välitilinpäätös, julkaistiin 25.5.2018, kun Suomessa ja koko EU-alueella ryhdyttiin soveltamaan EU:n yleistä tietosuoja-asetusta. Jatkossa Espoo julkaisee tietotilinpäätöksen vuosittain keväällä. Tietotilinpäätös laaditaan kahtena versiona: 1) johdolle suunnattuna raporttina sekä 2) suuremmalle yleisölle, kuntalaisille, kaupungin työntekijöille ja sidosryhmille, tarjottavana julkisena raporttina, joka julkaistaan Espoon verkkosivuilla.

Tietotilinpäätös on suunnattu myös valvontaviranomaiselle eli tietosuojavaltuutetun toimistolle. Tietosuoja-asetus painottaa osoitusvelvollisuutta. Käytännössä tämä tarkoittaa sitä, että organisaation on osoitettava raportoinnin, dokumentaation ja valvonnan keinoin, että se noudattaa kaikessa toiminnassaan asetuksen vaatimuksia.

Käsitteenä tietotilinpäätös ei ole vakiintunut. Tietosuojavaltuutettu suosittelee sen laatimista vuosittain. Tietotilinpäätöksellä voidaan kuvata myös laajemmin tietojohtamista, eli miten tieto näyttäytyy organisaation strategisena voimavarana. Jatkossa tietotilinpäätöksen näkökulmaa laajennetaan mahdollisesti Espoossa.

Ongelmien ratkaisu ei onnistu yksin vaan yhteistyön merkitys korostuu nopeasti muuttuvassa maailmassa. Tietotilinpäätöksen laadinnan koordinoinnista on vastannut kaupungin tietosuojavastaava, mutta laadintaan ovat osallistuneet erityisesti tietoturvapäällikkö sekä kaupungin tietosuojaryhmä, jossa on edustajat jokaiselta toimialalta sekä tietyistä avainyksiköistä kuten henkilöstöhallinnosta, lakiasiainyksiköstä, Länsi-Uudenmaan pelastuslaitoksesta ja asiakirjahallinnosta.

Oivaltavia lukuhetkiä toivottaen,

Juho Nurmi
Espoon kaupungin tietosuojavastaava

2 Tiivistelmä

Espoon kaupunki (jatkossa Espoo) kuvaa tässä tietotilinpäätöksessä, miten se on toteuttanut tietosuojaa ja tietoturvaa vuoden 2018 aikana. Sisältö painottuu EU:n tietosuoja-asetuksen toimeenpanoon, joka toteutettiin kaupunkitasoisena projektina.

Tietotilinpäätös korostaa vastuullisuutta tiedon käsittelemisessä. Monessakaan organisaatiossa Suomessa ei käsitellä niin paljoa erilaista sensitiivistä henkilödataa kuin suuressa kaupungissa. Espoon toiminnassa luottamus on elinehto. Luottamuksen merkitys korostuu tällä hetkellä, kun kuntalaisten palveluja digitalisoidaan. Ajureina ovat sekä kustannustehokkuus että tarve paremmille personoiduille palveluille. Digitaalisten palvelujen kehittäminen edellyttää tietoturvan ja tietosuojan huomioimista. Näiden elementtien on oltava sisään rakennettuina palveluissa jo niiden suunnitteluvaiheessa.

Espoo on siirtänyt IT-infraansa yhä laajemmin pilvipalveluratkaisuihin vuonna 2018 niiden joustavuuden ja kustannustehokkuuden vuoksi. Espoon ja käytännössä koko Suomen näkökulmasta vuoden 2018 merkittävin kybermaailman uhkatekijä oli organisaatioihin kohdistettu sähköpostitilien tietojenkalastelu, jonka tarkoituksena oli saada haltuun työntekijöiden sähköpostitunnuksia. Varastetuilla käyttäjätunnuksilla tavoitellaan yleensä taloudellista hyötyä seuraamalla organisaation maksuliikennettä. Lisäksi onnistuneeseen tietojenkalasteluun liittyy erilaisia maine- ja sääntelyriskejä. Lähes aina tietojenkalastelun seurauksena vaarantuu henkilötietoja, jolloin tapahtumasta on tehtävä ilmoitus tietosuojavaltuutetulle. Mikäli riski arvioidaan korkeaksi, on oltava yhteydessä myös loukkauksen kohteena oleviin henkilöihin.

Uudet kalastelukampanjat muuttuvat yhä älykkäämmiksi, jolloin niiden torjuminen on vaikeampaa. Vuonna 2018 henkilöstön tietoisuutta tietojenkalastelun vaaroista lisättiin koulutuksilla ja ohjeilla. Alkuvuodesta 2019 otetaan käyttöön teknisiä tietoturvakontrolleja, joilla kyetään pienentämään tuntuvasti tietojenkalasteluun lankeamisen todennäköisyyttä.

EU:n tietosuoja-asetuksen toimeenpanoprojektin tavoitteena oli varmistaa, että Espoon toiminta täyttää tietosuoja-asetuksen vaatimukset. Projektin tärkein ponnistus oli tietosuojan hallintamallin luominen, jolla varmistetaan, että tietosuojatyö ei jää irralliseksi projektiksi. Tietosuojan vastuut on määritelty kaupungin hallintosäännössä ja toimintaohjeissa sekä tietosuoja- ja tietoturvapolitiikassa ja säännöllisesti kokoontuva tietosuojaryhmä kehittää tietosuojaa. Haasteita projektille aiheutti viranomaisohjeiden puuttuminen ja lainsäädännön epäselvä tilanne. Asiantuntijat ovat kuvanneet tietosuoja-asetusta sen ansioista huolimatta monitulkintaiseksi ja vaikeaselkoiseksi.

Tietosuoja-asetuksen ydin on osoitusvelvollisuus, jolloin organisaation on osoitettava ohjeistuksen, dokumentaation ja koulutusten keinoin noudattavansa sitä. Toimeenpanoprojektissa tunnistettiin kehittämiskohteeksi henkilöstön kouluttaminen. Syksyllä 2019 kaupungin henkilöstölle hankitaan tietoturvan ja tietosuojan verkkokoulutussovellus.

Espoon tietoturvapäällikön yhdessä tietohallinnon ja sivistystoimen sekä espoolaisen kyberturvallisuusyrityksen kanssa järjestämä Hack with Espoo -hakkerointikurssi sai mediassa positiivista näkyvyyttä ja lisäsi tietoisuutta tietoturvan tärkeydestä ja uusista yhteistyötavoista. Tulevana vuonna myös muut kaupungit aikovat seurata Espoon mallia.

3 Tilannekuva

3.1 EU:n yleinen tietosuoja-asetus

EU:n yleistä tietosuoja-asetusta ryhdyttiin soveltamaan 25.5.2018 kaikkialla EU-alueella. Asetusta edeltänyt tietosuojalainsäädäntö oli suunniteltu aikakaudella, jolloin internet teki vasta tuloaan kuluttajien arkeen eikä sosiaalista mediaa ja älypuhelimia ollut vielä keksitty. Asetus on voimaanastumisensa jälkeen saavuttanut paljon näkyvyyttä ja herättänyt runsaasti keskustelua globaalisti. Sitä voidaankin pitää todella kunnianhimoisena ja tiukasti yksityisyyden suojaan suhtautuvana lainsäädäntönä. EU haluaa olla ihmislähtöisen ja eettisen digitaalisen maailman edelläkävijä, vaikka skeptikot pelkäävätkin tiukkojen tietosuojaperiaatteiden haittaavan yritysten kilpailukykyä erityisesti tekoälyn hyödyntämisessä. Tähän mennessä ainakin Kalifornian osavaltio ja Japani ovat halunneet seurata eurooppalaista mallia uudistamalla tietosuojalainsäädäntöään.

Vahva oikeusperusta ja perusoikeuksien kunnioitus voivat olla Euroopan vahvuus ja kilpailuetu kiihtyvässä globaalissa taistossa digitalisaation herruudesta. Tietosuoja-asetuksen tavoitteena on luoda digitaalisille palveluille toimiva yhteismarkkina koko EU-alueelle ja synnyttää uutta liiketoimintaa vastapainoksi yhdysvaltalaisille ja kiinalaisille teknologiayrityksille. Tällä hetkellä ainoastaan yksi eurooppalainen teknologiayritys mahtuu maailman arvokkaimpien teknologiayhtiöiden TOP20-listalle.[1] Lisäksi tietosuoja-asetuksen tavoitteena oli harmonisoida EU-alueen tietosuojalainsäädäntöä ja näin helpottaa yritysten toimintamahdollisuuksia.

Eurooppalaisen digitalisaatiokehityksen ja siinä onnistumisen ehdottomassa keskiössä ovat kansalaiset ja digitaalisten taitojen ja osaamisen kehittäminen sekä luottamuksen rakentaminen ja ylläpitäminen. Toistaiseksi tietosuoja-asetus on vielä ansioistaan huolimatta vaikeaselkoinen ja liian tulkinnanvarainen. Vasta tulevat oikeustulkinnat osoittavat, miten sitä tulisi käytännössä soveltaa ja minkälaisiin asioihin tulisi erityisesti kiinnittää huomiota. Kansalaisten arjessa tietosuoja-asetus on lisännyt avoimuutta: 1) yritysten ja organisaatioiden datankäsittelyn on oltava läpinäkyvää ja 2) asiakkaille on ilmoitettava suoraan vakavista tietoturvaloukkauksista. Suomessa asetus on lisännyt ihmisten tietoisuutta oikeuksistaan, mutta varsinaisia tietosuoja-asetuksen mukaisia tietopyyntöjä on tehty vähän.[2]

Useiden jäsenvaltioiden valvontaviranomaiset ovat aloittaneet tietosuojatarkastukset organisaatioissa sekä myös antaneet tuntuvia sakkoja räikeimmistä tietosuojarikkomuksista.[3] Suomessa tietosuojavaltuutetun toimisto ei ole vielä ryhtynyt toimenpiteisiin (tilanne 24.4.2019), johtuen kansallisen tietosuojalain myöhäisestä voimaantulosta. Lisäksi toimiston organisointi hakee vielä muotoaan.

3.2 Kansallinen tietosuojalainsäädäntö

Tietosuoja-asetuksen soveltamisen alkaessa jäi vanha henkilötietolaki (523/1999) voimaan eikä lainvalmistelussa ehditty muuttamaan muutakaan kansallista lainsäädäntöä vastaamaan tietosuoja-asetusta. Henkilötietolain kumoava tietosuojalaki (1050/2018) astui voimaan 1.1.2019. Lainsäätäjä ei ole vielä ehtinyt kokonaan uudistamaan kansallista erityislainsäädäntöä vastaamaan tietosuoja-asetusta (tilanne 24.4.2019).

[1] The Economist 23.3.2019: “Why big tech should fear Europe”.
[2] Sitran blogi 17.1.2019: ”Oma päätösvalta datan käytössä on ihmisille tärkeää”.
[3] DLA Piper GDPR data breach survey: February 2019.

Tietosuoja-asetuksen soveltamisen alkaminen lisäsi vuonna 2018 lainsäädännön soveltamiseen liittyvää hallinnollista työtä. Kansallisen lainsäädännön soveltaminen tuli arvioida niissä tilanteissa, jotka kuuluivat tietosuoja-asetuksen soveltamisalan piiriin, sillä kansallista lainsäädäntöä sovelletaan sellaisenaan vain, jos se ei ole ristiriidassa tietosuoja-asetuksen kanssa. Mikäli kansallinen lainsäädäntö on ristiriidassa tietosuoja-asetuksen kanssa eikä tulkinnalla voida poistaa ristiriitaa, sovelletaan suoraan tietosuoja-asetusta ja jätetään ristiriidassa oleva kansallinen lainsäädäntö soveltamatta.

Eduskunnassa oli vuonna 2018 käsiteltävänä tietosuojaan liittyviä lakihankkeita, kuten hallituksen esitys laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä sekä eräiksi siihen liittyviksi laeiksi (HE 159/2017 vp) ja hallituksen esitys laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ja eräiksi siihen liittyviksi muiksi laeiksi (HE 300/2018 vp). Sosiaali- ja terveystietojen toissijaista käyttöä koskeva lakiehdotus hyväksyttiin eduskunnassa vuoden 2019 maaliskuussa. Hallituksen esityksen perusteella lain tavoitteena on, että sosiaali- ja terveydenhuollon henkilötietoa voitaisiin tulevaisuudessa käyttää joustavammin muussa kuin henkilötietojen ensisijaisessa käyttötarkoituksessa, kuten esimerkiksi tietojohtamisessa sekä kehittämis- ja innovaatiotoiminnassa. Lain soveltamisen alettua tietoluvat myöntää sosiaali- ja terveysalan tietolupaviranomainen mm. niissä tilanteissa, joissa tietoja olisi tarpeen yhdistellä eri rekisterinpitäjiltä.

Sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevaa lakiluonnosta ei ole vielä hyväksytty eduskunnassa. Lakiluonnoksen tarkoituksena on mm. luoda edellytykset valtakunnallisten tietojärjestelmäpalveluiden käyttöön sosiaalihuollossa. Lisäksi lakiluonnoksen myötä luovuttaisiin laajasta suostumuksesta terveydenhuollossa ja siirryttäisiin potilaiden kielto-oikeuteen.

3.3 Tiedonhallintalaki

Tiedonhallintaa säännellään Suomessa tällä hetkellä useassa säädöksessä. Uusi tiedonhallintaa koskeva laki on valmistelussa. Tavoitteena on yhtenäistää ja korvata eräitä aiheeseen liittyviä lakeja. Lakiluonnos oli kommentoitavana syksyllä 2018. Myös Espoo kommentoi lakiluonnosta.

Laissa säädetään muun muassa julkisen hallinnon yleisistä velvoitteista tiedonhallintaan, julkisen hallinnon tiedonhallinnan yleisestä ohjauksesta, tietoaineistojen muodostamisesta ja sähköisestä luovuttamisesta, julkisen hallinnon tietoturvallisuuden perusteista, teknisten rajapintojen hyödyntämisestä sekä asianhallinnasta ja tietoaineistojen säilyttämisestä. Kuntasektorin näkökulmasta on merkittävää, että lain on tarkoitus kumota valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), jolloin tietoturvalle asetettavat vaatimukset tulevat jatkossa tietohallintalaista ja ne ovat velvoittavia kuntatoimijoille.

Ensimmäisessä vaiheessa tiedonhallintamallin ja rajapintojen on oltava valmiita vuoden 2021 alusta. Julkishallinnolla onkin tiedonhallinnan kehittämisen työlistalla tulevina vuosina muun muassa lokitietojen kerääminen, asianhallinta, asiarekisteri ja tietoturvallisuusvaatimukset.

3.4 Megatrendit ja teknologinen kehitys

Megatrendeillä tarkoitetaan ison mittakaavan kehityskulkuja. Tässä kappaleessa tarkastellaan erityisesti kaupungin lähitulevaisuuteen ja sen tiedonhallintaan vaikuttavia megatrendejä ja teknologisen kehityksen tuomia mahdollisuuksia ja uhkakuvia. Tällä hetkellä digitalisaatio, alustatalous, regulaatio ja ihmisten muuttuvat tarpeet muuttavat nopeasti kaupungin toimintaympäristöä. Muutokset kietoutuvat tietoon, sen hallintaan ja sen hyödyntämiseen.

Risto Linturi ja Osmo Kuusi kirjoittivat eduskunnan tulevaisuusvaliokunnalle keväällä 2018 ”Suomen sata uutta mahdollisuutta 2018–2037” -raportin, jossa esitettiin näkemyksiä siitä, miten yhteiskunta muuttuu ja miten siihen tulisi varautua. Tulevaisuuden kannalta keskeisiksi asioiksi nousevat esimerkiksi energian tuotanto, henkilöliikenne, materiaalit ja yksityisyydensuoja. Teknologian kehitykseen liittyy paljon muutakin kuin uusien keksintöjen tekninen mahdollisuus. Esimerkiksi lainsäädäntö vaikuttaa ratkaisevasti siihen, miten rohkeasti yritykset lähtevät kehittämään uusia innovaatioita. Myös ihmisten mieltymykset vaikuttavat siihen, miten teknologia kehittyy.[4]

Tekoälyn ja ohjelmistorobotiikan käyttö lisääntyy jatkuvasti kaikkialla yhteiskunnassa, myös julkishallinnossa. Tekoäly on paljon muutakin kuin PowerPoint-slideja. Hypetyksestä huolimatta se on jo konkretiaa ja sillä on mahdollista muuttaa julkishallinnon toimintatapoja mielekkäämpään suuntaan, kunhan virkamies istuu ajurin paikalla ja asiakkaiden luottamuksesta pidetään kiinni. Jo tällä hetkellä julkishallinnossa käytetään laajasti automaatiota tilanteissa, jotka eivät vaadi harkintaa. Tekoälyn myötä automatiikkaa voidaan soveltaa myös harkintaa sisältävissä päätöstilanteissa.

Tekoälystä on hyötyä muun muassa terveydenhuollon, energiankulutuksen vähentämisen, autojen turvallisuuden, maanviljelyn, ilmastonmuutoksen torjunnan ja rahoitusriskien hallinnan alalla. Tekoäly voi myös auttaa petosten ja kyberturvallisuusuhkien havaitsemisessa ja antaa lainvalvontaviranomaisille mahdollisuuden torjua rikollisuutta tehokkaammin. Se kuitenkin tuo myös mukanaan uusia haasteita työn tulevaisuuden kannalta ja nostaa esiin oikeudellisia ja eettisiä kysymyksiä.

Valtioneuvoston kanslian teettämässä raportissa on pohdittu tekoälyn hyödyntämismahdollisuuksia viranomaistoiminnassa. Suomalaiset suhtautuvat tekoälyn käyttöön yleensä positiivisesti, mutta luottamus edellyttää avoimuutta ja läpinäkyvyyttä. Viranomaisten on pystyttävä perustelemaan päätöksensä ja jos päätöksenteossa hyödynnetään oppivia algoritmeja, tämä on vaikeampaa. Toisaalta pitää miettiä, mitä tekoälyyn liittyvää osaamista kansalaisilta vaaditaan ja miten tasa-arvo toteutuu osaamisesta riippumatta. Tekoäly avaa kuitenkin viranomaistoimintaan runsaasti uusia mahdollisuuksia. Se voi parantaa ja nopeuttaa palvelua ja päätöksentekoa, tuoda uusia palvelukanavia asiakkaiden saataville tai parantaa yksilöiden huomioimista päätöksenteossa.[5]

Työ- ja elinkeinoministeriön vetämä Tekoälyaika-ohjelma on yksi Espoon uusista verkostoista. Mukaan on lähtenyt lähes 40 organisaatiota, joista suurin osa on suomalaisia pörssiyhtiöitä. Julkishallinnon organisaatioista mukana on Espoon lisäksi Verohallinto, Business Finland ja Väestörekisterikeskus.

Espoon kaupunki on mukana yhtenä perustajana maailman suurimman teknologia-alan järjestön IEEE:n hankkeessa, jonka tavoitteena on luoda kansainvälisesti laajalti hyväksytyt prosessit ja

[4] Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2018: Suomen sata uutta mahdollisuutta 2018-2037.
[5] Valtioneuvoston kanslian raportti 1.2.2019: Tekoäly viranomaistoiminnassa - eettiset kysymykset ja yhteiskunnallinen hyväksyttävyys.

sertifikaatit tekoälyn eettiselle soveltamiselle. Työstä odotetaan ensimmäisiä serfikaatteja vuoden 2019 aikana.

Osallistuminen Tekoälyaika-ohjelmaan ja IEEE:n verkoston toimintaan ovat jatkumoa pitkäjänteiselle tekoälyn kehittämistyölle Espoossa. Keväällä 2018 Espoo liittyi Suomen tekoälyn tutkimuskeskuksen FCAI:n jäseneksi (Finnish Center for Artificial Intelligence). Ensimmäisiä mittavia espoolaisia tekoälykokeiluja oli keväällä 2018 päättynyt, ohjelmisto- ja palveluyritys Tiedon kanssa toteutettu tekoälykokeilu ennakoivien palvelupolkujen rakentamiseksi.

Tasapainoinen yhteiskuntakehitys perustuu sille, että päätöksenteossa otetaan huomioon ihmisten erilaiset peruslähtökohdat ja sovelletaan nykyaikaisia toimintatapoja. Esimerkiksi tekoäly, täsmälääketiede ja sosiaaliset innovaatiot voivat mullistaa toimintatapamme samaan tapaan kuin antibiootit tai kuvantamismenetelmät aikoinaan. Uudet tavat auttavat tunnistamaan ihmisten tarpeita entistä paremmin ja ne tehostavat diagnostiikkaa, palveluvalintoja, lääkekehitystä ja omahoitoa.[6]

Radikaalien teknologioiden aiheuttaman yhteiskunnan transformaation ennakointi on kehityksen nopeutuessa entistä tärkeämpää[7]. Kaupungin näkökulmasta ja sen toimintaan vaikuttavia keskeisiä teknologian kehityspolkuja lähitulevaisuudessa ovat muun muassa tekoälyteknologiat ja erilaiset data-analytiikkaan liittyvät teknologiat. Lohkoketjuteknologiaa hyödynnetään Suomessa jo esimerkiksi kiinteistöjen omistuksiin liittyvissä kokonaisuuksissa. Lisäksi 5G ja esineiden internet vaikuttavat kaupungin toimintoihin yhä voimakkaammin.

[6] https://stm.fi/megatrendit
[7] Suomen sata uutta mahdollisuutta 2018-2037 - Yhteiskunnan toimintamallit uudistava radikaali teknologia https://www.eduskunta.fi/FI/tietoaeduskunnasta/julkaisut/Documents/tuvj_1%2B2018.pdf

4 Kaupungin tietoturvallisuus- ja tietosuojariskit

4.1 Keskeiset riskit ja uhat

Espoon kaupunkiin kohdistuneet tietoturvauhat vuonna 2018 ovat noudatelleet hyvin yleisiä lainalaisuuksia. Espoon kaupungin uhka- ja riskiympäristö noudattelee yleisellä tasolla hyvin paljon Kyberturvallisuuden vuosikatsauksessa 2018 kuvattuja ilmiöitä.[8]

Espoo on ottanut asteittain käyttöönsä muun muassa pilviteknologiaan perustuvan sähköpostipalvelun vuoden 2017 lopulta alkaen, ja näiden käyttäjätunnuksia on yritetty kalastella vuoden 2018 aikana selvästi aikaisempaa vuotta enemmän. Tämä ilmiö on näkynyt myös valtakunnallisella tasolla, muun muassa Kyberturvallisuuskeskuksen varoituksissa. Sähköposteihin liittyvä eritasoinen tietojenkalastelu voidaan arvioida suurimmaksi yksittäiseksi kaupunkiin vuonna 2018 kohdistuneeksi uhaksi.

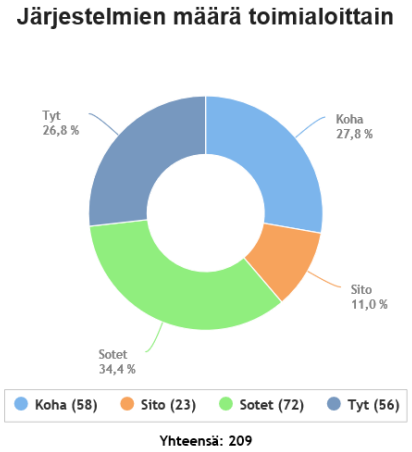
Toteutuneiden riskien osalta haavoittuvuus on ollut pääosin joko prosesseissa tai loppukäyttäjässä. Tämä tarkoittaa sitä, että rikollinen osapuoli, on hyödyntänyt pääsääntöisesti ihmisiin tai prosessiin kohdistuvaa haavoittuvuutta tai poikkeama on johtunut inhimillisestä virheestä joko prosessissa tai yksittäisen henkilön työtehtävissä. Tietoturvallisuuden kehittämisessä tulee teknisen kyvykkyyden lisäksi huomioida prosessien turvallisuus sekä haavoittuvuuksien inhimillinen ulottuvuus.

Kaupungin toiminnassa monet keskeiset suojattavat kohteet liittyvät laajoihin kokonaisuuksiin henkilötietoja. Kaupunki käsittelee toiminnassaan myös suuria määriä rahaa. Tieto- ja viestintäteknologian kehittyessä ja liittyessä yhä useampaan eri toimintoon kybertoimintaympäristö suojattavana kohteena korostuu entisestään.

4.2 Verkkopalveluympäristöt ja muut ICT-palvelut

Espoon kaupungilla konsernihallintoon kuuluva Tietohallintoyksikkö tuottaa kaupungin toiminnalle välttämättömiä infrapalveluja, kaupungin yhteisiä palveluja sekä toimiala- ja/tai tulosyksikkökohtaisia palveluja. Infrapalveluihin kuuluvat kokonaisuudet ovat loppukäyttäjäpalveluita, tietoliikennepalvelut, palvelin- ja kapasiteettipalvelut sekä käyttäjähallinta. Yhteiset ja toimiala tai tulosyksikkökohtaiset palvelut pitävät sisällään sovellukset sekä järjestelmät.

[8] Tietoturvan vuosi 2018, Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf



Espoossa käytettävät tietojärjestelmät luokitellaan niiden vaikuttavuuden ja vaativuuden perusteella ABCD-luokituksen mukaisesti. Luokituksessa vaikuttavuuteen liittyvät kriteerit liittyvät suoraan kaupungin prosessien kriittisyyteen.

A. Kuntalaisten näkökulmasta kriittinen tai yli toimialarajojen Espoon sisäiseen toimintaan laajasti vaikuttava

B. Kuntalaisten näkökulmasta merkittävä järjestelmä tai toimialalle kriittinen järjestelmä

C. Ei suoraa vaikutusta kuntalaisiin, haittaa laajasti Espoon työntekijöiden toimintaa yhdellä toimialalla

D. Ei suoraa vaikutusta kuntalaisiin, ei merkittävää haittaa usealle Espoon työntekijälle.

Tietojärjestelmien kriittisyysluokka ei korreloi automaattisesti henkilötiedon käsittelyn laajuutta tai järjestelmän sisältämää henkilötiedon määrää tai laatua. Se on henkilötiedon käsittelyyn liittyen suuntaa antava ja kuvastaa tietojärjestelmien suhdetta prosessien kriittisyyteen jatkuvuuden hallinnan näkökulmasta.

Rekisteriin liittyvät tietojärjestelmät määritellään tietosuojaselosteessa. Ne tietokokonaisuudet ja tietovarannot, joita käsitellään tietosuojaselosteessa määritellyllä tavalla, muodostavat rekisterin. Rekisteri on teknologiariippumaton, ja se voi käsittää useita tietovarantoja. Esimerkiksi henkilöstötietoja käsittävä rekisteri voi muodostua HR-tietokannasta, paperiarkistoissa olevista työsopimuksista ja vaikkapa sisäisistä työvuorolistoista; määräävää on se, että rekisterissä tiedot esitellään jäsennellyssä muodossa ja että rekisterin eri ilmentymissä henkilöstötietoja käsitellään samalla, rekisteriselosteessa määritellyllä, tavalla.

Kaupunki käyttää paljon ulkoistettuja palveluja palvelutuotannossaan sekä erilaisten pilviteknologioitten hyödyntäminen on kasvanut. Etenkin pilvipalveluihin siirryttäessä riskienhallinnan merkitys korostuu.

4.3 Jatkuvuuden hallinta

Jatkuvuuden hallinnalla tarkoitetaan prosessia, jolla turvataan ydintoiminnan ja sen prosessien jatkuvuuden turvaamista erilaisissa keskeytystilanteissa. Jatkuvuuden hallinta pitää sisällään kriisinhallinnan, jatkuvuus- ja toipumissuunnittelun. Yksinkertaisimmillaan esimerkiksi opetustoimessa keskeytystilanne voisi olla tietojärjestelmähäiriö, joka estäisi opetussovellusten hyödyntämisen. Jatkuvuussuunnittelussa tähän on varauduttu perinteisillä opetusmetodeilla, ja toipumissuunnitelmassa otetaan kantaa siihen, miten nopeasti ja missä järjestyksessä tietojärjestelmähäiriö korjataan ja palautetaan takaisin normaalitilaan.

Jatkuvuuden hallintaa voidaan kuvata myös seuraavilla toimenpiteillä:

- tunnistaa toimintansa uhkat, riskit, häiriötilanteet ja riippuvuudet
- Arvioi uhkien vaikutukset organisaatiossa ja sen toimijaverkostossa
- Organisoi ja toteuttaa menettelytavat häiriötilanteiden varalle
- Varmistaa kriittisten kumppaneidensa kyvyn toimia häiriötilanteissa
- Suojaa ydintoimintansa intressit ja arvontuotantokykynsä.

Espoossa jatkuvuuden hallintaa ohjataan ydintoiminnoista sekä niistä prosesseista, joilla voi olla vaikutuksia asiakkaiden terveydelle tai hyvinvoinnille, alkaen. Jatkuvuuden hallintaa ei ole järkevää ulottaa joka tasolle.

4.4 Hankinnat ja palveluostot

Espoo solmii sopimustoimittajiensa kanssa määrämuotoisia sopimuksia, joissa huomioidaan tietoturvaan, tietosuojaan ja jatkuvuuden hallintaan liittyvät kokonaisuudet. Riippuen tuotettavan palvelun laadusta, kriittisyydestä ja arvosta, sopimusehtoja ja liitteitä tarvittaessa tarkennetaan.

Lainsäädännön perusteella Espoo voi ulkoistaa henkilötietojen käsittelyä palveluntuottajille. Tietosuoja-asetuksen edellyttämä sopimusten päivitysprosessi on ollut Espoon kokoiselle organisaatiolle valtaisa urakka. Tietosuoja-asetus edellyttää, että henkilötietojen käsittelystä on sovittava sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo käsittelijää. Tämän vuoksi sellaiset sopimukset, joissa kaupunki oli ulkoistanut henkilötietojen käsittelyä palveluntuottajalle, oli päivitettävä vastaamaan asetuksen vaatimuksia. Sopimuksia on myös toisin päin, eli Espoo tuottaa palvelua esimerkiksi toiselle kunnalle. Rekisteröityjen näkökulmasta näiden sopimusten päivittäminen on yhtä tärkeää.

Sopimusten päivittäminen oli yksi EU:n tietosuoja-asetuksen toimeenpanoprojektin päätehtävistä. Strategiaksi valittiin riskiperusteinen lähestymistapa: kaikkein arvokkaimmat sopimukset päivitettiin ensimmäiseksi. Etusijalle asetettiin myös sellaiset sopimukset, joihin liittyi korkean riskiluokan tiedon käsittelyä.

5 Tietosuojan ja tietoturvallisuuden toteutuminen

5.1 EU:n tietosuoja-asetuksen toimeenpanoprojekti

Elokuussa 2017 asetettu ja saman vuoden lokakuussa käynnistynyt kaupunkitasoinen EU:n tietosuoja-asetuksen toimeenpanoprojekti, lyhyesti GDPR-projekti, pyrki varmistamaan, että Espoon kaupungin toiminta täyttää jatkossa EU:n tietosuoja-asetuksen vaatimukset. Vaikka Suomessa oli noudatettu henkilötietolakia lähes 20 vuotta ja kaupunki on käsitellyt pitkään erilaisia henkilötietoja, aiheutti tietosuoja-asetus muutoksia kaupungin toimintaan. Espoon on jatkossa osoitettava erityisesti dokumentaation ja koulutusten keinoin, että se noudattaa asetuksen vaatimuksia. Koska tietosuoja-asetusta ryhdyttiin soveltamaan 25.5.2018 alkaen, täytyi projektin saavuttaa tietyt minimitavoitteet päivämäärään mennessä. Projekti päättyi lokakuussa 2018.

Kaupunkitasoinen tietosuojan, tietoturvan, juridiikan ja riskienhallinnan asiantuntijoista koostunut projektiryhmä asetti projektille seuraavat tavoitteet: 1) Selvittää EU:n tietosuoja-asetuksen vaatimukset kaupungin toiminnalle; 2) Kartoittaa mahdolliset puutteet ja luoda suunnitelmat puutteiden korjaamiselle; 3) Rakentaa asetuksen edellyttämät prosessit tietosuojan ylläpidolle ja jatkuvalle kehittämiselle ja 4) Varmistaa, että Espoo noudattaa tietosuojalainsäädännön vaatimuksia.

Tavoitteet jaettiin vielä viiteen ydintehtävään, joita olivat: 1) nykytilakartoitus, 2) tietosuojan hallintamallin luominen, 3) osoitusvelvollisuuden toteuttaminen, 4) rekisteröityjen oikeuksien varmistaminen ja 5) sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden jalkauttaminen ydinprosesseihin.

Projekti täytti sille annetut tavoitteet. Sen tärkein ponnistus oli tietosuojan hallintamallin luominen, jolla varmistetaan, että tietosuojatyö ei jää irralliseksi projektiksi. Tietosuojan vastuut on määritelty kaupungin tietosuoja- ja tietoturvapolitiikassa ja säännöllisesti kokoontuva tietosuojaryhmä kehittää tietosuojaa systemaattisesti. Projektin jälkiarviointi toteutetaan kesällä 2019.

Haasteita projektille aiheutti viranomaisohjeiden puuttuminen ja monitulkintaisuus sekä lainsäädännön epäselvä tilanne.

5.2 Konsernihallinto

Konsernihallinnon (sisältäen konsernipalvelut) 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

Kaupungin tietosuojavastaava ja tietoturvapäällikkö on sijoitettu konsernihallinnon turvallisuus ja valmius -ryhmään. Espoossa tietosuojavastaava ja tietoturvapäällikkö tekevät tiivistä yhteistyötä. Kummankin vastuualue on osa kokonaisturvallisuutta ja erityisesti digitaalista turvallisuutta.

Tietosuojavastaava vastaa koko kaupungin tietosuojan kehittämisestä ja raportoi kaupungin johtoryhmälle. Tietosuojavastaavan erityisvastuualueena on konsernihallinto. Lisäksi hallintolakimies osallistuu aktiivisesti tietosuojan kehittämiseen konsernihallinnossa. Muut keskeiset henkilöt ovat hankintalakimies, hr-tietopäällikkö, työmarkkinalakimies, rekrytointiasiantuntija ja asiakirjahallinnon suunnittelija. Myös työterveyshuollossa on oma tietosuojan vastuuhenkilö.

Konsernihallinnossa täsmäkoulutukset kohdistettiin yksiköihin, joissa käsitellään paljon arkaluonteisia henkilötietoja. Kaiken kaikkiaan konsernihallinnosta ja konsernipalveluista osallistui näihin koulutuksiin arviolta 600 henkeä.

Tietosuoja-asetuksen toimeenpanoprojektin yhteydessä kaikille työntekijöille lähetettiin henkilökohtainen linkki Arjen tietosuoja -verkkokoulutukseen. Konsernihallinnon osalta osallistumisprosentti oli tyydyttävä 60 %. Alhainen tulos johtui teknisistä ongelmista sekä puutteellisesta raportoinnista ja viestinnästä.

Kokemuksen pohjalta päätettiin, että kaupungille on hankittava verkkokoulutussovellus tietosuoja- ja tietoturvakoulutuksille vuoden 2019 aikana. Muut tunnistetut kehittämiskohteet ovat:

- Tietoturva- ja tietosuojatietoisuuden lisääminen
  - Koulutussovelluksen ohella tietoisuutta voidaan lisätä täsmäkoulutuksilla, ohjeistuksella, viestinnällä ja johtoryhmävierailuilla
- Tietosuoja-asetuksen edellyttämät riskiarviot ja vaikutuksenarvioinnit
  - Tietosuojaan liittyvät riskit on arvioitu systemaattisesti uusien palvelujen ja tietojärjestelmien osalta, mutta vanhoja ei ole arvioitu kattavasti.
- Tietopyyntöprosessin kehittäminen
  - Parannetaan prosessin sujuvuutta ja kartoitetaan sähköistä työkalua.

5.3 Sosiaali- ja terveystoimi

Sosiaali- ja terveystoimessa käsitellään potilastietoa ja sosiaalihuollon asiakastietoa lakisääteisten palveluiden järjestämiseksi. Potilastietoa ja sosiaalihuollon asiakastietoa on säännellyt jo ennen tietosuoja-asetuksen voimaantuloa kansallinen erityislainsäädäntö, jossa on säädetty mm. lokivalvonnasta, käyttöoikeuksista ja tietojen kirjaamisesta.

Sosiaali- ja terveystoimessa on ennen tietosuoja-asetusta ollut mm. tietopyyntöprosessi, siihen liittyviä lomakkeita, tietosuojaselosteita ja ohjeita henkilökunnalle henkilötietojen käsittelystä. Tietosuoja-asetuksen voimaantulon myötä toimialalla on päivitetty mm. näitä dokumentteja. Toimialalle on laadittu tietosuojan ja tietoturvan omavalvontasuunnitelma. Sopimuksista, joiden perusteella toimiala on tietojen käsittelijä, on laadittu tietosuoja-asetuksen mukaiset selosteet käsittelytoimista. Toimialan sopimuksia on päivitetty vastaamaan tietosuoja-asetusta. Lisäksi toimialalla on järjestetty tietosuojaan liittyvää koulutusta henkilöstölle. Sosiaali- ja terveystoimessa on usean vuoden ajan toiminut toimialan tietosuojaryhmä, joka käsittelee toimialan kannalta olennaisia tietosuojakysymyksiä säännöllisesti.

Toimialalla on tunnistettu kehittämiskohteiksi vuodelle 2019 mm. tietosuoja-asetuksen mukaiset riski- ja vaikutustenarvioinnit sekä henkilöstön tietosuojaan liittyvän osaamisen ylläpitäminen ja lisääminen esim. koulutuksilla.

5.4 Sivistystoimi

Sivistystoimessa käsitellään henkilötietoja pääsääntöisesti lakisääteisiin tehtäviin perustuen. Isoimmat henkilötietoryhmät liittyvät opetuksen ja varhaiskasvatuksen järjestämiseen. Esimerkiksi opiskeluhuollon, opetuksen ja varhaiskasvatuksen järjestämiseen, erityisruokavalioihin, erityisryhmille varattuihin kuntosali- ja uimahallikortteihin sisältyy myös erityisten henkilötietoryhmien käsittelyä.

Tietoriskienhallinnan suunnittelijan johdolla käydään säännöllistä vuoropuhelua toimialan eri yksikköjen kanssa tietoturva- ja tietosuojariskeistä. Keskusteluissa käydään läpi mm. yksikön henkilötietojen käsittelytavat ja arvioidaan sen hetkistä tilaa, sekä pyritään tunnistamaan oleelliset tietoriskit (riskikartoitus). Tavoitteena on saavuttaa kokonaiskuva tietoturvallisuudesta ja määrittää riittävä tietoturvallisuuden taso kunkin yksikön kohdalla. Vuonna 2018 riskikartoituksia eri yksiköiden kanssa tehtiin yhteensä yhdeksän kappaletta. Toimialan sopimuksia ja tietosuojaselosteita on päivitetty tietosuoja-asetuksen voimaantulon myötä. Lisäksi toimialalla on järjestetty tietosuojaan liittyvää koulutusta henkilöstölle.

Toimialalla on tunnistettu kehittämiskohteiksi vuodelle 2019 mm. henkilöstön tietosuojaan liittyvän osaamisen ylläpitäminen ja lisääminen esim. koulutusten ja kirjallisten ohjeiden avulla sekä tarkoituksenmukaiset tekniset ratkaisut erilaisten tietojen säilyttämiseen.

5.5 Tekninen ja ympäristötoimi

Teknisessä ja ympäristötoimessa käsitellään henkilötietoja niin lakisääteisiin tehtäviin, rekisteröidyn suostumukseen kuin sopimukseen perustuen. Esimerkiksi vapaaehtoisessa maanhankinnassa ja -luovutuksessa henkilötietojen käsittely perustuu rekisteröidyn suostumukseen. Erityisiä henkilötietoryhmiä käsitellään hyvin vähän.

Tietosuoja-asetuksen voimaantulon jälkeen toimialan tietosuojaselosteet on suurelta osin päivitetty ja niitä pyritään pitämään ajan tasalla. Lisäksi on käyty läpi tarve sopimusten päivittämiselle ja kiinnitetty huomiota siihen, että henkilötietojen käsittely minimoidaan. Tästä esimerkkinä Locuksen väestötietoihin pääsyn rajoittaminen, missä väestötietojen käyttöoikeudet karsittiin minimiin. Rekisteröityjen oikeuksien takaamiseksi on myös keskitytty selkiyttämään tietopyyntöprosessia. Tavoitteena onkin ensi vuoden aikana saada se toimimaan entistä paremmin.

Kehittämiskohteina vuodelle 2019 on lisäksi mm. tietosuojaan liittyvän osaamisen lisääminen koko toimialan henkilöstöä ajatellen koulutusten ja paremman tiedottamisen avulla. Näin jokainen työntekijä tunnistaa, milloin ja missä määrin henkilötietoja on tarpeen käsitellä. Lisäksi tavoitteena on parantaa hallinnollista tietosuojaa ja kehittää tietosuojaan liittyvien riskien arviointia.

5.6 Länsi-Uudenmaan pelastuslaitos

Länsi-Uudenmaan pelastuslaitos -liikelaitoksessa henkilötietoja käsitellään lakisääteisten tehtävien lisäksi rekisteröidyn suostumukseen ja sopimuksiin perustuen.

Sopimuksista, joiden perusteella Länsi-Uudenmaan pelastuslaitos on tietojen käsittelijä, on laadittu tietosuoja-asetuksen mukaiset selosteet käsittelytoimista. Sopimuksia on päivitetty vastaamaan tietosuoja-asetusta. Tietosuoja-asetuksen voimaantulon myötä henkilötietojen käsittelyyn,

keräämiseen ja säilytystapaan on kiinnitetty erityistä huomiota ja tarveharkintaa. Tietosuojaan liittyvää koulutusta on järjestetty henkilöstölle.

Uudenmaan alueen pelastuslaitoksilla on käynnistetty yhteinen projekti tietosuojan ja tietoturvallisuuden kehittämiseksi. Pelastuslaitosten yhteinen tavoite on päästä tietoturvan osalta perustasolle ja tietyin osin korotetulle tasolle.

Kehittämiskohteena on osaamisen kehittäminen tietosuojaan liittyen välttämättömänä kaikissa tehtävissä, jotta tietoturvan ja tietosuojan merkitys arkipäivässä avautuu. Henkilöresurssin puute pelastuslaitoksessa hankaloittaa jonkun verran koko pelastuslaitoksen tietotaidon kehittämisessä ja ylläpitämisessä.

5.7 Tietosuojaryhmä

Espoon kaupungin tietosuojaryhmä perustettiin kaupunginjohtajan päätöksellä loppuvuodesta 2018. Kaupunginjohtajan päätöksellä toimialoja ja avainyksiköitä pyydettiin nimeämään edustajat ryhmään. Tavoitteena oli saada ryhmään laaja kattaus eri alojen asiantuntijoita tietosuojasta, tietoturvasta, riskienhallinnasta, ICT:stä ja juridiikasta. Ryhmän kokoonpano on seuraavanlainen:

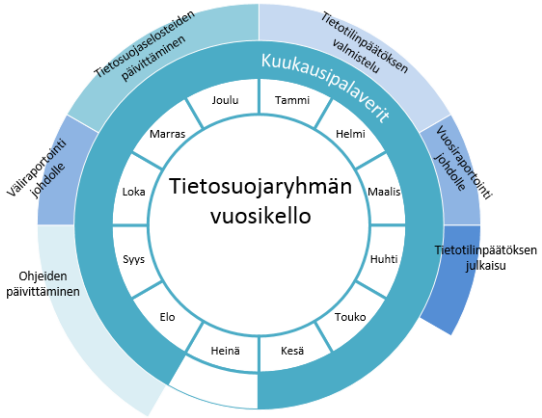
- tietosuojavastaava (puheenjohtaja)
- tietoturvapäällikkö (varapuheenjohtaja)
- teknisen tietoturvan asiantuntija
- HR-tietopäällikkö
- hallintolakimies
- sosiaali- ja terveystoimen toimialan edustajat
    - hallintopäällikkö
    - lakimies
    - asiakirjahallinnon suunnittelija
- sivistystoimen toimialan edustajat
    - lakimies
    - tietoriskienhallinnan suunnittelija
- teknisen ja ympäristötoimen toimialan edustaja
    - hallintopäällikkö
- Länsi-Uudenmaan pelastuslaitoksen edustaja
    - tukipalvelupäällikkö
- kaupunginarkiston edustaja
    - asiakirjahallinnon suunnittelija

Ryhmän tehtävä on määritelty Espoon 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.”*

Aluksi ryhmän keskeisenä tehtävänä oli varmistaa tietosuoja-asetuksen toimeenpanoprojektin tulosten jalkauttaminen. Tietosuojaryhmä kokoontui ensimmäisen kerran lokakuussa 2018. Ryhmä kokoontuu kuukausittain, joten vuoden 2018 aikana ryhmä kokoontui yhteensä kolme kertaa. Ryhmä raportoi puolivuosittain tietosuojan toteutumisesta kaupungin johtoryhmälle. Ryhmän kokouksissa käsiteltiin mm. seuraavia aihekokonaisuuksia:

- kansallisen tietosuojalain vaikutukset kaupungin toimintaan

- tietosuojan huomioiminen somessa
- julkisen hallinnon pilvipalvelulinjaukset
- tietoallasprojekti



Kuva: Tietosuojaryhmän vuosikello

5.8 Tietoturvaryhmä

Espoon kaupungin tietoturvaryhmä on ollut toiminnassa jo vuosia ja se kokoontuu säännöllisesti kuukausittain tietoturvapäällikön johdolla. Tietoturvaryhmän tehtäviin on kuulunut myös tietosuojaan liittyviä asiakokonaisuuksia, ja nämä tehtävät siirrettiin tietosuojaryhmälle kaupungin tietoturva- ja tietosuojapolitiikan päivityksen ja hyväksynnän yhteydessä.

Tietoturvaryhmän tehtäväksi on määritetty: ”*Tietoturvaryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä analysoi ja arvioi em. kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia ja linjauksia kaupungin tietoturvallisuuden parantamiseksi. Lisäksi ryhmä toimii koko kaupunkiorganisaation tukena tietoturva-asioissa.*”

5.9 Yhteistyöverkostot

Tietosuoja- ja tietoturvatyössä viralliset ja epäviralliset yhteistyöverkostot ovat osoittautuneet hyödyllisiksi areenoiksi kokemusten ja käytäntöjen vaihdolle. Verkostoyhteistyöllä resursseja kyetään hyödyntämään tehokkaasti. Tällä hetkellä suuret kaupungit kamppailevat samanlaisten haasteiden parissa, kun kansalaisten käyttäytymistottumukset muuttuvat ja digitalisaatiosta odotetaan apua palvelujen parantamiselle.

Espoon kaupungin tietosuojavastaava on osallistunut Helsingin kaupungin vetämään kaupunkiseudun tietosuojavastaavien yhteistyöryhmään. Ryhmä perustettiin syksyllä 2018 ja se kokoontuu kuukausittain. Lisäksi suuret kaupungit, Espoo, Helsinki, Tampere, Oulu ja Kuopio, muodostavat epävirallisen yhteistyöryhmän, joka kokoontuu Skypen välityksellä kuukausittain. Tapaamisilla oli suuri merkitys keväällä 2018, kun kaupungit valmistautuivat EU:n tietosuoja-asetuksen soveltamiseen. Tapaamisten teemat liikkuvat laajasti tietoturvan ja tietosuojan ympärillä.

Espoon tietosuojavastaava on pyrkinyt osallistumaan mahdollisuuksien mukaan Eurocities-verkoston tapaamisiin, joissa on käsitelty tietosuojaa ja kansalaisten digitaalisia oikeuksia. Tietosuojavastaava osallistui tammikuussa 2018 Brysselissä järjestettyyn riskienhallintatyöpajaan, josta pystyi ammentamaan oppia Espooseen sekä saamaan perspektiiviä muualla EU-alueella tapahtuvaan tietosuojatyöhön. Kapealla otannalla voidaan todeta, että Pohjoismaat ja Keski-Eurooppa ovat tällä saralla eturintamassa.

Koska Espoo on siirtämässä ICT-palveluitaan vahvasti pilvipalveluympäristöön, toteutettiin tietoturvapäällikön johdolla benchmarking-matka Haagin kaupunkiin Hollantiin. Haag on Espoota muutaman askeleen edellä siirtymän suhteen, ja matkalta saatiinkin arvokasta oppia erityisesti siitä, miten viestintään ja koulutukseen kannattaa panostaa, kun uutta teknologiaa otetaan käyttöön. Opit otettiin välittömästi käyttöön Espoon omassa työtilaprojektissa.

5.10 Ydintietojen hallinta

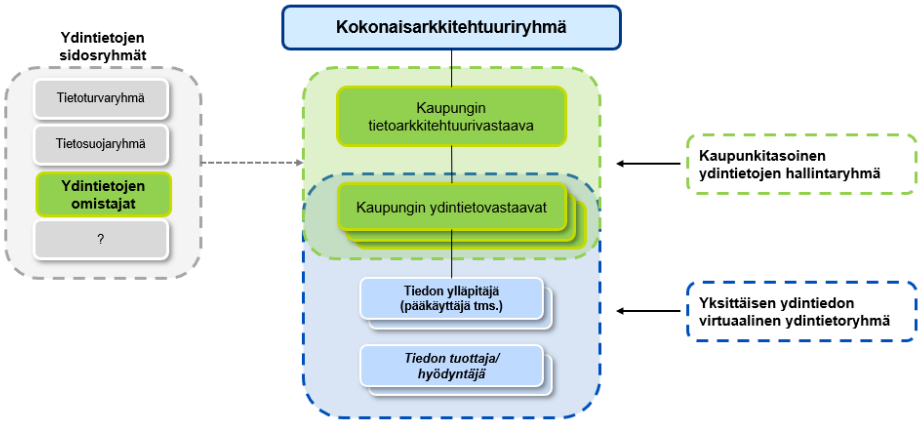
Kaupungissa aloitettiin ydintietojen mallinnus ja hallintamallin kehittäminen vuonna 2018. Ydintiedoilla tarkoitetaan sellaisia yhteisiä tietoja, joita hyödynnetään useissa eri järjestelmissä ja nykytilassa näitä tietoja myös ylläpidetään hajautetusti. Tavoitetilassa ydintiedot sijaitsevat tunnistetuissa lähdejärjestelmissä (masterjärjestelmät) ja tiedon sisältö sekä tiedon rakenne on määritelty. Tavoitetilassa lähdejärjestelmiä hyödynnetään tehokkaasti integroimalla, jolloin ajantasainen ja laadukas tieto on hyödynnettävissä kaupungin toimintoja tukevissa järjestelmissä.

Tunnistetut ydintiedot mallinnuksen ensimmäisessä vaiheessa ovat:

Tarkoituksena on laajentaa mallintamista myös toimialojen spesifeihin tietoihin, joka tarkoittaa kuvassa mainittujen tietojen kuvantamista, erityisesti asiakkuustietojen osalta. Nämä toimenpiteet edistävät jatkossa laadukkaan tiedon hyödyntämistä analytiikassa.

Ydintietojen ajantasaisuus ja niiden tehokas hyödyntäminen vaatii hallintamallin. Hallintamallia kehitetään edelleen vuosina 2019 – 2020. Tavoitteena on saattaa ydintietojen hallinta osaksi kokonaisarkkitehtuurityötä ja järjestelmien kehittämistä. Ydintietojen rakenteista ja lähdejärjestelmien tunnistamisesta vastaavat ydintietojen omistajat ja ydintietovastuuhenkilöt yhdessä järjestelmien pääkäyttäjien kanssa. Näitä mainittuja ydintietojen omistajuuksia ja uusia rooleja on kaupungissa jo tunnistettu kevään 2019 aikana. Alla luonnosteltua ydintietojen hallintamallia, johon vielä mahdollisesti vaikuttaa tiedonhallintalain asettamat velvoitteet. Ydintietojen hallintamalli saatetaan ensin osaksi kokonaisarkkitehtuurin hallintamallia ja periaatteita, myöhemmin mahdollisesti tiedonhallintamallia tai muuta vastaavaa mallia, jota tiedonhallintalaki tiedonhallintayksiköiltä edellyttää.

Kuvassa hallintamallin luonnostelua ja uusia tunnistettuja rooleja:



5.11 Hack with Espoo -hakkerointikurssi

Espoossa toteutettiin vuoden 2018 loppupuolella Suomessa ainutlaatuinen, lukiolaisille suunnattu eettisen hakkeroinnin kurssi. Kurssi toteutettiin yhteistyössä Second Nature Securityn sekä muiden yritysten ja viranomaisten kanssa, ja sillä opetettiin paitsi hakkerointiin liittyvien työkalujen käyttöä, myös siihen liittyvää etiikkaa. Koulutusvaiheen jälkeen lukiolaisille annettiin mahdollisuus testata kaupungin tietojärjestelmiä.

Kurssin aikana nuoret raportoivat testatusta tietojärjestelmästä yhteensä 7 eri puutetta, joista viisi liittyi palvelun käytettävyyteen ja kaksi tietoturvallisuuteen. Poikkeamien raportoinnin lisäksi kaupunki on hyötynyt kurssista myös muuten. Yleisesti kurssin näkyvyys on lisännyt organisaatiomme tietoisuutta ja ehkä kiinnostustakin tietoturvallisuuden ilmiöihin. Tietoisuuden lisääntyminen tarkoittaa, että asioita huomioidaan entistä paremmin, myös tiedostamattomalla tasolla.

Maailma ja teknologia muuttuvat entistä nopeammin ja myös meidän julkishallinnossa on pystyttävä siihen vastaamaan. Tämä tarkoittaa, että tarvitsemme myös turvallisuuden takaamiseksi ketterämpiä ja rohkeampia toimintatapoja. Tämän tyyppisen kurssin toteuttaminen toimii myös tässä eli madaltaa kynnystä kokeilla ja tehdä asioita uudella tavalla.

Hack with Espoo kurssi järjestetään myös vuonna 2019. Tänä vuonna kurssille pääsee opiskelijoita niin Espoon lukioista kuin Omnian ammatillisesta koulutuksestakin. Kurssin vaikutuspiirissä on noin 10000 nuorta.

5.12 TAISTO18-harjoitus

Kaupunki edellyttää sopimuskumppaneiltaan eri tasoisia varautumiseen ja jatkuvuuteen liittyviä suunnitelmia sekä niiden harjoittelua. Lisäksi kaupunki harjoittelee ja kehittää itse kykyään reagoida ja hallita eritasoisia poikkeamia ja häiriöitä. Vuonna 2018 Espoon kaupunki osallistui yhteen suurempaan tietotutuvaan ja tietosuojaan liittyvään harjoituskokonaisuuteen, Väestörekisterikeskuksen fasilitoimaan Taisto 18 – harjoitukseen.

Espoon kaupungin tarkennetut tavoitteet harjoituksessa olivat tietoturvapoikkeaman hallinta, testata ja kehittää poikkeamaprosessia koko organisaation kattavaksi sekä harjoitella toimintaa tilanteessa, jossa kaupunkiin on kohdistunut laaja henkilötietojen tietoturvaloukkaus. Harjoitukseen osallistui noin 30 henkeä kaupungin keskeisistä toiminnoista, tietohallinnosta, tietoturva- ja tietosuojaryhmistä sekä kaikilta toimialoita sekä kaikki keskeiset palveluntarjoajat, jotka osallistuvat poikkeamien hallintaan.

Harjoituksen havainnot ovat viety kehittämiskohteiksi ja niiden toteuttaminen on vastuutettu. Kaupunki kehittää harjoitustoimintaansa ja on päättänyt osallistua Taisto 19 harjoitukseen, mikäli sellainen järjestetään. Tämän lisäksi on tarkoitus harjoitella pienemmissä kokonaisuuksissa.

6 Arviointi ja mittarit

6.1 Keskeisiä tuloksia vuodelta 2018

Vuoden 2018 onnistumisiksi voidaan nostaa seuraavat toimenpiteet:

- **EU:n tietosuoja-asetuksen toimeenpanoprojektin läpivienti**
  - Projekti saatiin maaliin sovitun aikataulun mukaisesti, täytti sille asetetut tavoitteet ja pysyi alkuperäisen budjetin raameissa
  - Projektin puitteissa järjestettiin kymmeniä koulutuksia eri kohderyhmille. Läsnäolokoulutuksiin tai webinaareihin osallistui arviolta 2500 työntekijää.
  - Projektissa luotiin yhteensä 13 eri tasoista tietosuojaohjetta sekä muutamia lomakepohjia.
  - Projektissa luotiin raamit tietosuojaryhmän toiminnalle.

- **Hack with Espoo -hakkerointikurssi**
  - Lukiolaisten hakkerointikurssi oli ainutlaatuinen jopa maailman mittakaavassa ja se sai runsaasti positiivista huomiota mediassa. Konsepti herätti kiinnostusta valtionhallinnosta, kuntasektorilta, yliopistoista ja yrityspuolelta.
  - Kurssin toteutus oli malliesimerkki uudenlaisen yhteistyön mahdollisuuksista. Se oli kaupunkitasolla poikkihallinnollinen projekti, johon osallistuivat tietoturvapäällikkö, tietohallinto ja sivistystoimen toimiala. Lisäksi kurssin toteutukseen osallistui espoolainen 2NS-kyberturvallisuusyritys.
  - Kurssin avulla kyettiin lisäämään tietoturvatietoisuutta uudella, ei niin paperinmakuisella, tavalla.

- **Tietoisuuden lisääminen**
  - Espoon kaupungilla työskentelee yli 14 000 työntekijää hyvin erilaisissa rooleissa. Lisäksi toimialat ovat itsenäisiä ja niiden tehtävät ja tiedonkäsittely poikkeavat toisistaan merkittävästi. Tietoturva ja tietosuoja ovat edelleen tukitehtäviä, vaikka niiden merkitys on korostunut. Niillä mahdollistetaan turvallinen, luotettava ja lainmukainen toiminta. Koska resursseja on vajavaisesti, ne on käytettävä järkevästi. Kenties kustannustehokkain keino on lisätä työntekijöiden tietoisuutta oikeista toimintatavoista sekä tietoturvan ja tietosuojan uhkaympäristöstä. Miten arkityössä kannattaa toimia järkevästi ja minimoida riskit? Jos moka sattuu, miten tulee reagoida?
  - Kuluvan vuoden aikana on kyetty lisäämään kaupungin henkilöstön tietoisuutta tietoturvasta ja tietosuojasta. Tekemistä riittää silti edelleen paljon, sillä myös uhkaympäristö muuttuu nopeasti nopeasyklisessä maailmassa. Tietoisuutta voidaan lisätä monella tapaa. Kaupungilla on järjestetty paljon koulutuksia aihealueisiin liittyen. Lisäksi sekä tietoturvapäällikkö että tietosuojavastaava ovat pitäneet omaa säännöllisesti päivittyvää blogiaan kaupungin intranetissä.
  - Tietosuojavastaava teki kuukausikatsaus videoita tietosuoja-asetuksen toimeenpanoprojektin aikana.
  - Tietoturvapäällikkö ja tietosuojavastaava käynnistyvät digitaaliseen turvallisuuteen keskittyvän Suojatie-podcastin syksyllä 2018. Podcastiin kutsutaan myös kaupungin ulkopuolisia vieraita
  - Toimialojen tietosuojan ja tietoturvan yhdyshenkilöt ovat viestineet aktiivisesti omilla vastuualueillaan tietoturvasta ja tietosuojasta johdolle ja henkilöstölle.

- **Tilannekuvan parantaminen**
  - Tietoa tarvitaan päätöksenteon tueksi, todellisuuden ymmärtämiseen ja toimintaympäristön hahmottamiseen. Tällöin voidaan ennakoida tulevaa, arvioida potentiaalisia skenaarioita ja kohdistaa resursseja järkevästi. Tämän kaiken mahdollistamiseksi on alettu keräämään dataa tietoturvan ja tietosuojan tilannekuvan luomiseksi. Tämä tapahtuu edelleen manuaalisesti eikä saatavilla oleva data ole välttämättä laadultaan parasta mahdollista. Asiat kehittyvät kuitenkin askel askeleelta oikeaan suuntaan, kunhan päämäärä on olemassa.
  - Tietoturva- ja tietosuojapoikkeamia ryhdyttiin systemaattisesti tilastoimaan vuoden 2018 alusta. Tilastoinnin avulla pystytään arvioimaan uhkaympäristöä sekä kohdistamaan koulutusta sitä vaativiin kohteisiin. Lisäksi kyetään arvioimaan poikkeamien selvittelyn viemää työaikaa.
  - Tietoturva- ja tietosuojakoulutukset tilastoidaan systemaattisesti ja niistä pyritään keräämään aktiivisesti palautetta, johon myös reagoidaan.
  - Tietotilinpäätöksen tiedonkeruu on kelpo esimerkki tilannekuvan parantamiseen tähtäävistä toimista. Toimialat ovat koostaneet tiiviin raportin, jossa on vastattu 20:een tietosuojavastaavaan esittämään kysymykseen. Samalla toimialat voivat antaa palautetta tietosuojatyön onnistumisesta.
  - Tietoturvapäällikkö ja tietosuojavastaava pyrkivät aktiivisesti seuramaan regulaatiokehitystä ja uhkatrendejä niin kansallisesti kuin globaalisti osallistumalla yhteistyöverkostoihin kuntapuolella ja valtionhallinnossa.

6.2 Rekisteröityjen oikeuksien toteuttaminen

Espoon kaupunki kerää ja käsittelee asiakkaidensa henkilötietoja vain siinä määrin kuin se on tarpeellista palvelun tuottamiseksi. Henkilötietoja käsitellään rekisterin käyttötarkoituksen mukaan. Rekistereistä on laadittu EU:n yleisen tietosuoja-asetuksen mukaiset tietosuojaselosteet. Asiakkaalla on oikeus tietää, mitä tietoja hänestä kerätään. Jos tiedoissa on virheitä tai tiedot ovat epätarkkoja, asiakas voi vaatia niiden oikaisemista.

Jos tiedonkeruu perustuu suostumukseen, asiakas voi milloin tahansa peruuttaa antamansa suostumuksen ja vaatia tietojensa poistamista. Kaupungin palveluista suurin osa perustuu kuitenkin lakisääteisen velvoitteen noudattamiseen tai julkisen vallan käyttämiseen tai yleisen edun toteuttamiseen (usein mm. arkistointi, tilastointi, kehittämishankkeet). Asiakas ei voi niihin liittyvissä tapauksissa vaatia tietojensa poistamista.

Keväällä 2018, tietosuoja-asetuksen soveltamispäivämäärän 25.5.2018 lähestyessä, mediassa rummutettiin vahvasti kahta asetuksen tuomaa elementtiä: 1) sanktioriskiä ja 2) organisaation asiakkaiden tietopyyntötsunamia. Jälkimmäisellä viitataan tietosuoja-asetuksen mukaisiin tietopyyntöihin, joissa asiakas haluaa saada itselleen kaikki hänestä organisaation keräämät tiedot. Kumpikaan elementeistä ei ole toteutunut Suomessa ainakaan vielä. Ei ole tiedossa, että yhteenkään organisaatioon olisi kohdistunut tietopyyntötsunami pelotteluista huolimatta.

Espoossa kaupunkitasoinen tietopyyntöprosessi luotiin tietosuoja-asetuksen toimeenpanoprojektissa. Sosiaali- ja terveystoimen toimialalla on oma vakiintunut prosessinsa tietopyynnöille. Toimialalla tietopyyntöjen volyymit ovat olleet suuria jo ennen tietosuoja-asetusta, ja trendi näyttää jatkuvan.

Tällä hetkellä tietopyyntöprosessi toimii ainoastaan fyysisessä maailmassa, mutta sähköisen ratkaisun käyttöönottoa suunnitellaan vuoden 2019 aikana. Sähköinen ratkaisu ei ole vielä

käytössä asiakkaan luotettavaan tunnistamiseen liittyvien haasteiden takia. Tietopyynnön voi toimittaa joko 1) postitse tietosuojaselosteessa mainitulle yhteyshenkilölle osoitettuna tai 2) asioimalla henkilökohtaisesti asiointipisteessä tai kirjaamossa, jossa tarkistetaan henkilöllisyys. Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin kirjaamosta tai asiointipisteestä. Tiedot voidaan toimittaa hänelle myös postitse.

Paperimaailman tietopyyntöprosessiin liittyy tiettyjä tietosuoja- ja tietoturvariskejä, sillä hyvinkin sensitiivistä tietoa voidaan joutua lähettämään kaupungin sisällä kirjepostissa. Tämä on tunnistettu yhdeksi kehittämiskohteeksi.

Tietopyyntöjen tilastointi aloitettiin 25.5.2018. Tilastoinnissa on tärkeää huomioida, että aina ei ole selvää, onko kyseessä tietosuoja-asetuksen vai julkisuuslain mukainen tietopyyntö. Vuoden loppuun mennessä pyyntöjä on saapunut seuraavasti:

- Sosiaali- ja terveystoimi
  - esimiesten tai asiakkaiden pyynnöstä tehdyt lokiselvitykset 104
  - tarkastuspyynnöt arviolta 1400
- Muut toimialat
  - tietosuoja-asetuksen mukaiset tietopyynnöt yhteensä 30
  - julkisuuslain mukaiset tietopyynnöt 200

Luvuista voi päätellä, että lähes kaikki tietopyynnöt lähetetään sosiaali- ja terveystoimen toimialalle. Vaikka muilla toimialoilla pyyntömäärät ovat olleet arvioitua pienempiä, on pyynnöillä usein merkittävä työllistävä vaikutus, sillä tiedon etsiminen ja tulostaminen vanhoista tietojärjestelmistä ja paperiarkistoista on vaivalloista.

6.3 Poikkeamien hallinta

Tietoturvapoikkeamat voidaan jakaa karkeasti kahteen kategoriaan:

- Muut kuin henkilötietoihin kohdistuvat tietoturvapoikkeamat
- Henkilötietoihin kohdistuvat tietoturvapoikkeamat

Jälkimmäinen kategoria on tietosuoja-asetuksen piirissä. Ilmoitusvelvollisuus valvontaviranomaiselle ja rekisteröidyille on uusi velvollisuus organisaatioille. Suomessa henkilötietoihin kohdistuvia tietoturvaloukkauksia raportoitiin vuonna 2018 arviolta 2000. EU-tasolla luku on 50 000, ja maiden välillä on suuria eroja.[9] Mikäli henkilötietojen tietoturvaloukkauksesta saattaa aiheutua riskejä rekisteröityjen oikeuksille ja vapauksille, siitä on ilmoitettava tietosuojavaltuutetun toimistoon. Ilmoitus on tehtävä ilman aiheetonta viivytystä 72 tunnin sisällä siitä, kun tietoturvaloukkaus on havaittu.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava suoraan rekisteröidylle silloin, kun loukkaus aiheuttaa todennäköisesti korkean riskien rekisteröityjen oikeuksille ja vapauksille. Ilmoitus on tehtävä viipymättä, kunhan tapahtuman kannalta keskeiset asiat on selvitetty ja riskiä arvioitu.

Henkilötietojen tietoturvaloukkausten arviointiin on käytettävä harkintaa, varovaisuuttaa ja maalaisjärkeä. Tietosuojavaltuutetun toimisto ei ole linjannut tarkkaan millaisista loukkauksista pitää ilmoittaa ja vastaavasti millaisia loukkauksia ei tarvitse ilmoittaa heille. Vastuu arvioinnista jätetään organisaatiolle itselleen, joten riskienhallintaprossin täytyy toimia. Ennen ilmoituksen

[9] DLA Piper GDPR data breach survey: February 2019.

tekemistä on tehtävä aina perusteellinen riskiarvio tietoturvaloukkauksesta. Muuten vaarana on, että ylireagoidaan ja myös matalan riskin loukkaukset raportoidaan valvontaviranomaiselle.

Epäilyn tai havainnon tehneen työntekijän ei tule itse ilmoittaa epäilystään asiakkaalle tai julkisuuteen. Tietosuojaloukkauksen vaikutukset voisivat merkittävästi pahentua, jos uteliaat osaisivat alkaa etsiä loukkauksen kohteina olleita henkilötietoja.

Tietosuojaprojektissa laadittiin *Henkilötietojen tietoturvaloukkausten käsittelyohje*. Ohjeesta tiedotettiin intranetin etusivulla. Lisäksi intranetissä on ohjeistettu poikkeamien ilmoittamisesta, oli kyse sitten tietosuoja- tai tietoturvapoikkeamasta. Tietosuojaprojektin jäsenet viestivät poikkeamaprosessista omilla vastuualueillaan. Poikkeamaprosessista on muistutettu tietosuojakoulutusten yhteydessä. Poikkeamien käsittelystä kerrotaan esimieskoulutusten yhteydessä.

6.4 Osaamisen seuranta ja kehittäminen

Tietosuoja-asetuksen toimeenpanoprojektin yksi keskeinen tavoite oli parantaa kaupungin henkilöstön tietosuojaosaamista. Henkilöstön osaamisen seuranta ja kehittäminen on avainasemassa, sillä globaalisti on arvioitu, että 50 % tietoturvapoikkeamista johtuu inhimillisistä virheistä. Koulutuksilla ja tietoisuuden lisäämisellä voidaan kustannustehokkaasti vähentää tällaisia poikkeamia. Johdon ja esimiesten esimerkillisellä toiminnalla on myös merkittävä vaikutus.

Viime kädessä tietosuojasta vastaa kaupungin johto. Vastuukysymykset on määritelty kaupungin hallintosäännössä, tietoturva- ja tietosuojapolitiikassa sekä toimintaohjeissa. Kaupunginjohtaja vastaa kaupunkikonsernin sisäisen valvonnan ja riskienhallinnan mukaan lukien tietosuojan järjestämisestä asianmukaisella tavalla. Toimialajohtaja vastaa toimialan sisäisen valvonnan ja riskienhallinnan mukaan lukien tietosuojan järjestämisestä asianmukaisella tavalla. Henkilöstö vastaa omalta osaltaan ohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi tietoturvapäällikölle, tietosuojavastaavalle tai omalle esimiehelleen. Jokaisella on vastuu omaan tehtäväänsä liittyvän tietosuojan toteuttamisesta sekä tiedon ja tietojärjestelmien asianmukaisesta käytöstä.

Jokaiselle kaupungin työntekijälle lähetettiin henkilökohtainen linkki Arjen tietosuoja -koulutukseen, jossa työntekijä velvoitettiin katsomaan puolituntinen video sekä vastaamaan kymmeneen monivalintakysymykseen. Puutteellisesta viestinnästä ja toisaalta vähäisten raportointitoimintojen vuoksi suoritusprosentti jäi alhaiseksi, joskin yksikköjen ja toimialojen suoritusprosenteissa oli huomattavia eroja. Tulosten pohjalta päätettiin, että kaupungille hankitaan vuonna 2019 tietoturvan ja tietosuojan verkkokoulutussovellus, joka sisältäisi räätälöityjä osioita eri kohderyhmille ja mahdollistaisi älykkään raportoinnin.

Jokaiselle uudelle esimiehelle tarjottiin puolituntinen tietosuojakoulutus esimiehen perehdytyskoulutuksen yhteydessä tietosuojavastaavan toimesta. Vuonna 2019 koulutus viedään verkko-oppimisalustalle. Lisäksi Missä, mennään, Espoo -perehdytyspäivään sisältyy tietoturva- ja tietosuojaosio. Tietosuojavastaava ja tietoturvapäällikkö järjestävät puolivuosittain kaupunkitasoisen tietoturva- ja tietosuojakoulutuksen, jossa hyödynnetään myös ulkopuolisia asiantuntijoita.

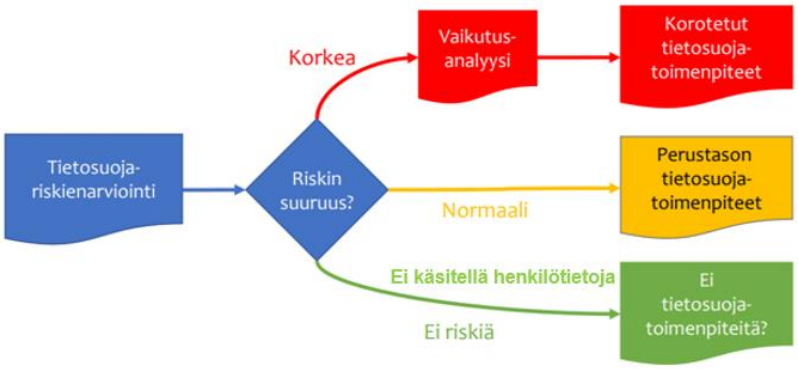
Koulutusten systemaattinen tilastointi on aloitettu vuoden 2018 alusta. Tietosuojaprojektin läsnäolokoulutuksiin tai webinaareihin osallistui arviolta 2500 työntekijää. Osa koulutuksista oli yleisluonteisia, osa taas oli kohdistettu tietyille avainryhmille.

6.5 Tietosuojan riskiarvioinnit

Espoon kaupunkikonsernin riskienhallintapolitiikka määrittää kaupungin tahtotilan riskienhallinnan tavoitteista, periaatteista ja käytännön toteuttamisesta. Tietosuoja-asetuksen lähtökohta on riskiperusteinen lähestymistapa. Käytännössä tämä tarkoittaa sitä, että organisaation on systemaattisesti kartoitettava sen henkilötietojen käsittelyyn kohdistuvat riskit, erityisesti korkean riskin kohteet, pyrittävä minimoimaan niitä ja arvioitava niitä säännöllisesti. Tällöin pienen riskin henkilötietojen käsittelyyn ei kohdisteta ylimitoitettuja toimenpiteitä, ja toisin päin. Esimerkiksi yhteystietoluettelon suojausvaatimukset ovat erilaiset kuin potilastietojärjestelmän. Tavoitteena on, että riskipohjaisen lähestymisen avulla tietosuojaan liittyvät velvoitteet ja suojaustoimet räätälöidään Espoon kaupungilla aina kyseiseen henkilötietojen käsittelyyn liittyvien ja havaittujen riskien pohjalta.

Tietosuojan kontekstissa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja, esimerkiksi syrjintää, identiteettivarkautta tai petosta. Rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyys ja vakavuus on määriteltävä tietojenkäsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan.

Tietosuoja-asetuksen kokonaan uusi riskienarviointivelvoite organisaatioille on tietosuojan vaikutustenarviointi eli DPIA (Data Protection Impact Assessment). Se on tehtävä, kun henkilötietojen käsittelyyn kohdistuu todennäköisesti korkea riski. Tyypillisiä esimerkkejä ovat uuden teknologian kuten tekoälyn hyödyntäminen ja terveysdatan käyttö.



Kuva: Tietosuoja-riskienarviointi Espoossa

Vaikutustenarvioinneille laadittiin oma prosessi tietosuojaprojektissa. Projekti laati määrämuotoisen lomakkeen vaikutustenarvioinneille sekä ohjeistuksen. Lisäksi Projektisalkkujärjestelmään rakennettiin automaattiset askelmerkit tietosuojan riittävälle huomioimiselle. Prosessi jalkautettiin ja se toteutuu varsin hyvin uusien järjestelmien ja palvelujen kohdalla.

Vuonna 2018 tietosuojan vaikutustenarviointeja tehtiin yhteensä 14. Koska kyseessä on kokonaan uusi prosessi ja vaatimus, toimintatapaa muokataan kokemusten, palautteen ja

viranomaisohjeistuksen perusteella. Ajoittain myös kohteen määrittely ja rajaaminen aiheuttavat haasteita. Vaikutustenarvioinneissa tunnistettiin seuraavia riskejä:

- laajat käyttöoikeudet tarpeeseen nähden
- lainsäädännön monitulkintaisuus, jolloin tietojen yhdistämistä ja data-analytiikkaa ei ole mahdollista toteuttaa
- käyttäjien ohjeistaminen on puutteellista, jolloin he voivat syöttää liikaa tietoa järjestelmään
- tiedon tallentuminen pilvipalveluympäristöön ja läpinäkyvyyteen liittyvät ongelmat, esim. kuka pääsee tietoon käsiksi

Vaikutustenarvioinnit tehtiin työpajoissa, joihin osallistui yleensä:

- toimialan lakimies
- substanssiasiantuntija
- tekninen asiantuntija
- palveluntuottajan edustaja
- tietosuojavastaava

Työpajoilla kyetään lisäämään tietoisuutta tietosuojan ja tietoturvan tärkeydestä, potentiaalisista riskeistä ja yleensäkin riskilähtöisestä ajattelutavasta.

Tietoriskien (sisältäen tietosuoja- ja tietoturvariskit) hallinnan kehittämiseen panostetaan kaupungilla vuoden 2019 aikana. Vastuu kehittämisestä on sekä tietosuoja- että tietoturvaryhmillä. Tällä hetkellä tietoriskien hallinta toteutuu parhaiten sivistystoimen toimialalla, jossa se on vastuutettu tietoriskienhallinnan suunnittelijalle. Tavoitteena on, että parempaa tilannekuvaa rakennettaan keräämällä yksiköiltä vuosittaiset riskiarviot.

6.6 Auditoinnit

Tietoturvaan ja tietosuojaan liittyviä tarkastuksia eli auditointeja voidaan toteuttaa monella eri tasolla ja menetelmällä. Espoossa arviointitavoiksi on määritelty muun muassa sisäinen arviointi, joka on Espoon tietoturvahenkilöstön tai asiantuntijoiden toteuttama, sisäinen tarkastus, joka on Espoon oma järjestelmällinen ja riippumaton tarkastus, sekä ulkoinen arviointi, jonka toteuttaa kaupunkiorganisaation ulkopuolinen ja riippumaton toimija. Tarkastuskohteesta ja laajuudesta riippuen tarkastuksissa käytetään soveltuvaa viitekehystä.

Tietojärjestelmiin kohdistetut ulkoiset tarkastukset keskitettiin vuonna 2018 henkilötiedon käsittelyn kannalta oleellisiin järjestelmiin. Vuodesta 2019 alkaen järjestelmiä tarkastetaan niiden kriittisyyden, vaikuttavuuden ja tietosisällön arkaluonteisuuden perusteella määritetyllä syklillä.

6.7 Todennetut kehittämiskohteet

Vuoden 2019 kehittämiskohteiksi on tunnistettu seuraavat osa-alueet:

- Henkilöstökoulutukset ja tietoisuuden kasvattaminen
    - Keskeisenä vuoden 2019 painopisteenä on henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.

- Lisätään yksilön tietoisuutta tietoturvasta ja tietosuojasta ja näin parannetaan asennetta ja käytöstä digiturvallisempaan suuntaan. Näin luodaan organisaatiossa uudenlaista toimintakulttuuria, ylläpidetään ja kehitetään olemassa olevien palveluiden turvallisuutta ja mahdollistetaan uutta teknologiaa hyödyntäviä palveluita.
- Tietoturvapäällikkö ja tietosuojavastaava osallistuvat Julkisen hallinnon digitaalisen turvallisuuden kehittämishankkeeseen (JUDO-hanke), jonka koordinoinnista vastaa Väestörekisterikeskus.

- Pilvipalvelujen tietoturvan parantaminen
  - Espoo on siirtänyt IT-infraansa laajemmin pilvipalveluratkaisuihin tavoitellen joustavuutta ja kustannustehokkuutta. Pilvipalvelujen käyttöön liittyy riskejä, jotka on tunnistettava ja minimoitava. Suomessa vuoden 2018 merkittävin kybermaailman uhkatekijä oli organisaatioihin kohdistettu sähköpostitilien tietojenkalastelu, jonka tarkoituksena oli saada haltuun työntekijöiden sähköpostitunnuksia. Microsoftin teettämässä tutkimuksessa arvioitiin, että yhden tietoturvapoikkeaman selvittäminen vie viisi henkilötyöpäivää.[10]
  - Vuonna 2019 henkilöstön tietoisuutta lisätään edelleen tietojenkalastelun riskeistä. Alkuvuodesta otetaan käyttöön uusia teknisiä tietoturvakontrolleja.
  - Panostetaan tiedon elinkaaren hallintaan. Tietosuoja-asetus edellyttää, että henkilötiedoilla on ns. minimisäilytysaika, joka tarkoittaa sitä, että tieto on poistettava, kun sille ei ole enää olemassa käyttötarkoitusta. Tietoa ei ole pakko hävittää vaan se voidaan myös anonymisoida.

- Tietoriskien hallinnan kehittäminen
  - Laaditaan tietosuojan vaikutustenarvioinnit kaikilla toimialoilla. Työ käynnistetään syksyllä 2019 ja saadaan valmiiksi vuoden 2020 aikana. Prosessi ja tarvittava ohjeistus laaditaan tietosuojaryhmässä.
  - Tietosuojavastaava ja tietoturvapäällikkö laativat toimintamallin yleisten tietoriskien kartoittamiseksi. Tavoitteena on saada parempaa tilannekuvaa tietoturvaan ja tietosuojaan liittyvistä riskeistä, jolloin niitä voidaan myös pienentää. Kevyt lähestymistapa on vuosittain toimialojen avainyksiköille täytettäväksi lähetettävä lomake.

- Tietoturvallisuuden hallintajärjestelmä ja tilannekuvan parantaminen
  - Espoossa on käynnissä isoja tietojärjestelmiin ja sähköisiin työympäristöihin liittyviä kehitys- tai muutosprojekteja, jotka valmistuvat vuoden 2019 aikana. Projektien yhteydessä kasvatetaan hallitusti kaupungin kyvykkyyksiä ennalta ehkäistä, havainnoida ja reagoida mahdollisiin tietoturvapoikkeamiin.
  - Uuden teknologian hyödyntäminen palveluiden ja turvallisuuden toteuttamisessa.

[10] A Forrester Total Economic Impact™ Study Commissioned By Microsoft October 2018.