Espoon kaupungin

TIETO-TILIN-PÄÄTÖS

2019

ESPOO
ESBO

SISÄLLYSLUETTELO

1 ESIPUHE

Moni julkishallinnon organisaatio on ryhtynyt julkaisemaan vuosittaisia tietotilinpäätöksiä. Tietotilinpäätös ei ole käsitteenä vakiintunut Suomessa. Kuntapuolella sillä on kuvattu tietosuojan toteutumista. Tällöin pitäisi paremminkin puhua tietosuojatietotilinpäätöksestä. Valtionhallinnossa tietotilinpäätöksen näkökulma on ollut tiedolla johtamisessa. Tietotilinpäätös voi olla johdolle tarkoitettu koontiraportti tai suurelle yleisölle osoitettu raportti luottamuksen lisäämiseksi.

Miksi Espoon kaupunki laatii vuosittain tietotilinpäätöksen? Kyseessä on 30-sivuinen raportti, jonka tekemiseen vaaditaan monen asiantuntijan työpanosta. **Tietotilinpäätöksellä rakennetaan luottamusta.** Tässä raportissa kerrotaan ylätasolla avoimesti henkilötietojen käsittelystä Espoossa ja toimenpiteistä, joilla turvataan kuntalaisten, omien työntekijöiden ja sidosryhmien kriittiset tiedot.

Tietosuojavaltuutettu suosittaa tietotilinpäätöksen laatimista osana osoitusvelvollisuuden toteuttamista. Pelkkä lainsäädännön noudattaminen ei riitä GDPR:n aikakaudella. Espoon on osoitettava dokumentaation ja raportoinnin keinoin, että sen toiminta täyttää GDPR:n vaatimukset. Tietotilinpäätöksen asema on merkittävä, vaikka sitä ei suoraan mainitakaan asetuksessa eikä kyseessä siten ole lakisääteinen dokumentti.

Tietotillinpäätös on työkalu kaupungin johdolle. Raportin avulla 1) kuvataan yhä nopeammin muuttuvaa toimintaympäristöä; 2) Espoon toimintaan vaikuttavia tunnistettuja tietoriskejä ja 3) toiminnan kehittämistä.

Tietoturvaa ja tietosuojaa voidaan kehittää oikeaan suuntaan jo oikealla asenteella, myönteisellä kulttuurilla ja tietoisuutta kasvattamalla. Työntekijän päivittäisillä valinnoilla ja henkilökohtaisella riskienhallinnalla on merkitystä. Tietotilinpäätöksellä halutaan lisätä niin henkilöstön kuin suuren yleisön tietoisuutta tietosuojasta ja tietoturvasta sekä tehdä näkyväksi näiden eteen tehtävää työtä.

Espoon toiminta on tietointensiivistä. Espoo korostaa tietotilinpäätöksessään vastuullisuutta tiedon käsittelemisessä. Espoo tarinan eli Espoon strategian hengessä tärkeintä on arjen sujuvoittaminen sekä asukas- ja asiakaslähtöisyys. Kun tietoturva ja tietosuoja pettävät, on tällä vaikutusta myös muihin yksilön oikeuksiin. Espoon tietotilinpäätöksen näkökulma on edelleen vahvasti tietosuojan ja tietoturvan toteuttamisessa, mutta tällä kertaa sen näkökulmaa on laajennettu enemmän tiedolla johtamiseen. Miten tieto näyttäytyy organisaation strategisena voimavarana? Miten Espoo hallitsee, hyödyntää ja johtaa tietoa erityisesti tietosuojan ja tietoturvan näkökulmasta? Näihin kysymyksiin tietotilinpäätös pyrkii antamaan vastauksen.

Aiemmin pelättiin, että Eurooppa jää teknologian, erityisesti tekoälyn, kehityksessä jälkeen Yhdysvalloista ja Kiinasta kuluttajien yksityisyyttä tiukemmin suojaavan lainsäädännön vuoksi. Nyt on alettu pohtimaan, voisiko GDPR:stä tulla globaali standardi, jota kannattaisi kopioida muualle. GDPR:n toimivuudesta on vielä liian aikaista tehdä johtopäätöksiä, mutta se on ainakin lisännyt tietoisuutta siitä, miten paljon meistä kerätään dataa verkkoympäristössä ja digivälineillä. Jopa eturivin artistit laulavat tietosuojan merkityksestä. Kuunnelkaapa JVG:n Netti ei unohda.

Espoo julkaisee tietotilinpäätöksestä kaksi erillistä versiota: 1) johdolle tarkoitetun sisäisen version ja 2) suuremmalle yleisölle tarkoitetun julkisen version, joka on saatavilla Espoon verkkosivuilla. Espoon kaupungin tietosuojaryhmä on vastannut pääosin tietotilinpäätöksen laadinnasta. Lisäksi Espoon kokonaisarkkitehtuuriryhmä on antanut oman panoksensa.

Toivoa herättäviä lukuhetkiä toivottaen,

Juho Nurmi
Espoon kaupungin tietosuojavastaava

Espoossa 20.3.2020

2 TIIVISTELMÄ

Espoo laatii vuosittain tietotilinpäätöksen tietosuojavastaavan 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.

Espoo otti käyttöön loppuvuodesta 2019 tietoturvan ja tietosuojan verkkokoulutuksen, jonka avulla jokainen kaupungin työntekijä käy läpi perusasiat. Verkkokoulutuksen avulla pienennetään tietoriskejä kustannustehokkaasti. Vuonna 2019 hieman yli puolet (53 %) havaituista henkilötietojen tietoturvaloukkauksista johtui työntekijän inhimillisestä virheestä. Verkkokoulutuksen jalkauttaminen jatkuu keväällä 2020.

EU:n tietosuoja-asetuksen (GDPR) soveltamisessa riittää edelleen työtä. Asetus on koettu vaikeaselkoiseksi ja monitulkintaiseksi. Tällä hetkellä ei ole täysin selvää, mitä GDPR:n puitteissa saa tehdä ja mitä ei saa tehdä. Erilaisten automatisointi- ja tekoälyratkaisujen yleistyessä tarvitaan mahdollisesti selkeämpää sääntelyä siitä, missä tapauksissa automatisoidut yksittäispäätökset ja profilointi ovat Suomessa sallittuja.

Myös Espoolla on tahtotila hyödyntää uutta teknologiaa ja tarjota kuntalaisille parempia ja kustannustehokkaita palveluita. Tämä työllistää tietosuojan ja tietoturvan asiantuntijoita. Luottamus on digitaalisissa palveluissa avainasemassa. Siitä on pidettävä kiinni kaikin keinoin. Riittävä tietosuoja on avainasemassa luottamuksen ylläpidossa.

Espoossa on panostettu tietosuojaa koskeviin vaikutustenarviointeihin läpi vuoden 2019. Vaatimustenmukainen työvaihe on onnistuttu jalkauttamaan projektiprosessiin, mutta tietoisuudessa ja osaamisessa on edelleen kehitettävää. Riskiperusteisella lähestymistavalla riskit kyetään tunnistamaan ennakolta, jolloin tietoturvakontrollit ovat linjassa riskitason kanssa. Vaikutustenarvioinnit ovat lisänneet riskitietoisuutta kokonaisvaltaisesti henkilöstön keskuudessa.

Pilvipalveluiden tietoturva oli pinnalla koko vuoden 2019. Kehittäminen jatkuu edelleen vuonna 2020. Pilvipalveluiden hallintaa, identiteetin hallintaa ja niiden käyttöön liittyviä vaatimuksia parannetaan.

Riittävä resursointi on keskiössä tietoturvan ja tietosuojan vaatimustenmukaisessa toteuttamisessa. Toimintojen erilaisuudesta ja laaja-alaisuudesta johtuen aikaa ei aina riitä pureutumaan toimialojen erityispiirteisiin tai niiden erityislainsäädännön ja toimintaympäristön asettamiin vaatimuksiin.

Tietosuojan kehittämiskohteiksi vuodelle 2020 tunnistettiin: 1) Verkkokoulutuksen jalkauttaminen; 2) Tietosuojan huomioiminen erilaisissa digikehitysprojekteissa; 3) Tietosuojan tilannekuvan selkiyttäminen ja 4) Tiedon elinkaaren hallinta.

Vaikka Espoon toimintaan ei ole kohdistunut todella kriittisiä tietoturvaloukkauksia vuonna 2019, on tärkeää tiedostaa, että loukkausten selvittäminen ja raportointi viranomaisille ja kuntalaisille vie omien asiantuntijoiden ja palveluntuottajien resursseja.

Avainluvut vuodelta 2019:

- 60 dokumentoitua henkilötietojen tietoturvaloukkausta
- 25 ilmoitusta tietosuojavaltuutetulle
- 25 ilmoitusta asiakkaille
- 20 toteutettua tietosuojan vaikutustenarviointia

Tarkempaa tietoa saat erityisesti tietotilinpäätöksen luvuista 6 ja 7.

3 YLEISKATSAUS JA TILANNEARVIO

3.1 Paluu tietotilinpäätökseen 2018

Espoon kaupunki (jatkossa Espoo) julkaisi historiansa ensimmäisen virallisen tietotilinpäätöksen huhti-toukokuussa 2019. Vuoden 2018 tietotilinpäätöksessä nostettiin esille neljä keskeistä kehittämiskohdetta. Kehittämiskohteiksi linjattiin: 1) tietoisuuden kasvattaminen; 2) pilvipalvelujen tietoturvan parantaminen; 3) tietoriskien hallinnan kehittäminen ja 4) tilannekuvan parantaminen. Seuraavaksi katsotaan pikaisesti, miten asiat ovat edistyneet Espoossa vuoden 2019 aikana.[1]

Henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen on avainasemassa minkä tahansa organisaation toiminnassa. Tämä pätee erityisesti Espooseen, jolla on hallussa valtavasti sensitiivistä dataa, jota järkevästi hyödyntämällä kuntalaisille kyetään tarjoamaan parempia palveluita ja toisaalta reagoimaan nopeasti vaikeasti ennustettavassa toimintaympäristössä. Espoo otti käyttöön loppuvuodesta 2019 tietoturvan ja tietosuojan verkkokoulutuksen, jonka avulla jokainen kaupungin työntekijä käy läpi digiturvan perusasiat Verkkokoulutuksen avulla pienennetään tietoriskejä kustannustehokkaasti. Verkkokoulutuksen jalkauttaminen jatkuu keväällä 2020.

Espoo ottaa enenevissä määrin eri tavoin pilvipalveluita hyödyntäviä ratkaisuja käyttöön, joten sen tietoturvan parantaminen nostettiin viime tilinpäätöksessä kehittämiskohteeksi. Pilvipalveluiden hallintaa, identiteetin hallintaa ja niiden käyttöön liittyviä vaatimuksia kehitetään edelleen.

1 Espoon kaupungin tietotilinpäätös 2018.

Riskiperusteinen lähestymistapa on hallitseva elementti tietosuoja-asetuksessa. Tämän vuoksi tietoriskien hallinnan kehittämiseen haluttiin panostaa aiempaa enemmän. Kun riskit on ennalta arvioitu ja niiden vaikutukset minimoitu, Espoo kykenee tekemään tietoon perustuvia päätöksiä, varmistamaan lainsäädännön vaatimusten noudattamisen ja säästämään kustannuksia. Tietoisuus tietosuojan vaikutustenarvioinnin tarpeellisuudesta henkilötietojen korkean riskin käsittelyssä on lisääntynyt. Näkemystä tukee arviointien kasvanut volyymi ja niiden laadun parantuminen. Vaikutustenarvioinnit ovat lisänneet riskitietoisuutta kokonaisvaltaisesti henkilöstön keskuudessa.

Tietoturvallisuuden kehittämisessä ja siihen liittyvissä investoinneissa on tärkeää huomioida tulevaisuuden kehityskulut. On tärkeää arvioida kokonaisvaltaisesti toimintaympäristöä, joka koostuu erilaisista teknologioista, prosesseista ja ihmisistä.

Tietoturvallisuuden hallintajärjestelmä ja tilannekuvan parantaminen nähtiin neljäntenä kehittämiskohteena. TTietoturvallisuutta kehitetään systemaattisesti vastaamaan sekä lainsäädännön että yleisen riskiympäristön vaatimuksia.

3.2 Regulaatioympäristö

3.2.1 EU:n tietosuoja-asetuksen vaikutukset

EU:n yleisen tietosuoja-asetuksen (jatkossa GDPR) soveltaminen aloitettiin koko EU-alueella kohta kaksi vuotta sitten 25.5.2018. Asetuksen toimivuudesta ei voi vielä tehdä merkittäviä johtopäätöksiä. Suomen soveltamiskokemuksista saa kattavan yhteenvedon oikeusministeriön (jatkossa OM) lausuntotiivistelmästä *EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa*. OM on kerännyt kokemuksia GDPR:n toimivuudesta syksyllä 2019. Kaikkiaan 75 organisaatiota antoi lausunnon. Mukana on sekä julkishallinnon että yksityisen sektorin toimijoita. Espoon kokemukset GDPR:n soveltamisesta eivät poikkea OM:n tiivistelmän hengestä.

GDPR on selkeästi lisännyt kansalaisten tietoisuutta. Yksityisyyden suojaan liittyvistä teemoista on kirjoitettu paljon myös Suomen mediassa, esimerkiksi

miten älypuhelinsovellukset keräävät käyttäjistä dataa, ja osittain tämän myötä ihmiset ovat aiempaa kiinnostuneimpia yksityisyydensuojastaan ja siitä, miten organisaatiot keräävät ja käsittelevät heidän tietojaan.

Kiinnostuksen lisääntyminen näkyy myös Espoon toiminnassa, mutta yleisesti Suomessa tietosuoja-asetuksen mukaisten tietopyyntöjen volyymi on ollut arvioitua pienempi julkishallinnossa. Tämä saattaa kertoa siitä, että Suomella on vankka asema luottamusyhteiskuntana ja kansalaiset luottavat viranomaisiin. Luottamus ei ole itsestään selvä asia, joten siitä on pidettävä kiinni kaikin keinoin. Riittävä tietosuoja on avainasemassa luottamuksen ylläpidossa.

OM:n tiivistelmän perusteella voidaan myös arvioida, että tietoisuus henkilötietojen käsittelyyn liittyvistä vaatimuksista on kasvanut merkittävästi suomalaisissa organisaatioissa. GDPR:n myötä tietosuoja on noussut konttorin perimmäisistä huoneista työntekijöiden arkikeskusteluun ja johtoryhmätasolle – ainakin kypsemmissä organisaatioissa.

GDPR on lisännyt läpinäkyvyyttä henkilötietojen käsittelystä. Organisaatiot kertovat asiakkaille läpinäkyvämmin henkilötietojen käsittelystä. Informoinnissa ja läpinäkyvyydessä on edelleen parantamisen varaa, sillä yleisesti tämä GDPR:n keskeinen velvoite hoidetaan tietosuojaselosteilla, joita ei ole kirjoitettu "kansan kielellä". Myöskään erityisryhmien tarpeita – esimerkiksi lasten – ei ole välttämättä huomioitu riittävällä tasolla.

Yrityssektorin osalta GDPR:n onnistumisiin voidaan laskea henkilötietojen käsittelyyn liittyvien käytäntöjen selkiyttäminen Euroopan sisämarkkinoilla. Koska lainsäädäntöä on harmonisoitu, yritysten on sujuvampaa operoida EU-alueella.

GDPR:n tavoitteena on parantaa kuluttajien yksityisyydensuojaa ja lisätä tätä kautta luottamusta digitaalisiin palveluihin. EU:n visioissa tämä synnyttäisi viime kädessä Eurooppaan varteenotettavia kilpailijoita amerikkalaisille ja kiinalaisille datajäteille, kun kuluttajat olisivat valmiita siirtämään datojaan kilpaileviin palveluihin. Hiljalleen on alettu jopa pohtia, voisiko GDPR:stä tulla globaali standardi, jota kannattaisi kopioida muualle. Esimerkiksi Kaliforniassa tuli voimaan 2020 alusta kuluttajien tietosuojaa koskeva laki. Sääntely antaa kuluttajille samankaltaisia parannettuja oikeuksia kuin GDPR.

GDPR:n soveltamisessa riittää edelleen runsaasti työtä. Asetus on koettu paikoin vaikeaselkoiseksi ja monitulkintaiseksi. Erilaisten automatisointi- ja tekoälyratkaisujen yleistyessä tarvitaan mahdollisesti selkeämpää sääntelyä siitä, missä tapauksissa automatisoidut yksittäispäätökset ja profilointi ovat Suomessa sallittuja. Kansallista henkilötietojen käsittelyä koskevaa sääntelyä sisältyy lukuisiin eri lakeihin, ja tästä johtuva tietosuojalainsäädännön pirstaleisuus aiheuttaa suurta epätietoisuutta kulloinkin sovellettavasta lainsäädännöstä ja lakien etusijajärjestyksestä.[2]

Mikä toimii?	Missä on parannettavaa?

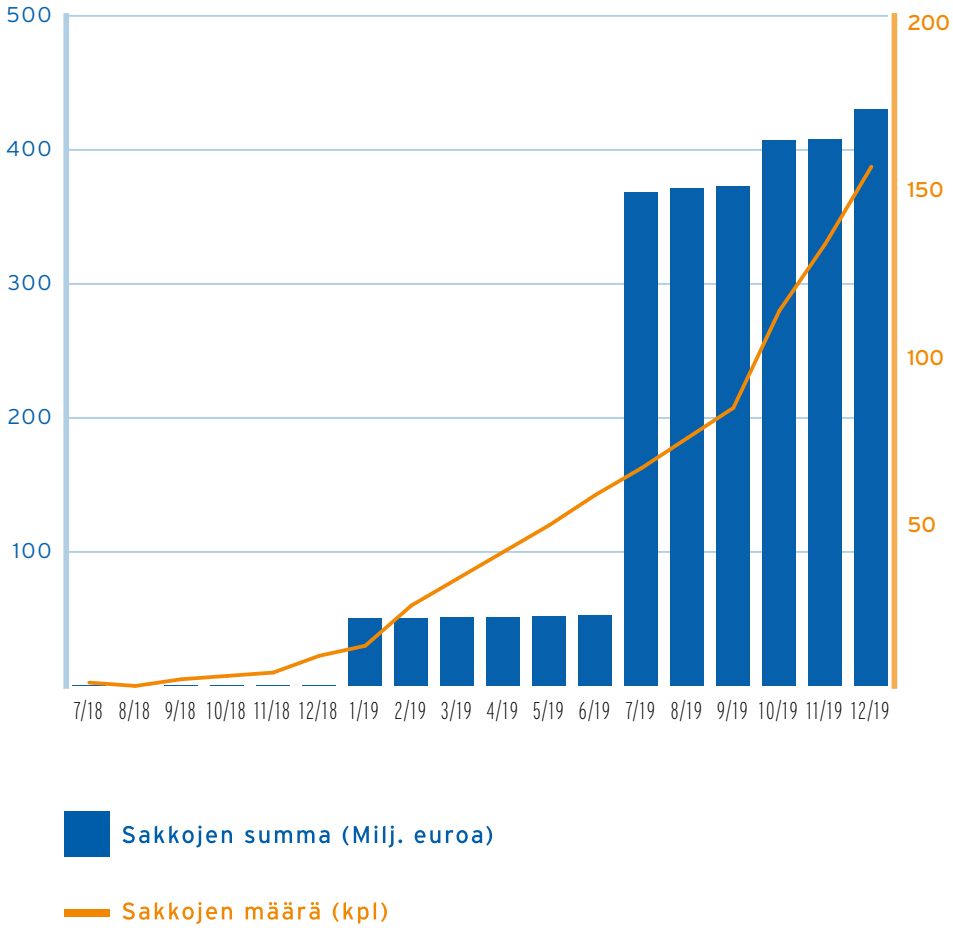
• Lisännyt tietoisuutta
  ◦ Kansalaiset
  ◦ Organisaatiot
• Lisännyt läpinäkyvyyttä
• Selkeyttänyt käytäntöjä Euroopan sisämarkkinoilla
• Osoitusvelvollisuus
• Ihmislähtöinen datatalous
	• Vaikeaselkoinen
	• Tulkinnanvarainen
	• Osoitusvelvollisuus
	• Tietosuojalainsäädännön pirstaleisuus
	• Valvovan viranomaisen resurssit

Kuva: GDPR:n vaikutukset Suomessa

Vaikka GDPR:n yhteydessä puhuttiin paljon sakoista keväällä 2018, ei valvontaviranomainen ole antanut Suomessa toistaiseksi ainuttakaan (tilanne 17.3.2020). Tilanne on hyvin erilainen EU:n tasolla, jossa sakkojen kokonaismäärä oli vuoden 2019 loppuun mennessä 430 miljoonaa euroa. Summa koostuu 147 tapauksesta. Suurimmassa osassa on annettu pieniä sakkoja. Suurin sakko on British Airwaysin riittämättömästä tietoturvasta Iso-Britan-

2 EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa: Lausuntotiivistelmä.

niassa saama 205 miljoonan euron sakko. Toistaiseksi Suomi ja Viro ovat ainoita maita, joissa sakkoja ei ole vielä annettu.[3] Suomessa viranomaiset eivät voi saada sakkoja, mutta joissakin EU-maissa tämä on mahdollista.



Kuva: GDPR-sakot 31.12.2019 mennessä (lähde: enforcementtracker.com)

3 enforcementtracker.com

3.2.2 Toisiolain soveltaminen

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019), eli toisiolaki, astui voimaan 1.5.2019. Laissa on useita siirtymäsäännöksiä. Lain tarkoituksena on mahdollistaa henkilötietojen tehokas ja tietoturvallinen käsittely ja lisäksi turvata yksilön luottamuksensuoja sekä oikeudet ja vapaudet henkilötietoja käsiteltäessä.

Laissa säädetään sosiaali- ja terveydenhuollon toiminnassa sekä sosiaali- ja terveysalan ohjaus-, valvonta-, tutkimus- ja tilastotarkoituksessa tallennettujen henkilötietojen käsittelystä tilastointiin, tieteelliseen tutkimukseen, kehittämis- ja innovaatiotoimintaan, opetukseen, tietojohtamiseen, sosiaali- ja terveydenhuollon viranomaisohjaukseen ja -valvontaan sekä viranomaisen suunnittelu- ja selvitystehtävään. Osa käsittelyperusteista on lainsäädännön näkökulmasta uusia, kuten tietojohtaminen sekä kehittämis- ja innovaatiotoiminta.

Toisiolaissa on keskitetty useiden rekisterinpitäjien henkilötietoihin kohdistuvien tietolupahakemusten käsittely kansalliselle tietolupaviranomaiselle Findatalle. Findata käsittelee tietolupahakemukset myös silloin, kun rekisteritiedot ovat peräisin yksityisiltä sosiaali- ja terveydenhuollon palvelunjärjestäjiltä taikka kyse on Kantapalveluihin tallennetuista tiedoista. Lakimuutoksen tavoitteena on sujuvoittaa ja nopeuttaa tietolupiin liittyvää käsittelyä ja keventää siihen liittyvää, rinnakkaisista lupamenettelyistä aiheutuvaa hallinnollista taakkaa. Siirtymäsäännösten vuoksi Findata ryhtyy käsittelemään tietolupahakemuksia 1.4.2020 alkaen. Toisiolaissa säädetään myös tietopyyntöjen hallintajärjestelmästä ja tietoturvallisesta käyttöpalvelusta, jonka kautta tietoja voidaan luovuttaa ja vastaanottaa.

3.2.3 Tekoälyn hyödyntäminen

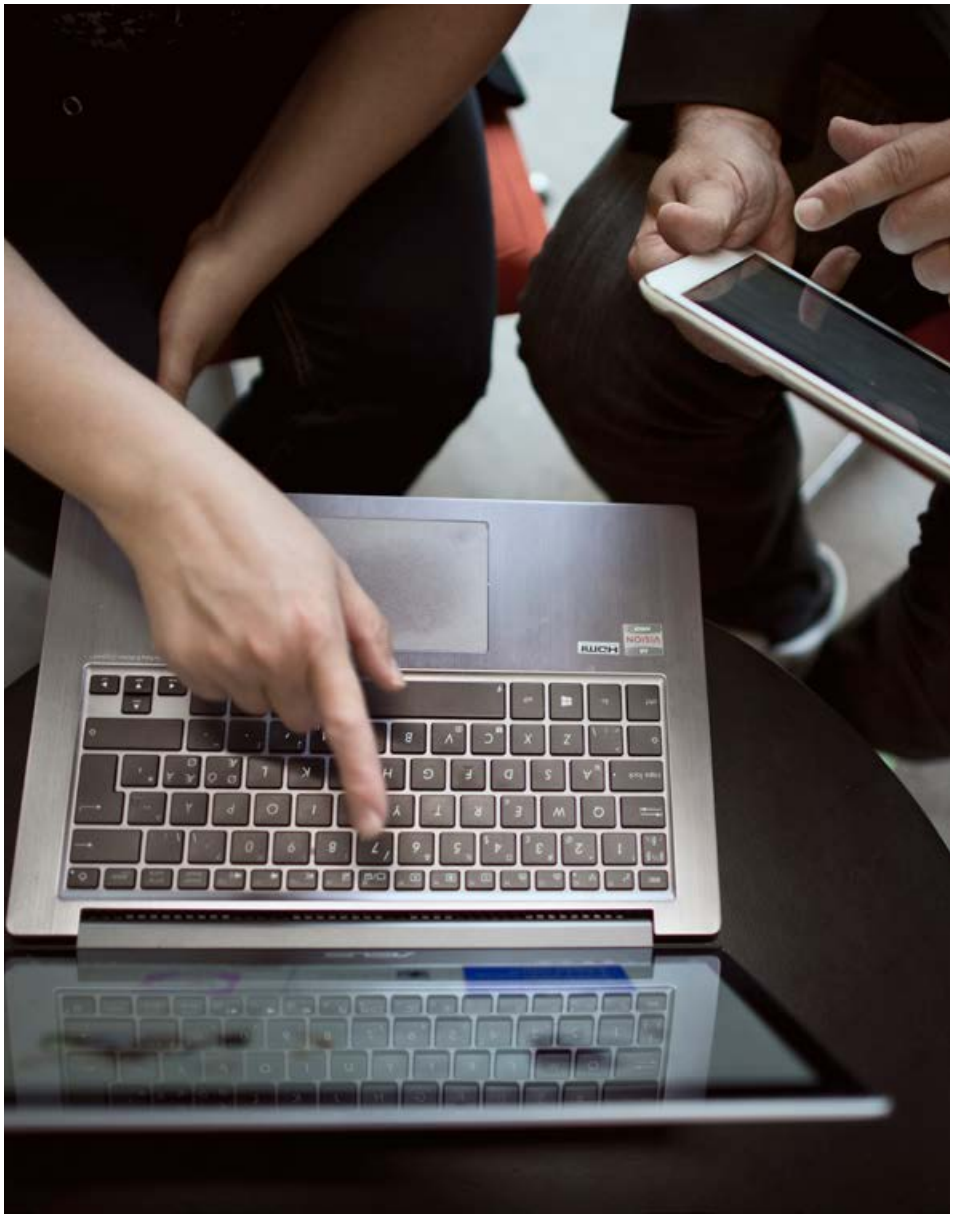
Mediassa on puhuttu vuonna 2019 runsaasti tekoälyn mahdollisuuksista ja uhkakuvista. Keskustelu on ollut ajoittain hyvinkin mustavalkoista. Kärjistetysti voisi todeta, että joko tekoäly ratkaisee kaikki vähintäänkin rutiineihin liittyvät työn tekemisen haasteet tai kansalaisista tulee valvontayhteiskunnan

orjia. Ymmärrettävästi on olemassa myös harmaita sävyjä. Ylipäänsä on tärkeää, että tekoälystä keskustellaan.

Yksityisyydensuojan näkökulmasta tekoälyn hyödyntämiseen liittyy riskejä, jotka pitää tunnistaa ja minimoida ennen sovellusten käyttöönottoa. Tekoälyn eettisyys herättää keskustelua. Tekoälyllä voidaan tehdä paljon pahaa, mutta myös hyvää. Tällä hetkellä ei ole täysin selvää, mitä saa GDPR:n puitteissa tehdä ja mitä ei saa tehdä. On vaadittu, että EU:n tasolla pitäisi olla GDPR:n lisäksi muuta tekoälyä koskevaa regulaatiota. Suomessa ei ole tekoälylakia, joka säätelisi nimenomaisesti tekoälyä. Toisaalta jo tällä hetkellä GDPR:n vaatimukset on huomioitava tekoälyn kehittämisessä. Asetus kieltää päätöksenteon, joka on yksinomaan automaattista tiettyjä poikkeuksia lukuun ottamatta. Sovellukset on myös suunniteltava siten, että niiden tekemien päätösten logiikka on helposti selitettävissä.[4]

Hallitusohjelmassa pyritään edistämään hallinnon ja koko yhteiskunnan digitalisaatiota. Siinä mainitaan erikseen lainmuutokset, joilla edistetään tekoälyn hyödyntämistä sosiaaliturvaetuuksien hakemisessa, käsittelyssä ja päätöksissä. Oikeusministeriössä on selvitetty viranomaisten automaattiseen päätöksentekoon liittyviä keskeisiä oikeudellisia kysymyksiä. Esiselvityksessä on pyritty täsmentämään hallinnon lainalaisuusperiaatteen, hyvän hallinnon periaatteiden, oikeusturvan, julkisuuden, läpinäkyvyyden, virkavastuun sekä tietosuojan toteutumisen edellytyksiä automaattisessa päätöksenteossa. Nyt tehdyn esiselvityksen pohjalta kartoitetaan julkisen hallinnon automaattisiin päätöksentekomenettelyihin liittyviä sääntelytarpeita.[5]

Tietosuojavaltuutetun toimisto on arvioinut toimintakertomuksessaan 2018 tietosuojan trendejä vuodelle 2019. Arviossa todetaan, että uudet teknologiat haastavat edelleen tietosuojan. Uusista teknologioista mainitaan erikseen kasvojentunnistus.[6] Ruotsissa valvontaviranomainen antoi 26 000 euron sakon Skellefteån kaupungin koululle kasvojentunnistusjärjestelmän käyttöönotosta. Järjestelmällä pyrittiin seuraamaan oppilaiden läsnäoloa



4 Blogi: Eettistä vai laillista tekoälyä? Mika Viljanen
5 Automaattiseen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeet: Esiselvitys.
6 Tietosuojavaltuutetun toimintakertomus 2018.

oppitunneilla. Sakko perustui siihen, ettei järjestelmän käyttöönotossa ollut tehty tietosuojan vaikutustenarviointia. Lisäksi tiedon käsittelyn minimointi ei toteutunut ja suostumus käsittelyperusteena katsottiin ongelmalliseksi. Suostumuksen tulisi perustua aitoon vapaaehtoisuuteen, mutta tämä ei toteutunut kasvojentunnistuksessa.[7]

Kasvojentunnistusteknologia on kehittynyt ja kaupallistunut valtavin harppauksin, eikä lainsäädäntö ole pysynyt perässä. Lisäksi teknologian luotettavuus on herättänyt epäluuloja. Se ei välttämättä kohtele kaikkia väestöryhmiä tasavertaisesti. Kasvojentunnistusteknologiasta on merkittävää hyötyä rikostorjunnassa, mutta sitä voidaan käyttää yksityisyyttä loukkaaviin ja muutoin vahingollisiin tarkoituksiin kuten kansalaisten massaseurantaan. Nämä dystooppiset uhkakuvat ovat toteutuneet Kiinassa. Euroopan komissio suunnittelee kieltävänsä viideksi vuodeksi kasvojentunnistusohjelmien käytön julkisilla paikoilla. Komissio näkee, että viiden vuoden aikalisä tuo asiantuntijoille ja poliitikoille aikaa laittaa tietosuojasääntelyn kuntoon.[8]

3.3 Megatrendit

Megatrendeillä tarkoitetaan ison mittakaavan kehityskulkuja. Tällä hetkellä digitalisaatio, alustatalous, regulaatio ja ihmisten muuttuvat tarpeet muuttavat nopeasti kaupungin toimintaympäristöä. Tieto- ja kyberturvallisuuteen eniten vaikuttavat megatrendit ovat teknologian murros sekä kaupungistuminen. Maailman poliittiset valtasuhteet ja jännitteet heijastuvat myös teknologia-aloille. Toimivat tietoliikenne- ja viestintäjärjestelmät ovat digitaalisessa maailmassa tärkeä osa yhteiskunnan perusinfrastruktuuria, mutta ne eivät ole riippumattomia poliittisista ideologioista, kansallisvaltioiden päämääristä tai kaupallisista intresseistä.

Venäjä on pidemmän aikaa valmistellut tilannetta, jossa se voisi irrottautua tarvittaessa globaaleista tietoverkoista ja internetistä. Sen tavoitteena on, reitittää 95 prosenttia internet-liikenteestään paikallisesti jo vuoden 2020 loppuun mennessä. Ensimmäiset kokeilut irrottautumisesta on tehty vuoden 2019 aikana. Runet nimellä kulkeva Venäjän oma verkko mahdollistaisi Venäjän riippumattomuuden ja toimintakyvyn globaalin verkon häiriötilanteissa.

Yhdysvaltain kauppaministeriö asetti toukokuussa 2019 kiinalaisen Huawein mustalle listalle, joka tarkoitti sitä, että yhdysvaltalaiset yhtiöt eivät saa tehdä sen kanssa yhteistyötä tai ostaa sen tuotteita. Huawei on yksi maailman suurimmista verkkolaitteiden valmistajista. Luottamuspulan perusteena on pelko siitä, että Huawei vakoilee kiinan hallituksen hyväksi. Syksyllä 2019 Yhdysvallat aikoi estää Adoben ohjelmistojen käytön Venezuelassa. Vuosi 2019 tullaankin muistamaan siitä, että suurvallat ovat ottaneet teknologiayhtiöt oman ulkopolitiikkansa välineiksi.

Teknologian käyttö painostuksen välineenä herättää kysymyksen myös kaupallisten ohjelmistojen käyttövarmuudesta. Tilauspohjaisissa ohjelmistoissa käyttölisenssi tarkistetaan ohjelmaa käynnistettäessä. Tämä antaa ohjelmistotoimittajalle periaatteessa mahdollisuuden estää ohjelman toiminta koska tahansa. Teknologiayhtiöiden käyttäminen osana talouspakotteita tai vallankäyttöä saattaa myös johtaa tilanteeseen, jossa amerikkalaisyhtiöiden merkitys vähenee muun maailman alkaessa etsiä vaihtoehtoja.

7 How to interpret Sweden's first GDPR fine on facial recognition in school. IAPP 27.8.2019.
8 Julkisilla paikoilla tapahtuva kasvojentunnistus aiotaan kieltää väliaikaisesti. HS 22.1.2020.

4 TIEDONHALLINTA

4.1 Tiedonhallintalain toimeenpano

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.[9]

Tiedonhallintamallin laatimiselle on vuoden siirtymäaika eli tiedonhallintamalli tulee olla kuvattuna 31.12.2020 mennessä. Tämä tarkoittaa kaupungin toimintaympäristön kuvaamista (palvelut ja prosessit), toiminnassa syntyvien tietoaineistojen tunnistamista ja kuvaamista, muodostuvien tietovarantojen tunnistamista ja kuvaamista, tietojärjestelmien kuvaamista sekä toimintaympäristön tietoturvallisuustoimenpiteiden dokumentointia. Laissa asetetaan myös vaatimuksia tietoaineistojen digitalisoimiseksi siirtymäajalla, integraatioiden ja katseluyhteyksien rakentamiseksi sekä tietoturvallisuustoimenpiteiden kehittämiseksi siirtymäajoin aina vuoden 2023 loppuun asti.

4.2 Kokonaisarkkitehtuurityö

Käytännössä tiedonhallintalain velvoitteet kytkeytyvät Espoon kaupungissa olemassa olevaan kokonaisarkkitehtuurityöhön, joka on toiminnan, tiedonhallinnan ja tietoteknologian systemaattista kehittämistä kaupungin strategian eli Espoo-tarinan mukaiseen suuntaan. Siinä huomioidaan kaupungin organisaatio kokonaisuutena sidosryhmineen.

Kaupungin tiedonhallinnassa kokonaisarkkitehtuuri luo näkyvyyttä siihen, mitä on, ja siihen, mitä kaikkea tavoiteltuja uudistuksia suunnitellessa tulisi ottaa huomioon. Se mahdollistaa strategisen kehittämisen, luo yhteentoimivuutta tietojärjestelmien ja organisaation osien välille, auttaa varmistamaan tietoturvan ja tietosuojan toteutumista, sekä tukee kaupungin toimialoja ja yksiköitä heidän omassa kehittämistyössään.

Espoossa tiedonhallintaa toteutetaan osana jo toimivaa kokonaisarkkitehtuurityötä. Tiedonhallinnalle ei siis järjestetä toimeenpanon aikana omaa hallinnollista yksikköä vaan työtä tehdään kaupunkitasoisesti verkostona. Kokonaisarkkitehtuurityö ja siihen liittyvät kuvaukset ja menetelmät kattavat suurelta osin lain velvoittaman tiedonhallintamallin sisällön. Toimeenpanon työ on lähinnä koota yhteen kaupungin eri toiminnoissa olevia tietoja ja kuvauksia sekä päättää yhteisesti niiden keskitetty sijainti ja tavat ylläpitää sisältö ajantasaisena. Näitä kuvauksia on laadittu mm. palvelusalkkuun, tietojärjestelmäsalkkuun ja muihin erilaisiin kokonaisarkkitehtuurin kuvaustyökaluihin. Lain edellyttämä muutosvaikutusten arviointimenettely tehdään osana kokonaisarkkitehtuurityötä. Vuoden 2020 aikana päivitetään kokonaisarkkitehtuurin käsittelyn dokumentointi vastaamaan muutosvaikutusten arviointia ja tiedonhallintamallin ylläpitoa.

4.2.1 Toiminta-arkkitehtuurityö

Tiedonhallintamalliin kuvattava tiedonhallintayksikön eli kaupungin toimintaympäristö on toiminta-arkkitehtuuriin lukeutuvaa kuvausta. Toiminta-arkkitehtuurikuvauksiin liittyy asiakkaat, palvelut, palveluja tuottavat prosessit ja niihin liittyvät sidosryhmät.

Johdon toiminta-arkkitehtuurikuvaukset ovat liiketoimintamallikuvauksia, joissa kuvataan (liike)toiminnan strateginen iso kuva ja toiminnan suorituskykyyn vaikuttavat kyvykkyydet sekä ylätason prosessit. Operatiivisen toiminnan kuvaustaso on tarkemmalla tasolla sisältäen liiketoimintamallia yksityiskohtaisempia palvelu- ja prosessikuvauksia. Toiminta-arkkitehtuuri on kokonaisarkkitehtuurin ydin: organisaatiossa olevat tiedot ja järjestelmät tulevat kaupungin toimintaa ja palveluja. Kaupungin prosesseissa tapahtuvilla muutoksilla on usein vaikutuksia toiminnassa hyödynnettäviin tietoihin, tietovarantoihin ja tietojärjestelmiin. Siksi on tärkeää tunnistaa toiminnan

9 Tiedonhallintalain täytäntöönpano. Valtiovarainministeriö.

nykytilan prosessit ja niihin kytkeytyvät tiedot ja järjestelmät, jotta muutoksen aiheuttamat vaikutukset voidaan arvioida ja saattaa hallitusti toimintaan. 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 tietoturvallinen toimintaympäristö.

4.2.2 Ydintietojen hallinta ja tietoarkkitehtuurityö

Ydintietojen hallinnan tavoitteena on, että kerran tallennettu tieto on ajan tasalla ja saatavilla kaikkialla, missä sitä tarvitaan. Ydintiedoilla tarkoitetaan kaupungin toiminnan keskeisiä kohteita (esim. asiakkaat, palvelut, tilat) kuvaavaa tietoa, jota hyödynnetään useissa toiminnoissa ja eri tietojärjestelmissä läpi kaupungin toiminnan. Ydintietojen hallinta on tiedonhallinnan laadun kehittämistä. Laadukas, jäsennelty, käyttökelpoinen, ajantasainen ja saatavilla oleva tieto mahdollistaa tietojen laajemman hyödynnettävyyden tiedolla johtamisessa.

Ydintietojen hallinta on osa kokonaisarkkitehtuuriin kuuluvaa tietoarkkitehtuurin kokonaisuutta. Ydintietojen hallinta on pitkäjänteistä työtä, jonka tulokset näkyvät parantuneena toiminnan tehokkuutena ja parempana koettuna palvelun laatuna etenkin digitaalisessa asiakasrajapinnassa joidenkin vuosien aikajänteellä. Espoossa toteutettiin kaupunkitasoisten ydintietojen kartoitus vuonna 2018. Vuoden 2019 aikana samassa yhteydessä laadittu kaupunkiyhteisten ydintietojen hallintamalli jalkautettiin käyttöön. Ydintietojen hallinta jatkuu kunkin ydintietoalueen osalta tietoisuuden lisäämisellä tiedonhallinnan laadun merkityksestä, kehittämistarpeiden tunnistamisella sekä kehittämistoimenpiteillä.

4.2.3 ICT-arkkitehtuurityö

ICT-arkkitehtuuri (ICTA) on toimintamalli Espoon kaupungin kokonaisarkkitehtuurityön tietojärjestelmä- ja teknologianäkökulmien tarkentamiseen ja jalkauttamiseen, jota toteuttaa Espoon kaupungin tietohallinto. ICTA-toiminto tekee kokonaisarkkitehtuuriryhmän kanssa aktiivista yhteistyötä kaupungin strategisten tavoitteiden edistämiseksi.

ICTA-hallinta vastaa ICT-teknisten ratkaisujen ja teknologioiden yhteentoimivuudesta, tarkoituksenmukaisuudesta, muunneltavuudesta ja tehokkuudesta huomioiden kaupungin toimialojen tarpeet, kokonaisarkkitehtuurin tavoitteet ja periaatteet sekä kaupungin olemassa olevan ICT-ympäristön vaatimukset. ICTA-ryhmä vastaa ICT-ratkaisujen teknologiavalinnoista sekä siitä, että ne noudattavat teknisten linjausten toteutumista.

Mitä iloa ICTA-hallinnasta on?

- Kaikki ICTA-näkökulmat katetaan asiaankuuluvalla roolituksella ja organisoitumisella
- Vältytään turhilta / päällekkäisiltä ICT-hankinnoilta ja parannetaan laatua
- Helpotetaan ICT-hankintojen läpivientiä ja ICT-kehitysprojektien sujuvuutta
- Tarjotaan tukea, työkaluja ja arviointia ICT-kehitysprojekteille ja -hankinnoille

ICTA-hallinnan ja -työn tuloksena Espoon kaupungilla on vuoden 2019 aikana määritelty, kuvattu ja osin käyttöönotettu esim. seuraavia ICTA-ratkaisuita:

- Integraatioarkkitehtuurin kuvaaminen sekä keskitetysti hallittu integraatioalusta, joka tukee yhtenäistä tiedon jakelua ja välitystä tietoturva ja tietosuoja huomioiden.
- Analytiikan arkkitehtuurin kuvaaminen sekä keskitetty analytiikkaratkaisu, joka mahdollistaa osaltaan tiedolla johtamisen teknisen alustan avulla.
- Järjestelmäarkkitehtuurin kuvaaminen sekä kuvaamistyökalun (Järjestelmäsalkku) kehittäminen, jolla toteutetaan tiedonhallintalain asettamia velvoitteita tietojärjestelmien välisten tietovirtojen, siirtotapojen ja järjestelmäarkkitehtuurin kuvaamisen osalta.
- ICTA-linjaukset ml. integraatioiden, analytiikan ja teknisen tietoturvan linjaukset
- ICTA-hallinnan kytkeminen Espoon kaupungin projektimalliin ja projektinhallintatyökaluun.

4.3 Tiedolla johtaminen

Kaupungin johtaminen voidaan nähdä asiakkuuksien hallinnan, palvelujen järjestämisen ja palvelujen tuottamisen muodostamana kokonaisuutena. Johtamisen tavoitteena on kuntalain mukaisesti edistää asukkaiden hyvinvointia ja alueen elinvoimaa sekä järjestää asukkaille palvelut taloudellisesti, sosiaalisesti ja ympäristöllisesti kestävällä tavalla. Kaupungin toiminta on tänä päivänä monien muiden organisaatioiden tavoin tietointensiivistä. Tiedolla johtaminen tarkoittaa kaupungin tietovarantojen ja prosessien valjastamista päätöksenteon tueksi. Oleellista tässä on toiminnan kannalta tärkeän tiedon tunnistaminen sekä sen analysoiminen ja jakaminen kaupungin eri organisaatioyksiköiden päätöksenteon kannalta keskeisille päätöksentekijöille oikeaan aikaan.

Espoossa tiedolla johtamista kehitetään Johtamisen ja talousohjauksen järjestelmäuudistuksessa. Uudistuksen tavoitteena on tukea asukas- ja asiakaslähtöisen Espoo-tarinan tavoitteiden toimeenpanoa uudistamalla johtamisen ja talousohjauksen tieto- ja toimintamalleja, prosesseja ja tietojärjestelmäkokonaisuutta.

Tiedolla johtamisen kehittämiseksi Espoossa on vuoden 2019 aikana luotu tekninen valmius edistyneiden analytiikkaratkaisujen toteuttamiseksi sekä suunniteltu tätä tukeva toimintamalli. Tämä Saaga-nimellä kutsuttu analytiikka-alusta mahdollistaa mm. koneoppimisen ja tekoälyn hyödyntämisen. Analytiikkaratkaisuja voidaan toteuttaa esimerkiksi kiinteistöjen mittausdatan analysointiin, asiakaspalautteiden ohjaamiseen, oppimisen analytiikkaan tai tekoälyhankkeisiin yhdessä muiden kumppanien kanssa. Saaga-alusta mahdollistaa kaupungin eri toiminnoille yhteisen data- ja analytiikkaympäristön kehittämisen ja ylläpidon. Samalla myös analytiikkaan liittyvät tietosuoja- ja tietoturvakysymykset pystytään ratkaisemaan hallitusti. Analytiikka-alustan mahdollistamia hyötyjä ovat tiedon keräämisen ja käsittelyn automatisointi, tarkemman ja kattavamman tiedon saaminen päätöksenteon tueksi aikaisemmin vaiheessa, sekä uuden ymmärryksen luominen suurten tietomassojen analysoinnin kautta.

5 ESPOOSEEN KOHDISTUVAT TIETORISKIT

5.1 Keskeiset riskit ja uhat

Modernisoituva yhteiskunta, erilaisten digitaalisten järjestelmien yhä laaja-alaisempi käyttö, vanhojen toiminnallisuuksien muuttuminen digitaaliseksi sekä tiedon hyödyntämisen ja jalostamisen lisääntyminen ja kehittyminen laajentavat tieto- ja kyberturvallisuuteen liittyvää uhkaympäristöä. Tiedon luotettavuus vaarantuu, jos ulkopuoliset tahot pääsevät käsiksi tietoon, johon heillä ei tulisi olla pääsyä. Tiedon eheys vaarantuu, jos tieto voi muuttua joko teknisen virheen takia tai ihmisen aiheuttamana, eikä paikkansa pitävyyteen voida luottaa. Tiedon saatavuus vaarantuu, jos tieto ei ole tarvitsijoiden saatavilla tarvittavana aikana. Kyberuhkat voivat kohdistua myös fyysiseen maailmaan, jos kybermenetelmillä kyetään vaikuttamaan järjestelmien toimintaan ja aiheuttamaan fyysistä tuhoa. Kyberuhka ei ole kohdeorganisaatioille erillinen, tekninen ilmiö, vaan sillä voi olla merkittäviä vaikutuksia organisaation ydintoimintaan.

Espoon uhkaympäristö noudattelee globaaleja trendejä. Henkilöstöön kohdistuu huijauksia, joilla yritetään varastaa käyttäjätunnuksia, joita hyödynnettäisiin edelleen petoksiin tai laajempiin hyökkäyksiin. Lisäksi huijarit ja tietojenkalastelijat voivat päästä organisaation tietojärjestelmiin ja hyötyä varastamistaan tiedoista. Osa huijauksista on hyvin uskottavia ja hyvin kohdennettuja, ja ne voivat toteutuessaan aiheuttaa tuntuvia taloudellisia tappioita.

On huomioitava, että hyökkääjä pyrkii käyttämään tavoitteensa saavuttamiseksi sopivinta haavoittuvuutta. Edellisissä kappaleissa olleissa esimerkeissä hyödynnettäisiin ihmisissä (kalastelu) ja prosesseissa (esim. laskutushuijaus) olevia haavoittuvuuksia. Tietoverkkojen kautta tapahtuvissa rikoksissa tai rikoksen yrityksissä ei siis aina pyritä ohittamaan teknistä suojatoimenpidettä, vaan vaikuttamaan tilanteenmukaisesti otollisimpaan haavoittuvuuteen, jolloin tekniset suojakeinot eivät välttämättä toimi.

5.2 Verkkopalveluympäristöt ja muut ICT-palvelut

Tietohallinto tuottaa kaupungin toiminnalle välttämättömiä infrapalveluja, kaupungin yhteisiä palveluja sekä toimiala- ja/tai tulosyksikkökohtaisia palveluja. Infrapalveluihin kuuluvat: loppukäyttäjäpalvelut, tietoliikennepalvelut, palvelin- ja kapasiteettipalvelut sekä käyttäjähallinta.

Espoossa käytettävät tietojärjestelmät luokitellaan niiden vaikuttavuuden ja vaativuuden perusteella ABCD-luokituksen mukaisesti:

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 kuvastaa tietojärjestelmien suhdetta prosessien kriittisyyteen jatkuvuuden hallinnan näkökulmasta. Kaupunki käyttää paljon ulkoistettuja palveluja palvelutuotannossaan sekä erilaisten pilviteknologioitten hyödyntäminen on kasvanut. Pilvipalveluihin siirryttäessä riskienhallinnan merkitys korostuu.

5.3 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 samalla tavalla joka tasolle.

5.4 Hankinnat ja palveluostot

Espoo toimii käytännössä aina rekisterinpitäjänä hankinnoissa. Harvoissa tapauksissa Espoo voi toimia henkilötietojen käsittelijänä tai kyse on yhteisrekisterinpitäjyydestä (GDPR 26 artikla), jossa osapuolet määrittelevät yhdessä käsittelyn tarkoitukset ja keinot. Hankinnoissa on myös tunnistettu tapauksia, joissa kumpikin osapuoli on itsenäinen rekisterinpitäjä. Tällöin kyse on henkilötietojen luovutuksesta Espoolta toiselle rekisterinpitäjälle, ei siirrosta. Hankinta voi myös sisältää useita käsittelytoimenpiteitä ja käyttötarkoituksia. Kumppani voi toimia saman palvelukokonaisuuden osalta sekä henkilötietojen käsittelijänä että rekisterinpitäjänä. Pilvipalveluhankinnoissa kuvioon liittyy usein alihankkijoita, jotka voivat toimia molemmissa rooleissa.

Roolien määrittely on tietosuojan ydintä ja ensiarvoisen tärkeää, jotta tiedetään kuka vastaa tietosuojasääntöjen noudattamisesta ja miten rekisteröidyt voivat käytännössä käyttää oikeuksiaan. Roolit ja näistä johtuvien tietosuojavelvoitteiden toteuttaminen voivat vaikuttaa merkittävästi hankinnan kohteen lopulliseen hintaan.

Espoossa toteutettiin mittava sopimusten päivitysurakka GDPR:n toimeenpanoprojektin yhteydessä 2017- 2018. Koska sopimusmassa oli valtaisa, projektissa valittiin riskiperusteinen lähestymistapa. Sopimuksen arvo ja tiedon kriittisyys vaikuttivat sopimusten päivittämisen priorisointiin.

6 TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTUMINEN

6.1 EU:n tietosuoja-asetuksen soveltaminen

Espoossa GDPR on lisännyt niin henkilökunnan kuin kuntalaisten tietoisuutta omista oikeuksistaan ja tietosuojan vaatimustenmukaisuudesta. Henkilöstön tietoisuuden parantaminen erityisesti koulutukseen panostamalla on tärkeässä roolissa. Globaali trendi on, että yli 50 % tietosuojaan ja tietoturvaan liittyvistä poikkeamista johtuu työntekijän inhimillisestä virheestä. Hyvänä esimerkkinä voidaan mainita kalasteluviestit, joilla pyritään manipuloimaan käyttäjää. Ilkeät hakkerit eivät hakkeroi niinkään tietojärjestelmiä vaan ihmisiä.

Tietosuojavaltuutetun toimisto mainitsi 28.1.2020 järjestetyssä Tietosuoja-päivä-tapahtumassa, että valvovan viranomaisen tarkastustoiminta painottuu seuraaviin kokonaisuuksiin:

1. osoitusvelvollisuuden toteuttaminen
2. tietosuojaa koskevat vaikutustenarvioinnit
3. heikossa asemassa olevien tietosuoja
4. kasvojentunnistusteknologia

Espoossa on panostettu tietosuojaa koskeviin vaikutustenarviointeihin läpi vuoden 2019. Koska kyseessä on ollut kokonaan uusi prosessi, sen jalkauttaminen on edellyttänyt kokeilemista ja jatkuvaa kehittämistä, esimerkiksi mikä on oikea kokoonpano työpajoissa. Vaatimustenmukainen työvaihe on onnistuttu jalkauttamaan projektiprosessiin, mutta tietoisuudessa ja osaamisessa on edelleen kehitettävää. Riskiperusteisella lähestymistavalla mahdolliset riskit kyetään minimoimaan proaktiivisesti, jolloin tietoturvakontrollit ovat linjassa riskitason kanssa.

Tietosuojaryhmä oin viestinyt erityisesti velvollisuudesta ilmoittaa henkilötietoja koskeva tietoturvaloukkaus. Suuresta ja monikerroksisesta organisaatiosta huolimatta ilmoitusprosessi on jalkautettu onnistuneesti Espoossa, mutta asian tärkeydestä viestiminen vaati vielä ponnistuksia.

GDPR:n perusasiat ovat edelleen pinnalla. Kuka on rekisterinpitäjä ja kuka käsittelijä? Mikä on henkilötietoa? Miten vastuista sovitaan? Espoossa tehdään runsaasti erilaisia digikokeiluja startup-yritysten kanssa. Näissä tapauksissa keskusteluun on noussut henkilötietojen käsittelyperuste. Missä määrin viranomaistoiminnassa voidaan käyttää suostumusta käsittelyperusteena? Yleensä suostumus ei viranomaistoiminnassa ole pätevä peruste käsitellä henkilötietoja. Käsittelyn tulee perustua lakisääteisen tehtävän toteuttamiseen tai tietosuojalain 4 §:n 1 momentin 2 kohtaan (käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi). On kuitenkin tunnistettu tilanteita, joissa henkilötietojen käsittely ei ole välttämätöntä viranomaisen lakisääteisen tehtävän hoitamiseksi, mutta tietyn palvelun tuottaminen ei ole mahdollista ilman henkilötietojen käsittelyä.

Toinen linjausta kaipaava asia on tietosuojariskien tunnistamisen tarpeellisuus esimerkiksi etukäteen täytettävän kysymyspatteriston avulla. Havaintojen perusteella voidaan todeta, ettei sopimus yksissään riitä varmistamaan riittävää tietosuojan tasoa.

6.2 Konsernihallinto

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 (sähköinen ja manuaalinen)

Vuonna 2019 Espoo hankki kaupunkitasoisen asiakirja- ja rekisteritietojen pitkäaikaissäilytykseen soveltuvan säilytysjärjestelmän. Kansalliset määräykset täyttävä SÄRMÄ-säilytysjärjestelmä mahdollistaa eri tietojärjestelmissä tuotettujen myös henkilötietoja ja salassa pidettäviä tietoja sisältävien tietoaineistojen vastaanoton ja säilyttämisen. SÄRMÄ tukee sähköisten asiakirja-aineistojen säilyvyyttä alkuperäisinä, eheinä, luotettavina, käytettävinä ja todistusvoimaisina.

Espoon talouden tietojärjestelmät ovat vanhentuneet ja ne tullaan korvaamaan uusilla järjestelmillä vaiheittain. Projekti kulkee nimellä JoTo eli johtamisen ja talousohjauksen tietojärjestelmäkokonaisuus. Käyttöönottotavoite on viimeistään vuoden 2022 alussa. Tuolloin korvataan kaikki perustaloushallinnon järjestelmät ja otetaan käyttöön ensimmäinen vaihe suunnittelu-, analytiikka ja raportointijärjestelmistä. Järjestelmien kehittäminen toiminnan raportoinnin osalta jatkuu vuosia. Nykyiset talousjärjestelmät säilyvät käytössä vuoden 2021 loppuun saakka. Uudet järjestelmät vähentävät koko kaupungissa rutiinityötä ja helpottavat johtajien, esimiesten ja asiantuntijoiden tiedonsaantia sekä taloustehtäviä.

Espoo hankki analytiikan kokonaisratkaisun suomalaisyritysten yhteenliittymältä syksyllä 2019.[10] Kokonaisratkaisu on nimeltään Saaga, ja sen avulla Espoo pyrkii automatisoimaan rutiiniprosesseja ja yhtenäistämään tiedonkäsittelykäytänteitä, jolloin erityisesti tietoriskejä kyetään arvioimaan ennakolta ja tekemään hallittuja päätöksiä etenemisestä. Ohjelmistorobotti voi esimerkiksi syöttää, hakea tai yhdistellä tietoja eri järjestelmistä sekä muodostaa työstään raportteja. Lopullisena tavoitteena on tarjota kuntalaisille parempia palveluita.

Konsernihallinnon kehittämiskohteet seuraavat kaupunkitason linjauksia. Verkkokoulutuksen jalkauttaminen vaatii työtä. Samoin tietosuojan vaikutustenarviontien sujuvoittamiseen ja parempaan huomioimiseen projektiprosessissa panostetaan.

6.3 Sosiaali- ja terveystoimi

Sosiaali- ja terveystoimi tuottaa lakisääteisiä sosiaalihuollon ja terveydenhuollon palveluita kuntalaisille. Tämän vuoksi sosiaali- ja terveystoimessa käsitellään merkittäviä määriä salassa pidettäviä potilastietoja ja sosiaalihuollon asiakastietoja.

Sosiaali- ja terveystoimessa on vuonna 2019 kehitetty tietosuojaa etenkin henkilökunnan koulutusten, ohjauksen ja neuvonnan kautta. Vuonna 2019 otettiin käyttöön Lifecare-potilastietojärjestelmä. Tällöin mm. koulutettiin henkilökuntaa. Lisäksi vuonna 2019 valmistauduttiin sosiaalihuollon asiakastiedon arkiston käyttöönottoon, jonka yhteydessä selvitettiin esim. henkilökunnan käyttöoikeuksia. Sosiaali- ja terveystoimessa on havaittu kehittämiskohteiksi mm. tietosuojan riskienarvioinnit sekä käyttöön otettavaan teknologiaan liittyvät tietosuojakysymykset.

Toimialan toimintaympäristö on muutostilassa. Tämä johtuu mm. laajoista lainsäädäntöuudistuksista, kuten sote-uudistuksesta sekä vammaislainsäädäntö- ja asiakasmaksulainsäädäntöuudistuksista. Lisäksi toimintaympäristössä on entistä enemmän kiinnostusta teknologian hyödyntämiseen (kuten robotiikka) ja tiedolla johtamiseen.

6.4 Sivistystoimi

Sivistystoimessa henkilötietojen käsittely perustuu pääsääntöisesti lakisääteisiin tehtäviin. Isoimmat henkilötietoryhmät liittyvät opetuksen ja varhaiskasvatuksen järjestämiseen. Erityisten henkilötietoryhmien käsittelyä sisältyy mm. opiskeluhuoltoasioihin, erityisryhmien uimarannekkeisiin sekä erityisruokavalioihin. Tietoturva- ja tietosuojariskeistä käydään säännöllistä vuoropuhelua ja yhdessä arviointia toimialan eri yksikköjen kanssa tietoriskienhallinnan suunnittelijan johdolla.

Toimialalla on tunnistettu kehittämiskohteiksi vuodelle 2020 mm. henkilöstön tietosuojaan liittyvän osaamisen ylläpitäminen ja lisääminen sekä tarkoituksenmukaiset tekniset ratkaisut erilaisten tietojen säilyttämisessä. Kaupunki-

10 Espoo hankki 5 miljoonan analytiikkaratkaisun. Tivi 30.9.2019.

tasoiset ratkaisut, sensitiiviset työtilat ja henkilöstön verkkokoulutustyökalu tietoturvan ja -suojan oppimisessa otetaan käyttöön koko toimialalla.

6.5 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.

Vuoden 2019 aikana teknisessä ja ympäristötoimessa on kiinnitetty yhä paremmin huomiota tietosuojan huomioimiseen jokaisen päivittäisessä työssä ja pyritty varmistamaan, että tietosuojaan liittyvä osaaminen on hyvällä tasolla. Henkilöstöä on kannustettu hyödyntämään sekä kaupunkitasoisia että ulkopuolisia koulutuksia. Rekisteröityjen oikeuksien takaamiseksi on pyritty siihen, että tietopyyntöprosessi olisi selkeämpi. Tavoitteena on löytää tähän mahdollisimman hyvä toimintamalli vuoden 2020 aikana.

Lisäksi toiveena on, että vuoden 2020 aikana voitaisiin varmistua koko toimialan sopimusten olevan kunnossa tietosuojan osalta. Toimialan henkilöstölle on toiveissa saada yhä kattavampaa ohjeistusta ja lisää yhteisiä koulutuksia. Tavoitteena on parantaa myös hallinnollista tietosuojaa ja kehittää tietosuojaan liittyvien riskien arviointia sekä hyödyntää uutta teknologiaa tietosuoja huomioiden.

6.6 Länsi-Uudenmaan pelastuslaitos

Länsi-Uudenmaan pelastuslaitoksessa henkilötietojen käsittely perustuu pääsääntöisesti lakisääteisiin tehtäviin. Isoimmat henkilötietoryhmät liittyvät pelastuslaitoksen työvuorosuunnitteluun ja henkilöstön soveltuvuuden arviointiin (fyysinen toimintakyky ja henkilöturvallisuusselvitykset). Erityisten henkilötietoryhmien käsittelyä sisältyy työkykyarviointeihin.

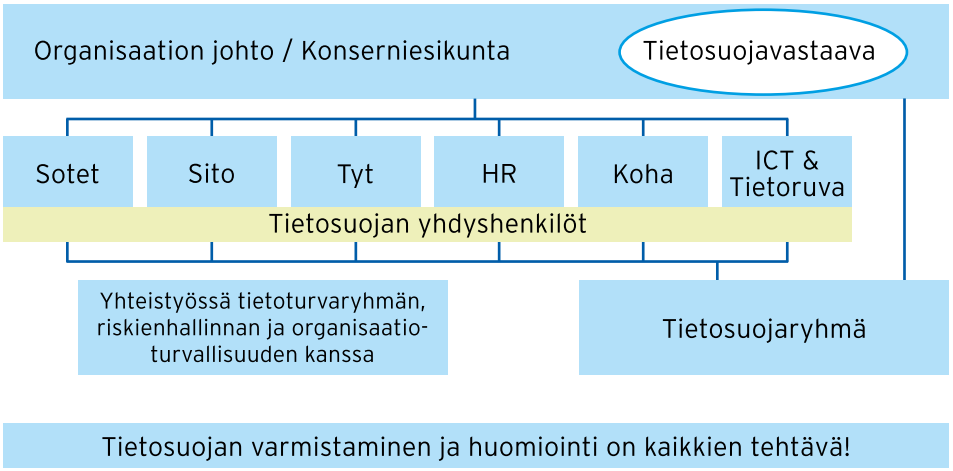
Tietoturva- ja tietosuojariskeihin on pelastuslaitosten kumppanuusverkostossa luotu omat ohjeistot ja kumppanuusverkostossa sekä Uudenmaan alueen pelastuslaitosten kesken käydään säännöllistä vuoropuhelua ja suunnitellaan yhteistä arviointikehikkoa tietoturvallisuuden ja tietosuojan tason arvioimiseksi.

Pelastuslaitoksissa on tunnistettu kehittämiskohteiksi vuodelle 2020 mm. henkilöstön tietosuojaan liittyvän osaamisen ylläpitäminen ja lisääminen sekä tarkoituksenmukaiset tekniset ratkaisut erilaisten tietojen säilyttämisessä. Pelastuslaitosten käytössä on yhteinen verkkokoulutusalusta (Pelastusopiston Moodle, Koulumaali), jonka tietoturvatentin suorittaminen on pakollista koko henkilöstölle.

6.7 Tietosuojaryhmä

Kaupunginjohtajan päätöksellä nimetyn tietosuojaryhmän 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.*

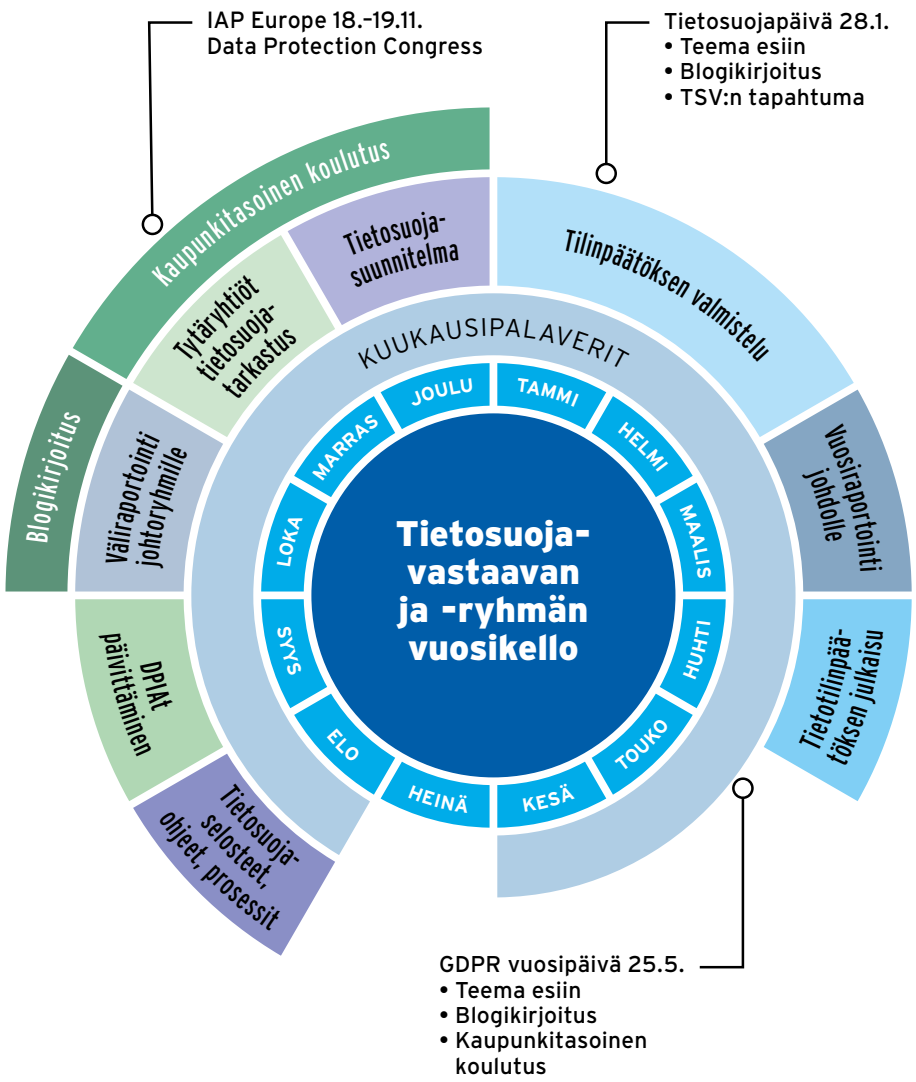
Kaupunkitasoinen, tietosuojan, tietoturvan, riskienhallinnan, juridiikan ja asiakirjahallinnon asiantuntijoista koostuva ryhmä kokoontui tietosuojavastaavan johdolla vuoden 2019 aikana kuukausittain heinäkuuta lukuun ottamatta yhteensä 11 kertaa. Osallistuminen kokouksiin oli aktiivista. Voidaan perustellusti todeta, että toimialat ja avainyksiköt ovat sitoutuneet ryhmän toimintaan ja kokeneet sen hyödylliseksi.



Kuva: Tietosuojaryhmän kokoonpano

Vuonna 2019 tietosuojaryhmän tehtävänä oli erityisesti jalkauttaa tietosuoja-asetuksen toimeenpanoprojektissa tuotettuja linjauksia ja ohjeistuksia kaupungin toimintaan sekä seurata kansallista ohjeistusta tietosuoja-asetuksen soveltamisesta. Tietosuojaryhmän kokouksissa käsiteltiin erityisesti seuraavia asioita:

- tiedonkeruu vuoden 2018 tietotilinpäätökseen
- tietosuojan vaikutustenarvionitien kehittäminen
- toisiolain vaikutukset
- tiedonhallintalain vaikutukset
- lokien käsittely
- henkilötietojen tietoturvaloukkaukset
- digi- ja analytiikkakokeilut
- ei-strukturoidun henkilötiedon käsittely ja tiedon luokittelu
- tietoturvaparannukset
- Espoon ja tietosuojavaltuutetun tapaaminen



Kuva: Tietosuojavastaavan ja -ryhmän vuosikello

Tietosuojaryhmän keskeiset onnistumiset vuonna 2019 olivat:

- vuoden 2018 tietotilinpäätöksen laatiminen
- tietoturvan ja tietosuojan verkkokoulutus
- kameravalvonnan tietosuojaohje
- tiedon luokittelumalli
- monitoimitilojen tietosuojaohje
- WhatsAppin käytön linjaukset
- tietosuojan vaikutustenarvioinnit
- kaupunkitasoinen etätyöohjeistus
- analytiikkaympäristön tietosuojavaatimukset

6.8 Tietoturvaryhmä

Espoon kaupungin tietoturvaryhmä on ollut toiminnassa jo vuosia ja se kokoontuu säännöllisesti kuukausittain tietoturvapäällikön johdolla. Tietoturvaryhmään kuuluu jäseniä kaikilta toimialoilta, Länsi-Uudenmaan pelastuslaitoksesta, konsernihallinnosta ja tietohallinnosta.

Tietoturvaryhmän tehtäväksi on määritetty tietoturva- ja tietosuojapolitiikassa: *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.*

Operatiivisia tietoturvaan liittyviä asioita edistetään tietohallinnon johtamissa yhteistyöryhmissä, joissa on edustettuna kaupungin tietoturvahenkilöstön lisäksi tärkeimpien kumppanien palvelupäälliköitä ja tietoturvapalveluista vastaavia henkilöitä. Näiden yhteistyöryhmien tavoitteena on erityisesti yhteensovittaa kehityshankkeita, tietoturvatapahtumiin reagoimista ja parantaa monen välistä yhteistyötä tietoturvallisuuteen liittyen.

6.9 Yhteistyöverkostot

Tietosuojavastaava ja tietoturvapäällikkö ovat osallistuneet aktiivisesti Helsingin kaupungin vetämään tietosuojan yhteistyöryhmään. Ryhmä on kokoontunut kuukausittain ja sen toiminta on koettu Espoossa hyödylliseksi. Ryhmässä on käsitelty erityisesti seuraavia aiheita:

- tekoälyn hyödyntäminen ja profilointi
- suostumuksen käyttö viranomaistoiminnassa
- evästeet
- tietotilinpäätöksen laatiminen
- henkilötietojen tietoturvaloukkaukset

Tietosuojavastaava ja tietoturvapäällikkö osallistuvat lisäksi suurten kaupunkien epäviralliseen tietoturvan ja tietosuojan yhteistyöryhmään. Ryhmään osallistuvat Espoon ohella Helsinki, Tampere, Oulu ja Kuopio. Ryhmä kokoontuu verkon välityksellä kuukausittain. Ryhmässä on keskusteltu seuraavista aiheista:

- tiedonhallintalain toimeenpano
- käyttöön otettavat tietoturvakontrollit
- O365-ympäristö
- tietoturvaloukkaukset

Tietosuojavastaava on vuonna 2019 osallistunut säännöllisesti eurooppalaisten kaupunkien Eurocities-verkostoon, jonka jäsen Espoo on. Verkoston alajaosto Knowledge Society Forum käsittelee tekoälyn ja yleisesti datan hyödyntämiseen liittyviä suuria kokonaisuuksia, jotka koskettavat kaikkia suuria eurooppalaisia kaupunkeja. Lisäksi kantaa otetaan eettisiin kysymyksiin ja kansalaisten oikeuksiin datataloudessa. Knowledge Society Forum kokoontui vuoden aikana kolme kertaa: Barcelonassa, Eindhovenissa ja Kölnissä. Tapaamisista on saatu tärkeää perspektiiviä EU:n kokonaistilanteesta. Voimme ylpeästi todeta, että Suomi ja Espoo kulkevat eturintamassa. Hyvin harvassa maassa on vastaavia julkishallinnon tietovarontoja kuin Suomessa eikä kansalaisten luottamus julkishallintoon ole samalla tasolla.

Espoon tietosuojavastaava osallistui Brysselissä 20.-21.11.2019 järjestettyyn IAPP Europe Data Protection Congress 2019 -tapahtumaan. Kyseessä on jokavuotinen Euroopan suurin tietosuojatapahtuma, johon osallistui yli 2000 tietosuojan ammattilaista eri puolelta Eurooppaa ja globaalisti niin julkishallinnosta kuin yksityiseltä sektorilta. Tapahtuma myytiin loppuun jo lokakuussa. Konferenssi käsitteli tietosuojaa laajalla rintamalla. Monessa puheenvuorossa pohdittiin GDPR:n toimivuutta. Toisena päivänä EU:n kilpailupolitiikasta vastaava komissaari Margrethe Vestager puhui keynote-puheenvuorossaan siitä, että ihmisillä pitäisi olla vahvempi kontrolli heistä erilaisilla teknologioilla kerättävään dataan. EU:n kilpailupolitiikalla on suuri merkitys. Sen avulla luodaan reunaehdot, joiden avulla EU-alueelle synnytetään liiketoimintaa, joka ottaa paremmin huomioon yksityisyydensuojan. Kilpailu ja tietosuoja kulkevat siis käsi kädessä.

Kaupungin henkilöstö osallistuu aktiivisesti tietoturvallisuuteen liittyviin verkostoihin. Kaupungin tietoturvapäällikkö on jäsenenä tiedonhallintalautakunnassa ja useampi henkilö osallistuu Vahti-toimintaan. Kaupungilta on edustaja myös Vahti-johtoryhmässä. Tämän lisäksi kaupungin henkilöstö osallistuu muihin tarkoituksen mukaisiin tietoturvallisuuteen liittyviin verkostoihin.

6.10 Hack with Espoo -hakkerointikurssi

Espoossa toteutettiin vuoden 2019 loppupuolella toisen kerran, Suomessa ainutlaatuinen, lukiolaisille suunnattu eettisen hakkeroinnin kurssi. Kurssi toteutettiin yhteistyössä 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 4 tietoturvallisuuteen liittyvää haavoittuvuutta. 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 julkishallinnon 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 2020. Kurssille pääsee opiskelijoita niin Espoon lukioista kuin Omnian ammatillisesta koulutuksestakin. Kurssin vaikutuspiirissä on noin 10 000 nuorta.

7 ARVIOINTI JA MITTARIT

7.1 Rekisteröityjen oikeuksien toteutuminen

Tietosuojaselosteilla vastataan Espoossa GDPR:n (12 – 14 artikla) läpinäkyvyys- ja informointivaatimuksiin. Käytännössä selosteella viestitään asiakkaalle tai työntekijälle, mitä tietoja hänestä kerätään ja miten niitä käsitellään tietyssä palvelussa. Selosteet ovat julkisia dokumentteja, jotka on koottu keskitetysti Espoon verkkosivuille. Tietosuojaselosteet on pyritty laatimaan palveluittain, mutta tässä riittää vielä kehittämistä Espoossa. Osa tämän hetkisistä tietosuojaselosteista kuvaa henkilötietojen käsittelyä yksittäisessä tietojärjestelmässä. Palvelukeskeinen näkökulma on tässä mielessä erilainen henkilötietolain aikaiseen rekisteriajatteluun verrattuna. Tietosuojaselostetta ei löydy käsitteenä suoraan GDPR:stä, mutta sitä käytetään Suomessa yleisesti rekisteröidyn informointiin.

Espoossa tietosuojaselosteiden tarkistusprosessi sisältyy tietosuojaryhmän vuosikelloon. Selosteet tarkistetaan vuosittain syksyllä. Tietosuojaselosteen yhdyshenkilön velvollisuus on tarkistaa, että seloste on ajan tasalla, jolloin rekisteröidylle kyetään tarjoamaan asianmukainen tiivistelmä henkilötietojen käsittelystä. Toimialan tietosuojan yhdyshenkilö koordinoi oman toimialansa tarkastusprosessia.

Tietosuojaselosteiden lukumäärä 31.12.2019

Toimiala	Lukumäärä
Espoo yhteensä	179
Konsernihallinto	57
Sivistystoimi	54
Sosiaali- ja terveystoimi	20
Tekninen ja ympäristötoimi	37
Länsi-Uudenmaan pelastuslaitos	11

Kuva: Tietosuojaselosteiden lukumäärä Espoossa

Espoon verkkosivuilla kerrotaan tarkemmin, miten rekisteröidyt voivat käyttää oikeuksiaan, esimerkiksi mitä tietoja asiakkaasta on syntynyt asiakkaan käyttämässä palvelussa. Espoossa rekisteröityjä koskevat tietopyynnöt ovat kauttaaltaan suuntautuneet sosiaali- ja terveystoimen toimialalle. Pyyntöihin on pääsääntöisesti kyetty vastaamaan GDPR:n edellyttämässä yhden kuukauden aikaraamissa. Vaikka tietopyyntöjen volyymi on ollut vähäinen sosiaali- ja terveystoimen toimialaa lukuun ottamatta, tietosuojavastaava on saanut vuoden aikana runsaasti yhteydenottoja kuntalaisilta Espoon henkilötietojen käsittelyn periaatteista. Laajoissa, useita toimialoja koskevissa tietopyynnöissä, tiedonkeruu on ollut haasteellista. Tällöin asiakasta on yleensä pyydetty tarkentamaan tietopyyntöä.

Espoossa ei ole vielä käytössä sähköistä prosessia GDPR:n mukaisen tietopyynnön toimittamiselle. Haasteet liittyvät asiakkaan luotettavaan tunnistamiseen. Kaupungin on varmistettava, ettei synny tilanteita, joissa luovutettaisiin vahingossa väärän asiakkaan henkilötietoja tietopyynnön esittäjälle. Kaupunki pyrkii saamaan sähköisen työkalun tietopyynnöille vuoden 2020 aikana osana palvelujen digitalisointia. Myös tietopyyntöjen kaupunkitasoista tilastointia kehitetään ja sujuvoitetaan edelleen vuoden 2020 aikana. Ajoittain ei ole selvää, onko kyseessä julkisuuslain vai GDPR:n mukainen tietopyyntö.

Tietopyynnön voi toimittaa joko 1) postitse tietosuojaselosteessa mainitulle yhteyshenkilölle osoitettuna tai 2) asioimalla henkilökohtaisesti asiointipisteessä tai kirjaamossa, jossa tarkistetaan henkilöllisyys. Sosiaali- ja terveystoimen toimialalla tietopyynnön voi jättää myös henkilökohtaisen asioinnin yhteydessä sosiaali- ja terveydenhuollon toimintayksikössä. Asiakas voi tulla noutamaan pyytämänsä tiedot kaupungin kirjaamosta tai asiointipisteestä. Tiedot voidaan toimittaa hänelle myös postitse.

GDPR:n mukaisten tietopyyntöjen lukumäärä 2019

Toimiala	Lukumäärä
Espoo yhteensä	2560
Konsernihallinto	13
Sivistystoimi	9
Sosiaali- ja terveystoimi	2400
Tekninen ja ympäristötoimi	Ei tiedossa
Länsi-Uudenmaan pelastuslaitos	1
Kaupunginarkisto	137

Kuva: GDPR:n mukaiset tietopyynnöt Espoossa 2019

Lokitietojen tarkastuspyynnöt koskevat käytännössä ainoastaan sosiaali- ja terveystoimen toimialaa. Kuntalaiset ovat kiinnostuneita ja tarkkoja yksityisyydensuojastaan, joten pyyntöjen määrä on suuri.

Vuoden aikana tehdyt lokiselvitykset	2015	2016	2017	2018	2019
Tehdyt lokiselvitykset yhteensä, kpl	53	67	62	104	69
- joista sisäisiä	19	17	16	21	14

Kuva: Sosiaali- ja terveystoimen toimialan lokiselvitykset 2015 – 2019

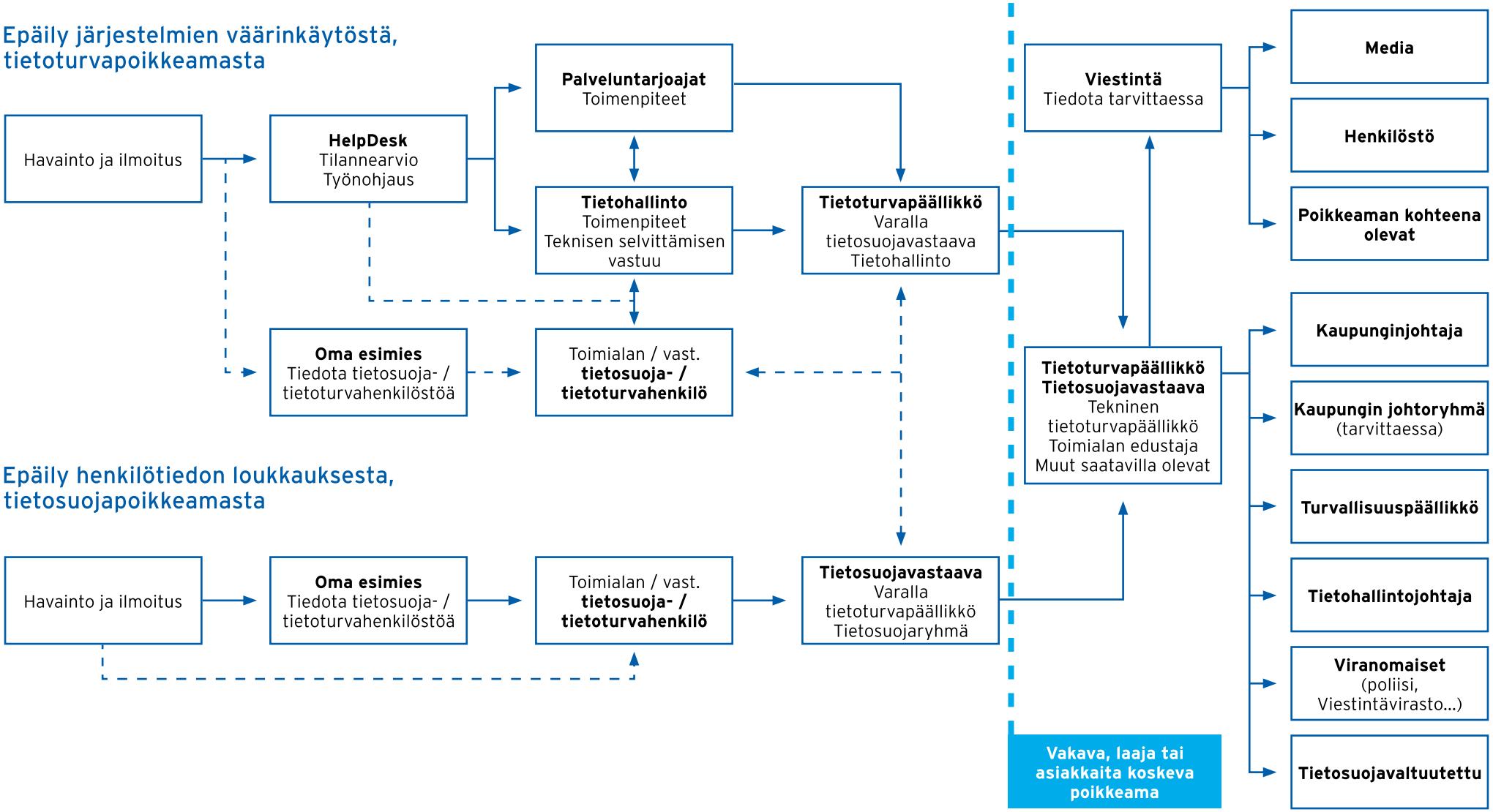
7.2 Poikkeamien hallinta

7.2.1 Tietoturvapoikkeamat

Espoossa tietoturvapoikkeamia arvioidaan niiden vaikutusten perusteella, kohdistuvatko ne saatavuuteen, eheyteen vai tiedon luottamuksellisuuteen. Lisäksi tietosuojan näkökulmasta arvioidaan, onko poikkeaman tai loukkauksen kohteena ollut henkilötietoja.

Poikkeamia tilastoitiin vuonna 2019 yhteensä 120 kappaletta. Lukuun sisältyvät tietojärjestelmiin tai tiedonsiirtoverkkoihin liittyneet häiriöt, jotka aiheuttivat hetkellisiä käyttökatkoja tietojärjestelmään tai johonkin fyysiseen sijaintiin. Tiedon luotettavuuteen kohdistuneita tapauksia oli koko määrästä 47 prosenttia. Tyypillisin tapausesimerkki on inhimillisien virheiden seurauksena tapahtunut käsittelyvirhe.

Poikkeaman jälkeen pyritään arvioimaan siihen vaikuttaneet juurisyyt, jotta niiden syntyminen voidaan minimoida. Tilastoinnin perusteella pyritään selvittämään erilaisia trendejä ja poikkeamiin vaikuttaneita juurisyitä, jotta niiden minimoimiseksi pystytään tekemään oikeanlaisia ja oikein mitoitettuja toimenpiteitä.



Kuva: Tietoturvapoikkeamien käsittelyprosessi Espoossa

7.2.2 Henkilötietojen tietoturvaloukkaukset

Tietosuojavaltuutetulle on lähetetty yli 6 000 ilmoitusta tietoturvaloukkauksista vuoden 2019 loppuun mennessä[11]. Aikajana alkaa GDPR:n soveltamispäivämäärästä 25.5.2018. Espoossa tietosuojavastaava ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetulle, jos loukkauksesta voi aiheutua riski henkilöiden oikeuksille ja vapauksille. Ilmoitus on tehtävä viimeistään 72 tunnin kuluessa siitä, kun loukkaus on tullut ilmi. Jos päädytään siihen, että tietoturvaloukkauksesta ei tarvitse ilmoittaa tietosuojavaltuutetulle, dokumentoidaan, millä perusteella ilmoitus on katsottu tarpeettomaksi. Jos loukkaus todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille, on siitä ilmoitettava loukkauksen kohteeksi joutuneelle henkilölle.

Espoossa on olemassa prosessi henkilötietojen tietoturvaloukkauksille, ja 72 tunnin aikamääreeseen on kyetty pääsääntöisesti vastaamaan. Henkilöstön tietoisuutta ilmoitusvelvollisuudesta pyritään parantamaan koulutusten ja ohjeistuksen avulla. Joissain yksikössä aihetta sivutaan säännöllisesti tiimikokouksissa.

Espoossa ryhdyttiin tilastoimaan tietoturvaloukkauksia systemaattisesti vuoden 2018 alusta. Vuosia 2018 ja 2019 ei kuitenkaan kannata verrata tosiinsa, sillä tietoisuuden kasvu korreloi vahvasti loukkausten lukumäärän kanssa. Paremminkin tietoturvaloukkausten lukumäärän kasvu voi kertoa siitä, että henkilöstö suhteutuu vakavammin tietoturva- ja tietosuojakysymyksiin. Vasta vuoden 2020 tietotilinpäätöksessä on perusteltua toteuttaa vertailua edelliseen vuoteen.

Yle julkaisi verkkosivuillaan 3.10.2019 tietojen kalastelua (ns. phishing-hyökkäykset) käsittelevän artikkelin, jossa pureuduttiin myös Espoon kaupunkiin maaliskuussa 2019 kohdistettuun huijaukseen. Tuolloin 11 kaupungin työntekijää klikkasi huijausviestiä ja syötti lopulta käyttäjätunnuksensa ja salasanansa huijaussivustolla. Näin rikollinen taho pääsi käsiksi työntekijän sähköpostin ja OneDriven sisältöön. Kaupunki päätyi viranomaisarvioiden ja käytettävissä olevan lokitiedon perusteella riskiarviossaan siihen, että tapauksesta ei kohdistuisi korkeaa riskiä yksilöille. Riskiarviossa huomioitiin myös huijausviestiin langenneiden työntekijöiden työrooli. Espoo arvioi, että työntekijät eivät käsittelisi laajamittaisesti henkilötietoja. Tietosuojavaltuutettu oli omassa riskiarviossaan eri mieltä Espoon kanssa. Valvontaviranomainen määräsi Espoon ilmoittamaan tietoturvaloukkauksesta sen kohteena mahdollisesti oleville yksilöille.[12]

Tapahtumaketju kertoo tietosuoja-asetuksen osoitusvelvollisuus-vaatimuksesta. Todistustaakka on organisaatiolla itsellään loukkausten selvittämisessä. Espoon on kyettävä aukottomasti todistamaan, että tiedot eivät ole vaarantuneet. Näin ei tapahtunut tässä tapauksessa.

Tietosuojavaltuutettu lähetti Espoolle kolme määräystä koskien tietoturvaloukkauksen puutteellista informointia rekisteröidylle. Espoo reagoi määräyksiin tietosuojavaltuutetun ohjeiden mukaisesti ja toimitti valvontaviranomaiselle vaaditun lisäselvityksen.

Henkilötietojen tietoturvaloukkaukset Espoossa 2019

Toimiala	Yhteensä	Tietosuoja-valtuutettu	Rekisteröity
Espoo yhteensä	60	25	25
Konsernihallinto	11	2	2
Sivistystoimi	9	6	6
Sosiaali- ja terveystoimi	35	15	15
Tekninen ja ympäristötoimi	5	2	2

Kuva: Henkilötietojen tietoturvaloukkaukset Espoossa 2019.

11 Tietosuojavaltuutettu on saanut 5 600 ilmoitusta tietoturvaloukkauksista. Karjalainen 27.11.2019.

12 Huijarit murtautuivat kaupungin työntekijöiden sähköposteihin Nigeriasta. Yle 3.10.2019.

Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019

Toimiala	Yhteensä	%
Espoo yhteensä	60	100
Työntekijän erehdys tai väärä toimintatapa	32	53
Tietomurto tai muu tahallinen teko	6	10
Palveluntuottajan virhe	12	20
Prosessivirhe	5	8.5
Tekninen virhe	5	8.5

Kuva: Henkilötietojen tietoturvaloukkausten syyt Espoossa 2019.

7.3 Osaamisen seuranta ja kehittäminen

Globaali trendi on se, että reilusti yli puolet kaikista organisaation tietoturvaloukkauksista johtuu yksilön inhimillisistä virheistä. Espoossa panostetaan erityisesti henkilöstön kouluttamiseen, osaamisen parantamiseen ja tietoisuuden kasvattamiseen. Espoossa on työntekijöitä arviolta 14 500 ja 770:llä erilaisella tehtävänimikkeellä. Lisäksi kaupungilla on 610 lakisääteistä tehtävää.[13] Yksi perusmalli ei sovi millään jokaiselle, koska vaatimustaso vaihtelee.

Tietosuojavastaava ja tietoturvapäällikkö ovat ottaneet koulutuksissaan avoimen ja positiivisen lähestymistavan tietosuojaan ja tietoturvaan. Oleellista on, että viestin tuojaa ei rangaista. Hänet pitäisi paremminkin palkita. Tällöin saadaan tarpeellista tietoa mahdollista puutteista, jolloin ne myös kyetään korjaamaan. Perustyöntekijälle tärkein ohje on nopea reagointi. Hänen ei tarvitse miettiä poikkeaman vakavuusastetta. Epäselvässä tilanteessa ilmoitus on parempi tehdä kaiken varalta turhaan kuin jättää tekemättä. Pienistä asioista kannattaa nillittää. Kun kiinnitetään huomiota pieniinkin poikkeamiin, kulttuuria, tietoisuutta ja tilannekuvaa saadaan parannettua. Harjoittelun avulla organisaatio kykenee reagoimaan ja toimimaan tosipaikan tullen tehokkaammin.

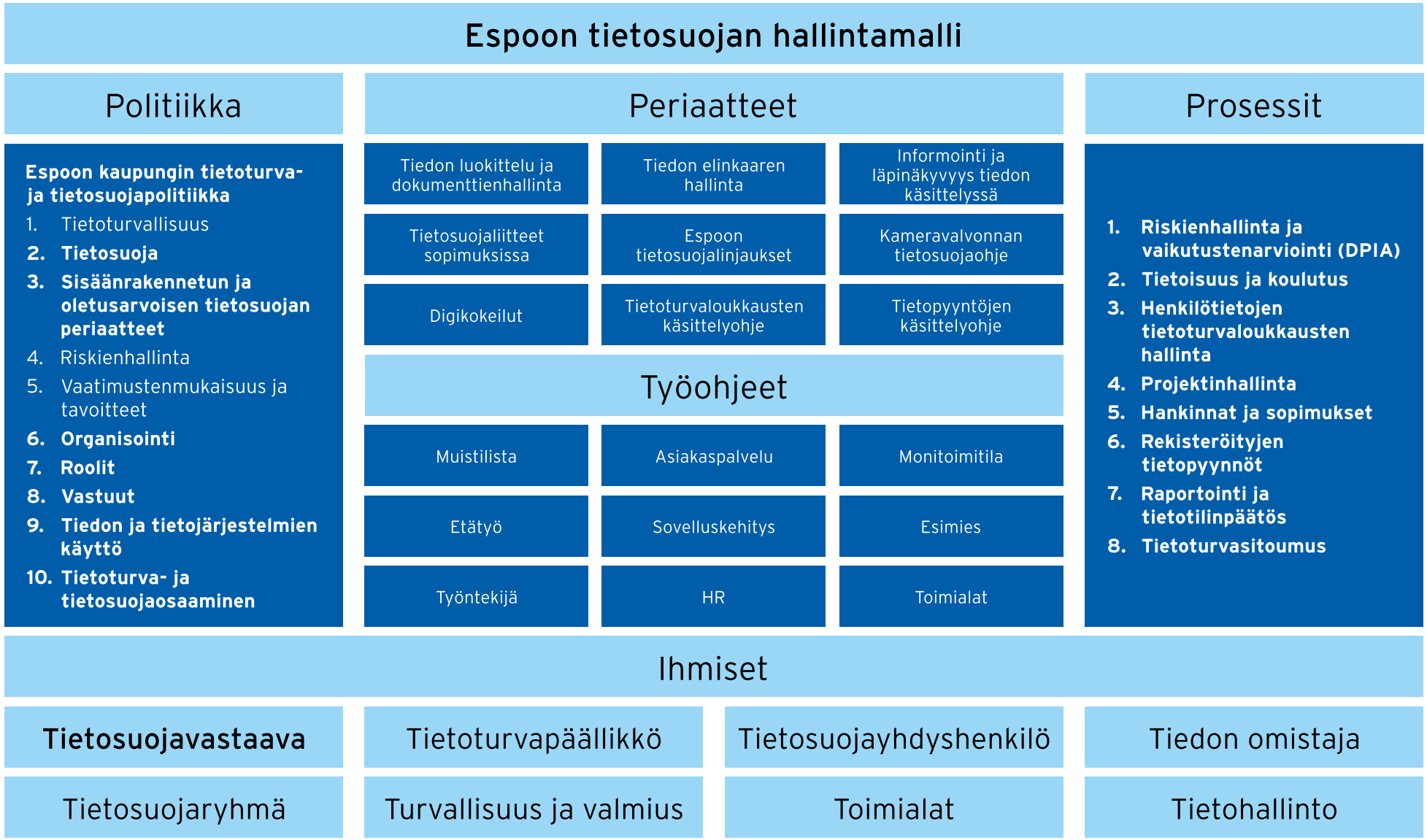
13 Kuntien tehtävät ja velvoitteet. VM:n täydennysraportti 2015.

Henkilöstökoulutuksissa merkittävin panostus oli verkkokoulutuksen käyttöönotto loppuvuodesta 2019. Koulutusta pilotoitiin konsernihallinnossa ja sen käyttöönottoa laajennetaan kaikille toimialoille keväällä 2020. Verkkokoulutuksella on merkittäviä hyötyjä:

- Tavoitteena on perehdyttää, parantaa osaamista ja pienentää riskejä.
- Aikaa ja kustannuksia säästyy.
- Esimies kykenee seuraamaan ja varmistamaan, että alaiset ovat suorittaneet koulutuksen.
- Verkkokoulutuksen tilastodatan avulla kyetään tunnistamaan koulutustarpeita.

Vaikka pääpanostus vuonna 2019 oli verkkokoulutuksen jalkauttamisessa, kouluttamiseen ja tietoisuuden kasvattamiseen panostettiin samanaikaisesti monella rintamalla:

- Puolivuosittain järjestettävään uuden työntekijän Missä mennään Espoo -perehdytyspäivään sisältyy puoli tuntia kestävä tietoturvan ja tietosuojan tietoisku
- Tietosuojavastaava järjestää puolivuosittain kaupunkitasoisen tietoiskun ajankohtaisesta tietosuojateemasta. Koulutuksissa on käsitelty laajasti myös tietoturvaa ja niissä vierailee usein ulkopuolisia asiantuntijoita.
- Toimialojen omat spesifit koulutukset
- Uuden esimiehen verkkokoulutus
- Tietosuojavastaava ja tietoturvapäällikkö kirjoittavat Espoon intranetin blogiin arviolta neljästi vuodessa ajankohtaisesta teemasta.
- Tietosuojavastaava ja tietoturvapäällikkö kokeilivat omaa Suojatie-podcastia, joka julkaisi kaikkiaan viisi jaksoa vuoden 2019 aikana. Jaksoissa keskusteltiin vieraiden kanssa tekoälystä, kyberturvallisuudesta, eettisestä hakkeroinnista, Internet of Thingsistä ja muista pinnalla olevista aiheista. Sarja on julkinen ja sitä voi kuunnella myös Spotifyssa.
- Tietosuojavastaava vierailee syksyisin toimialojen johtoryhmissä ja käy läpi kuluvan ajankohtaistilanteen tietosuojan osalta.
- Läsnäolokoulutuksiin osallistui vuoden 2019 aikana arviolta 1100 työntekijää.



Kuva: Espoon tietosuojan hallintamalli

7.4 Tietoriskien hallinta

Tietojärjestelmien tekninen suojaus on vain pieni osa tietoriskien hallintaa. Muita vaikuttavia kokonaisuuksia ovat johtaminen, henkilöstön toiminta, sidosryhmäyhteistyö ja toimitilat. Espoon kaupunkikonsernin riskienhallintapolitiikka määrittää kaupungin tahtotilan riskienhallinnan tavoitteista, periaatteista ja käytännön toteuttamisesta. Johdon vastuu on linjattu Espoon hallintosäännössä sekä tietoturva- ja tietosuojapolitiikassa, jonka kaupunginhallitus on hyväksynyt 28.5.2018. Tietosuoja-asetuksen lähtökohta on riskiperusteinen lähestymistapa. Käytännössä tämä tarkoittaa sitä, että korkean riskin henkilötietojen käsittelyyn on kohdennettava enemmän resursseja kuin matalan riskin. Samaan aikaan tietosuojavastaavan on keskistyttävä työssään terveystiedon ja heikossa asemassa olevien, erityisesti lapsien, henkilötiedon käsittelyyn.

Tietosuojan vaikutustenarvioinnit nostettiin kehittämiskohteeksi jo Espoon vuoden 2018 tietotilinpäätöksessä. Tietoriskien hallinta on painottunut vuoden 2019 aikana erityisesti vaikutustenarviointeihin, joissa näkökulma on rekisteröityjen oikeuksiin kohdistuvissa riskeissä. Vastaavasti tietoturva tarkastelee riskejä organisaation näkökulmasta.

Rekisterinpitäjän yleisenä velvoitteena on huomioida toiminnassaan henkilötietojen käsittelyn riskit ja kohdistaa tarvittavat toimenpiteet niiden minimoimiseksi (GDPR 24 artikla). Rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyys ja vakavuus on määriteltävä tietojenkäsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan (GDPR:n johdanto-osa 76). Ilman tietosuojan vaikutustenarviointia Espoo ei pysty osoittamaan noudattavansa osoitusvelvollisuutta ja riskiperusteista lähestymistapaa esimerkiksi silloin, kun hankittavassa tietojärjestelmässä käsitellään laajasti terveysdataa. Vaikutustenarvioinneilla kerätään ennen kaikkea oleellista tietoa päätöksenteon tueksi. Espoolla on olemassa ohjeistus, kriteeristö ja prosessi vaikutustenarvioinneille.

Lähes varma (4)	Kohtalainen	Merkittävä	Sietämätön	Sietämätön
Todennäköinen (3)	Vähäinen	Kohtalainen	Merkittävä	Sietämätön
Mahdollinen (2)	Merkityksetön	Vähäinen	Kohtalainen	Merkittävä
Epätodennäköinen (1)	Merkityksetön	Merkityksetön	Vähäinen	Kohtalainen
(↑) Todennäköisyys Vaikutus (→)	Vähäinen (1)	Kohtalainen (2)	Merkittävä (3)	Kriittinen (4)

A = Käyttäjien inhimilliset virheet
B = Digikokeilut ja analytiikka
C = Kalasteluviestit
D = Sopimukset
E = Puutteellinen riskienhallinta
F = Pilvipalvelujen tietoturva
G = Vanhat tietojärjestelmät
H = Tiedon elinkaaren hallinta

Kuva: Espoon toiminnassa yleisesti tunnistetut tietoriskit

Tietosuojan vaikutustenarvioinnin prosessia on hiottu moneen kertaan vuoden 2019 aikana. Vaikutustenarvioinnit on koettu hyödyllisiksi, vaikka ne vaativat yleensä runsaasti monen asiantuntijan työpanosta. Kyseessä ei ole staattinen dokumentti vaan jatkuvasti päivitettävä ja ylläpidettävä. On tärkeää kiinnittää huomiota havaittujen jäännösriskien seurantaan. Juuri tämän vuoksi vaikutustenarviointien tarkastus sisältyy tietosuojaryhmän vuosikelloon, jolloin vastuuhenkilö käy dokumentin sisällön läpi vuosittain

ja päivittää sen tarpeen mukaan. Hyväksi toimintamalliksi on vakiintunut työpajatyöskentely, johon osallistuvat yleensä:

- projektipäällikkö tai toiminnasta vastaava (omistaja)
- it-projektipäällikkö
- tarvittaessa palveluntuottajan edustaja
- toimialan lakimies
- tietosuojavastaava
- tietoturvapäällikkö tai teknisestä tietoturvasta vastaava it-päällikkö

Työpajoissa tunnistettiin seuraavanlaisia riskejä:

- läpinäkyvyys
- epäselvä käsittelyperuste
- tiedon elinkaaren hallinta
- laaja näkyvyys tietoon
- tiedon minimointivaatimus ei toteudu
- evästeet
- puutteelliset lokitiedot
- tiedonsiirto EU/ETA-alueen ulkopuolelle

Tietosuojan vaikutustenarvioinnit 2019

Toimiala	Lukumäärä
Espoo yhteensä	20
Konsernihallinto	11
Sivistystoimi	3
Sosiaali- ja terveystoimi	6
Tekninen ja ympäristötoimi	0
Länsi-Uudenmaan pelastuslaitos	0

Kuva: Tietosuojan vaikutustenarvioinnit Espoossa 2019

7.5 Auditoinnit

Auditointikäytäntöjä on yhtenäistetty ja edelleen kehitetty vuoden 2019 aikana. Käytäntöjä tullaan tarkemmin jalkauttamaan vuonna 2020.

Sisäinen tarkastus on toteuttanut tietosuojaan liittyviä auditointeja toimialoilla. Painotus on ollut tietosuojaselosteiden kattavuudessa ja ajantasaisuudessa sekä tietopyyntöprosessin sujuvuudessa. Havaintojen perusteella laajat, kaupunkitasoiset tietopyynnöt tuottavat haasteita. Koska sähköistä prosessia ei ole olemassa, tiedon kokoaminen toimialoilta koordinoidusti ei ole sujuvaa eikä asiakkaan palvelukokemus ole missään tapauksessa Espoo tarinan hengen mukainen. Pahimmassa tapauksessa asiakas saattaa joutua noutamaan tietojaan useampaan otteeseen. Prosessissa on siis edelleen kehitettävää.

Kaupungin tilintarkastuksen yhteydessä toteutettiin ulkopuolisen konsultin johdolla kattava tietosuojan auditointi loppuvuodesta 2019. Tarkastuksessa ei arvioitu yksittäisiä järjestelmiä vaan se kohdistui hallinnolliseen kokonaisuuteen. Myöskään kontrollien toiminnallista tehokkuutta ei testattu miltään tietyltä ajanjaksolta. Tarkastuksessa haastateltiin Espoon tietosuojavastaavaa sekä käytiin systemaattisesti läpi Espoon tietosuojadokumentaatiota.

Keskeiset kehittämistarpeet olivat seuraavissa osa-alueissa:

- Tietosuojariskien hallinta
  - Tietosuojaan liittyvät riskit tulisi huomioida organisaation säännöllisessä (tieto)riskien arvioinnissa.
  - Prosesseihin ja järjestelmiin liittyvät riskit, kontrollit, riskin käsittely sekä kehitystarpeet tulisi dokumentoida ja rekisteröidä yhtenäisellä tavalla esim. rekisteriin/taulukkoon, josta kokonaiskuvaa voidaan arvioida.
- Henkilötiedon elinkaaren hallinta ja sisäänrakennettu tietosuoja
  - Hyväksytyt henkilötiedon yksilöinnin häivyttämiseen liittyvät menettelyt/periaatteet tulisi laatia.
  - Käyttöoikeuksien laajuuden rajoittaminen työtehtävien mukaiseksi tulee varmistaa riittävillä käyttöoikeushallinnan menettelyillä (esimerkiksi rooleja käyttämällä).

- Tiedonohjaussuunnitelma (TOS) tulisi täydentää ja sitä tulisi soveltaa tietojen käsittelyssä. Tiedon poistomenettelyt tulisi määrittää.
- Sopimusten ja ulkoistusten hallinta
  - Toimittajariskien hallinnan prosessi tulisi kuvata.
- Tietosuojan ja tietoturvan valvonta
  - Tietosuojakontrollien ja -prosessien tarkoituksenmukaisuutta ja tehottuutta valvovat ja varmistavat jatkuvat/ajoittaiset toimenpiteet tulisi kuvata. Tietoturva-auditointien periaatteet tulisi kuvata.

Lisäksi tietosuojavastaava on soveltanut julkishallinnon käyttöön tarkoitettua *Julkisen hallinnon GDPR-itsearviointityökalua*.[14] Tietosuojavastaava on arvioinut työkalun avulla tietosuojan vaatimustenmukaisuutta yhdessä tietoturvapäällikön ja teknisen tietoturvan it-päällikön kanssa. Työkalu on todettu erittäin hyödylliseksi. Arviointi on osa tietosuojaryhmän vuosikelloa.

7.6 Todennetut kehittämiskohteet

Kehittyvä ja muuttuva toimintaympäristö asettaa turvallisuudelle valtavan haasteen. Miten mahdollistetaan tiedon avoin käyttö, lisääntynyt verkottuneisuus sekä älykkäiden laitteiden tuoma lisäarvo palveluntuotannolla ja toisaalta turvataan kaupungin kriittiset prosessit, tiedot ja tietovarannot? Kaikessa päätöksenteossa ja resurssoinnissa on huomioitava tietoturvallisuus, koska palvelujen tuottaminen ja niiden tukemat ICT-ratkaisut muuttuvat yhä monimutkaisemmiksi.

Konsernin ja tietohallinnon tietoturvaan liittyvät roolit ovat tyydyttävällä tasolla, joka tarkoittaa, että suunniteltuja toimenpiteitä pystytään toteuttamaan ja edistämään. Sen sijaan toimialoille olisi perustettava tai allokoitava lisää rooleja tai työaikaa, joissa keskitytään tietoturvallisuuteen. Toimintojen erilaisuudesta ja laaja-alaisuudesta johtuen konsernilla ei ole aikaa eikä resursseja pureutua toimialojen erityispiirteisiin tai niiden erityislainsäädännön tai toimintaympäristön asettamiin vaatimuksiin.

Tietoturvallisuuteen liittyvät investoinnit ovat tyypillisesti euromääräisesti suuria. Kehittämisen ja investointien tulee olla tulevaisuuteen katsovia ja mahdollisuuksien mukaan myös teknologiariippumattomia. Tietoturvallisuuden kehittämiseen on pystyttävä investoimaan, jotta siihen liittyvä korjausvelka ja tunnistetut riskit voidaan minimoida.

Tietosuojan osalta kehittämiskohteet vuodelle 2020 ovat seuraavat:

1. Verkkokoulutuksen jalkauttaminen kaupunkitasoisesti onnistuneesti
   - Tavoitteena on, että verkkokoulutus on otettu käyttöön kaikilla toimialoilla ja kaikissa yksiköissä.
   - 80 % kaupungin työntekijöistä on suorittanut koulutuksen vuoden 2020 loppuun mennessä.
2. Tietosuojan huomioiminen erilaisissa digikehitysprojekteissa
   - Nykyistä projektiprosessia selkeytetään, jotta voidaan varmistaa, että tietosuojavaatimukset huomioidaan kokonaisvaltaisesti sellaisissa projekteissa, joihin liittyy henkilötietojen käsittelyä.
   - Kehittämiskohteella on vahva yhteys riskienhallintaan. Rekisterinpitäjän velvoitteena on huomioida toiminnassaan henkilötietojen käsittelyn riskit ja kohdistaa tarvittavat toimenpiteet niiden minimoimiseksi. Mikäli henkilötietojen käsittelyyn liittyviä riskejä ei arvioida esimerkiksi kysymyspatteriston avulla, Espoo ei pysty osoittamaan noudattavansa osoitusvelvollisuutta ja riskiperusteista lähestymistapaa eikä saamaan riittävästi tietoa päätöksenteon tueksi.
   - Lopputuloksena sujuvoitetaan käyttöönottoprosessia, kun roolit ja vastuut on selkeästi määritelty (kuka tekee, mitä tekee, kenelle tehdään).
3. Tietosuojan tilannekuvan parantaminen ja selkiyttäminen
   - Ulkopuolinen näkemys tarjoaa uudenlaisia näkökulmia tietosuojan kehittämiseen ja ennen kaikkea riippumattoman arvion vaatimustenmukaisuuden nykytilasta..
   - Toteutetaan vuoden 2020 aikana laaja GDPR-auditointi.

14 Valtiovarainministeriön tietosuojan yhteishankkeiden materiaalit.

4. Tiedon elinkaaren hallinnan parantaminen
    - GDPR edellyttää huolehtimista tiedon elinkaaren hallinnasta. Kun perustetta tiedon säilyttämiselle ei ole joko organisaation omasta toiminnasta tai lainsäädännöstä johtuvasta syystä, tieto pitää joko poistaa tai arkistoida historialliseen tai tieteelliseen käyttöön.
    - Espoossa haaste ei ole, että arvokasta tietoa tuhoutuisi vaan se, että sirpaleisen henkilötiedon poistamisesta ei huolehdita. Tällaisella ei-strukturoidulla henkilötiedolla tarkoitetaan sellaista tietoa, jota ei ole mahdollista tallentaa, yleensä teknisestä syystä, sille tarkoitettuun tietojärjestelmään. Syy saattaa olla se, että tietojärjestelmä on vanha eikä se tue olemassa olevaa prosessia.
    - Tiedon elinkaaren hallintaa ja turvallista säilyttämistä parannetaan ottamalla käyttöön sensitiivisen tiedon työntila O365-ympäristössä vuoden 2020 aikana. Tälle kehittämiskohteelle perustettiin jo projekti loppuvuodesta 2019.