

Tietotilinpäätös 2023





Kuva: Freepik

Johdanto

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

Tietotilinpäätöksen tarkoituksena on arvioida tietosuojan ja tietoturvan toteutumista kaupungilla vuoden aikana ja kuinka kaupungin kyberturvallisuutta koskeva toimintaympäristö on muuttunut, sekä mitä haasteita ja onnistumisia kaupungin eri toiminnot kohtasivat.

Tietotilinpäätös on julkinen asiakirja, jolla kaupunki tuo läpinäkyvyyttä sen toimintaan julkisena organisaationa. Kuntien lisäksi tietotilinpäätöksiä laativat muun muassa Suomen Pankki, Kela, Maanmittauslaitos ja eri hyvinvointialueet.

Tämä vuoden 2023 tietotilinpäätös on aikaisempaa tiiviimpi ja myös tulevista tietotilinpäätöksissä pyritään korostamaan asialähtöisyyttä.

Espoossa 28.03.2023

Sisällysluettelo

Johdanto	2
1 Muutokset ulkoisessa toimintaympäristössä ja megatrendit.....	4
2 Tiedonhallinta ja kokonaisarkkitehtuurityö, tiedon hyödyntämisen kehittäminen.....	5
3 Konsernihallinto	6
3.1 Hankinnat.....	6
3.2 Tietosuojarahja ja henkilötietojen suojaaminen	6
3.3 Tietoturvaryhmä ja toimintaympäristön seuranta.....	7
4 Kasvun ja oppimisen toimiala	9
5 Elinvoiman tulosalue	10
6 Kaupunkiympäristön toimiala.....	11
7 Arviointi ja mittarit	13
7.1 Rekisteröityjen oikeuksien toteutuminen.....	13
7.2 Tietoturvapoikkeama ja -uhat.....	14
7.3 Henkilötietojen tietoturva- ja tietosuojaloukkaukset.....	14
8 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen	16
9 Tietoriskien hallinta osana Espoon palveluita.....	17



Kuva: Heidi-Hanna Karhu

1 Muutokset ulkoisessa toimintaympäristössä ja megatrendit

Megatrendeissä vuonna 2023 Ukrainan kriisin, eli Venäjän hyökkäyssodan Ukrainaan, vaikutukset olivat edelleen runsaasti esillä julkisissa keskusteluissa, mutta erityisesti loppuvuotta kohden kriisin jatkumisesta ja poikkeusoloihin varautumisesta muodostui tavanomainen osa kansallista toimintaympäristöä.

Tekoälyn käytön vahvistuminen ja saatavuus kasvoivat huomattavasti aikaisempiin vuosiin verrattuna, jonka seurauksena myös Espoolla laadittiin paikallistason ohjeistusta tekoälyn käytölle. Tekoälyn käyttöön liittyy edelleen huolia tietojensiirron, poistettavuuden ja luotettavuuden osalta.

Kansallisessa toimintaympäristössä keskustelu tiedonhallintalain toteuttamisesta siirtyi kohti NIS2-direktiivin toteuttamista ja sen myöhemmin mukanaan tuomia lainsäädännöllisiä muutoksia. Mahdollisesti koskien kuntia virkavelvollisuuksien tarkentumisena ja erilaisina toimenpidesuosituksina, kuten raportointina Kyberturvallisuuskeskukselle. Muutoksista on odotettavissa tarkempia lisätietoja 2024-2025 aikana.

Espoon paikallisessa toimintaympäristössä toteutettiin viimeiset toimet siirtymässä hyvinvointialueille, eli kaupungin hyvinvoinnin ja terveyden toimiala siirtyi lopullisesti historiaan. Nähtävissä oli myös verkkohuijareiden siirtyminen paikallisemmalle tasolle huijausviestien kieliasun muuttuessa uskottavammaksi ja kohteiden valikoituessa yksittäisiksi espoolaisiksi toimijoiksi.



Kuva: Pixabay

2 Tiedonhallinta ja kokonaisarkkitehtuurityö, tiedon hyödyntämisen kehittäminen

Kaupunkitasoisella kokonaisarkkitehtuurityöllä mahdollistetaan tiedonhallinnan strateginen kehittäminen, luodaan yhteentoimivuutta toimintamallien, tietojärjestelmien ja organisaation osien välille, autetaan varmistamaan tietoturvan ja tietosuojan toteutumista, sekä tuetaan kaupungin toimialoja ja tulosyksiköitä heidän omassa kehittämissyössään.

Vuoden 2023 aikana aloitettiin työ tiedonhallinnan velvoitteiden ja niiden toimeenpanon selkeyttämiseksi kaupungin toiminnassa. Työssä tarkasteltiin tiedonhallinnan velvoitteita kokonaisuutena käsittäen tiedonhallintalain, tietosuojasääntelyn, arkistolain ja julkisuuslain velvoitteet.

Työssä pyrittiin löytämään näiden velvoitteiden toteuttamiseksi sujuvia toimintamalleja, jotka samalla tukevat Espoo-tarinan tavoitteiden saavuttamista. Samalla tunnistettiin tarve lisätä tietoisuutta tiedonhallinnan velvoitteista sekä niiden osaamista läpi kaupungin organisaation.

Kokonaisarkkitehtuurityötä kehitettiin siten, että toiminnan muutokset ja muutoksen läpivienti pystyttäisiin paremmin huomioimaan osana ICT-kehittämistä. Tämä tarkoittaa myös miten toiminnalliset tarpeet ja vaatimukset kuvataan kehittämisprojekteissa, jotta hankittavat tai toteutettavat ratkaisut vastaisivat tarpeisiin kustannusvaikuttavilla tavoilla

Tiedon hyödyntämisen kyvykkyksiä kehitettiin eri tavoin. Vuoden alussa Espoolla otettiin käyttöön uusi johtamisen ja talousohjauksen tietojär-

jestelmä, joka parantaa tiedolla johtamisen kyvykkyksiä taloustiedon ja tavoitteiden seurannan osalta. Myös muita kaupungin data-alustaa hyödyntäviä raportointiratkaisuja kehitettiin ja kehittämisen tueksi laadittiin tietotuotteiden hallintamalli. Kaupungin tulosyksiköt kehittivät tiedon hyödyntämistä toteuttamalla erilaisia työpöytä näkymiä tarpeisiinsa. Tiedon hyödyntämistä päätöksenteon tukena kehitettiin vaikuttavuudella johtamisen piloteissa.

Organisaatorajat ylittävää hyvinvointitiedon hyödyntämistä kehitettiin Espoon aloitteesta Valtiovarainministeriön digikannustinrahoitusta saaneessa yhteistyöprojektissa, johon osallistuvat Espoon lisäksi Länsi-Uudenmaan hyvinvointialue ja alueen kunnat.

3 Konsernihallinto

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

3.1 Hankinnat

Espoon kaupungin Hankintakeskus vastaa hankintalain soveltamisalaan kuuluvien hankintojen valmistelusta, poislukien kaupunkiympäristön toimialan rakennusurakat ja suunnittelukilpailut.

Hankinnoissa käytetään vakiomuotoisia henkilötietojen käsittelyä koskevia sopimusliitteitä, joita päivitetään tarvittaessa lainsäädännön muutoksia ja tulkintoja vastaavasti.

Hankintakeskuksella on oma tietosuojaryhmä, johon myös kaupungin tietosuojavastaava kuuluu ja jossa käsitellään kaikki hankintakeskuksen kilpailuttamat hankinnat. 2023 aikana ryhmä korjasi toimintaa havaitessaan puutteita.

Hankinnoissa tietosuojaan liittyvät puutteet koskivat enimmäkseen kansainvälisiä tiedonsiirtoja ja niiden riittävää huomioimista. Tähän on odotet-

tavissa 2024 aikana lisätarkennuksia EU-tasaisen sääntelyn kehittyessä, jolla voi olla vaikutuksia muun muassa kaupungin tuleviin ja käytössä oleviin pilvipalveluhankintoihin.

3.2 Tietosuojaryhmä ja henkilötietojen suojaaminen

Espoossa tietosuojan tilannetta ja toteutumista seuraa kaupunkitasoinen tietosuojaryhmä. Tietosuojaryhmään kuuluvat muun muassa toimialojen tietosuojan yhdyshenkilöt, jotka omalta osaltaan huolehtivat toimialansa erityislainsäädännön huomioimisesta tietosuojatyössä.

Osa tietosuojaryhmän jäsenistä siirtyi vuoden 2023 alussa Länsi-uudemaan hyvinvointialueen (LUVN) palvelukseen. Hyvinvoinnin ja terveyden palvelut olivat keskeinen osa kaupunkitasoista tietosuojaa, koska palveluissa käsiteltiin runsaasti salassa pidettäviä ja erityisiin henkilötietoryhmiin kuuluvia tietoja. Näitä olivat muun muassa etninen alkuperä, terveystiedot ja seksuaalinen suuntautuminen.

Terveyteen ja hyvinvointiin liittyvät järjestelmät ja rekisterinpitäjyydet siirtyivät LUVN:lle, mutta osa vuotta 2023 vanhemmista arkistoista jäi kaupungille. Tietosuojaoselosteita päivitettiin ja eri sopimuksia kunnan ja toimittajien kanssa tarkistettiin -myös kunnan ja LUVN:n välillä, jotta esimerkiksi tilaavavonta ei esty.

Tietosuojavaltuutetun toimisto ja hallinto-oikeuden päätöksien mukaan Espoon koulujen käyttämä Google Workspace for Education –oppimisympäristön käsittelyperuste ei ole ollut tietosuoja-asetuksen mukainen. Päätöksestä ja päätöksen seuraamuksista ohjelmiston käytön jatkokon keskusteltiin ryhmässä, jonka lopputuloksena kaupunki valitti päätöksestä korkeimpaan hallinto-oikeuteen. Hallinto-oikeuden päätös ei ole vielä tätä kirjoitettaessa lainvoimainen, vaan siihen odotetaan ratkaisua korkeimmas- ta hallinto-oikeudesta.

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

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

3.3 Tietoturvaryhmä ja toimintaympäristön seuranta

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

Vuoden aikana ryhmässä käsiteltiin muun muassa seuraavia tietoturvaa ja tietosuojaa koskevia muutoksia:

- **Tiedonsiirtoja Yhdysvaltoihin**, joista pääkaupunkiseudun yhteinen kirjastotoiminta sai Apulaistietosuojavaltuutetulta huomautuksen Google Analyticsin käytöstä. Ryhmä suositteli, että yhdysvaltalaisten analytiikkatyökalujen käyttöä tulee välttää ja tiedonsiirtojen vaikutuksia tulee arvioida jatkossa tarkemmin.
- **Hyvinvointialue -siirtymän** vastuita ja yhteisiksi jäävien palveluiden pääsynhallintaa, sekä väliaikaisten ratkaisuiden purkua. Pysyviksi jäävien tietoturvaa ja tietosuojaa suositeltiin arvioimaan uudelleen kirjallisilla tietoriskien ja henkilötietojen vaikutustenarvioinneilla.
- **Ryhmän oman toiminnan ja toimintaympäristön seurannan tavoitteita**, joissa Espoon ja kuntien yleisenä haasteena ovat organisaatioyksiköiden ylittävän viestinnän haasteet, sekä resurssointi. Resurssoinnin todettiin nojaavan kunkin kunnan hallintosäännöissä ja toimintaohjeissa oleviin linjauksiin, joka voi hajauttaa esimerkiksi lakisääteisen tehtävän suorittamisen eri organisaatioyksiköihin.

- **Huijausviesteihin** kuukausittain erehtyvien työntekijöiden lukumäärää, joka kaikkien yksiköiden välillä oli yhteensä 5-10, eli 60-120 onnistunutta huijausta vuodessa. Näistä suurin osa estettiin automatiikan avulla, mutta keinoja ihmisten erehtymisen tai tahallisen toiminnan estämisestä harkittiin. Esimerkiksi yhteystietojen peittämistä Espoo.fi-sivuilla ja erillisen varoitussivun asettamista ulkopuolisille linkeille, mutta ryhmä päätyi toteamaan nykyisten teknisten ja hallinnollisten keinojen olevan riittäviä.
- **Henkilöstön kouluttamista**, jossa ryhmä totesi kunnalla olevan tarve luoda erillinen koulutussuunnitelma kuntatyön erityisiä tietoturva vaatimuksista varten, joita muodostuu kuntia koskevasta lainsäädännöstä, hallinnollisista toimintatavoista ja käytössä olevien ohjelmien erityispiirteistä.

Kokonaisuutena kaupungin sisäinen toimintaympäristö oli vakaa, mutta ulkoinen kehittyi kohti tekoälyn käyttöä ja uskottavampia huijausyrityksiä kohti, joita räätälöidään aikaisempaa enemmän Espoosta julkisesti tarjolla olevien tietojen pohjalta. Pitkällä aikajänteellä anonyymeistä viestintäkanavista muodostuu jatkuvasti vaarallisempia portteja kaupungin toiminnan jatkuvuudelle.



Kuva: Heidi-Hanna Karhu

4 Kasvun ja oppimisen toimiala

Kasvun ja oppimisen toimialalla henkilötietojen käsittelyn isoimmat henkilötietoryhmät liittyvät opetuksen ja varhaiskasvatuksen järjestämiseen.

Kasvun ja oppimisen toimialan suurin projekti 2023 oli DigiOnen tuotekehitystyö, minkä tavoitteena oli luoda oppimisen ja koulutuksen järjestelmiä yhteen kokoava valtakunnallinen digitaalinen palvelualusta.

Kehitystyö ei pysynyt alkuperäisessä aikataulussa, eikä suunniteltuja käyttöönottoja pystytty tekemään 2023. Espoon osalta DigiOne päättyi keväällä 2024, kun Espoon kaupunginhallitus päätti irrottautua hankkeesta.

Teknisiä tietoturvariskejä ja haavoittuvuuksia selvitettiin vuoden aikana, jotka myös korjattiin.

Otaniemen lukiossa paljastui marraskuussa 2023 tietoturvapoikkeama, kun osana verkon tietoturva-analysointia paljastui useampia lukion oppilaskannettavia, joihin oli luotu local admin - käyttäjätunnuksia. Local admin - käyttäjätunnusten avulla opiskelijat olivat asentaneet koneille sekä opiskeluissa tarvittavia ohjelmia, mutta myös esim. pelejä ja muita opiskeluun liittymättömiä ohjelmistoja. Luvattomien käyttäjätunnusten asentaminen perustui yleisesti tiedossa olevaan Windows-käyttöjärjestelmän haavoittuvuuteen, tähän liittyvää informaatiota on helposti saatavilla mm. internetin eri keskustelupalstojen yhteydestä. Ilmiön paljastuttua osoittautui, että lukiolaiskannettavien hakkerointi oli opiskelijoiden keskuu-

nessa varsin yleistä, tietoturvapoikkeaman piiriin kuuluvia tietokoneita oli lopulta muutamia satoja. Koneet uudelleenasennettiin Espoon kaupungin palveluntarjoajan toimesta, ja suoritettiin useampia muita toimenpiteitä opiskelijoiden ja opettajien tietoisuuden lisäämiseksi tietoturvaan liittyvistä Espoon kaupungin käytänteistä ja ohjeistuksista.

Varhaiskasvatuksen toiminnanohjausjärjestelmä eVaka on usean eri kunnan yhteistyössä tuottama varhaiskasvatuksen toiminnanohjausjärjestelmä, jonka kehitys aloitettiin Espoossa 2017. Järjestelmässä toteutettiin vuoden aikana uusia toiminnallisuuksia, kuten palveluohjauksen viestit, loma-ajankyselyt, tulotietojen sähköinen toimittaminen, varhaiskasvatuspaikkatakuu ja eri asiakirjojen siirtäminen sähköisiksi.

Google Workspace for Education opiskeluympäristöön liittyen kesäkuussa 2023 Espoon kaupunki sai Helsingin hallinto-oikeudelta päätöksen. Hallinto-oikeus yhtyi aikaisemmin tietosuojavaltuutetun antamaan näkemykseen siitä, ettei kaupungilla ole ollut mahdollisuutta valvoa ja ohjeistaa riittävästi Googlen suorittamaa henkilötietojen käsittelyä. Päätöksestä on valitettu korkeimpaan hallinto-oikeuteen, johon Espoo edelleen odottaa vastausta.

Kasvun ja oppimisen toimialalla on vuodelle 2024 kehittämiskohteiksi tunnistettu edelleen asiakirjojen sähköisen käsittelyn ratkaisujen kehittäminen ja käyttöönotto. Henkilöstön tietosuojan osaamisen ylläpitämiseen ja lisäämiseen panostetaan edelleen sekä tietosuojaprosessien kehittämiseen. Tulevan vuoden aikana on tarkoitus jatkaa auditointeja hallinnollisten tietoriskien osalta. Erityisesti kiinnitetään huomiota siihen, miten sensitiivisiä dokumentteja käsitellään ja säilytetään.



Kuva: Taru Turpeinen

5 Elinvoiman tulosalue

Elinvoiman tulosalue vastaa kaupungin elinvoiman, kilpailukyvyyn ja vetovoiman vahvistamisesta sekä edistää kuntalaisten ja asiakkaiden hyvinvointia, yhteisöllisyyttä ja osallisuutta yhteistyössä toimialojen ja kumppaneiden kanssa. Elinvoiman tulosalueeseen kuuluvat Elinkeino ja työllisyys tulosityksikkö, Kulttuurin tulosityksikkö sekä Liikunnan ja urheilun tulosityksikkö. Tulosityksiköt vastaavat muun muassa kaupungin liikunta- ja kulttuuritoiminnoista, kirjastoista, museoista sekä laajasti elinkeinon ja työllisyyden tehtävistä. Vuoden 2023 aikana päätettiin, että Espoon kaupungin hyvinvoinnin, terveyden ja osallisuuden edistämisen tehtävät keskitetään Elinvoiman tulosalueelle perustettavaan tiimiin.

Vuonna 2023 Elinvoiman tulosalue valmistautui tulevaan TE-palveluiden uudistukseen, jonka myötä TE-palvelut ja näiden työntekijät siirtyvät kuntien vastuulle. Palveluiden järjestämisvastuu siirtyy kunnille vuoden 2025 alussa. Järjestämisvastuun siirto aiheutti kysymyksiä vastuunjaosta, toimintatapojen yhteensovittamisesta, henkilökunnan osaamisesta, koulutuksesta, sekä käytettävien työkalujen valinnassa. Puutteet näissä voivat aiheuttaa uusia tietoturva- ja tietosuojariskejä, joita siirtymäaikana pyritään poistamaan.

Kulttuurin tulosityksikössä käynnistettiin vuonna 2023 uusi kokoelmanhallintajärjestelmän käyttöönottoprojekti. Uudesta järjestelmästä tavoitellaan merkittävää parannusta paitsi toiminnallisuuden, myös tiedonhallinnan ja tietoturvan osalta.

Vuonna 2022 arvioitiin Liikunnan tulosityksikön varausjärjestelmä ja Elinkeino- ja työllisyystulosityksikön asiakashallintajärjestelmä lisäsuojatoimia edellyttäväksi järjestelmiksi. Vuoden 2023 aikana aloitettiin projekti, jonka tavoitteena oli korvata käytössä oleva tilavarausjärjestelmä uudenaikaisemmalla järjestelmällä sekä kirjaston Varaamo-niminen palvelu, jolla pystytään varaamaan kirjaston ja palvelutorin kokoustiloja, varattavia laitteita ja muita resursseja. Elinkeino- ja työllisyystulosityksikön asiakashallintajärjestelmän osalta suunniteltiin uudistusta järjestelmään.



6 Kaupunkiympäristön toimiala

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

Vuoden 2023 aikana kaupunkiympäristön käyttämiä tiloja katselmoitiin turvallisuuskävelyn aikana, josta kerättyjen huomioiden pohjalta turvallisuuspuutteita korjattiin. Kaupunkiympäristön toimialan ylläpitämissä kaupungin työtiloissa on jatkokehitetty yhdessä toimialojen kanssa turvallisuusjärjestelmiä kuten kamera- ja murtohälytysjärjestelmiä. Näillä toimilla toimiala pyrkii varmistamaan kaupungin toimitilojen turvallisuuden esimerkiksi toimistotiloissa ja kouluissa.

Osa toimialan henkilöstöstä siirtyi vuoden alussa Länsi-Uudenmaan hyvinvointialueelle, jonka yhteydessä kaupungin ja hyvinvointialueen tarvitsemia järjestelmien käyttöoikeuksia selvitettiin ja uusittiin yhteistyön sopimusmalleja muun muassa tietojen luovutuksen osalta. Toimiala on turvannut muun muassa pelastustoimen tietojen saannin pelastustoimitehtävissä ja HSY:n tietojen käytön.

Tarvittavista järjestelmistä tehtiin tarkemmat tietosuojan vaikutustenarvioinnit. Toimialan tietojen käsittelyssä on jatkuva tarve turvapostien ja

sähköpostien salaamiselle, ja niiden käyttöä on tarkennettu. Lisäksi henkilöstöä on ohjeistettu käymään kaupungin yleinen tietosuojaja- ja tietoturvakoulutus, jolla varmistetaan henkilöstön riittävä osaamisen taso.

Sovellusten käyttöjärjestelmiin suoritettiin kaupallisilta toimijoilta tilattuja tietoturva-auditointeja ja järjestelmien käyttövaltuushallintaa kehitettiin. Toimiala teki dokumenttienhallintaan liittyvän selvityksen, missä muun muassa tunnistettiin aineistojen tallennuspaikkojen kehitystarpeet.

Kuntapaikkatietojärjestämän käyttöönoton yhteydessä tietoturva-vaatimuksia tarkennettiin ja tilapalveluiden sähköisen kauppapaikan kehittäminen aloitettiin.



Kuva: Elena Savina

7 Arviointi ja mittarit

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

7.1 Rekisteröityjen oikeuksien toteutuminen

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

2023 aikana todettiin, että kaupungin tietosuojaselosteet ovat pääosin riittäviä, mutta niitä voisi edelleen yhtenäistää ja kertoa kuinka rekisteröidyt voivat hyödyntää tiedonsaantioikeuksiaan. Muun muassa tietosuojavaltuutetun ja hallinto-oikeudet päätökset Googlen palveluiden käytöstä (Tietosuojavaltuutettu 13.12.2022) tulevat edellyttämään muutoksia selosteisiin

ja niiden pohjana toimiviin tietojenkäsittelyn perusteisiin, sekä vaikutustenarviointeihin. Tietosuojaselosteita oli 31.12.2023 Espoolla yhteensä 137 kappaletta:

Tietosuojaselosteiden lukumäärä 31.12.2023

Toimiala	Lukumäärä
Espoo yhteensä	137
Konsernihallinto	33
Elinvoima	32
Kasvu ja oppiminen	19
Tekninen ja ympäristötoimi	52
Yleinen	1

Tietopyynnön voi toimittaa postitse tietosuojaselosteessa mainitulle yhteyshenkilölle tai asioimalla henkilökohtaisesti asiointipisteessä tai kirjaamossa, missä tarkistetaan asiakkaan henkilöllisyys. Tapauksissa, joissa henkilö pyytää tuntemattomasta sähköpostiosoitteesta kaikkia henkilö-

tietojaan, tätä pyydetään ensin tunnistautumaan asiointipisteellä käsittelyn aloittamista varten.

Nykyisillä kaupungin prosesseilla pelkkää sähköpostiosoitetta ei voida pitää lain julkisen hallinnon tiedonhallinnasta 906/2019 § 14 mukaisena riittävän tietoturvallisena vastaanottajan tunnistamistapana, koska laaja tiedonkeruu todennäköisesti johtaa salassa pidettävän tiedon muodostumiseen. Useimmat 2023 aikana kaikkia tietoja vain sähköpostilla pyytäneistä ei saapunut tunnistautumaan. Tietopyyntöprosessin sähköistäminen toisi ratkaisun moneen tietopyyntöihin liittyvään haasteeseen.

7.2 Tietoturvapoikkeama ja -uhat

Espoon asuntojen nimissä lähetettiin huijaustekstiviestejä, joissa vastaanottajia kehoitettiin muuttamaan vuokralaskujensa vastaanottava pankkitili. Tekstiviestien käyttö ei ollut uutta, mutta 2023 paikallisen espoolaisen toimijan käyttäminen kyllä. Samoin uskottava suomenkielen käyttö, joka viittasi Suomessa toimivaan tahoon. Trendi jatkui loppuvuoden ajan rehtorien ja koulujen nimissä, johon hyökkääjät olivat etsineet tietoja kaupungin julkisilta sivuilta ja some-alustoilta.

Espoon perusopetuksessa ja lukiossa paljastui vuoden aikana kaksi laajempaa huomiota saanutta tietoturvapoikkeamaa. Kyseisissä tapauksissa opiskelijat pystyivät palauttamaan hallussaan oleviin kaupungin tietokoneisiin tehdasasetukset, jolloin opiskelijat olivat voineet asentaa omia ohjelmia ja pelejä. Tämä oli mahdollista, koska Windows-käyttöjärjestelmässä oli tunnettu ominaisuus, jonka käyttö ei tuolloin oltu kaupungin tai kaupungin laitetoimittajan puolesta estetty. Kuvaus tapahtuneesta:

- Otaniemen lukiossa kävi ilmi osana verkon tietoturva-analysointia, että oppilailla oli käytössä useita läppäreitä, joihin oli luotu

paikallisen järjestelmänvalvojan käyttäjätunnus. Tämän ei pitänyt olla mahdollista

- Järjestelmänvalvojan tunnuksilla opiskelijat olivat asentaneet koneille sekä opiskeluissa tarvittavia ohjelmia, mutta myös pelejä ja muita opiskeluun liittymättömiä ohjelmistoja
- Ilmiön paljastuttua osoittautui, että lukiolaiskannettavien estojen ohittaminen ominaisuutta hyödyntämällä oli opiskelijoiden keskuudessa varsin yleistä. Poikkeaman piiriin kuuluvia tietokoneita oli lopulta muutamia satoja
- Tietokoneet asennettiin uudelleen ja kaupunki tiedotti opiskelijoita ja opettajia tietoturvaan liittyvistä kaupungin käytänteistä ja ohjeistuksista, jotka ovat ehto läppärin myöntämiselle
- Tietoturvapoikkeama sai julkisuuden huomiota eri uutismedioissa

Espoo on panostanut tietosuojan ja -turvan paremmin huomioimiseen pilvipalvelussa hankkimalla Googlen Plus-lisenssit, joiden avulla tietojenkäsittely voidaan rajata EU/ETA alueelle. On kuitenkin mahdollista, että 2024-2025 Googlen palveluiden käyttöä joudutaan arvioimaan uudelleen.

Kaupunkiympäristön toimialalla koettiin läheltä piti -tilanne, jossa kaupungin maakaapelien sijaintitiedot olivat vaarantua useiden muiden asiakastietojen kera. Syynä tähän oli toimittajan vanhentunut palvelin, joka oli määrä poistaa mutta se oli jätetty aktiivisena verkkoon. Lisätutkimuksen jälkeen palvelimesta vastuussa oleva toimittaja vahvisti, että tietomurto ei koskettanut Espoota. Tapaus osoitti kuitenkin, että nykyisillä megatrendeillä kaupungin kaapelien ja tilojen sijaintitietoja on tarpeen suojella ja toimittajien tietoturvan tasoa testata.

7.3 Henkilötietojen tietoturva- ja tietosuojaloukkaukset

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

Tietosuojaloukkausten määrä vuonna 2023 oli 41 kappaletta. Eniten henkilötietojen tietosuojaloukkauksia tapahtui kasvun ja oppimisen toimialalla, joita oli 18 kappaletta. Muilla toimialoilla tapahtui yksittäisiä henkilötietojen tietosuojaloukkauksia, joilla ei ollut yhdistävää tekijää tai erityistä motiivia. Kaikkia tapahtumia ei välttämättä kuitenkaan raportoida tai niitä ei osata tunnistaa.

Näistä tietosuojavaltuutetulle ilmoitettiin 18 ja asianomaisille rekisteröidyille 20 poikkeamasta. Tietosuojaloukkausten keskimääräinen lukumäärä on pysynyt samana vuodesta 2020 alkaen ja 2023 suuria muutoksia ei nähty. Keskiarvo tietosuojaloukkauksille on 66 tapausta vuodessa.

Esimerkkeinä vuonna 2023 esiin tulleista tietosuojaloukkauksista: päiväkotia vaihtaneen lapsen terveydentilaa koskevat paperit toimitettiin uuteen päiväkotiin ja ne katosivat. Toisessa tapauksessa epäiltiin, että asiakkaalle oli vahingossa lähetetty toisen asiakkaan tiedot. Näissä ja muissa vuoden tapahtumista suurin syy loukkauksille ovat edelleen inhimilliset erehdykset, joista tavanomaisia syitä ovat esimerkiksi väärän liitteen valinta, tietojen lähettäminen väärälle vastaanottajalle tai liian laajalla jakelulla, tai vastaava vahingossa tapahtuva tietojen paljastuminen sivulliselle.

Myös palveluntuottajien virheet johtuvat usein samasta syystä ja vähäisessä määrin esimerkiksi vanhentuneen ohjelmaversion aiheuttamasta tietomurrosta. Kaupunki vastaa rekisterinpitäjänä myös palveluntuottajien aiheuttamista tietosuojavirheistä.



Kuva: Freepik

8 Riittävän henkilöstön tietoturvaan ja tietosuojaan perehtyneisyyden osoittaminen

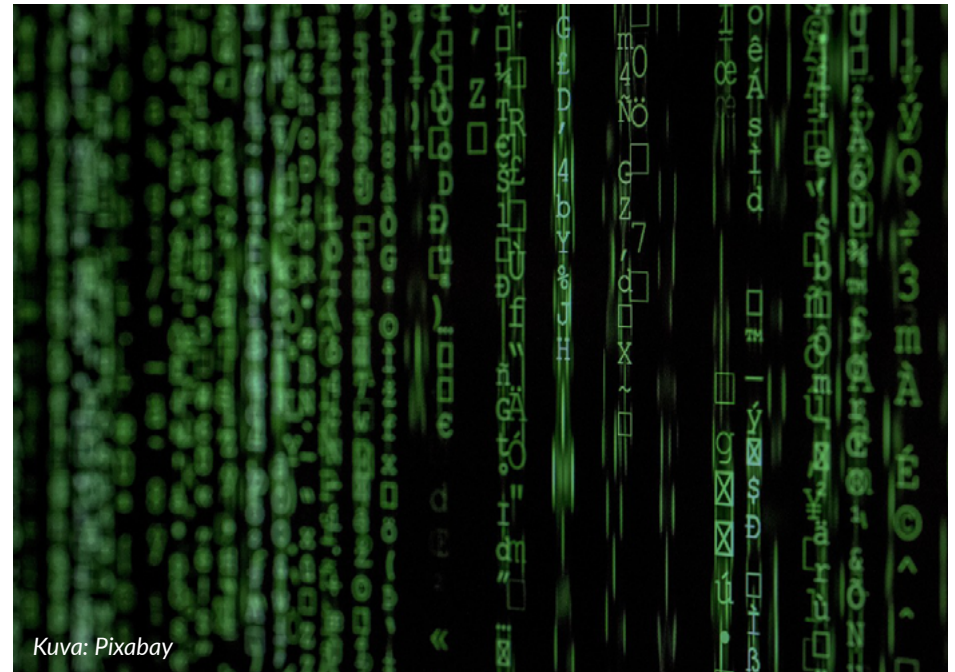
Espoolla on noin 11 000 työntekijää, jotka hoitavat laajaa kirjoa kaupungin lakisääteisiä tehtäviä. Tehtävien hoitamisen edellyttää tiedon tuottamista ja käsittelyä, josta osa on salassa pidettäviä tai paljastuessaan potentiaalisesti vahingollista kunnan tai rekisteröityjen eduille.

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

Aikaisemmin vuonna 2022 Espoo siirsi tietoturva- ja tietosuojakoulutukset uudelle videokoulutuslustalle, jonka avulla henkilöstön perehtyneisyyttä kaikille saatavilla olevaan tietoturvan ja tietosuojan peruskurssiin on mahdollista seurata. Vuonna 2023 kurssi uudistettiin omaksi kokonaisuudekseen ja siihen sisällytettiin myös kaupungin omaa videotuotantoa. Siirron myötä 2023 vanhemmat suoritteet vanhentuivat ja työntekijöitä kehoitettiin suorittamaan uudistettu kurssi.

Tulevan vuoden aikana kurssia tullaan jatkokehittämään tiiviimmäksi ja paremmin hyökkääjien tavanomaisia huijausmetodeja huomioivaksi. Henkilöstöltä saadun palautteen perusteella valmiina ostettavat videokurssit eivät toistaiseksi täytä tarvittavia laatuvaatimuksia niiden sisällön ja tiiviynen osalta, sekä sisällön nopean vanhenemisen johdosta. Esimerkiksi

tekoälyn käyttöä aikaisempaa uskottavamman, kokonaan suomenkielisen keskustelun luomiseksi huijausyrityksen yhteydessä.



Kuva: Pixabay

9 Tietoriskien hallinta osana Espoon palveluita

Yleisen tietosuoja-asetuksen artikla 24:n mukaisesti tietosuojan vaikutustenarvioinneissa näkökulmana on rekisteröityjen oikeuksiin kohdistuvat riskit. Lisäksi lain julkisen hallinnon tiedonhallinnasta 906/2019 § 13 mukaisesti Espoon kaupungin on selvittettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Tietoriskien arviointeja suoritettiin Espoon eri järjestelmistä vuoden 2023 aikana noin 22 kappaletta, joissa arvioitiin toimintojen valmistautumista esimerkiksi tietomurtoon, sähkökatkoihin ja tietojen väärentämiseen, sekä kehoitettiin suorittamaan riittävä määrä teknisiä tai hallinnollisia tarkastuksia palveluiden ja järjestelmien todellisen tilanteen selvittämiseksi.

Tuloksien perusteella varautumista on tehty pitkälti teknisestä näkökulmasta ja suojautuminen on riittävää, mutta hallinnollisissa toimissa on parannettavaa. Esimerkiksi suojattavan tiedon käsittelyn seuranta ja voimassa olevien käyttöoikeuksien elinkaarenhallintaa tulisi tarkentaa. Sähkökatkoihin varautuminen nojaa pitkälti varavoimaan, jonka on usein arvioitu kestävän enintään 48 tuntia, jolloin varautumista pitempiin poikkeusoloihin ei ole katsottu tarpeelliseksi.

Kokonaisuutena Espoon kaupunki on varautunut normaaliolojen häiriötilanteisiin riittävästi, mutta eri toimien yksityiskohdissa ja tosiasiallisen tilanteen varmistamisessa on 2024-2025 edelleen kehitettävää.

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





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