Rauma

TIETOTILINPÄÄTÖS 2020

Rauman kaupunki 9.2.2021

Tieto- ja asianhallinnan poikkihallinnollinen tiimi

Tietosuojavastaava

Rauman kaupunginhallitus 1.3.2021, 87§

SISÄLLYS

1 Tietotilinpäätöksen tarkoitus

Rauman kaupungin tietotilinpäätös laaditaan osana tilinpäätöstä ja sen tarkoitus on kuvata ja arvioida tieto- ja asianhallinnan sekä tietosuojan ja tietoturvan tilannetta Rauman kaupungilla. Se toimii sisäisen ja ulkoisen valvonnan tietojen käsittelyn kokonaistilanteen raporttina. Tietotilinpäätöksen tarkoituksena on osoittaa, että noudatamme EU Yleinen tietosuoja-asetusta ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimimme niin myös käytännössä. (artikla 24, Rekisterinpitäjän vastuu).

Tietotilinpäätöksen tarkoitus on toimia johdon työvälineenä palveluja kehitettäessä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan. Rauman kaupungin strategian yhtenä tavoitteena on sähköisten asiointipalvelujen toteuttaminen, joten meille on tärkeää huolehtia henkilötiedon käsittelyn ja tallentamisen turvallisuudesta koko tiedon elinkaaren ajan.

Kaupungin organisaatiossa noudatetaan kaupunginvaltuuston syksyllä 2019 hyväksymää tietosuojapolitiikkaa sisältäen tietoturvan ja siinä kuvattua tietosuojan organisaatiorakennetta. Tietosuojan koordinointi ja kehittäminen tapahtuvat tieto- ja asianhallinnan poikkihallinnollisen tiimin kautta. Tietotilinpäätöksen laatimisesta on vastannut tietosuojavastaava.

Rauman kaupunki kehittää tietojohtamisen kokonaisuutta osana Valtiovarainministeriön rahoittamaa hanketta: *Työalustoja virtaviivaistamalla hyvinvointia ja elinvoimaa koko Rauman seudulle.* Laki julkisen hallinnon tiedonhallinnasta tuli voimaan 1.1.2020. Lain tarkoituksena on edistää tiedonhallinnan yhdenmukaisuutta, tietoturvallisuutta ja kunnan digitalisointia. Tiedonhallinnan kokonaisuutta kuvataan Arterin ARC - ohjelmiston avulla.

Tietotilinpäätös itsessään on julkinen asiakirja, mutta sen liitteet ovat salaiset koskien tietosuojaan- tai tietoturvaan liittyviä raportteja, tunnuslukuja sekä kehittämisehdotuksia.

Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä. Tunnusluvut ja raportit toimitetaan puolivuosittain ja tarvittaessa.

2 Tietosuojan – ja tietoturvallisuuden toteuttaminen

Rauman kaupungin tietosuoja- ja tietoturvaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa EU yleinen tietosuoja-asetuksen velvoitteiden mukaisesti. Henkilötietojen vastuullisen käsittelyn periaatteet on jalkautettu osaksi palveluprosesseja ja toimintojen jatkuvaa kehittämistä.

Hallinto

Tietosuojan ja tietoturvan koordinointi tapahtuu osana tieto- ja asianhallinnan poikkihallinnollista tiimiä. Rauman kaupungin tietosuojavastaava on rekisteröityjen, henkilökunnan sekä tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä kaupungin sisällä sekä eri sidosryhmien kanssa. Kaupungin tietosuojavastaava kuuluu Kuntaliiton ylläpitämään valtakunnalliseen tietosuojavastaavien verkostoon. Sosiaali- ja terveystoimialalla jatkaa oma nimetty tietosuojan yhdyshenkilö sekä tietosuojatyöryhmä, koska toimialalla käsitellään pääosin erityislainsäädännön alaista arkaluonteista tietoa. Sosiaali- ja terveystoimialan tietosuojakäytänteissä tehdään tiiviistä yhteistyötä myös Satasairaalan tietosuoja- ja turvahenkilöiden kanssa. Myös sivistystoimialalla on toiminut tietosuojan yhteyshenkilöitä liittyen Chromebookien ja sen eri sovellusten käyttöönottoon.

Rauman kaupungin tietosuojaa ja tietoturvaa ohjaa kaupunginvaltuuston 18.6.2018 (§56) hyväksymä tietosuojapolitiikka, joka on laadittu EU:n yleisen tietosuoja-asetuksen, sen artikloiden ja muun noudatettavan keskeisen lainsäädännön mukaisesti ja se pitää sisällään myös tietoturvan. Tietosuojapolitiikka päivitettiin syksyllä 2019 ja se hyväksyttiin kaupungin johtoryhmässä 13.8.2019. Tietosuojapolitiikka tukee Rauman kaupungin strategian mukaisesti palvelujen tuottamista asukaslähtöisesti, tehokkaasti ja turvallisesti.

Tietosuojapolitiikka ja tietoturva 2019 sisältäen seuraavat liitteet:

1 Keskeiset käsitteet ja sanasto
2 Tietosuojan organisointi, roolit ja vastuut
3 Tietoturvapoikkeamien käsittelyprosessi
4 Tietosuoja- ja tietoturvarikkomusten seuraamustaulukko

Toimintaohjeet

Henkilöstön tietosuoja ja tietoturva - sivusto toimii intranetissa, Jemmassa ja sieltä löytyvät kaikki materiaalit, linkit, ohjeet ja lomakkeet. Jemmaan on koottu tietosuojaselosteet, joissa kuvataan henkilötietojen käsittelyperiaatteet: tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet.

HUONEENTAULUT

Henkilötietojen käsittelyn periaatteet huoneentaulu
Tietoturvallisuuden ja tietosuojan huoneentaulu 2019

OHJEET / LOMAKKEET

Kieltäytymistodistus tarkastusoikeuden toteuttamisesta
Kieltäytymistodistus tiedon korjaamisvaatimukselle
Ohje HaiPro tietoturvapoikkeamien ilmoituskäytäntö
Ohje Kameravalvonta
Ohje Salasanaohje
Ohje Tietoturvapoikkeamien käsittely

TIETOSUOJALIITE

Henkilötietojen käsittelyn ehdot, tietosuojaliite
HANSEL Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja (2017)
OHJE Henkilötietojen käsittely palvelusetelitoiminnan sääntökirjoissa

Kuntalaisia varten Rauman kaupungin internet sivuille on koottu yleisiä tietosuojaperiaatteita kuntalaisten oikeuksia. Rekisteröityjen informoimiseksi on julkaistu kuntalaisten henkilötietoja koskevat ja valiokuntien hyväksymät tietosuojaselosteet (EU Yleinen tietosuoja-asetus, artiklat 13 ja 14).

Rekisterinpitäjä huolehtii, että työntekijät jo oletusarvoisesti käsittelevät vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste ja henkilöstön tulee olla tietoisia siitä missä kaikkialla henkilötietoja sijaitsee ja miten niitä käytetään. Rekisterinpitäjä on myös vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. (EU Yleinen tietosuoja-asetus, artikla 24)

Sosiaali- ja terveystoimialan lakisääteinen Asiakastietojärjestelmien omavalvontasuunnitelma tarkentaa asiakastietojen käsittelyä sosiaali- ja terveystoimialalla ja se on hyväksytty viimeksi toimialan johtoryhmässä alkuvuonna 2021.

Henkilöstön koulutus

Alkuvuonna henkilöstön koulutusta varten käytettiin Valtiovarainministeriön yhteishankkeessa laatimaa Arjen tietosuoja-kokonaisuutta. Viime vuonna valtio julkaisi eOppivan tietosuojan ja tietoturvan koulutusosiot myös kuntien käyttöön. Todistus tietosuojakoulutuksesta tallennetaan Osaamisrekisteriin. Henkilöstölle on järjestetty keskitettyä koulutusta tietoturvasta liittyen digiajan uhkakuviin kotona ja töissä, pilvipalveluista sekä mobiililaitteiden tietoturvallisesta käytöstä. Tietosuojavastaava on pitänyt koulutusta tarpeen mukaan yksiköissä.

Henkilökunnan osaamista seurataan ja koulutusraportti on osana tietotilinpäätöstä. Henkilökunnan tietosuojaosaamisen arviointia ei toteuteta tällä hetkellä systemaattisesti, mutta esimiehet seuraavat sitä kuitenkin tarkasti. Koulutusta kehitetään keskitetysti henkilöstöpalvelujen koulutussuunnittelun kanssa.

Kaupungin henkilöstöstä Arjen tietosuoja –nettitestin vuoden 2020 loppuun mennessä on suorittanut yhteensä 2098 henkilöä luvun ollen n. 73 % koko henkilöstöstä. eOppivan kautta todistuksen osaamisrekisteriin on tallettanut 232 työntekijää. Tietosuoja –koulutus toteutetaan osana työntekijöiden perehdytysohjelmaa. Jatkossa kaikki uudet työntekijät, kesätyöntekijät ja opiskelijat tekevät nettitestin, jos työtehtäviin liittyy henkilötietojen käsittelyä. Myös luottamushenkilöiltä edellytettiin videon katsominen.

Tietosuojaa ja tietoturvaa koskevista asioista tiedotetaan säännöllisesti henkilöstölehdessä sekä sähköpostissa. Henkilöstön keskitettyjen koulutusten suunnittelussa huomioidaan tietosuoja ja tietoturva sekä keväisin että syksyisin.

Tietosuoja ja tietoturvakoulutuksia on suoritettavissa myös kaupungin hankkimassa Wistec-koulutusympäristössä.

Riskiperusteinen lähestymistapa

EU:n yleisessä tietosuojavelvoitteessa edellytetään, että riskit on otettava huomioon sisäänrakennettua ja oletusarvoista tietosuojaa toteutettaessa (artikla 25). Velvoitteet ja suojatoimet on suhteutettava tietokäsittelyjen aiheuttamaan riskiin (artikla 32). Korkeamman riskin henkilötietojen käsittely edellyttää enemmän panostamista teknisiin ja hallinnollisiin toimenpiteisiin, kun taas vähäisen riskin toiminta ei aiheuta merkittävää uhkaa rekisteröidyn yksityisyyden suojalle. (Korpisaari, Pitkänen ja Warma-Lehtinen, 2018.)

Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä hallitaan järjestelmällisesti ja ennakoivasti. Rauman kaupungin rekisterinpitäjät arvioivat henkilötietojen käsittelyyn liittyvät riskit ja valitsevat arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet osana organisaation muuta riskienhallintasuunnitelmaa talousarvion yhteydessä. Tiedonhallintalain velvoitteissa edellytetään myös riskiperustaista lähestymistapaa, joten tätä tullaan kehittämään myös jatkossa.

Tietosuojan vaikutustenarvioinnin sekä tarvittaessa ennakkokuulemisen tulisi tehdä sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Tätä vaikutustenarviointia (PIA/DPIA) sekä ennakkokuulemista (artikla 35 ja 36) ei ole vielä toteutettu.

3 Tiedonhallinta, tietovarannot ja tietovirrat

Tiedonhallinta

Laki julkisen hallinnon tiedonhallinnasta tuli voimaan 1.1.2020. Laissa säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta sekä viranomaisten tiedonhallinnan järjestämisestä ja kuvaamisesta.

Kaupungin hallintosäännön mukaan kaupunginhallitus vastaa siitä, että tiedonhallintalain 4.2 §:n vastuut, käytännöt ja valvonta on määritelty kunnassa. Tämän pykälän mukaisia vastuita ei ole vielä toteutettu.

Tiedonhallintalain (906/2019) vaatimuksiin on alettu valmistautua.

Tiedonhallintamallin on sisällettävä vähintään tiedot:

1) toimintaprosesseja kuvaavista nimikkeistä, prosessista vastaavasta viranomaisesta, prosessin tarkoituksesta sekä prosessin sidoksista muihin prosesseihin;
2) tietovarantojen nimikkeistä, kuvaukset tietovarantojen sidoksista toimintaprosesseihin ja tietojärjestelmiin sekä luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä *tietosuoja-asetus*, 30 artiklan 1 kohdassa tarkoitetun selosteen sisällöstä tai, jos selostetta ei tarvitse tietosuoja-asetuksen mukaan laatia, tietovarannosta vastaavasta viranomaisesta, tietovarannon käyttötarkoituksesta, keskeisistä tietoryhmistä tietoaineistoissa, tietojen luovutuskohteista ja tietojen säilytysajoista;
3) tietoaineiston arkistoon siirtämisestä, arkistointitavasta ja arkistopaikasta tai tuhoamisesta;
4) tietojärjestelmien nimikkeistä, tietojärjestelmästä vastaavasta viranomaisesta, tietojärjestelmän käyttötarkoituksesta, tietojärjestelmän liittymistä muihin tietojärjestelmiin ja liittymissä käytettävistä tiedonsiirtotavoista;
5) tietoturvallisuustoimenpiteistä.

Tietovarannot

Tietovarannolla tarkoitetaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettäviä tietoaineistoja sisältävää kokonaisuutta, jota käsitellään tietojärjestelmien avulla tai manuaalisesti.

Kaupungilla on käytössä esim. seuraavat tietovarannot; perusopetuksen tietovaranto, asianhallinnan tietovaranto jne. Tietovarantojen kuvaamista jatketaan.

Keskeiset tietojärjestelmät

Kaupungilla on sekä keskitettyjä koko konsernin tietojärjestelmiä että toimialakohtaisia järjestelmiä, joista keskeisimmät ovat:

- ➔ Personec F – henkilöstöohjausjärjestelmä
- ➔ Visma Intime Plus - talousohjausjärjestelmä
- ➔ ProConsona sosiaalityö - sosiaalipalveluiden tietojärjestelmä
- ➔ Tweb – asianhallintajärjestelmä
- ➔ Lifecare– potilastietojärjestelmä
- ➔ Primus/Wilma – oppilashuollon tietojärjestelmä
- ➔ Trimble Locus – paikkatietojärjestelmä
- ➔ Axiell Aurora – kirjastotietojärjestelmä
- ➔ Timmi – tilojen varausjärjestelmä

Tietovirrat

Tietovirtojen kannalta yksi keskeisimmistä tietojärjestelmistä on Visma Intime Plus-talousjärjestelmä, johon on erilaisia liittymiä useista kaupungin tietojärjestelmistä, joissa käsitellään rahavirtoja.

Trimble Locus ja ProConsona järjestelmissä tarvitaan ajan tasalla olevia väestötietoja, jotka kopioidaan säännönmukaisesti Digi- ja väestötietoviraston aineistosta.

Tiedonhallinnan toteuttamisen vaatimusten mukaisesti tietovirtojen kuvaukset on aloitettu ja välineeksi on valittu Arter Oy:n toimittama ARC sovellus.

Vuoden 2020 alussa on astunut voimaan myös laki digitaalisten palvelujen tarjoamisesta (306/2019), josta käytetään myös nimitystä saavutettavuusdirektiivi. Kaupungin nettisivut on päivitetty lain vaatimusten mukaisesti.

Tiedonhallintalain 28§ mukaista asiakirjajulkisuuskuvausta on alettu laatia.

4 Asianhallinta

Assi (Tweb) on Triplan Oy:n toimittama asianhallintajärjestelmä, jossa pidetään yllä kaupungin diaaria, ja joka toimii keskitettynä sähköisten asiakirjojen tallennuspaikkana. Raumalla käytössä ollut KuntaToimisto ohjelmakokonaisuus korvattiin marraskuun 2020 aikana kokonaisuudessaan uudella järjestelmällä, joka on ollut Raumalla käytössä tallennuspaikkana jo useamman vuoden. Assin täysimääräinen käyttöönotto on tärkeä askel useiden eri lakien vaatimusten toteuttamisen kannalta.

Valmu on viranhaltijoille ja muille valmistelutehtäviä tekeville tarkoitettu lomakepohjainen työkalu, jolla tehdään viranhaltijapäätökset, esitykset toimielimille, esityslistat ja pöytäkirjat. Valmussa rakenteisina tehtävät asiakirjat tallentuvat Assi asianhallintajärjestelmään.

Asianhallintajärjestelmää ja siihen liittyvien muiden sovellusten tallentamista ohjaavaa tiedonohjaussuunnitelmaa ylläpidetään Triplan Oy:n WebArkki sovelluksessa.

Uuden järjestelmän myötä asiakirjojen julkisuutta ja käyttöoikeuksia pystytään hallinnoimaan yksityiskohtaisemmin ja lisäksi käyttäjien toimista järjestelmässä kertyy kattavat lokitiedot, joista on mahdollista saada tulostettua erilaisia raportteja pääkäyttäjien toimesta. Kirjaamot päätettiin säilyttää vielä toimialakohtaisina, mutta palvelukeskuksen myötä tulee tapahtumaan siirtyminen keskitettyyn kirjaamoon, minkä Assi mahdollistaa hyvin.

Assin ja Valmun käyttäjät on koulutettu kattavasti vuoden 2020 aikana. Tämän lisäksi käyttäjille on tehty Rauman omat versiot käyttöohjeista. Koulutustallenteet ja ohjeet, sekä muuta tietoa on saatavilla Jemmasta. Järjestelmän käyttäjillä on suuri vastuu siitä, että kaikki tapahtuu tietoturvallisesti.

Koulutusta ja tiedottamista on jatkettava vuoden 2021 aikana tiiviisti. Tämän lisäksi myös tiedonohjaussuunnitelmaan tehdään jatkuvasti täydentämistä ja korjauksia.

5 Tietosuoja- ja hankintasopimukset

Rauman kaupunki huomioi voimassa olevissa sekä uusissa sopimuksissa Kuntaliiton ja Hanselin valmistelemaa `Henkilötietojen käsittelyn ehdot` -tietosuojaliitettä. Toimintaperiaate on valmisteltu Rauman kaupunginlakimiehen kanssa. Kaupunginhallitus hyväksyi vuonna 2018 käytännön, jossa kaupunki toimii yhdenmukaisesti kaikkien toimittajien kanssa ja tietosuojaliitteen mukaisia ehtoja sovelletaan kaikissa Rauman kaupungin henkilötietojen käsittelyyn liittyvissä sopimussuhteissa. Toimialat lisäävät henkilötietojenkäsittelyn ehdot –liitteen sopimusten mukaisesti toimittajille.

Nyt sopimuskäytäntöä on valmisteltu uudelleen ja siihen on tuotu mukaan vaihtoehtoisia hyväksymismalleja henkilötietojen käsittelyn ehdoiksi. Hankinnoissa/hankkeissa voi olla tarpeen hyväksyä myös muunlainen sopimusehto, kuten puhtaasti JIT2015 sopimusehdot liitteineen, toimittajien omat sopimusehdot tai hankintarenkaan kilpailutukseen liittyvät ehdot. Aina on kuitenkin varmistettava, että sopimusehdot ovat EU:n yleisen tietosuoja-asetuksen (EU 679/2016) mukaiset.

6 Rekisteröidyn oikeudet ja niiden toteutuminen

Rauman kaupunki pyrkii noudattamaan henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kaupungin nettisivuilta (artiklat 13 ja 14).

Rauman kaupungin nettisivuilta löytyy rekisteröidyille tarkoitettu Tietosuojasivusto. Nettisivuilta löytyvät rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja korjaamisvaatimuslomakkeet (artiklat 15, 16).

Raumalla on käytössä Suomi.fi -viestit -palvelu, jonne tunnistautumalla asiat saa hoidettua tietoturvallisesti. Rauman nettisivuilla ohjeistetaan asiakkaita siten, että jos lähetettävä tietopyyntö sisältää henkilötietoja tai koskee aineistoa joka sisältää henkilötietoja, on suositeltavaa lähettää pyyntö suomi.fi –viestit palvelun välityksellä. Tämä koskee julkisuuslain perusteella tehtävien tietopyyntöjen lisäksi myös rekisteritietojen tarkastuspyyntöjä. Mahdollinen löydetty aineisto voidaan vaivattomasti toimittaa sähköisessä muodossa viestit-palveluun.

Henkilötietojen tietoturvaloukkauksesta ilmoitetaan valvontaviranomaiselle 72 tunnin kuluessa, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Tietosuojavastaava teki vuoden 2019 aikana yhteensä seitsemän ilmoitusta tietosuojavaltuutetulle.

Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta ilmoitetaan rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietosuojavastaavan, hallintopäällikön ja tietohallintopäällikön harkinnan mukaan. Rekisteröityihin tietosuojavastaava on ollut yhteydessä kirjeitse ja puhelimitse sekä henkilökohtaisten tapaamisten kautta.

7 Seuranta

Suomessa kansallisena valvontaviranomaisena toimii tietosuojavaltuutettu. Toiminnassaan tietosuojavaltuutettu on itsenäinen ja riippumaton. Tietosuojavaltuutettu on Euroopan tietosuojaneuvoston jäsen.

Tämä tietotilinpäätös on merkittävä rekisterinpitäjän osoitusvelvollisuuden toteuttamisen kannalta. Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät tekijät ja tätä seurantaa kehitetään jatkuvasti. Myös tuleva tiedonhallinta tuo apua tiedonkäsittelyn seuraamiseen ja arviointiin.

Henkilökunnalla on velvollisuus raportoida havaitsemistaan tietoturvapoikkeamista HaiPro- ohjelmalla, jonka ohjeet ja linkit löytyvät intranetista, Jemmasta. HaiProssa on myös mahdollisuus ilmoittaa kehittämisehdotuksista. Ilmoitukset toimivat tärkeänä osana tietoturvan kehittämistä ja koulutustarpeiden kartoitusta ja arviointia. Vuonna 2020 kirjattiin yhteensä 52 tietoturvapoikkeamaa (v. 2019 kirjattiin 86), joista merkittävä riski oli 19 poikkeamassa. Poikkeamista yhdessä todettiin vakava riski ja se liittyi Nortamon perhekeskuksen äänieristykseen. Perhekeskukseen järjestettiin katselmus, jossa oli paikalla eri hallinnonalojen edustus. Vuonna 2019 yksi vakava riski liittyi tietojen kalasteluyritykseen.

Tietosuojatilinpäätöksen raportissa salaisina (JulkL 24§, kohta 7) on kuvattu seuraavat tietosuojamittarit:

1. Henkilötietojen käsittely ja kehittämiskohteet
2. Tietoturvapoikkeamat
3. Henkilöstön koulutukset
4. Tietosuoja- ja tietoturvatilanteen itsearviointi
5. Sosiaali- ja terveystoimialan tietosuoja

8 Arviointi ja kehittäminen

Tietoturva- ja tietosuojakartoitus / Tilintarkastusyhteisö

Rauman kaupungin tilintarkastusyhteisön it-asiantuntija, tarkastaja suoritti loppuvuodesta 2019 vuoden 2019 tilintarkastuksen työohjelmaan kuuluneen Rauman kaupungin tietoturva- ja tietosuojakartoituksen. Kartoituksessa varmistettiin, että kaupungin keskeisimpien tietojärjestelmien riskienhallinta, tietoturvaturvallisuus sekä tietosuoja-asiat ovat tarkoituksenmukaisesti organisoitu, ohjeistettu ja järjestetty.

Merkittäviä riskejä tai puutteita ei havaittu käytössä olevassa tietotekniikassa. Tietoturvan sekä tietosuojan osalta ei myöskään havaittu merkittäviä puutteita. Suosituksia esitettiin lähinnä hallinnollisen tietoturvallisuuden ja tietosuojan osalta ohjeistuksien tarkentamiseen ja yhdenmukaistamiseen, koska ohjeistuksia on useissa eri dokumenteissa. Peruskäyttäjille suunnattujen tietoturva- ja tietosuojaohjeiden noudattamisen valvontaan sekä ohjeistuksien jalkauttamiseen tulee myös kiinnittää huomiota. Tietoturvallisuuden hyvä perustaso ja mahdollisten tietosuojariskien toteutumisen estäminen ja hallinta riippuvat paljolti siitä, millainen osaamistaso ja riskitietoisuus ovat todellisuudessa peruskäyttäjillä kaupungin laajassa organisaatiossa.

Kartoituksessa kiinnitettiin huomiota, miten palvelutoimittajat hallitsevat, ylläpitävät ja pääosin omistavat kaikki keskeiset prosessit, ohjelmistot, tekniset laitteistot ja tietojärjestelmät, joita Rauman kaupunki käyttää tietojärjestelmäpalveluissaan. Palvelusopimuksiin esitettiin tehtäväksi tarkennuksia riskienhallinnan osalta ja liittämään ns. GDPR liitteet niiden tietojärjestelmien osalta, joista ne vielä puuttuvat. Kaupungin palvelinten ylläpito, konesalitilat, varmistusten ottaminen, kahdennetut kriittisimmät reitittimet sekä palomuurilaitteistot käytiin läpi.

Rauman kaupungin tietoturvaa uhkaavia ulkoisia ja sisäisiä riskejä olisi suositeltavaa uudelleenarvioida vuosittain. Uudelleen arvioinnissa huomioidaan muuttuva tilanne käyttäjille suunnatuissa palveluissa ja tietojärjestelmissä (Saas-palvelut). Suositeltavaa olisi tehdä sisäistä ja ulkoista auditointia, joka antaisi tietoa mahdollisesta kouluttautumistarpeesta, kehittämistarpeesta sekä ohjeistuksien ajan tasalla pitämisen tarpeista.

Tietosuojan osalta organisointi, roolit ja vastuut ovat selkeästi esitetty ”Rauman kaupunki, tietosuojapolitiikka ja tietoturva” dokumentin liitteessä (kaupunginvaltuusto 18.6.2018 §56). Koska myös tietoturvallisuustyö edellyttää organisointia ja organisaatioissa toimivien henkilöiden vastuiden ja tehtävien määrittämistä, vastaavan tyyppinen tehtävä- ja vastuunjakomäärittely olisi suotavaa tehdä myös tietoturvan osalta. Tietoturvallisuustyössä tarvitaan jatkuvaa tilanteen seuraamista, uhkiin varautumista ja reagointia poikkeustilanteisiin. Tietoturvallisuus- ja tietosuojatyö ovat osa toimi- ja palvelualueiden sisäistä valvontaa ja riskienhallintaa.

Tietosuoja-asioissa ei löydetty huomautettavaa. Tietosuoja-asioissa on noudatettu EU tietosuoja-asetuksen ja kansallisen tietosuojalain määräyksiä ja suosituksia. Tietosuojaohjeistusta on kattavasti tarjolla käyttäjille. Tietosuojakoulutusta on tarjottu kaupungin henkilöstölle ja erityisryhmille.

Digi- ja väestötietoviraston JUDO –hanke

Rauman kaupunki osallistui Digi- ja väestötietoviraston JUDO –hankkeen työpajoihin. Hankkeesta on saatu paljon materiaalia ja vinkkejä tietosuojan ja tietoturvan parantamiseksi.

Käytännön osaamistason arvioimiseksi ja parantamiseksi osallistuimme valtakunnalliseen tietosuojan ja –turvan Taisto20 –harjoitukseen marraskuussa 2020.

Rauman kaupunki vastasi marraskuussa 2020 valtiovarainministeriön sekä Digi- ja väestötietoviraston yhdessä toteuttamaan kyselyyn koskien kuntien merkittävimpiä digitaalisen turvallisuuden riskejä ja niiden arviointia.

GDPR –itsearviointityökalun avulla toteutettu itsearviointi osoittaa keskeisimpien puutteiden liittyvän tietosuojan vaikutustenarvioinnin tekemiseen, henkilötiedon anonymisointiin, pseudonymisointiin ja henkilötietovirtojen kuvaamiseen, henkilötietoja sisältävien tallenteiden tuhoamiseen sekä sopimusten ja ulkoistusten hallintaan.

Kehittäminen

Rauman kaupunki on ollut mukana Digi- ja väestötietoviraston JUDO-hankkeessa, jossa kehitetään julkisen hallinnon digiturvan johtamista ja hallintaa sekä henkilöstön digiturvaosaamista.

JUDO-hanke tukee julkista hallintoa turvallisten ja luotettavien palveluiden kehittämisessä vuosina 2019–2021.

Valtakunnallinen tuki ja tuotetut materiaalit sekä verkkotyöpajat ovat auttaneet tietosuoja-asetuksen ja tietosuojalain velvoitteiden täytäntöönpanossa. Tietojen käsittelyn hallintaa tullaan parantamaan jatkossa tiedonhallintalain periaatteiden mukaisesti huomioiden digiturvallisuuden viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan. Tietoturvallisuuden toteuttamiseksi on mahdollista myös jatkossa ottaa käyttöön hallintamalleja esim. ISO/IEC 27001 ja niihin liittyviä auditointeja.

Keskeisinä kehittämistoimia ovat vuonna 2020 olleet uusien etäopetus- ja kokouskäytäntöjen käyttöönotto – ja osaaminen viruspandemian edellyttämien toimintamuutoksen vuoksi. Lisäksi eOppivan tietosuoja- ja tietoturvakoulutuksia julkaistiin kuntien henkilöstölle. Tietosuoja- ja tietoturvaosaamista painotettiin osana perehdytysprosessia. Tietosuojaselosteet päivitettiin saavutettavuusdirektiivin mukaiseksi kaupungin nettisivuille. Henkilöstöä informoidaan jatkuvasti liittyen erilaisiin tietoturvapoikkeamiin tai tietojen kalasteluyrityksiin.

Tietoverkon turvallisuus

Osana Rauman kaupungin tietojärjestelmien ja tietoverkon turvallisuuden kartoittamista ja parantamista, on vuoden 2020 lopussa hankittu ulkoinen (internetistä) tunkeutumistestaus kaupungin julkisia ip-osoitteita kohtaan. Testauksessa on ollut tarkoitus selvittää erilaisten standardien mukaisten menetelmien ja käytäntöjen avulla internetiin avoinna olevat julkiset ip-osoitteet ja portit sekä samalla selvittää, kuinka pitkälle ko. porteista on mahdollista päästä kaupungin järjestelmiin ja onko järjestelmissä mahdollisia haavoittuvuuksia.

Lisäksi loppuvuonna 2020 hankittiin palvelu verkkolevyjen tiedostojen skannaukseen. Tällä GDPR -data-analyysillä selvitetään ensisijaisesti henkilötietoja sisältävät verkkolevyjen tiedostot (esim. hetu). Työ kattaa kaikki Rauman kaupungin verkkolevyt.

Tieran polku

Rauman kaupunki on päättänyt ottaa osaa ”Polku Tieraan” –selvitykseen. Kuntien Tiera Oy selvittää, millaisella resursseilla kaupungin tietotekniikkapalvelut tulisi tänä päivänä hoitaa ja millaisella kumppanuudella Tiera olisi valmis toimimaan Rauman kaupungin kanssa.

Lopuksi

Henkilöstön osaaminen on tärkeä kaupungin strateginen tavoite. Tietosuoja- ja tietoturvaosaaminen on noussut keskeiseksi organisaatioiden menestystekijäksi erilaisten kalasteluyritysten ja kyberuhkien vuoksi. Kalastelukampanjat ovat yhä älykkäämpiä ja niiden torjuminen on vaikeampaa, joten henkilöstön valmiuksia osata toimia tietoturvaohjeiden mukaisesti tullaan kehittämään! Henkilöstön tietoturvapoikkeamien ilmoittaminen on osoittautunut hyväksi keinoksi lisätä tietoisuutta asian tärkeydestä.

Jatkuva vaatimus palvelujen digitalisoinnista asettaa korkeita vaatimuksia IT-palvelutuotantoon, mikä edellyttää jatkuvaa parantamista myös tietosuojassa ja tietoturvassa.

LÄHTEET

EU Yleinen tietosuoja-asetus 2016. Luettavissa: http://www.privacy-regulation.eu/fi/index.htm

EU Tietosuojan kokonaisuudistus, VAHTI raportti, 2016. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Korpisaari, Pitkänen ja Warma-Lehtinen. 2018. Uusi tietosuojalainsäädäntö. Alma Talent Oy.

Laki digitaalisten palvelujen tarjoamisesta (306/2019). Luettavissa: https://www.finlex.fi/fi/laki/alkup/2019/20190306

Laki julkisen hallinnon tiedonhallinnasta (906/2019). Luettavissa: https://www.finlex.fi/fi/laki/alkup/2019/20190906?search%5Btype%5D=pika&search%5Bpika%5D=tiedonhallinta

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019). Luettavissa: https://www.finlex.fi/fi/laki/alkup/2019/20190552?search%5Btype%5D=pika&search%5Bpika%5D=552%2F2019

Rauman kaupunki, tietosuojasivut. Luettavissa: https://www.rauma.fi/kaupunki-ja-hallinto/asiointi/tietosuoja/

Rauman kaupunki, Tietosuojapolitiikka ja tietoturva, 2019. Luettavissa: https://www.rauma.fi/wp-content/uploads/2018/08/Tietosuojapolitiikka-ja-tietoturva_2018.pdf

Tietosuojalaki (1050/2018). Finlex. Luettavissa: https://www.finlex.fi/fi/laki/alkup/2018/20181050

Tietosuojavaltuutetun toimisto, 2018. https://tietosuoja.fi/etusivu

Valtiovarainministeriö, Arjen tietosuoja 2018. Luettavissa: https://arjentietosuoja.fi/fi/#/front