TIETOTILINPÄÄTÖS 2019

Kaupunginhallitus hyväksynyt 31.3.

Rauman kaupunki Helmikuu 2020

Tieto- ja asianhallinnan poikkihallinnollinen

tiimi Kristiina Kuusio, tietosuojavastaava

SISÄLLYS

1 Tietotilinpäätöksen tarkoitus

Rauman kaupungin tietotilinpäätös laaditaan osana tilinpäätöstä ja sen tarkoitus on kuvata ja arvioida tietosuojan ja tietoturvan tilannetta Rauman kaupungilla. Se toimii sisäisen ja ulkoisen valvonnan raporttina tietojen käsittelyn kokonaistilasta. Tietotilinpäätöksen pääpaino on tietosuojassa sekä tietoturvassa sekä EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuden toteutumisessa (artikla 24, Rekisterinpitäjän vastuu). Organisaation tulee osoittaa noudattavansa asetusta ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä.

Rauman kaupungin strategian keskeinen tavoite on sähköisten asiointipalvelujen toteuttaminen. Kaupunki käsittelee paljon kuntalaisia koskevia tietoja, joten kaupungille on tärkeää huolehtia henkilötiedon käsittelyn ja tallentamisen turvallisuudesta. Tietotilinpäätöksen tarkoitus on toimia johdon työvälineenä palveluja kehitettäessä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan.

Rauman kaupungin organisaatiossa noudatetaan kaupunginvaltuuston kesäkuussa 2018 hyväksymää ja syksyllä 2019 päivitettyä tietosuojapolitiikkaa sisältäen tietoturvan ja siinä kuvattua tietosuojan organisaatiorakennetta. Tietosuojan koordinointi ja kehittäminen tapahtuvat tieto- ja asianhallinnan poikkihallinnollisessa tiimissä. Tietotilinpäätöksen laatimisesta on vastannut tietosuojavastaava.

Laki julkisen hallinnon tiedonhallinnasta tuli voimaan 1.1.2020. Laki tulee edistämään tiedonhallinnan yhdenmukaisuutta, tietoturvallisuutta ja kunnan digitalisointia. Tiedonhallinnan kokonaisuutta on lähdetty kehittämään Raumalla ja se tulee jatkossa olemaan myös osana tietotilinpäätöstä.

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 kaupunki on sisäänrakentanut tietosuoja- ja tietoturvaperiaatteita EU yleinen tietosuoja-asetuksen velvoitteiden mukaisesti. Tietosuoja on kaikkien yhteinen asia niin työntekijöiden kuin luottamushenkilöidenkin ja tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Henkilötietojen vastuullisen käsittelyn periaatteet on jalkautettu osaksi normaalia toimintaa ja toimintojen jatkuvaa kehittämistä.
Keskeisinä kehittämistoimina vuonna 2019 ovat olleet salatun sähköpostin käyttöönotto, tietoturvallisen tulostamisen ohjeistus sekä ohjeet sisäisen postin jakelukäytännöissä. Myös erilaisia varoitus- ja ohjeistusviestejä toimitetaan lähes viikoittain käyttäjille liittyen erilaisiin tietoturvapoikkeamiin tai tunnusten kalasteluyrityksiin

Tietosuoja ja tietoturva nivottiin projektissa osaksi kaupungin toimintaa ja niiden koordinointi tapahtuu osana tieto- ja asianhallinnan poikkihallinnollista tiimiä. Rauman kaupungin nimetty, lakisääteinen tietosuojavastaava toimii tehtävässä 50%:n työpanoksella. Tietosuojavastaava on rekisteröityjen, henkilökunnan sekä tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä kaupungin sisällä sekä eri sidosryhmien kanssa. 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.

Rauman kaupungin tietosuojaa ja tietoturvaa ohjaa kaupunginvaltuuston 18.6.2018 (§56) hyväksymä ja politiikka, 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 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

Tietosuojapolitiikka tukee Rauman kaupungin strategian mukaisesti palvelujen tuottamista asukaslähtöisesti, tehokkaasti ja turvallisesti. Tietosuoja ja tietoturva sivusto toimii Jemmassa ja sieltä löytyvät kaikki materiaalit, linkit, ohjeet, tietosuojaselosteet ja lomakkeet. Jemmaan on koottu keskeiset henkilötietojen käsittelyn tietosuojaselosteet, joissa kuvataan henkilötietojen käsittelyperiaatteet: tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet.

Rauman kaupungin internet sivuilla on kuvattu tietosuojaperiaatteita, kuntalaisten oikeuksia sekä kuntalaisten henkilötietoja koskevat ja valiokuntien hyväksymät tietosuojaselosteet rekisteröityjen informoimiseksi (EU Yleinen tietosuoja-asetus, artiklat 13 ja 14).

Rekisterinpitäjä vastaa, 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 johdon katselmuksessa elokuussa 2019.

Rauman kaupunki on osallistunut Valtiovarainministeriön (VM) asettamiin valtakunnallisiin yhteishankkeisiin: Juhta – julkisen hallinnon tietohallinnon neuvottelukunta ja VAHTI – julkisen hallinnon digitaalisen turvallisuuden johtoryhmä aina päätösseminaariin 4.12.2018 saakka. Sen jälkeen kaupunki on ollut mukana Digi- ja väestötietoviraston JUDO-hankkeessa, jossa kehitetään julkisen hallinnon digiturvan johtamista ja hallintaa, 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.

Henkilöstön koulutus

Koko henkilöstön koulutusta varten käytetään Valtiovarainministeriön yhteishankkeessa laatimaa Arjen tietosuoja-kokonaisuutta; netissä katsottava video ja nettitesti. Todistus suorituksesta 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. Tietoturvasta on julkaistu nyt eOppivassa kaksi verkkokoulutuskokonaisuutta: Digiturvallinen työelämä ja Toimi turvallisesti digimaailmassa verkkokoulutukset, joita on tarkoitus jatkossa myös hyödyntää tietoturvakoulutuksessa.

Henkilökunnan osaamista seurataan ja koulutusraportti on osana tietotilinpäätöstä. Henkilökunnan tietosuojaosaamisen arviointia ei toteuteta tällä hetkellä systemaattisesti. Harkittavaksi tulee systemaattisempi kouluttautuminen ja seuranta esim. Navicre tai Granite verkkojärjestelmillä. Sosiaali- ja terveystoimialan valtakunnalliset Kelan Kanta –verkkokoulut on lopetettu, joten korvaava järjestelmä tulisi hankkia. Kaupungin henkilöstöstä Arjen tietosuoja –nettitestin vuoden 2018 loppuun mennessä on suorittanut yhteensä 2072 henkilöä luvun ollen n. 71 % koko henkilöstöstä. Arjen 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.

Tietosuojaohjeet (tallennettu Jemmaan)

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

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

Rauman kaupungin tiedonhallinnan, tietovarantojen sekä niihin liittyvien tietovirtojen kokonaistilanteen kuvausta ei ole laadittu, mutta järjestelmäluettelo on ja sitä on hyödynnetty henkilötietojen kartoituksessa (järjestelmäluettelo on tietosuojatilinpäätöksen raportin liitteenä).

Vuoden 2020 alusta voimaan astuneen tiedonhallintalain (906/2019) vaatimuksiin on alettu valmistautua.
Lain vaatimuksia ovat mm.

- tiedonhallintayksikön ja tiedonhallintamallin määrittely
- toimintaprosessien kuvaaminen
- tietovarantojen sekä tietoaineistojen kuvaaminen
- tietoturvallisuuden ja tietosuojan huomiointi

Vuoden alussa on astunut voimaan myös laki digitaalisten palvelujen tarjoamisesta (306/2019), josta käytetään myös nimitystä saavutettavuusdirektiivi.

Toimintatapojen kehittämisessä huomioidaan tiedonhallintalain mukainen tiedonhallintamalli henkilötietojen käsittelyn osalta), ICT-hankintojen tietosuojavaatimukset ja sopimusmallit, tietovirtakaaviot, henkilötietojen hallinta ja kulku sekä henkilötietoja sisältävät tietojärjestelmät.

4 Tietosuoja- ja hankintasopimukset

Rauman kaupunki huomioi voimassaolevissa sekä uusissa sopimuksissa Kuntaliiton ja Hanselin valmistelemaa `Henkilötietojen käsittelyn ehdot` -tietosuojaliitettä. Toimintaperiaate on valmisteltu Rauman kaupunginlakimiehen kanssa. Kaupunginhallitus hyväksyi käytännön, jossa kaupunki toimii yhdenmukaisesti kaikkien toimittajien kanssa ja tietosuojaliitteen mukaisia ehtoja sovelletaan kaikissa Rauman kaupungin henkilötietojen käsittelyyn liittyvissä sopimussuhteissa. Toimialat on vastuutettu toimittamaan liite sopimusten mukaisille toimittajilleen.

5 Rekisteröidyn oikeudet ja niiden toteutuminen

Rauman kaupunki pyrkii noudattaa 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).

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.

6 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. Viime vuonna kirjattiin 86 tietoturvapoikkeamaa tai läheltä piti tilannetta. Poikkeamista yhdessä todettiin vakava riski ja se 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

7 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 oli käytettävissä tietoturvaa ja tietosuojaa käsittelevää voimassa olevaa ohjeistusta ja dokumentointia. Lisäksi hän haastatteli konsernipalvelujen toimialajohtajaa, hallintopäällikköä sekä tietohallintopäällikköä.

Kartoituksen tavoitteena oli varmistaa, 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.

Kartoituksessa todettiin, että kuntalaisille tarjottavaa informaatiota rekisteröidyn oikeuksista ja niiden toteutumisesta tiedotetaan kaupungin nettisivuilla (päivitetyt tietosuojaselosteet). Sieltä löytyvät myös rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja oikaisupyyntölomakkeet.

Erillisessä tarkastusmuistiossa oli tietoturvallisuus- ja tietosuojatyötä kehittämään esitetty toimenpidesuosituksia, jotka on käyty laajemmalla joukolla läpi ja määritelty, miten suositukset toteutetaan. 1.1.2020 voimaan tullut, neljän vuoden periodilla toteutettava, tiedonhallintalaki vaikuttaa juuri näihin esille tulleisiin huomioihin.

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 Taisto19 –harjoitukseen marraskuussa 2019.

Rauman kaupunki vastasi Valtiovarainministeriön julkisen hallinnon vuoden 2018 Digiturvakyselyyn tammikuussa 2019.

GDPR –itsearviointityökalun arvio tietosuojan tilanteesta asetukseen nähden laadittiin tähän raporttiin kolmannen kerran. Itsearviointi toteutettiin ensimmäisen kerran tietosuojaprojektin päättyessä toukokuussa 2018 ja toisen kerran tietotilinpäätökseen tammikuussa 2019.
Taulukko käsittää ne aihealueet ja vaatimukset, jotka tietosuoja-asetuksen ja hyvien käytäntöjen mukaisen tietosuojan ja tietoturvan hallinnan ja henkilötietojen käsittelyn tulee täyttää. Keskeiset huomiot ja tunnusluvut tietosuojan ja tietoturvan kehittämistoimenpiteistä on raportoitu erikseen (salainen, Julkisuuslaki 24§, kohta 7).

Itsearviointi osoittaa, että muutamalla osa-alueella asetuksen vaatimuksenmukaisuus on hieman parantunut edellisestä vuodesta. Keskeisimmät puutteet liittyvät tietosuojan vaikutustenarvioinnin tekemiseen, henkilötiedon anonymisointiin, pseudonymisointiin ja henkilötietoja sisältävien tallenteiden tuhoamiseen sekä sopimusten ja ulkoistusten hallintaan.

Lopuksi

Rauman kaupungilla henkilöstön osaaminen on tärkeä strateginen tavoite. Tietosuoja- ja tietoturvaosaaminen on noussut keskeiseksi menestystekijäksi jo koko maailmaa koskevan kyberuhankin takia. Digitalisaation lisääntyessä organisaatioiden sähköpostitileille kohdistetaan jatkuvasti tietojenkalasteluviestejä, joissa yritetään saada haltuun käyttäjätunnuksia tai muuta luottamuksellista tietoa. Lähes aina tietojenkalastelu aiheuttaa runsaasti ylimääräistä työtä. Seurauksena saattaa vaarantua henkilötietoja, jolloin tapahtumasta on tehtävä ilmoitus tietosuojavaltuutetulle. Kalastelukampanjat ovat yhä älykkäämpiä ja niiden torjuminen on vaikeampaa, joten henkilöstön valmiuksia osata toimia tietoturvaohjeiden mukaisesti tullaan kehittämään!

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