TIETOTILINPÄÄTÖS 2018

Kaupunginvaltuusto hyväksynyt 25.3.2019 § 27, RAU/276/07.01.00/2019

Kristiina Kuusio, tietosuojavastaava
kristiina.kuusio@rauma.fi

Tieto- ja asianhallinnan poikkihallinnollinen tiimi

Rauma

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, johdon työvälineenä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan. Tietotilinpäätöksellä vastataan EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, Rekisterinpitäjän vastuu). Organisaation tulee osoittaa noudattavansa asetusta ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä. Rekisterinpitäjä vastaa osoitusvelvollisuuden (accountability) toteuttamisesta.

Rauman kaupungin organisaatiossa noudatetaan kaupunginvaltuuston kesäkuussa 2018 hyväksymää tietosuojapolitiikkaa sisältäen tietoturvan ja siinä kuvattua tietosuojan organisaatiorakennetta. Tietosuojan koordinointi ja kehittäminen toteutuvat tieto- ja asianhallinnan poikkihallinnollisessa tiimissä ja kehittämistoimenpiteet esitetään kaupungin johtoryhmälle päätettäväksi.

Tietotilinpäätöksen laatimisesta on vastannut tietosuojavastaava ja se on käsitelty tieto- ja asianhallinnan poikkihallinnollisessa tiimissä.

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 valmistautui tietosuoja- ja tietoturvan toteuttamiseen ja EU yleinen tietosuoja-asetuksen velvoitteisiin erillisellä projektilla, joka toteutettiin ajalla 1.11.2017 – 31.5.2018. Projekti käynnisti asetuksen mukaisen, luottamuksellisen toimintakulttuurin rakentamisen, jossa tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa (mukaan lukien luottamusmiehet). Projektista laadittiin loppuraportti, josta käy ilmi projektin tulokset ja jatkokehittämistoimet. Tulokset raportoitiin kaupungin johdolle ja kaupunginhallitukselle. Rauman tietosuojaprojektissa on osallistuttu Valtiovarainministeriön (VM) työpajoihin ja hyödynnetty sieltä saatua materiaalia.

Tietosuoja ja tietoturva nivottiin projektissa osaksi kaupungin toimintaa ja tällä hetkellä niiden koordinointi on osana tieto- ja asianhallinnan poikkihallinnollista tiimiä. Rauman kaupungille nimettiin lakisääteinen tietosuojavastaava (50%:n työpanos), joka on organisaation asiantuntija, tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa. Sosiaali- ja terveystoimialalle nimettiin tietosuojan yhdyshenkilö.

Rauman kaupungin tietosuojaa ja tietoturvaa ohjaa kaupunginvaltuuston 18.6.2018 (§56) hyväksymä politiikka, joka on laadittu EU:n yleisen tietosuoja-asetuksen, sen artikloiden ja muun noudatettavan keskeisen lainsäädännön mukaisesti ja se pitää sisällään myös tietoturvan.

Tietosuojapolitiikka ja tietoturva 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. Henkilötietojen käsittelyä ohjaa **sisäänrakennetun tietosuojan periaate** edellyttäen, että tietosuojaperiaatteet ovat osana henkilötietojen käsittelyä niiden kaikissa vaiheissa. Tietosuoja ja tietoturva sivusto on avattu henkilöstön intranettiin, Jemmaan, josta löytyvät kaikki materiaalit, linkit ja ohjeet.

Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjä oletusarvoisesti käsittelee 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.

Tietosuoja-asetuksen informointivelvoite (artiklat 13 ja 14) edellyttävät organisaatiota informoimaan läpinäkyvästi sen toteuttamasta henkilötietojen käsittelystä. Rauman kaupungin henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet.

Valiokunnan hyväksymät tietosuojaselosteet on tallennettu toimialoittain kaupungin nettisivuille, jossa ne toimivat asiakkaiden informaatioasiakirjoina.

Henkilötietojen käsittelyn kartoitus on nyt tehty keskeisten henkilötietoa sisältävien tietojärjestelmien osalta ja kuvattu lähinnä järjestelmäkohtaisesti.

Sosiaali- ja terveystoimialalla on laadittu Asiakastietojärjestelmien omavalvontasuunnitelma, joka on hyväksytty viimeksi toimialan johdon katselmuksessa elokuussa 2018.

Tietosuoja- ja tietoturvatyön organisointi ja tietosuojavastaavan rooli on merkittävä tekijä myös tietoturvan kannalta. Ennen kaikkea pitäisi muistaa, ettei tietosuojaa ole olemassa ilman tietoturvaa. Tietoturvallisuuden toteuttamiseksi olisi mahdollista ottaa käyttöön hallintamalleja esim. ISO/IEC 27001 ja niihin liittyviä auditointeja.

Rekisterinpitäjä on tietosuoja-asetuksen (artikla 24) mukaan vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia.

Henkilöstön koulutus

Syksyllä tietosuoja-asetuksen vaatimusten valmistelua varten hankittiin Tieran kautta lakimiehen koulutusta kaupungin johdolle sekä esimiehille. Koko henkilöstön koulutusta varten verrattiin kahta eri verkossa toteutettavaa tietosuojakoulutusohjelmaa ja päätettiin ottaa käyttöön Valtiovarainministeriön laatima Arjen tietosuoja-kokonaisuus; netissä katsottavaa video ja nettitesti, koska ne on laadittu tätä valmistelua varten ja niitä kehitetään koko ajan valtion toimesta ja ne ovat myös maksuttomia. Henkilöstölle on järjestetty myös tietosuojavastaavan koulutusta keskitetysti sekä yksiköittäin.

Kaupungin henkilöstöstä Arjen tietosuoja –nettitestin vuoden 2018 loppuun mennessä on suorittanut yhteensä 1962 henkilöä eli n. 67 % koko henkilöstöstä. Arjen tietosuojakoulutus: video + testi toteutetaan osana perehdytysohjelmaa. Jatkossa kaikki uudet työntekijät, kesätyöntekijät ja opiskelijat tekevät nettitestin, jos työtehtäviin liittyy henkilötietojen käsittelyä. Myös luottamushenkilöiltä edellytettiin videon katsominen.

Henkilöstölle tietosuoja ja tietoturvan sivusto on kaupungin intranetissa, Jemmassa. Sieltä löytyvät ajankohtaiset tietosuojaan liittyvät asiat, ohjeet, tietosuojaselosteet ja lomakkeet. Tietosuojasta pyritään säännöllisesti myös tiedottamaan henkilöstölehdessä. Tietosuojavastaava on käynyt esittämässä asetuksen vaatimuksia myös toimialojen johtoryhmissä ja aamukahvitilaisuuksissa. Tietosuojapolitiikka on esitelty myös valiokunnissa.

Sähköpostilla on tiedotettu asiasta projektin aikana liittyen mm. Arjen tietosuojakoulutusten suorittamiseen ja tietoturvapoikkeamien ilmoittamiskäytäntö.

Henkilöstön koulutusta täydennetään keskitetyllä tietosuojakoulutuksella ja on varattu aiheelle pysyvä varaus henkilöstökoulutusohjelmaan keväisin ja syksyisin.

Tietosuojaohjeet (tallennettu kaupungin intranettiin)

Tietosuojan ja tietoturvan huoneentaulu
Henkilötietojen käsittelyn periaatteet (Tietosuojaperiaatteet 5 artikla)
Salasanaohje
Kameravalvonnan ohje

Riskiperusteinen lähestymistapa

EU:n yleisessä tietosuojavelvoitteessa edellytetään, että riskit on otettava huomioon sisäänrakennettuna ja oletusarvoista tietosuojaa toteutettaessa (artikla 25). Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. 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 ja kuvattu toimialoittain talousarviossa 2019. Kooste riskiarviosta on raportissa (salainen, Julkisuuslaki 24§, kohta 7).

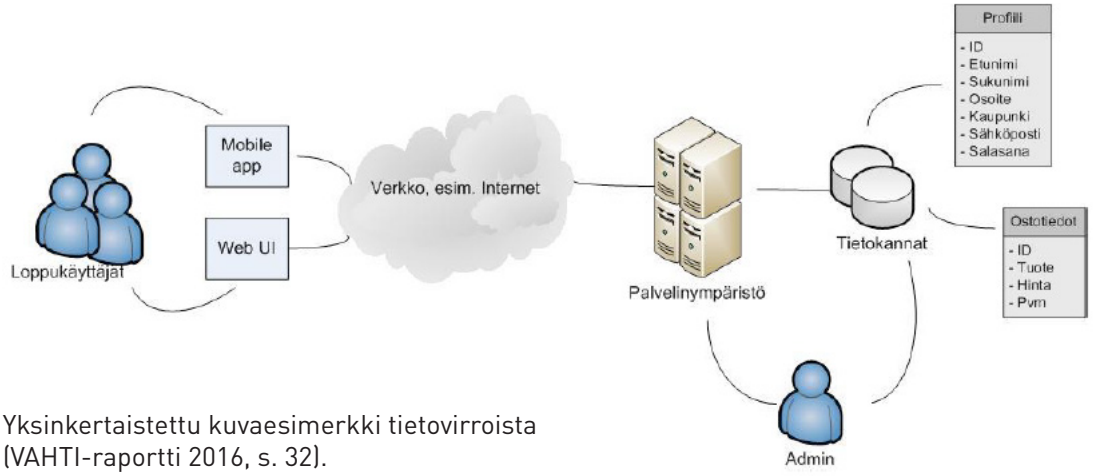
Riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarvioinnin sekä tarvittaessa ennakkokuulemisen tulisi tehdä sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarviointi edellyttää riskiarviota, koska vain korkeariskisistä toimenpiteistä laaditaan arviointi.

Tietosuojaan ja yksilön vapauksiin suunniteltuja henkilötietojen käsittelytoimien 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).

Jatkossa tarkoitus olisi huomioida tiedonhallintalaki kokonaisuuden hallinnassa (tiedonhallintamalli ja tiedon elinkaari) sekä tarpeen ja käyttötarkoituksen mukaan seuraavia seikkoja: kokonaisarkkitehtuuri (JHS 179), tietojärjestelmäarkkitehtuuri ja tietovarannot. Tietovirtojen (viranomaiset, yksityiset, muut) tulisi vastata kysymyksiin keneltä ja kenelle esim. seuraavan kaavion mukaisesti.



Yksinkertaistettu kuvaesimerkki tietovirroista (VAHTI-raportti 2016, s. 32).

Toimintatapojen dokumentoinnissa tulisi jatkossa huomioida tiedonhallintalain mukainen tiedonhallintamalli tai kokonaisarkkitehtuurikuvaus (henkilötietojen käsittelyn osalta), tiedonohjaussuunnitelma, sekä 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 toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kaupungin nettisivuilta (artiklat 13 ja 14).

Rauman kaupungin nettisivuille on avattu Tietosuojasivusto rekisteröidyille asian tiedottamista varten. Nettisivuilta löytyvät rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16).

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille 72 tunnin kuluessa. Tietosuojavastaava teki vuoden 2018 aikana yhden ilmoituksen tietosuojavaltuutetulle.

Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava 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.

6 Seuranta ja mittaaminen

Tämän tietotilinpäätöksen tehtävänä on avata tärkeää tietoa organisaation tietosuojan nykytilasta, sillä se on merkittävää rekisterinpitäjän osoitusvelvollisuuden toteuttamisen kannalta. Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät tekijät.

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

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

1. Henkilötietojen käsittely
    - tietosuojaselosteet
    - henkilörekisterien tarkastuspyynnöt
    - toimintaohjeet
2. Tietoturvapoikkeamat
3. Tietosuoja- ja tietoturvaprosessit
4. TAISTO – harjoituksen raportti
5. GDPR itsearvioinnin raportit (2 kpl)
6. TietosuojaAsetuksen OsoitusKriteeristö (TAOK)
7. Henkilöstön koulutusraportti
8. Tietosuojaan ja tietoturvaan liittyvät riskit talousarviossa 2019
9. Sosiaali- ja terveystoimialan lokitietojen tarkistukset

7 Arviointi ja kehittäminen

EU Yleinen tietosuoja-asetus on otettu organisaatiossamme vastaan kiitettävästi ja organisaatio pyrkii vastaamaan asetuksen tuomiin haasteisiin, joskin monella osa-alueella on vielä kehitettävää. Keskeisenä ohjaavana dokumenttina toimii jo edellä mainittu tietosuojapolitiikka ja tietoturva.

Rauman kaupunki osallistui valtakunnalliseen tietosuojan ja –turvan Taisto18 –harjoitukseen. Raportin mukaan sijoituimme aika lähelle vastaajien keskiarvoa. Yhteenvetoraportin mukaan olemme tunnistaneet kehityskohteita toiminnassanne harjoituksen aikana. Ohjeiden ja vastuiden päivittäminen tukee niin tietosuojan kuin -turvan kehittämistä. Samoin myös prosessien, vastuunjaon toiminnan varmistaminen ja riskiarviointi tietoturvaloukkauksissa tukee kehittämistä. Myös ilmoituskäytännön hiominen tietosuojavaltuutetulle on tärkeää.

Rauman kaupunki vastasi Valtiovarainministeriön julkisen hallinnon vuoden 2017 tieto- ja kyberturvallisuutta koskevaan kyselyyn tammikuussa 2018. Keskeiset huomiot tietosuojan ja tietoturvan kehittämistoimenpiteistä on raportoitu erikseen (salainen, Julkisuuslaki 24§, kohta 7). Tietosuojaprojektissa osallistuttiin Valtiovarainministeriön (VM) työpajoihin ja hyödynnettiin sieltä saatua materiaalia. Rauman kaupunki on laatinut julkisen hallinnon GDPR –itsearviointityökalun avulla arvion tietosuojan tilanteesta asetukseen nähden. Itsearviointi toteutettiin ensimmäisen kerran tietosuojaprojektin päättyessä toukokuussa 2018 ja nyt itsearviointi laadittiin tähän 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. Vaatimukset jakautuvat tietosuojan hallintaan sekä tiedon elinkaarta ja prosesseja koskeviin vaatimuksiin. Jokainen osa-alue ja vaatimus on numeroitu. Osa-alueessa 12 on käsitelty tietojärjestelmien hallintaan ja tietoturvallisuuteen liittyviä aihealueita. Osa-alueet on avattu tarkemmin raportissa olevassa taulukossa.

Itsearviointi osoittaa, että monella osa-alueella asetuksen vaatimuksenmukaisuus on parantunut viime vuodesta. Itsearviointityökalu antaa hyvät suuntaviivat jatkotyöskentelyyn ja kehittämiseen. Tietoturvallisuusosio on pysynyt lähes samana.

Henkilökunnan osaamiseen on kiinnitetty huomiota koko ajan. Koulutusraportti on osana tietosuojan raporttia. Jatkossa olisi tarkoitus ottaa käyttöön valtakunnallinen eOppiva tietosuojakoulutus, kun se toivottavasti saadaan myös kuntien työkaluksi. Henkilökunnan tarpeita kuunnellaan koulutuksen, ohjeistuksen sekä prosessien tuntemisen lisäämiseksi.

Henkilökunnan tietosuojaosaamisen arviointia ei toteuteta tällä hetkellä systemaattisesti. Ehkä se on aiheellista miettiä myös lähivuosien aikana.

Henkilökunnalla on velvollisuus ja mahdollisuus raportoida havaitsemistaan tietoturvapoikkeamista HaiPro- ohjelmalla, jonka ohjeet ja linkit löytyvät intranetista, Jemmasta. Ilmoitukset toimivat tärkeänä osana tietoturvan kehittämistä ja koulutustarpeiden kartoitusta ja arviointia.

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

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

Rauman kaupunki, Tietosuojapolitiikka ja tietoturva, 2018. 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

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

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