

Helsingin kaupungin tietosuoja, käytännön kokemuksia ja vinkkejä

Juhta/Vahti työpaja 22.8.2018

Päivi Vilkki, Helsingin kaupungin tietosuojavastaava, varatuomari

Helsinki

Helsingin kaupungin erityispiirteitä

- Paljon työntekijöitä: kaupungilla on n. 38.000 työntekijää, joista valtaosa käsittelee henkilötietoja.
- Kaupunki jakautuu:
 - neljä toimialaa: sosiaali- ja terveystoimiala, kasvatuksen ja koulutuksen toimiala, kaupunkiympäristön toimiala sekä kulttuurin ja vapaa-ajan toimiala
 - kolme virastoa: kaupunginkanslia, tarkastusvirasto ja pelastuslaitos
 - viisi liikelaitosta: liikennelaitos (HKL), palvelukeskusliikelaitos, taloushallintopalveluliikelaitos, työterveysliikelaitos ja rakentamispalveluliikelaitos (Stara)
- Uusi organisaatio: 31.5.2017 saakka kaupungilla oli runsaat 30 virastoa, joista toimialat muodostettiin.
- Runsaasti tietojärjestelmiä, joita on lähes 800. Henkilötietoja käsitellään runsaassa 400 tietojärjestelmässä.

Tietosuojatyön organisointi Helsingin kaupungilla

Kaupunkitasoisesti

- Kaupunginhallitus vastaa hallintosäännön mukaisesti siitä, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista.
- Kaupunkitasoisen tietosuojavastaavan on ottanut virkaan kaupunginhallitus. Hallinnollisesti tietosuojavastaava sijoittuu kaupunginkanslian hallinto-osastolle. Tietosuojavastaavan asema ja tehtävät määräytyvät suoraan EU:n tietosuoja-asetuksen 38. ja 39. artiklan nojalla ja tietosuojavastaava raportoi suoraan kaupungin ylimmälle johdolle.
- Tietosuojavastaavalla on apunaan tietosuojatiimi, johon kuuluu kaupungin tietosuojalakimies, joka avustaa tietosuojavastaavaa tämän tehtävissä ja toimii tietosuojavastaavan sijaisena. Lisäksi tietosuojatiimiin on tulossa vielä kaksi asiantuntijaa.
- Tietoturva-asioissa tietosuojavastaavan tukena toimii tietohallinto ja erityisesti tietoturva-asiantuntija.

Toimiala/virasto/liikelaitoskohtaisesti

- Kuhunkin toimialaan, virastoon ja liikelaitokseen on nimetty tietosuoja-asioiden vastuuhenkilö, joka toimii yhteyshenkilönä kyseisen organisaation ja tietosuojavastaavan välillä, opastaa ja neuvoa omaa organisaatiotaan tietosuoja-asioissa, osallistuu oman organisaationsa tietosuoja-vaikutusten arviointiin sekä uusien tietojärjestelmien hankintoihin, mikäli tietojärjestelmät käsittelevät henkilötietoja.
- Lisäksi toimialoilla, virastoissa ja liikelaitoksissa on oltava nimetty vastuuhenkilö myös tietoturva-asioissa.

Tietosuojatyöryhmä

- Kaupungilla on kansliapäällikön asettama tietosuojatyöryhmä, jonka tehtävänä on valmistella EU:n tietosuoja-asetukseen ja sitä täydentävään kansalliseen lainsäädäntöön liittyviä toimenpiteitä.
- Työryhmään kuuluvat tietosuojavastaava, tietosuojalakimies ja edustajat kultakin toimialalta, virastosta ja liikelaitoksesta.
- Ryhmä on viime kevätkauden kokoontunut 2 viikon välein ja käynyt läpi tietosuojalainsäädännön vaatimia toimia kaupungilla. Jatkossa tietosuojatyöryhmä kokoontuu kerran kuussa.
- Tietosuojatyöryhmä voi tarvittaessa jakautua alatyöryhmiin ja käyttää ryhmän ulkopuolisia asiantuntijoita.
- Lisäksi tietosuojatiimi tulee pitämään erillisiä tapaamisia yksitellen toimialojen, virastojen ja liikelaitosten tietosuojan ja tietoturvan vastuuhenkilöiden kanssa.
- Työryhmässä on myös jaettu hyviä käytäntöjä eri toimialojen, virastojen ja liikelaitosten kesken.

Tietosuojatyön aloitus Helsingin kaupungilla

Tietosuojalinjaukset ja henkilötietojen analysointi

- Kaupunginhallitus hyväksyi 7.8.2017 kaupungin tietosuojalinjaukset, joita on tarkoitus täydentää myöhemmin.
- Toimialoille, virastoille ja liikelaitoksille lähetettiin käytössä olleiden henkilörekisterien analysointia varten lomake täyttöohjeineen. Analysoinnin tavoitteena oli selvittää, mitä henkilötietovirtoja kaupungilla kulkee ja mitä muutoksia tietojärjestelmiin tarvitaan niiden saattamiseksi tietosuoja-asetuksen mukaiseksi, sekä kerätä tietoa, jota tarvitaan uusiin rekisteriselosteeseen.
- Tehtyjä analysointeja voidaan hyödyntää myös tietosuoja-asetuksen 30. artiklan mukaisissa selosteissa käsittelytoimista.

Henkilötietojen analysointi käytännössä

- Analysoinneilla hahmotettiin mm. seuraavat pääkysymykset:
 1. Kuka on rekisterinpitäjä ko. tietojen osalta.
 2. Missä tietojärjestelmissä rekisterin henkilötietoja käsitellään.
 3. Mikä on tietosuoja-asetuksen mukainen laillinen käyttötarkoitus tietojen käsittelylle.
 4. Mitkä ovat rekisterin sisältämät henkilötietoryhmät ja rekisteröityjen ryhmät.
 5. Sisältääkö rekisteri arkaluonteisia henkilötietoja / erityisiä henkilötietoja. Jos sisältää, mikä on näiden tietojen käsittelyperuste.
 6. Henkilötietojen säilytysaika. Miten henkilötiedot poistetaan järjestelmästä säilytysajan loputtua.
 7. Henkilötietojen säännönmukaiset luovutukset.
 8. Kerääkö tietojärjestelmä kaikesta henkilötietojen käsittelystä käyttäjälokitietoja.
 9. Miten henkilötiedot on suojattu teknisesti.
 10. Mitä sopimusmuutoksia tarvitaan.

Helsingin kaupungin määrittelemät tietosuojalainsäädännön vaatimat tehtävät

Tietosuojaryhmän jaottelu tietosuoja-asetuksen edellyttämistä tehtävistä kaupungilla

1. Kaupunki antaa rekisteröidyille ohjausta heidän oikeuksistaan ja mahdollisuuden toteuttaa niitä
2. Sopimukset, jotka koskevat henkilötietoja käsitteleviä tietojärjestelmiä tai joissa sovitaan henkilötietojen käsittelystä, saatetaan toteuttamaan tietosuoja-asetuksen vaatimukset
3. Kaupungin henkilötietoja käsittelevälle henkilöstölle annetaan opetusta ja ohjeistusta tietosuoja-asetuksen vaatimuksista
4. Kaupungilla toteutetaan sisäänrakennettu ja oletusarvoinen tietosuoja
5. Henkilörekisterien tietoturvasta huolehditaan

1. Kaupunki antaa rekisteröidyille ohjausta heidän oikeuksistaan ja mahdollisuuden toteuttaa niitä

- Rekisteröidyille annetaan tietoa kaupungin eri palveluissa kerättävistä henkilötiedoista ja rekisteröityjen oikeuksista ja niiden käyttämisestä kaupungin Internet-sivuilla, jotka julkaistiin 18.5.18. [linkki](#)
- Lisätietoa annetaan henkilörekisterien rekisteriselosteissa, joihin on linkki edellä mainitulta sivulta. Rekisteriselosteet antavat lisätietoa esim. henkilötietojen käsittelyn oikeusperusteesta, rekisterin tietosisällöstä ja tietojen säilytysajoista.
- Omien rekisteritietojensa pyytämiseksi ja tietojen korjausvaatimuksen tekemiseksi kaupunki on järjestänyt rekisteröidyille sähköisen, vahvasti tunnistetun yhteyden. Kaupungin taholta vastataan rekisteröidylle sähköisesti. Tämä toteutetaan asiointi.hel.fi –kanavan avulla, joka käyttää suomi.fi:n vahvaa tunnistautumista. Linkit tietopyynnön ja tietojen korjausvaatimuksen tekemiseksi löytyvät em. sivuilta.

1. Kaupunki antaa rekisteröidyille ohjausta heidän oikeuksistaan ja mahdollisuuden toteuttaa niitä, jatkoa

- Tietojen pyytäminen ja korjausvaatimuksen tekeminen sähköisesti:
 - Tietojen pyytämiseksi ja korjausvaatimuksen tekemiseksi on kaupungin Internet-sivuilla linkit, joista aukeaa valikko 12 kohteeseen, jossa on eroteltuina toimialat, virastot ja liikelaitokset. Niiden kohdalla on selostettuna, mitä asioita kussakin käsitellään.
 - Rekisteröity voi klikata sitä kohdetta, josta hän haluaa tiedot. Hän myös valitsee, haluaako hän tiedot joltain määrättyltä ajalta, jotkin määrättyt asiakirjat vai kaikki tietonsa (jatkossa ”muuten yksilöidyt tiedot”). Lisäksi hän tarkentaa, mitä asiaa hänen pyyntönsä koskee, jotta pyyntö voidaan kohdentaa oikeaan rekisteriin.
- Lisäksi on olemassa prosessi paperisen tietopyynnön ja korjausvaatimuksen tekoon ja myös ohjauksen rekisteröityjen oikeuksista saa paperisena.
- Paperiset pyynnöt ja korjausvaatimukset ottaa vastaan kaupungin kirjaamo. Lähiaikoina myös toimialojen palvelupisteet alkavat ottaa niitä vastaan oman toimialansa osalta.
- Uuteen Oodi-kirjastoon tulevaan kaupungin neuvontapisteeseen suunnitellaan jaettavaksi ohjeistusta tietopyynnöistä ja korjausvaatimuksista.

Ensimmäinen tehtävä käytännössä

- Omia rekisteritietoja sähköisesti pyydettäessä kullakin toimialalla, virastossa tai liikelaitoksessa tietopyyntöjen kokoaja (tarkoittaa useampaa nimettyä käyttäjää yhdellä sähköpostiosoitteella) saa tiedon pyynnöstä.
- Sieltä pyyntö kulkee rekisterin vastuuhenkilön kautta rekisterin yhteyshenkilölle, joka kerää pyydetyt tiedot. Rekisterin yhteyshenkilö toimittaa tiedot rekisterin vastuuhenkilölle, joka tarkastaa tiedot ja lähettää ne tietopyyntöjen kokoajalle. Tietopyyntöjen kokoaja toimittaa tiedot asiakkaalle.
- Tietojen kulku kaupungin sisällä ja myös lähettäminen asiakkaalle kaipaavat vielä hiomista. Nyt pystytään lähettämään asiakkaalle pieni määrän tietoa asiointi.hel.fi:n kautta, isompi määrä pitää lähettää salatulla sähköpostilla.
- Vastaavasti toimitaan tiedonkorjausvaatimusten kanssa.
- Manuaaliset pyynnöt vastaanottaessaan kirjaamo tarkastaa tiedon pyytäjän tai korjausvaatimuksen tekijän henkilöllisyyden. Pyyntölomakkeen voi pyytää kirjaamolta tai tulostaa kaupungin Internet-sivuilta.
- Manuaalisesti pyydetyt tiedot lähetetään asiakkaalle kirjepostilla.

2. Tietojärjestelmiä ja henkilötietoja koskevat sopimukset saatetaan toteuttamaan tietosuoja-asetuksen vaatimukset

- Uusiin sopimuksiin, jotka koskevat henkilötietoja käsitteleviä tietojärjestelmiä tai joissa sovitaan henkilötietojen käsittelystä, laitetaan kilpailutusvaiheessa mukaan kaupungin tietoturvallisuusliite (sisältää tietosuojaa ja tietoturvaa koskevat ehdot) tai erityistapauksessa vastaavat, tietosuoja-asetuksen mukaiset ehdot täyttävä liite.
- Vanhoihin, 25.5.2018 jälkeen jatkuviin vastaaviin sopimuksiin, kaupungin tietoturvallisuusliite on pyritty neuvottelemaan mukaan tai tapauskohtaisesti on käytetty muuta, tietosuoja-asetuksen ehdot täyttävää liitettä.
 - Toimialat/virastot/liikelaitokset ovat saaneet ohjausta ja hoitaneet neuvottelut itsenäisesti toimittajien kanssa.
 - Kaupungin kannalta merkityksellisimpien toimittajien kanssa on neuvoteltu pääkysymyksistä keskitetysti ja kaupunkitasoisesti.

Toinen tehtävä käytännössä

- Hankaluutena sopimusten osalta on ollut, että kuntasektorilla ei ole ollut yhtä tietosuojaliitettä, jota kaikki olisivat voineet tarjota sopimuskumppaneille.
- Kaupungin oman liitteen osalta on ohjeistettu, että liitettä saa muokata palvelun luonteen mukaan.
- Vanhoihin sopimuksiin on kaupungin liite osin saatu, osin neuvottelut ovat vielä kesken.
- Suurten toimijoiden kanssa, kuten Tieto Oyj ja CGI on neuvoteltu kaupunkitasoisesti. Toimialat/virastot/liikelaitokset ovat saaneet käyttää vanhoihin sopimuksiin täten neuvoteltua liitettä, jos ovat sen hyväksi havainneet.

3. Kaupungin henkilötietoja käsittelevälle henkilöstölle annetaan opetusta ja ohjeistusta tietosuoja-asetuksen vaatimuksista

- Tietosuojavastaava ja tietosuojalakimies ovat tehneet henkilötietoja käsittelevälle henkilöstölle 30 minuutin videokoulutuksen tietosuojan perusasioista, joka kaikkien henkilötietoja käsittelevien tulee katsoa.
- Koulutus sisältää: lainsäädännön tilanne, vastuut tietosuojan toteuttamisessa, henkilötietojen käsittelyn periaatteet, henkilötietojen käsittelyn lainmukaisuus, erityisiä henkilötietoryhmiä koskeva käsittely, henkilötunnuksen käsittely, henkilörekisterit ja rekisteröidyn oikeudet, sopimuksista, julkisuuslaki, tietoturvaloukkauksesta ilmoittaminen, käytännön ohjeet.
- Lisäksi kaikkien henkilötietoja käsittelevien tulee suorittaa 10 kysymyksen tentti. Esimiesten tulee dokumentoida, että heidän alaisensa ovat suorittaneet tentin.

3. Kaupungin henkilötietoja käsittelevälle henkilöstölle annetaan opetusta ja ohjeistusta tietosuoja-asetuksen vaatimuksista, jatkoa

- Lisäksi tietosuojavastaava ja tietosuojalakimies ovat pitäneet koulutuksia toimialojen, kaupunginkanslian ja yhden liikelaitoksen avainhenkilöille. Koulutusten pitoa tullaan jatkamaan.
- Myös toimialojen tietosuojan ja tietoturvan vastuuhenkilöt ovat pitäneet koulutuksia omilla toimialoillaan tietosuojavastaavan laatiman aineiston pohjalta.
- Tietosuojatyöryhmän alatyöryhmä on valmistellut henkilöstön ohjeistukseksi tietosuojakäsikirjan. Siinä selostetaan henkilötietojen käsittelyn periaatteet, käsittelyorganisaatio ja merkittävimmät pääprosessit.
- Kaupungilla on oma Tietosuoja-sivusto, jolta ohjeistusta on saatavissa ja josta myös koulutusvideot löytyvät.

Kolmas tehtävä käytännössä

- Tietosuojatentin ajankohdasta on ohjeistus, että se tulee kaikkien henkilötietoja käsittelevien suorittaa lokakuun loppuun mennessä.
- Tietosuojavastaavan ja tietosuojalakimiehen ”live-koulutuksia” on tähän mennessä ollut 12 kpl ja kuulijoita niillä on ollut n. 900. Osassa näistä on ollut mukana myös toimialojen omia tietosuoja- ja tietoturvan vastuuhenkilöitä, jotka ovat myös pitäneet edellä mainittujen koulutusten lisäksi omia koulutuksiaan.
- Yksi koulutus on videoitu ja se on katsottavissa kaupungin sisäisillä sivuilla.
- Tietosuojakäsikirjan tekoon osallistui 7 tietosuojatyöryhmän juristia.

4. Kaupungilla toteutetaan sisäänrakennettu ja oletusarvoinen tietosuoja

- Koulutus, tietosuojakäsikirja ja muu ohjeistus tähtäävät osaltaan siihen, että kaikessa henkilötietojen käsittelyssä tietosuoja olisi kaupungin toiminnassa sisäänrakennettu ja oletusarvoinen ja kaikki asetuksen edellyttämät tekniset ja organisatoriset toimenpiteet tulivat toteutettua.
- Kaupungin ylimpien virkamiesten tietoisuutta on lisätty myös sillä, että tietosuojavastaava on kiertänyt kertomassa tietosuojalainsäädännön vaatimuksista toimialojen, virastojen ja liikelaitosten johtoryhmissä.
- Kaupungilla aletaan valmistella tietosuoja-asetuksen 30 artiklan mukaisia selosteita käsittelytoimista ohjaamaan omaa toimintaa ja valvontaviranomaisia varten Tietosuojavaltuutetun pohjaa käyttäen.
- Kaupungilla aletaan valmistella tietotilinpäättöä.

5. Henkilötietoja sisältävien tietojärjestelmien tietoturvasta huolehditaan

- Ensimmäiseksi asiaksi oli otettu tietojärjestelmien lokitus.
- Kaupungissa toimi lokien käsittelyhanke, joka kartoitti tietojärjestelmät, joissa on erityisiä henkilötietoja ja teki suunnitelmat jatkosta.
- Tietojärjestelmiä aletaan uudistaa toimialoilla, virastoissa ja liikelaitoksissa suunnitelmien mukaan ja siitä raportoidaan tietosuojatyöryhmälle.
- Jatkosuunnitelmia tietoturvasta huolehtimiseksi laaditaan.

Muita asioita

- Tietoturvaloukkausten varalta kaupungilla on valmisteltu menettelyohjeistus.
- Menettelyohjeistus keskittyi suurelta osin tietojärjestelmiin tapahtuviin hyökkäyksiin, mutta paperiprosessit ovat kuitenkin osoittautuneet erityisen haavoittuviksi ja niihin tulee jatkossa keskittyä enemmän.
- Ohjeistuksia tietoturvaloukkaustapauksiin täsmennetään.
- Työkalua tietosuoja koskevaa vaikutustenarviointia tehtäessä myös täsmennetään.

Yhteenveto

Yhteenveto Helsingin suuntaviivoista

- Tietosuojatyötä aloitettaessa on tärkeää hahmottaa käsiteltävät henkilötietovirrat ja organisoida tietosuojatyö hyvin.
- Rekisteröidyille tulee antaa ohjausta heidän oikeuksistaan ja mahdollisuus toteuttaa niitä.
- Sopimukset, jotka koskevat henkilötietoja käsitteleviä tietojärjestelmiä tai joilla sovitaan henkilötietojen käsittelystä, tulee saattaa tietosuoja-asetuksen mukaisiksi.
- Henkilötietoja käsittelevälle henkilöstölle tulee antaa opetusta ja ohjeistusta tietosuoja-asetuksen vaatimuksista.
- Sisäänrakennettu ja oletusarvoinen tietosuoja tulee toteuttaa.
- Henkilötietoja sisältävien tietojärjestelmien tietoturvasta tulee huolehtia.
- Erityisenä huomiona: sosiaali- ja terveydenhuoltoa koskeva lainsäädäntö nousee esiin tietosuoja-asetuksen ohella.

Helsinki