



Savonlinna

Savonlinnan kaupungin tietotilinpäätös 2019

Johtoryhmä 18.5.2020

Kaupunginhallitus XX.X.2020

SISÄLTÖ

1.	TIETOTILINPÄÄTÖKSEN TARKOITUS	3
2.	TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN	4
3.	TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT	6
4.	LAINSÄÄDÄNTÖ JA MUU OHJEISTUS.....	7
5.	REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN	8
6.	ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN	9
7.	SEURANTA JA MITTARIT	10

1. TIETOTILINPÄÄTÖKSEN TARKOITUS

Tietotilinpäätös on kuvaus organisaation henkilötietojen käsittelyn nykytilasta ja arvio tietosuojaan toteutumisesta. Lisäksi se sisältää henkilötietojen käsittelyyn ja tietoturvaan liittyviä yleisiä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuoja- ja tietoturvatyön tekemistä ja kehittämistä sekä lisätä tekemisen vaikuttavuutta.

Tietotilinpäätös on tarkoitettu ensisijaisesti kaupungin sisäiseen käyttöön johtamisen ja sisäisen valvonnan raportiksi. Se toimii myös suunnittelun ja toiminnan ohjauksen sekä johtamisen tukena. Tietotilinpäätöksellä pyritään lisäämään luottamusta ja läpinäkyvyyttä. Se on myös keskeinen dokumentti EU:n yleisen tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa lakien ja määräysten, hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan noudattamista.

Osoitusvelvollisuuteen kuuluu mm. se, että organisaation sopimuksissa ja alihankinnoissa on huomioitu tietosuojaan ja -turvan vaatimukset. Lisäksi rekisterinpitäjän tulee huomioida rekisteröidyn henkilötietojen käsittelyä koskevat oikeudet ja käsittelyyn kohdistuvat riskit. Rekisterinpitäjän tulee huolehtia siitä, että henkilöstöllä ja ulkopuolisilla henkilötietojen käsittelijöillä on tarvittava ohjeistus ja osaaminen.

Savonlinnan kaupunki kunnioittaa tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita. Henkilötietojen käsittelyssä noudatetaan seuraavia asetuksen mukaisia henkilötiedon käsittelyn vaatimuksia:

1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate
2. käyttötarkoitussidonnaisuuden periaate
3. tietojen minimoinnin periaate
4. täsmällisyyden periaate
5. säilytyksen rajoittamisen periaate
6. eheyden ja luottamuksellisuuden periaate.

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä (Savonlinnan kaupunginhallitus) on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudelta vaihtelevat riskit ja suhteutettava toimenpiteet näiden mukaisesti.

Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tila- ja käytönvalvontaa, pääsynhallintaa, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytäntöjen sekä sertifikaattien käyttöä.

Tietotilinpäätöksellä varmistetaan ja lisätään luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita, toteutetaan teknisiä ja organisatorisia toimenpiteitä sekä käsitellään henkilötietoja asetuksen mukaisesti. Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista, työelämän tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista.

Vuoden 2019 tietotilinpäätös on ensimmäinen Savonlinnan kaupungilla ja sen painopiste on ensisijaisesti tietosuojaa ja tietoturvaa koskevissa asioissa. Dokumentti on kokonaisuudessaan julkinen ja se laaditaan yhteistyössä eri asiantuntijoiden kesken (tietohallintopäällikkö, tietosuojavastaava ja arkistosihteeri). Kokoamisesta vastaa tietosuojavastaava. Dokumentti on käynyt kommenttikierroksella myös tietosuojatyöryhmällä, johon kuuluu tietohallintopäällikön ja tietosuojavastaavan lisäksi kaupungin hallintojohtajalakimies, hallintopäällikkö sekä tietoturva-asiantuntijat tekniseltä ja sivistystoimialalta. Tietotilinpäätös raportoidaan kaupunginjohtajan johtoryhmässä ja viedään tarvittaessa tiedoksi kaupunginhallitukseen.

2. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Savonlinnan kaupungin tietotilinpäätös on osa kaupungin tietoturvapoliittikkaa, riskienhallintaa ja sisäistä valvontaa. Merkittävä askel Savonlinnan kaupungin tietosuoja- ja tietoturvatyön etenemiseksi oli päätoimisen tietosuojavastaavan rekrytointi maaliskuun alussa 2019. Tietosuojavastaavan palveluja Savonlinnan kaupungilta ostavat myös Rantasalmen, Sulkavan ja Enonkosken kunnat, Itä-Savon koulutuskuntayhtymä (Ammattiopisto SAMledu) sekä vuoden 2020 alusta lähtien myös Savonlinnan Vuokratalot Oy.

Vuoden aikana tietosuojavastaava on kartoittanut käytössä olevat henkilörekisterit yhteistyössä rekistereiden vastuu-/yhteyshenkilöiden kanssa. Tietosuoja-asetuksen mukainen informointivelvoite henkilötiedon käsittelystä toteutetaan kaupungin [verkkosivuilla](#), josta löytyy henkilörekistereiden [tietosuojaselosteet](#).

Voimassa olevat tietosuojaselosteet sisältävät myös asetuksen mukaisen tietosisällön henkilötiedon käsittelytoimista. → **Selosteiden ylläpito on jatkuvaa.** → **Vastuu tietojärjestelmien pääkäyttäjillä ja tietosuoja-vastaavalla.**

Henkilöstön koulutusta ja ohjausta muuttuneeseen tietosuojalainsäädäntöön ja tietoturvaan on toteutettu pitkin vuotta toimialoilta tulleiden tarpeiden perusteella. Lisäksi henkilöstön tulee suorittaa tietosuojaa ja tietoturvaa koskeva verkkokoulutus kerran vuoteen. Vuonna 2019 koulutuksen suoritti 219 työntekijää ja suoritusten arvioinnin kokonaistulos oli 93%. → **Jatkossa tulee edelleen painottaa ja muistuttaa henkilöstöä verkkokoulutuksen vuosittaisesta toteuttamisesta.** → **Vastuu tietosuojavastaavalla ja esimiehillä.**

Myös henkilöstön koulutus on jatkuvaa. → **Henkilöstön tulosalutasoinen koulutus ja tiedottaminen digi- ja kyberturvallisuudesta sekä tietosuojasta on asetettu kehittämiskohteeksi myös vuodelle 2020 (Jory § 283, 9.12.2019).** → **Vastuu tietosuojavastaavalla.**

Henkilötiedon käsittelyn lainmukaisuus on huomioitu myös työelämän tietosuojan kehittämisessä. Henkilöstöhallinnon päivitetty tietosuojaseloste täyttää informointivelvoitteen, perehdytysopasta on tarkennettu

tietosuoja- ja tietoturvan osalta sekä henkilötiedon käsittelyyn on laadittu erilliset kaupunginhallituksen hyväksymät kirjalliset tietosuoja-asetuksen mukaiset ohjeet. Ohjeet löytyvät [Savnetista](#). Esimiehille on pidetty tarpeen mukaan infotilaisuuksia ja koulutusta tietosuojasta ja tietoturvasta. → ***Esimiesten vastuuta uuden työntekijän tietosuoja- ja tietoturva-asioiden perehdytyksessä tulee painottaa entistä enemmän. Myös tietosuojavastaava on käytettävissä uuden työntekijän perehdytyksessä ja kouluttamisessa. → Vastuu asian edistämisestä esimiesfoorumiin henkilöstöpäälliköllä, käytännön toteutuksesta tietosuojavastaavalla ja esimiehillä.***

Tietosuoja- ja tietoturvan riskiperusteista lähestymistapaa korostetaan osana arjenhallintaa ja viime kädessä se toteutetaan kaupungin vuosittaisen toimialakohtaisen kokonaisvaltaisen riskikartoituksen ohessa. Samassa yhteydessä toteutetaan myös tietosuoja- ja tietoturvan sisäinen valvonta. Riski- ja häiriöilmoitusten tekemiseen on otettu uusi toimintamalli käyttöön vuoden 2019 aikana. Ilmoitusten seurannasta vastaavat tietosuojavastaava ja tietohallintopäällikkö. Myös poikkeamailmoitusten hallintaan on luotu uusi toimintamalli. → ***Henkilöstöä tulee edelleen muistuttaa häiriö- ja poikkeamailmoitusten tekemiseen. Kyberuhkia ja digiturvallisuutta koskeva tiedottaminen on jatkuvaa. → Vastuu tiedottamisesta on tietohallintopäälliköllä ja tietosuojavastaavalla.***

Hankinnoissa ja sopimushallinnassa tietosuojavastaava on tehnyt yhteistyötä hankintatoimen kanssa. Henkilötiedon käsittelyä sisältävissä palveluiden ja tietojärjestelmien hankinnoissa tulee huomioida tietosuoja jo kilpailutusvaiheessa ja viimeistään sopimushallinnassa. → ***Palveluntuottajan/ohjelmistotoimittajien kanssa tehtäviin sopimuksiin tulee sisällyttää palvelun/ohjelmiston mukaan (pilvipalvelu/omakoneympäristö) tietosuojaliite tai sopimus henkilötietojen käsittelystä. → Vastuu sopimuksesta päättävällä viranhaltijalla.***

Kaupunki osallistuu jatkuvasti myös erilaisiin hankkeisiin, joissa käsitellään henkilötietoja. Hankehallinnassa henkilötiedon käsittelyn suunnittelua painotetaan jo hankehakemusvaiheessa ja henkilöstöä on ohjeistettu otamaan tietosuojavastaava mukaan suunnitteluun jo hanketta suunniteltaessa.

Tietosuoja-asetuksen mukainen tietosuoja-vaikutusten arviointi edellyttää oikea-aikaista osallistumista toiminnan ja hankintojen suunnitteluun. Erityisesti tietojärjestelmähankinnat edellyttävät myös tietosuoja-asetuksen vaatimusten toteutumisen huomiointia. → ***Tietosuoja-vaikutusten arviointi edellyttää oikea-aikaista osallistumista toiminnan ja hankintojen suunnitteluun. Erityisesti tietojärjestelmähankinnat edellyttävät myös tietosuoja-asetuksen vaatimusten toteutumisen huomiointia. → Tietosuoja-vaikutusten arviointi edellyttää oikea-aikaista osallistumista toiminnan ja hankintojen suunnitteluun. Vuonna 2019 tietosuoja-vaikutusten arviointi on ollut vielä lähes olematonta. → Vastuu sopimuksen tietosuojaliitteestä päättävällä viranhaltijalla, tietohallintopäälliköllä ja tietosuojavastaavalla.***

Kaupungin ATK-palvelukeskuksen palvelut

Savonlinnan kaupungin hallintopalveluihin kuuluva seitsemän työntekijän atk-palvelukeskus huolehtii kaupungin tietoteknisistä palveluista sekä työasema- että palvelinympäristön osalta. Valtaosaa palvelinsovelluksista käytetään omassa konesalissa olevasta palvelinympäristöstä. Konesali on varustettu lämpötilan valvonnalla ja savutunnistimin. Työasemat hankitaan kilpailutetun sopimuksen pohjalta neljän vuoden leasingilla.

Savonlinnan kaupungin hallintoverkkoon on pääsy työasemien kautta vain kaupungin työntekijöillä esimiehen pyynnöstä myönnettyillä käyttäjätunnuksilla. Käyttöoikeudet ohjelmistoihin ja tietovarantoihin määritellään käyttäjäkohtaisesti esimiehen pyynnön perusteella. Työtehtävien niin vaatiessa hallintoverkon ulkopuolelta on verkon palveluihin mahdollista päästä erikseen määritellyllä vpn-yhteydellä (Virtual Private Network). Savnetissa on henkilöstölle erillinen [ohje](#), joka ohjeistaa etätöön toteuttamisen VPN-yhteydellä.

Työasemien tietoturvakäsittely leasing-kauden päättyessä kuuluu sopimukseen 3StepIT:n kanssa. Tuhottavat tietovälineet varastoidaan Encore-tietoturvapalvelun säiliöihin, jotka palveluntuottaja noutaa sovituin väliajoin.

Toimisto-ohjelmistojen osalta vuoden 2019 aikana käynnistettiin selvitys Microsoftin pilvipalveluiden käyttöönotosta. Projekti kestää vuoteen 2021 ja konsulttina toimii Sulava Oy. Tietoturva on avainasemassa O365-palveluiden käytössä. Myös eri toimialoilla on toteutettu uusia järjestelmähankintoja ja päivityksiä, jota mahdollistavat paremmin tietosuoja-asetuksen mukaiset vaatimukset.

3. TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT

Organisaation tulee suunnitella ja kuvata tiedonhallinnan, tietovarantojen ja tietovirtojen kokonaistilanteensa. Tämä tapahtuu esimerkiksi **kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten** avulla. Tarkoituksena on selvittää sitä, miten tietoa hallitaa sen koko **elinkaaren** ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineinä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määriteltä asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on oltava ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Henkilötietorekistereiden kartoituksen yhteydessä määriteltiin rekistereiden vastuuhenkilöiden ja tietosuoja-vastaavan toimesta läpi rekisterien käyttötarkoitus ja tietosuoja-asetuksen mukainen oikeusperusta henkilötiedon käsittelylle. Samassa yhteydessä kartoitettiin myös rekistereiden tietosisältö, henkilötietojen käsittelijät ja mahdolliset luovutukset. Henkilötiedon säilytysaikaa rekistereissä ohjaa Kansallisarkiston määräykset pysyvästi säilytettävistä asiakirjatiedoista ja niiden säilytysmuodosta ja Kuntaliiton suositukset.

Säilytysajat on kuvattu kaupungin arkistosihteerin ylläpitämään ja hallinnoimaan tiedonohjaussuunnitelmaan. Tiedonohjaussuunnitelmaa (TOS), ylläpidetään Tiedonohjausjärjestelmässä (TOJ). Tiedonohjaussuunnitelma pohjautuu Kuntien yhteiseen tehtäväluokitukseen, joka sisältyy valmiina tiedonohjausjärjestelmään. Säilytysaikojen määrittelyn lisäksi tiedonohjaussuunnitelma sisältää tiedot mm. asiakirjallisten tietojen julkisuusluokasta ja henkilötietoluonteesta. Tavoitteena on, että SÄHKE 2 -määrityksen mukainen tiedonohjaussuunnitelma toimisi Asianhallintajärjestelmän taustalla seuraavan versiopäivityksen käyttöönotossa. Henkilörekistereiden rekisterikohtaisissa tietosuojaselosteissa viitataan säilytysajoista edellä mainittuun TOS:iin. Säilytysajoja ei ole ylläpitohaasteiden takia kuvattu selosteissa sen tarkemmin.

Savonlinnan kaupungin keskeisiä tietojärjestelmätoimittajia ovat CGI Oyj, Visma Public Oy, Visma Enterprise Oy ja Tieto Oyj. Tietoliikennepalveluiden kokonaisvaltaisena toimittajana Blue Lake Communications Oy on tietoturvan kannalta ratkaisevassa asemassa.

Talous- ja henkilöstöhallinnon ohjelmistoja käytetään Visman pilvipalvelusta ja näin ollen Visma Public Oy toimii henkilötietojen käsittelijänä. Paikkatietopalveluiden tietojärjestelmää käytetään CGI Oyj:n pilvipalvelusta ja palveluntarjoaja toimii myös henkilötietojen käsittelijänä, koska tietojärjestelmä sisältää käyttäjärekisterin lisäksi Savonlinnan väestötiedot. Muilta osin kaikkia operatiivisia sovelluksia käytetään omasta palvelinympäristöstä.

Savonlinnan kaupungilla on käytössä Innofactor Oyj:n Dynasty- Asianhallintajärjestelmä, jolla hallitaan asioiden vireilletuloa, valmistelua ja päätöksentekoa. Asianhallintajärjestelmä käsittää Asianhallinnan (diaari), Kokoushallinnan (esityslistat ja pöytäkirjat), Viranhaltijapäätökset ja Julkaisupalvelun. Dynasty-julkaisupalvelu kattaa kokoushallinnan esityslistojen ja pöytäkirjojen sekä viranhaltijapäätösten julkaisun yleisessä tietoverkossa. Esityslistassa ja kokouspöytäkirjassa sekä viranhaltijapäätöksessä julkaistaan ainoastaan tiedonsaannin kannalta välttämättömät henkilötiedot, joita ilman kuntalaisten on mahdotonta tai vaikeaa arvioida sitä, tulisiko päätöksestä hakea muutosta. Järjestelmä mahdollistaa asiakirjojen sisältämien henkilötietojen poistumisen automaattisesti tietoverkosta oikaisuvaatimus- tai valitusajan päättyessä.

Lakisääteiset palvelut on kuvattu ja ylläpidetään Suomi.fi Palvelutietovarannossa. Varhaiskasvatuksen toimipaikoista, varhaiskasvatuksessa olevista lapsista ja heidän huoltajistaan sekä varhaiskasvatuksen henkilöstöstä viedään tiedot Opetushallituksen Varda-tietovarantoon.

Kaupungin käytössä olevat tietojärjestelmät on luetteloitu ja keskeisistä tietojärjestelmistä on tehty tietojärjestelmäselosteet jo aiemmin. → ***Tietojärjestelmäselosteita ja kokonaisarkkitehtuurikuvausta ei uuden Tiedonhallintalain (906/2019) mukaan jatkossa tarvita, mutta järjestelmäluettelo liittymätietoineen on tarpeen kuvata osana tiedonhallintamallia. Näin ollen kaupungin tietojärjestelmäkuvaus vaatii päivitystä, joka on tarkoitus toteuttaa vuoden 2020 aikana.***

4. LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Julkishallinnon organisaatiot noudattavat **Suomen ja EU:n lainsäädäntöä**. Kuntien tiedonhallintaa ohjaavat mm.

- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Tietosuoja-asetus (EU 679/2016)
- Tietosuojalaki (1050/2018)
- Arkistolaki (831/1994) ja uutena lakina myös
- Laki julkisen hallinnon tiedonhallinnasta (906/2019, ts. Tiedonhallintalaki)
- sekä useat muut yleis- ja erityislait ja Kuntaliiton ohjeistukset.

Lisäksi toimintaa ohjaavat sisäiset ja ulkoiset **rahoittajat** (projektit, hankkeet) ja omat ohjeistukset henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista.

Kaupungin tietosuojaa ja tietoturvaa koskee mm. seuraavat organisaation sisäiset ohjeet:

- Henkilötiedon käsittelyn yleisohje
 - Tietosuojan muistilista asiakaspalveluun
 - Tietosuojan muistilista esimiehelle
 - Tietosuojan muistilista työntekijälle
- Perehdyttämisopas
- Peruskäyttäjä tietoturvaohje
- Salatun sähköpostin salasanan vaihtaminen
- Tietoturvapoliittika
- Työnantajalle kuuluvien sähköpostien avaaminen
- Verkkosijaintiin tallentaminen
- VPN-yhteyden luominen
- Älypuhelimien käyttöohjeet

Tietosuojaa ja tietoturvaa koskevan lainsäädännön seurannan vastuu on tietosuojavastaavalla ja tietohallintopäälliköllä, samoin kuin tietosuojaa ja tietoturvaa koskevien toimintamallien ja ohjeiden työstäminen ja päivittäminen. Kaupungin tietosuojatyöryhmä kokoontuu vuositasolla kvartaaleittain ja työryhmässä käydään läpi mm. muuttuvaa tietosuojalainsäädäntöä ja sen vaikutusta oman organisaation toimintaan, ohjeisiin, toimintamalleihin sekä koulutustarpeisiin. Tietosuojatyöryhmä käsittelee myös mahdolliset tietosuoja-/tietoturvapoikkeamat ja niitä koskevat vaikutusten arvioinnin ja ilmoitusvelvollisuudet.

5. REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN

Jokaisella on perustuslaillinen oikeus henkilötietojensa suojaan. Tietosuoja on yksilön perusoikeus, jonka tarkoituksena on turvata rekisteröidyn oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisterinpitäjän velvollisuus on huolehtia rekisteröidyn oikeuksien toteutumisesta. Näitä ovat muun muassa rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy tietoihin ja oikeus oikaista virheellisiä tietoja. Lisäksi rekisteröidyillä on oikeus tietyillä rajauksilla saada tieto sosiaali- ja terveydenhuollon käyttö ja -luovutustiedoista.

Rekisterinpitäjän tulee informoida rekisteröityjä henkilötietojen käytöstä avoimesti ja selkeästi. Rekisterinpitäjän tulee myös varautua mahdollisiin henkilötietojen tietoturvaloukkauksiin ja harjoitella niihin varautumista käytännössä. Henkilötietojen tietoturvaloukkauksia ovat mm., että tiedot lähetetty väärälle vastaanottajalle, suojaamaton tiedonsiirtoväline on hävinnyt esim. USB-tikku, haittaohjelmatartunta, kyberhyökkäys ja hakkerointi. Rekisterinpitäjän tulee tilastoida henkilötietojen tietoturvaloukkaukset ja ilmoittaa niistä

tietosuojavaltuutetun toimistolle ja tietyn edellytyksin myös rekisteröidyille. Henkilötietojen käsittelijöillä on velvollisuus puolestaan ilmoittaa henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle.

Henkilötiedon käsittelyä koskeva informointi toteutetaan kaupungin kotisivuilla sijaitsevien [tietosuojaselosteiden](#) avulla. Lisäksi toimialoilla ja keskushallinnossa henkilötietoja käsitteleviä henkilöitä on ohjeistettu antamaan myös suullista informointia henkilötiedon käsittelystä ja opastamaan rekisteröidyt tutustumaan kotisivuilla oleviin selosteisiin. Kotisivuilla ja tietosuojaselosteissa on ilmoitettu tietosuojavastaavan yhteystiedot, jotta rekisteröidyt voivat ottaa henkilötiedon käsittelyä koskevissa asioissa yhteyttä myös tietosuojavastaavaan.

Tietosuojalainsäädännön mukaista tarkastusoikeutta käyttäessään rekisteröityjä on tietosuojaselosteissa ohjeistettu olemaan ensisijaisesti yhteydessä tietosuojavastaavan, joka edelleen on yhteydessä kyseisen rekisterin yhteyshenkilöön. Tietosuojavastaava ja rekisterin yhteyshenkilö suunnittelevat yhdessä toteutusprosessin huomioiden, että rekisteröidyn henkilöllisyys tulee varmistettua. Tarkastuspyynnön toteuttamista koskevissa epäselvyyksissä lopullisen päätöksenteon tekee rekisterin vastuuhenkilö. Jos henkilötietoja ei jostain syystä luovuteta, niin rekisteröityä ohjataan kääntymään tietosuojavaltuutetun toimiston puoleen. Myös rekisterin tietosisällön lopullisen korjaustarpeen arvioi epäselvissä tapauksissa rekisterin vastuuhenkilö. Vuoden 2019 aikana tietopyynnot ovat olleet ensisijaisesti julkisuuslain mukaisia tietopyyntöjä. Tietosuojalainsäädännön mukaisia rekisteröidyn tarkastusoikeuspyyntöjä ei ole esiintynyt.

Henkilötietojen tietoturvaloukkauksien seurannan vastuu on tietosuojavastaavalla ja tietohallintopäälliköllä. Ilmoitusvastuu valvovalle viranomaiselle on tietosuojavastaavalla. Hallintamallissa on mukana kaupungin tietosuojatyöryhmä, joka tekee lopullisen päätöksen mm. rekisteröidyille ilmoittamisesta. Kaupunki on ollut kahtena peräkkäisenä vuonna (2018 ja 2019) mukana valtakunnallisessa Väestörekisterikeskuksen (nyk. Digi- ja väestövirasto) organisoimassa Taisto -tietoturva- ja tietosuojaloukkausten hallinnan harjoituksissa. Harjoituksiin on tarkoitus osallistua myös jatkossa. → **Henkilöstön tulee kiinnittää huomiota Tietosuoja- ja tietoturva-poikkeamien ilmoittamiseen. Ilmoituskynnys tulee olla mahdollisimman matala, jotta ongelmiin päästään käsiksi riittävän ajoissa ja tietosuoja-asetuksen mukainen 72 tunnin ilmoitusvelvollisuus voidaan toteuttaa.** → **Tietosuojavastaava muistuttaa henkilöstöä asiasta kahdesti vuodessa (syksy/kevät).**

6. ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN

Organisaation tulee arvioida tietosuojan ja -turvan tilanne toimintapolitiikan, poikkeamien, mittareiden, ja muiden kuvausten sekä mahdollisten asiakas- ja henkilöstön palautteiden avulla ja verrata kehitystä aiempiin vuosiin. Henkilöstön osaamisen sekä toimintaprosessien arviointi ja kehittäminen ovat myös tärkeitä arvioinnin kohteita. Tarkoituksena on tuoda esille myös keskeiset kehittämistavoitteet ja arvioida niiden toteutumista säännöllisesti.

Koska kaupungin tietotilinpäätös on ensimmäinen, niin seurantamittareita vuodelle 2019 ei oltu aiemmin luotu. Näin ollen toimintaa arvioidaan lähinnä kehittämistoimenpiteiden toteutumisen näkökulmasta.

Vuoden 2019 aikana on toteutettu tietoturvallisuuteen vaikuttavia kehittämistoimia seuraavasti:

- Päätoimisen tietosuojavastaavan nimeäminen
- Tietoturvapoliitiikan ja tietoturvaohjeiden päivitys (kj:n jory 28.1.2019, § 25)
- Henkilötiedon käsittelyn yleisohje (kh 19.12.2019, § 516)
 - Tietosuojan muistilista asiakaspalveluun
 - Tietosuojan muistilista esimiehelle
 - Tietosuojan muistilista työntekijälle
- Tietosuojaa koskevat asiat päivitetty perehdytysoppaaseen (12/2019)
- Työnantajalle kuuluvien sähköpostien avaaminen -ohjeistus päivitetty (12/2019)
- Kuvallisten henkilökorttien käyttöönotto
- Osallistuminen Väestörekisterikeskuksen TAISTO19 tietoturva- ja tietosuojaloukkausten hallinnan harjoitukseen (19.11.2019)
- Kaupungintalon konesalin UPS-järjestelmän akuston laajennus (varokäyntiaika 90 minuuttia)
- Kaupungintalon avainjärjestelmän uusinta (12/2019)
- Henkilöstölle pidetty toimialakohtaisia koulutustilaisuuksia ja Navisec-koulutuksen on suorittanut 219 työntekijää.

Toiminnan kehittämiskohteita v. 2020 on kuvattu kursivoituna aiemmissa kappaleissa nykytilannekuvausten ohella.

Muuttuva lainsäädäntö tuo myös jatkuvia tietoturvan ja tietosuojan kehittämistarpeita. Vuonna 2020 voimaan tullut **Tiedonhallintalaki (906/2019)** tuo veloitteita tuleville vuosille tietoturvan, tietosuojan ja tiedonhallinnan kehittämiseksi (mm. tiedonhallintamalli tulee kuvata vuoden 2021 alkuun mennessä). Tulevien vuosien kehittämiskohteet määrittyvät pitkälti kyseisen lain edellyttämistä vaatimuksista. Tällä hetkellä asian edistämiseksi odotetaan vielä lain mukanaan tuoman uuden toimielimen Tiedonhallintalautakunnan ja Kuntaliiton suosituksia. Laki aiheuttaa mm. vastuiden määrittelyä, useiden dokumenttien päivittämistarpeita ja uusia tietojärjestelmävaatimuksia. Myös **Laki digitaalisten palveluiden tarjoamisesta (306/2019)** veloittaa viranomaisia edistämään digitaalisten palvelujen saatavuutta, laatua, tietoturvallisuutta sekä sisällön saavutettavuutta ja siten parantamaan jokaisen mahdollisuuksia käyttää yhdenvertaisesti digitaalisia palveluja. Lisäksi **lisääntyneet kyberuhkat** vaativat uusia teknisiä ratkaisuja sekä henkilöstön koulutusta ja tietoturvan tietoisuuden lisäämistä.

7. SEURANTA JA MITTARIT

Organisaation on kehitystyössään ja laadunhallinnassa hyvä kuvata toimintaansa erilaisilla mittareilla. Tietosuojaa ja tietoturvaa koskevista mittareista osa palvelee organisaation omaa tarvetta ja osa mittareita ovat

sellaisia, joita joudutaan raportoimaan muualle. Mittareista on apua jatkuvaan laadun seurantaan, ne helpottavat raportoinnin toteutusta ja määrittävät tietosuojaa- ja tietoturvaa koskevia kehitystarpeita.

Jatkossa tietosuojan ja tietoturvan tilaa kuvaavat mm. seuraavat tunnusluvut:

- Rekisteröidyn oikeuksien toteutuminen > henkilötietojen tarkastus-, oikaisu- ja poistopyyntöjen määrät
- Valvontaviranomaisten mahdolliset selvityspyynnot > määrät
- Tietoturvaloukkausilmoitukset valvontaviranomaiselle > määrät
- Tietoturvaloukkausilmoitukset rekisteröidyille > määrät
- Mahdolliset muuta vakavat tietoturvapoikkeamat > määrät
- Tietojärjestelmät > määrät
- Koulutusten toteutuminen > Navisec-osallistujamäärät ja läsnäolokoulutusten määrät ja osallistujat

Tietoturvallisuuden tilaa arvioidaan säännöllisesti myös kansallisella tasolla, kun kaupunki osallistuu valtakunnalliseen Digi- ja väestötietovirasto (ent. Väestörekisterikeskus) organisoimaan Digitaalisen toimintaympäristön turvallisuustilanteen kyselyyn.

Myös kustannusten seurantaan on kiinnitettävä huomiota. Kaupungin tietohallinnon kustannukset jakautuvat atk-palvelukeskuksen ja toimialojen kesken. Atk-palvelukeskus maksaa yhteisesti käytössä olevan ympäristön kulut kuten työasemavuokrat, tietoliikennepalvelut ja Microsoftin lisenssimaksut. Katteen kuluilleen atk-palvelukeskus saa toimialoilta perittävistä laiteveloituksista. Toimialat maksavat omassa käytössään olevien tietojärjestelmien käytön. Jokaisella tietojärjestelmällä on toimialalla vastuuyksikkö ja pääkäyttäjä, jotka on kirjattu Savnet-intranetissa julkaistuun tietojärjestelmäluetteloon.

Tietohallinnon ja atk-palvelukeskuksen toiminta sekä painopistealueet on kuvattu vuosittain päivitettävässä tieto- ja viestintäteknikkasuunnitelmassa.