ORIMATTILAN KAUPUNKI

TIEDONHALLINNON VASTUUT JA TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Kh 14.12.2020

1. JOHDANTO

Tiedonhallinta on tiedon keräämistä, organisointia ja tallettamista niin, että tieto saadaan käyttöön tarkoituksenmukaisesti ja hallitusti. Tässä asiakirjassa tiedonhallinnalla tarkoitetaan julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, myöh. tiedonhallintalaki) määritelmän mukaisesti viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista.

Kaupungin johto määrittää tietoturva- ja tietosuojapolitiikassa ne periaatteet, toimintatavat, vastuut ja tavoitteet, joita noudatetaan Orimattilan kaupungin tietoturva- ja tietosuojatyön kehittämisessä.

Tällä asiakirjalla määritetään tiedonhallintalain mukaisesti niin tiedonhallintalakiin kuin muuhun lainsäädäntöön perustuvien tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut Orimattilan kaupungin toiminnassa. Politiikka toimii perustana kaupungin tietoturvaa ja tietosuojaa koskeville alaohjeille, jotka tarkentavat ja ohjeistavat näiden asioiden käytäntöön soveltamisessa.

2. TIEDONHALLINNAN VASTUUT

2.1 Kaupungin tiedonhallinnan johtaminen

Orimattilan kaupunki on tiedonhallintalaissa tarkoitettu tiedonhallintayksikkö. Tiedonhallintayksikön johtajana toimii hallintosäännön mukaisesti kaupunginhallitus. Kaupunginhallitus vastaa siitä, että tiedonhallintalain vastuut, käytännöt ja valvonta on määritelty.

Tiedonhallintalain mukaan kaupunginhallituksen on huolehdittava, että:

Toimija	Vastuut
Kaupunginhallitus	Vastuu asianhallinnan ja palvelujen tiedonhallinnan järjestämisestä sekä tietoaineistojen säilyttämisen järjestämisestä (21 §, 25 - 27 §). Tietoturvan seuranta ja tietoturvapolitiikan hyväksyminen
Kaupunginjohtaja	Vastuu tietoturvan toteutumisesta Kaupunginjohtaja vastaa kriisiviestinnästä mukaan lukien ulkoinen tietoturvaviestintä.
Talous- ja hallintojohtaja	Tietoturvan kehittäminen ja organisointi sekä raportointi koko organisaation tasolla

Toimialajohtaja	Tietoturvan kehittäminen kaupungin yhteisten linjausten mukaisesti ja toteutumisesta vastaaminen omalla toimialalla sekä toteutumisen raportointi. Tietojärjestelmien tietoturvallisen käytön ohjeistaminen yhteistyössä tietojärjestelmän vastuuhenkilön kanssa
Henkilöstö	Määräysten ja ohjeiden noudattaminen sekä tietosuojan ja tietoturvan kannalta poikkeavien tapahtumien ilmoittaminen omalle esimiehelle, talous- ja hallintojohtajalle, henkilöstövastalle tai it-tukeen asian luonteen mukaan
Esimies	Tietoturvaperehdytys, omaisuuden hallinta, avainten ja työvälineiden luovutus ja palautus sekä käyttöoikeuksien hakeminen/poistopyyntöjen tekeminen annettujen ohjeiden mukaan oman yksikkönsä osalta
Tietosuojavastaava	Henkilötietojen käsittelyn valvonta. Henkilökunnan tukeminen ja ohjeistaminen tietosuojaan liittyvissä kysymyksissä. Tietosuojaan liittyvä sisäisen viestintä.
Tietohallintopäällikkö (ulkoistettu palvelu)	Tukee tietoturvapolitiikan toteuttamisessa ja antaa mm. järjestelmähankinnoista lausunnon tietoturvaan ja kokonaisarkkitehtuuriin liittyen, sekä vastaa teknisen tietoturvaturvan toteutumisen raportoinnista voimassa olevan sopimuksen puitteissa.
ICT-palvelujen tuottaja (ulkoistettu palvelu)	Vastuu tietoturvan toteutumisesta teknisessä ja tuotannollisessa tietojärjestelmäympäristössä voimassa olevan sopimuksen puitteissa
Tietojärjestelmän pääkäyttäjä	Tietoturvan, tietosuojan ja käyttöoikeuksien hallinnan toteuttaminen (ellei käyttöoikeushallinta ole muutoin vastuutettu)
Tietojärjestelmän omistaja	Tietojärjestelmän ja sen sisältämän tiedon tietoturvan, riskienhallinnan ja jatkuvuuden hallinta. Vastaa, että järjestelmäkuvaukset on laadittu ja ovat ajantasaisia.
Henkilöstöasioiden tallentajat	Tietoturvan ja tietosuojan toteutuminen henkilöstöprosessin kaikissa vaiheissa.
Tietohallinnon ohjausryhmä	Tietoturvan toteutumisen ja riittävyyden seuranta. Kaupunginjohtaja nimeää ryhmän, jossa on kaikkien toimialojen edustus sekä tietohallintopäällikkö. Ryhmän puheenjohtajana toimii talous- ja hallintojohtaja.

3. Asianhallinta ja palveluiden tiedonhallinta

3.1 Asiarekisteri

Toimialat ja toimielimet hoitavat niiden järjestettäväksi annettuja lakisääteisiä tehtäviä. Tehtävien hoitamisen tukena tarvitaan rekistereitä. Asiarekisteriin rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Rekisteröinti on tehtävä viipymättä. Rekisteritietojen avulla asiakirjat yksilöidään, todennetaan niiden saapuminen ja lähettäminen sekä löytyminen. Asiarekisterin tai sen osan julkisia merkintöjä voi hyödyntää tiedonsaantia koskevien pyyntöjen yksilöimiseksi. Asiarekisterin tarkoitus on edistää julkisuusperiaatteen, hyvän hallinnon ja oikeusturvan toteutumista. Palveluja tuotettaessa tietoaineistojen hallinta on järjestettävä siten, että tietoaineistosta muodostettavat asiakirjat ovat haettavissa jollakin tietokokonaisuudet yksilöivällä tunnuksella esimerkiksi kiinteistötunnuksella tai henkilötunnuksella. Näin tiedot voidaan antaa siihen oikeutetulle vaivattomasti.

Orimattilan kaupungin rekisterinpitäjänä toimii kaupunginhallitus tai ao. valiokunta/lautakunta. Rekisterinpitäjällä on vastuu rekisterissään olevista henkilötiedoista ja niiden käsittelystä. Rekisterinpitäjällä on velvoite määritellä henkilötietojen käsittelyperuste. Rekisterinpitäjän on myös pystyttävä osoittamaan, että henkilötietojen käsittelyssä noudatetaan tietosuojalainsäädäntöä.

Jokaisella rekisterinpitäjällä tulee olla laadittuna rekisterikohtainen tietosuojaseloste ja rekisterikohtainen tietosuojariskien arviointi. Nämä dokumentit toimitetaan tietosuojavastaavalle.

Lisäksi tietosuoja otetaan huomioon kaupungin (rekisterinpitäjä) ja henkilötietojen käsittelijän (esim. järjestelmätoimittaja) välissä sopimuksissa EU:n yleisen tietosuoja-asetuksen mukaisesti, jolloin henkilötietojen käsittelijän vastuu määritellään kirjallisella sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään (kaupunkiin). Sopimuksessa on määriteltävä vähintään käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

Toimialojen asiahallinnon vastuuhenkilöt huolehtivat tehtäväalueellaan ohjeiden ja lainsäädännön noudattamisesta sekä tietojärjestelmäuudistuksissa rekistereiden, tietojen ja järjestelmien elinkaaren hallinnasta sekä huomioivat tiedonhallinnan ja säilyttämisaikojen vaatimukset. Näiltä osin asiahallinnon vastuuhenkilöt ovat yhteydessä keskusarkistoon. Lisäksi yksiköissä on nimetty arkistovastaavia, jotka toimivat yhteyshenkilöinä kaupunginarkistosta vastaavan kanssa.

Arkistoyhdyshenkilöt viestivät yksiköissä tapahtuvista muutoksista ja tarpeista kaupungin-arkistoon, hoitavat paperiarkistojen hoitamisen sekä edistävät tiedonohjaussuunnitelmatyötä (TOS).

3.2 Tietoaineistojen säilytystarpeen määrittäminen

Tietojen säilyttämisaikojen perusteet säädetään usein laissa. Jos näin ei ole, on säilytysaikoja määritettäessä otettava huomioon tietoaineiston alkuperäisen käyttötarkoituksen mukainen tarpeellisuus viranomaisen toiminnassa; luonnollisen henkilön tai oikeushenkilön etujen, oikeuksien, velvollisuuksien ja oikeusturvan toteuttaminen ja todentaminen; sopimuksen tai muun yksityisoikeudellisen oikeustoimen oikeusvaikutus tai vahingonkorvausoikeudelliset ja rikosoikeudelliset vanhentumisajat.

Tietosuoja-asetuksen perusteella säilytysajat määrittelee henkilötietojen osalta rekisterinpitäjä ja arkistolain perusteella muiden asiakirjojen säilytysajat arkistonmuodostaja. Lisäksi Kansallisarkisto

päättää arkistolain nojalla julkishallinnon toimijoiden pysyvästi säilytettävistä asiakirjatiedoista ja niiden säilytysmuodosta.

Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla. Arkistoon siirrettävät asiakirjat määritellään arkistolain perusteella osana arkistotoimen tehtäviä.

3.3 Tietopyynnöt (Julkisuuslaki ja Tietosuoja-asetus)

Tietopyynnöllä tarkoitetaan viranomaisten toiminnan julkisuudesta annetun lain (621/199, jatkossa julkisuuslaki), tietosuoja-asetuksen sekä muun erityislainsäädännön tarkoittamia viranomaiselle tehtyjä tietopyyntöjä.

Jokaisella on oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tiedon antaminen viranomaisen asiakirjasta, joka ei vielä ole julkinen, on viranomaisen harkinnassa. Salassa pidettävästä viranomaisen asiakirjasta tai sen sisällöstä saa antaa tiedon vain, jos niin erikseen laissa säädetään. Julkisuuslaissa on lisäksi erikseen säädetty asianosaisen laajemmasta tiedonsaantioikeudesta viranomaisen asiakirjoihin.

Tiedon asiakirjan sisällöstä antaa se viranomaisen henkilöstöön kuuluva, jolle se hänen asemansa ja tehtäviensä vuoksi muuten kuuluu. Viranomaisen asiakirjan sisällöstä annetaan tieto suullisesti taikka antamalla asiakirja viranomaisen luona nähtäväksi ja jäljennettäväksi tai kuunneltavaksi tai antamalla siitä kopio tai tuloste. Tietopyynnöt on käsiteltävä viivytyksettä ja tieto julkisesta asiakirjasta on annettava mahdollisimman pian, kuitenkin viimeistään kahden viikon kuluessa siitä, kun viranomainen on saanut asiakirjan saamista koskevan pyynnön. Jos pyydettyjä asiakirjoja on paljon tai niihin sisältyy salassa pidettäviä osia tai jos muu niihin rinnastettava syy aiheuttaa sen, että asian käsittely ja ratkaisu vaativat erityistoimenpiteitä tai muutoin tavanomaista suuremman työmäärän, asia on ratkaistava ja tieto julkisesta asiakirjasta annettava viimeistään kuukauden kuluessa siitä, kun viranomainen on saanut asiakirjan saamista koskevan pyynnön.

Mikäli pyydettyä tietoa ei voida antaa, tietopyytäjän on mahdollista siirtää asia viranomaisen ratkaistavaksi. Viranomaisen asiakirjan antamisesta päättää julkisuuslain mukaan se viranomainen, jonka hallussa asiakirja on.

Viranomaisen henkilörekisteristä saa julkisuuslain 16 §:n mukaan antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja. Jos luovutuksensaajalla ei ole tällaista oikeutta, voidaan julkinen tieto henkilörekisteristä antaa antamalla asiakirja nähtäväksi, kuunneltavaksi tai jäljennettäväksi tai antamalla siitä suullisesti tieto. Henkilötietoja voi luovuttaa suoramarkkinointia ja mielipide- tai markkinatutkimusta varten vain, jos niin erikseen säädetään tai jos rekisteröity on antanut siihen suostumuksensa. Pääsääntöisesti näihin tarkoituksiin ei anneta henkilötietoja.

Tietosuoja-asetuksen ((EU) 2016/679) 15 artiklan mukaan rekisteröidyllä on oikeus saada pääsy itseään tai huollettavaansa koskeviin henkilötietoihin. Rekisteröidyllä voi olla oikeus myös vastustaa käsittelyä, pyytää käsittelyn rajoittamista tai pyytää tietojen poistamista henkilörekisteristä.

Mikäli tietoja ei voida tietosuojalain (1050/2018) 33 §:n tai 34 §:n nojalla luovuttaa, tulee rekisteröidyltä tiedustella, haluaako tämä kirjallisen ilmoituksen. Jos tietoja ei perustellusta syystä voida antaa, on asiasta tietopyytäjän pyynnöstä tehtävä muutoksenhakukelpoinen päätös tai tietosuoja-asetuksen nojalla kirjallinen ilmoitus. Mikäli rekisteröity katsoo, että rekisterinpitäjä ei ole käsitellyt henkilötietoja lainmukaisesti tai on tyytymätön tietopyynnön ratkaisuun, on tällä oikeus kannella tietosuojavaltuutetulle.

4. Tietoturvallisuus ja tietosuoja

4.1 Tietoturvallisuus

Tietoturvallisuus(tietoturva) on tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarantuisi. Tietoturvallisuus on kiinteä osa kaupungin palveluita, toimintaa ja jokaisen tiedon käyttäjän päivittäistä työtä. Tietoturvallisuus kattaa kaikki tietojenkäsittelytehtävät, myös erityyppisten dokumenttien arkistoinnin. Mikäli tietoihin sisältyy henkilötietoa, tietoturvassa on huomioitava tietosuojan tuomat vaatimukset.

Tietoturvallisuuden tavoitteet:

−tiedon saatavuus: että tieto, tietojärjestelmä tai palvelu on saatavilla ja hyödynnettävissä, valtuutetuille käyttäjille, haluttuna aikana ja vaaditulla tavalla. Saatavuuden varmistamiseksi ylläpidetään riittävää kapasiteettia, vikasietoisia toteutuksia, varmuuskopiokäytäntöjä sekä käytetään luotettavaksi todettuja teknisiä ratkaisuja.

−tiedon eheys ja kiistämättömyys: tiedon ajantasaisuutta, oikeellisuutta ja alkuperäisyyttä siten, että tietokokonaisuuteen, kuten asiakirjaan, tehdyt muutokset voidaan jälkikäteen todentaa. Kiistämättömyyden toteutumista tuetaan kattavilla ja keskitetyillä tapahtumien kirjaus- ja lokienhallintakäytännöillä. Eheydellä tarkoitetaan myös tietojen merkityksellistä yhteen toimivuutta siten, että tietojen siirto järjestelmästä toiseen voidaan toteuttaa tiedon eheys säilyttäen.

−tiedon luottamuksellisuus: tiedon käytön rajoittamista siten, että tietoja voivat käsitellä vain siihen oikeutetut henkilöt ja tietojärjestelmät lakien ja ohjeiden mukaisesti. Luottamuksellisuuteen liittyy kiinteästi pääsynhallinta, jolla varmistetaan kontrolloitu käyttöoikeuksien ylläpito työtehtävien ja -roolien mukaisesti.

4.2 Tietosuoja

Tietosuojan tavoitteena on velvoittavien tietosuojasäädösten toimenpiteiden toteutuminen siten, että henkilön riittävä yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietojen käsittelyssä varmistuvat.

Yksityisyyden suojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käsittelyltä. Laissa on määritelty tilanteet, jolloin henkilötiedon käsittely on sallittua. Tietosuojan lähtökohtana on sisäänrakennettu ja oletusarvoinen tietosuoja. Sisäänrakennetulla tarkoitetaan, että tietosuoja otetaan huomioon kaikissa tiedonkäsittelyn vaiheissa. Oletusarvoinen tietosuoja tarkoittaa sitä, että tiedonkäsittely-ympäristömme on lainsäädännön vaatimusten mukainen. Tietosuojan lähtökohdat ja periaatteet on huomioitava kaikessa henkilötiedon käsittelyssä.

Henkilötietojen käsittelyssä tavoitteeseen päästään toteuttamalla tietosuoja-asetuksen rekisterinpitäjälle osoittamat velvollisuudet ja todentamalla, että kaupungin kaikissa toiminnoissa toteutetaan tietosuoja-asetuksessa määriteltyjä henkilötietojen käsittelyn periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti, täsmällisesti ja läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään ainoastaan käyttötarkoituksen mukainen määrä
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

Henkilötiedon määritelmät:

Henkilötieto on tietoa, jonka perusteella henkilö voidaan tunnistaa suoraan tai välillisesti yhdistämällä tietoja eri lähteistä. Henkilötiedon käsittely edellyttää aina laista löytyvää käsittelyperustetta: rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleistä etua koskeva tehtävä tai julkinen valta, rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Erityinen henkilötieto (arkaluontoinen henkilötieto) on tietoa, josta ilmenee rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskeva tieto, seksuaalinen suuntautuminen tai käyttäytyminen sekä geneettinen tai biometrinen tieto henkilön tunnistamista varten. Erityisen henkilötiedon käsittely on lähtökohtaisesti kielletty. Poikkeuksista säädetään lainsäädännössä mm. EU:n yleinen tietosuoja-asetus ja tietosuojalaki. Erityisiä henkilötietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Salassa pidettävä henkilötieto on henkilötietoa, joka on määrätty lainsäädännössä (esim. julkisuuslaki, laki potilaan asemasta ja oikeuksista sekä laki sosiaalihuollon asiakkaan asemasta ja oikeuksista) salassa pidettäväksi ja sen käsittelyä säädetään lailla. Salassa pidettävää henkilötietoa saa käsitellä vain sellainen taho, jolla on siihen lakiin perustuva oikeus.

Henkilörekisteri tarkoittaa jäsenneltyjä henkilötietoja sisältävää tietojoukkoa. Henkilörekisterit on muodostettu lain mukaisen käsittelyperusteen nojalla, tietyn käyttötarkoituksen vuoksi. Jokaisella henkilörekisterillä on vastuullinen rekisterinpitäjä.

4.3 Tietoaineistoihin ja tietojärjestelmiin liittyvät roolit

Kaupungin tietoon ja tietojärjestelmiin liittyy useita toiminnallisia rooleja, jotka voivat olla lakisääteisiä tai niillä varmistetaan tietoturvan ja tietosuojan toteutuminen kaikilla organisaation tasoilla.

Tiedon omistaja: Toimialan operatiivinen johto toimii tiedon omistajana. Tiedon omistaja vastaa toimintaansa liittyvän tietoaineiston luokittelusta, elinkaaren hallinnasta sekä suojaamisesta. Tiedon omistajan tehtävä on varmistaa, että kyseinen tieto säilyttää eheyden ja luottamuksellisuuden. Tiedon omistaja varmistaa, että riittävät kontrollit tiedon suojaamiseksi on toteutettu ja data on suojattu riittävällä tasolla.

Rekisterinpitäjä: Henkilörekisterillä on vastuullinen rekisterinpitäjä, jotka ovat kaupunginhallitus, valiokunnat, johtokunnat, kaupunkirakenteen tehtäväalueen jaostot sekä yhteyshenkilönä on palvelujohtaja tai toimialajohtaja tai liikelaitoksen johtaja. Rekisterinpitäjä määrittää henkilötietojen käsittelyn tarkoituksen ja keinot.

Tietojärjestelmän omistaja: Tietojärjestelmän omistaja on sen toimialan/tulosalueen/yksikön operatiivinen johto, jonka toimintaa ja tietojenkäsittelyä varten järjestelmä on hankittu. Mikäli tietojärjestelmä on yhteiskäyttöinen, määritellään sille yksi omistaja, joka vastaa perustehtävien lisäksi tietojärjestelmän käytön koordinoinnista, kehittämisestä ja kulujen jakamisesta. Omistaja määrittelee järjestelmän käyttöoikeudet ja pääkäyttäjät.

Tiedon käsittelijä: Tiedon käsittelijä on sopimuksella määritelty palvelun tuottaja tai järjestelmän toimittaja, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Sidosryhmät, toimittajat ja muut kaupungin ulkopuoliset tahot, joilla on pääsy kaupungin tietoihin ja tietojärjestelmiin sitoutuvat kaupungin ohjeisiin.

Tietovarannosta vastaava viranomainen: Rekisterinpitäjät tai tietovarannoista vastaavat viranomaiset sekä virkamiehet tai työntekijät, joilla on kokonaisvastuu rekisterinpidosta (rekisterinpitäjän edustaja) tai tietovarannosta. Tietovarantoja koskeviin vastuisiin kuuluu myös semanttisesta yhteen toimivuudesta huolehtiminen.

Tietojärjestelmäympäristössä käytetään tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Työasemat ovat it-palveluiden tuottajan järjestelmässä.

Pääsy kaupungin tietoverkkoon ja –järjestelmiin sekä käyttöoikeudet kaupungin hallinnoimaan tietoon myönnetään käyttövaltuuspolitiikan mukaisesti työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet sekä pääsy tietoverkkoon tulee poistaa palvelussuhteen päättyessä tai keskeytyessä.

5. Tietoriskien hallinta

Kaupungin on selvitettävä olennaiset tietojenkäsittelyyn, kehittämiseen ja hankintoihin kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti koko tiedon elinkaaren ajalle. Riskienhallinnan tulee kattaa tietoaineistot, tietovarannot ja tietojärjestelmät sekä digitaalisen toimintaympäristön kyber- ja yhdistelmäuhkat. Riskit ja hallintatoimenpiteet tulee huomioida myös jatkuvuussuunnittelussa, jonka avulla pyritään takaamaan tiedon tai tietojärjestelmän riittävä saatavuus. Tietoturvariskit arvioidaan tiedon eheyden, luottamuksellisuuden ja saatavuuden näkökulmasta suhteessa osapuolten oikeuksiin ja velvollisuuksiin, uhkan vakavuuteen ja kustannuksiin. Tietosuojariskit tulee arvioida rekisteröidyn näkökulmasta. Lisäksi tietyissä tilanteissa tulee toteuttaa vaikutusten arviointi, mikäli rekisteröidyn oikeuksiin tai vapauksiin kohdistuu riskejä henkilötiedon käsittelystä.

6. Tiedon luokittelu ja elinkaaren hallinta

Tiedon käsittelyä ohjaa julkisuuslaki sekä muu tiedonkäsittelyä ja henkilötiedon käsittelyä määrittelevä lainsäädäntö ja ohjeistus. Julkisuuslain mukaan viranomaisen asiakirjat ovat julkisia, ellei lainsäädännössä muuta määrätä.

Tiedon luokittelun tarkoituksena on varmistaa tiedon käsittelyn turvallisuus ja vaatimustenmukaisuus läpi tiedon elinkaaren. Kaupungissa tieto ja sen käsittelytoimet luokitellaan julkisuuslain sekä tietosuoja-asetuksen perusteella kolmeen luokkaan:

- Julkinen,
- Sisäinen
- Salassa pidettävä.

Neljäs luokka, henkilökohtainen tieto, on otettu käyttöön, jotta voidaan varmistaa yksityisyyden suoja työnantajan laitteissa olevaan henkilökohtaiseen tietoon liittyen. Turvakiellosta ja sen kohteena olevien tietojen käsittelystä säädetään laissa väestötietojärjestelmästä ja väestörekisterikeskuksen varmennepalveluista (661/2009) 36 §:ssä ja 37 §:ssä. Turvakiellon tarkoitus on suojella turvakiellon omaavan henkilön omaa turvallisuutta. Kaupunki noudattaa kaikessa turvakiellon alaisen tiedon käsittelyssä lainsäädäntöä ja käsittelyohjeita.

Julkinen tieto on tietoa, joka voidaan luovuttaa vapaasti ulkopuolelle ja voidaan käsitellä rajoituksetta kaupungin tietojärjestelmissä. Julkinen tieto voi sisältää vain julkista henkilötietoa. Henkilörekisteritietoon tulee kuitenkin aina olla laillinen käsittelyperuste.

Sisäinen tieto on ei-julkista tietoa tai henkilötietoa, joka on tarkoitettu vain kaupungin palvelu-alueen, yksikön tai yksittäisen työntekijän tai työntekijäryhmän käyttöön eli sisäiseen käyttöön. Sisäistä tietoa ei saateta kaupungin ulkopuolelle, paitsi niille kaupungin ulkopuolisille työntekijöille, joilla on oikeus käyttää tietoja erillisen sopimuksen perusteella. Sisäistä tietoa ei koske julkisuuslain säädökset, koska se ei ole julkisuuslaissa tarkoitettu viranomaisen asiakirja (esim. valmisteluaineisto, jota ei vielä annettu eteenpäin esittelyä ja päätöksentekoa varten).

Salassapidettävä tieto on tietoa, joka on julkisuuslain 24.1 § mukaan salassa pidettävää. Tietoa voivat käsitellä vain ne työntekijät (tuottajan työntekijät), joiden nimenomaisiin työtehtävien tiedon käsittely kuuluu. Tiedon luovuttaminen vaatii aina tietojen omistajan luvan. Salassa pidettävää henkilötietoa ovat esim. palvelun asiakkuus tai erityinen henkilötieto. Erityisen henkilötiedon käsittelyssä on noudatettava Tietosuojalain 6 § vaatimuksia.

Henkilökohtainen tieto on tieto tai asiakirja, joka ei liity työhön ja jota lyhytaikaisesti käsitellään työnantajan laitteilla tai sovelluksissa. Tallennettaessa käytettävä Henkilökohtainen -kansiota.

Eri tehtävissä käsiteltävien tietojen elinkaaren hallinta suunnitellaan tiedonohjaussuunnitelmien (TOS) avulla. Tiedonohjaussuunnitelmassa kuvataan kuntien yhteisen tehtäväluokituksen mukaisesti kaupungin tehtäviin liittyvien asiakirjojen ja tietojen säilytysaika, julkisuusluokka, salassapito ja sen perusteet sekä käsittelyvaiheet ja säilytystapa.

Konsernitoimiala koordinoi tiedon elinkaaren hallinnan kokonaisuutta ja ohjeita sekä tukee toimialoja tiedon hallinnan suunnittelussa. Toimialojen ja liikelaitosten asiakirjahallinnon vastuuhenkilöt ja yksiköiden arkistoyhdyshenkilöt vastaavat siitä, että toimintaan liittyvät tietoaineistot on luokiteltu ja niiden käsittely ja säilyttäminen tai arkistointi on ajantasaisesti määritelty tiedonohjaussuunnitelmassa. Tietoa tulee käsitellä luokittelun ja käsittelysääntöjen mukaisesti sekä analogisesti että sähköisesti.

7. Saavutettavuus

Laki digitaalisten palveluiden tarjoamisesta velvoittaa kaupunkia tekemään verkko-palveluistaan eli verkkosivustoista ja mobiilisovelluksista saavutettavuusvaatimusten mukaisia.

Saavutettavuus tarkoittaa, että verkkosisältöä voi käyttää erilaisilla avustavilla teknologioilla (kuten näkövammaisten käyttäjien ruudunlukuohjelmilla), erilaiset käyttäjät pääsevät sisältöön käsiksi ja pystyvät käyttämään toimintoja mahdollisista rajoitteista huolimatta ja sisältö toistuu oikein eri päätelaitteilla.

Saavutettavuusvaatimusten lisäksi laissa säädetään viranomaisten digitaalisten palvelujen järjestämisestä ja velvoitetaan tarjoamaan asiakkailleen mahdollisuuden viestiä viranomaisen kanssa sähköisesti.

8. Valvonta

Tiedonhallinnan, tietoturvan ja tietosuojan kokonaisuuteen liittyvien säädösten, määräysten ja ohjeiden noudattamiseen liittyvästä sisäisestä valvonnasta vastaa kaupunginhallitus ja operatiivinen

johto osana sisäisen valvonnan normaalia toimintaa. Tietosuojavastaava ja tarvittaessa sisäinen tarkastus arvioivat tiedonhallinnan kokonaisuuteen liittyvän sisäisen valvonnan toteutumista osana tarkastustoimintaa.

Tietosuojan ja tietoturvan teknisten ja organisatoristen suojatoimien riittävästä toteuttamisesta vastaa tiedon omistaja. Tietosuojan toteutumista seuraa tietosuojavastaava. Kaikista havaituista tietosuojapoikkeamista on viipymättä ilmoitettava tietosuojavastaavalle. Rekisterinpitäjällä on velvollisuus raportoida edelleen tietosuojavaltuutetulle poikkeamista, joissa henkilön yksityisyyden suoja on vaarantunut.

ICT-infrastruktuurin tietoturvaan liittyvästä valvonnasta vastaavat tietohallinto ja ICT-sopimuskumppani yhteistyössä toimialojen ja kanssa. Tietohallinnon ohjausryhmä koordinoi valvontaa.

Henkilöstö on ohjeistettu tunnistamaan ja raportoimaan tietoturva- ja tietosuojapoikkeamat esimiehelleen sekä yksikön tietoturva ja tietosuoja-asiantuntijalle. Poikkeamasta tehdään tietosuojavastaavan tuella asianmukainen selvitys, joka on käsiteltävä mahdollisimman pian. Kaikki kaupungin toteutuneet poikkeamat käsitellään yhtenäisen toimintamallin mukaisesti.

9. Rikkomusten käsittely

Tietoturvallisuuden tai tietosuojan laiminlyönti voi aiheuttaa vakavaa haittaa tai vahinkoa kaupungille ja kansalaisille. Kaupungin tiedonhallinta-, tietoturva- ja tietosuojaohjeiden noudattamatta jättäminen tai niiden vastainen toiminta voi olla peruste huomautukselle, varoitukselle, työsuhteen irtisanomiselle tai rikosoikeudellisille seuraamuksille. Salassapitovelvollisuuden rikkominen on asianomistajarikos, jolloin asianomainen henkilö voi tehdä asiasta rikosilmoituksen. Jokainen kaupungin henkilökuntaan kuuluva on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä lähimmälle esimiehelleen tai tietoturvavastaavalle. Sopimuskumppaneiden tietoturva- ja tietosuojarikkeiden ilmetessä tilaaja pyytää tuottajalta kirjallisen vastineen tapahtuneesta. Väärinkäytökset voivat johtaa sopimuksen purkamiseen ja/tai vahingonkorvausvastuuseen.

10. Seuranta ja raportointi

Tietoturvan vastuuhenkilöt, tietosuojavastaava sekä toimialojen määrittelemät asianhallintavastaavat kokoavat yhdessä tietohallinnon ohjausryhmän kanssa vuosittain tiedonhallinnan, tietoturvan ja tietosuojan raportin (tietotilinpäätöksen) kaupunginhallitukselle. Raportointi toteutetaan tilinpäätösaikataulussa. Tarvittaessa erillisistä asioista voidaan raportoida johdolle tai kaupunginhallitukselle. Tiedonhallinnan, tietoturvan ja tietosuojan näkökulmat nousevat esille lisäksi säännöllisesti raportoinnissa vuoden toisessa osavuosikatsauksissa ja tilinpäätöksessä.

11. Hyväksymismenettely

Kaupunginhallitus hyväksyy tiedonhallinnan vastuut ja tietoturva- ja tietosuojapolitiikka -asiakirjan sekä siihen kohdistuvat muutokset.

Tarkentavat tiedonhallinnan, tietoturvan ja tietosuojan kokonaisuuteen liittyvät kaupungin yhteiset ohjeet laaditaan ja päivitetään erikseen. Henkilöstön koulutustarve otetaan huomioon vuosittain laadittavassa koulutussuunnitelmassa.