

Mikkelin kaupungin tiedonhallintapolitiikka

SISÄLLYSLUETTELO

1	Tiedonhallintapolitiikka	4
1.1	Tiedonhallintapolitiikan tarkoitus ja soveltamisala	4
1.2	Mikkelin kaupungin ja toimintaympäristön vaikutukset tiedonhallintaan	4
1.3	Tiedonhallinta ja sitä koskeva sääntely	5
2	Tiedonhallinnan periaatteet, tavoitteet ja riskienhallinta	8
2.1	Periaatteet ja tavoitteet.....	8
2.2	Riskienhallinnan kehittäminen	10
3	Tiedonhallinnan vastuut	11
3.1	Kaupunginhallituksen ja kaupunginjohtajan vastuut	11
3.2	Toimielinten vastuut	11
3.3	Tiedonhallinnan asiantuntija- ja järjestämisvastuut.....	12
3.4	Tietosuojavastaavan vastuut ja kaupunkikonsernin tietoturva- ja tietosuojatyöryhmä..	13
3.5	Palvelualueiden vastuut ja tiedonhallintatyöryhmä.....	14
3.6	Tietojärjestelmän omistajan ja pääkäyttäjän vastuut	15
3.7	Esimiehen yleiset vastuut.....	15
3.8	Viranhaltijan ja työntekijän yleiset vastuut	16
3.9	Tieto- ja viestintätekniikan palvelujen hankintoihin liittyvät vastuut.....	17
4	Tiedonhallinnan kuvaukset, tiedottaminen ja toiminta häiriötilanteissa	18
4.1	Tiedonhallintamalli	18
4.2	Tiedonhallinnan muutosvaikutusten arviointi ja tietosuojan vaikutustenarviointi	19
4.3	Kuvaus asiakirjajulkisuuden toteuttamiseksi.....	19
4.4	Tietosuojaselosteet	20
4.5	Tiedonohjaussuunnitelmat	20
4.6	Tietotilinpäätös	21
4.7	Tiedonhallinnasta tiedottaminen	21
4.8	Toiminta häiriötilanteissa.....	22
5	Asiakirjahallinnon ja arkistotoimen toimintaohjeet	23
5.1	Asiakirjahallinnon ja arkistotoimen toimintaohjeiden tarkoitus ja soveltamisala	23
5.2	Asiakirjahallinnon ja arkistotoimen tehtävät ja tavoitteet	23
5.3	Asiakirjojen ja niitä vastaavien tietojen säilytysarvon määrittäminen	24
5.4	Asianhallinta ja palvelujen tiedonhallinta	25
5.5	Asiakirjojen ja niitä vastaavien tietojen säilyttäminen	26
5.6	Asiakirjojen ja niitä vastaavien tietojen pitkäaikaissäilyttäminen ja arkistointi.....	27

5.7	Kaupunginarkisto	29
5.8	Asiakirjojen ja niitä vastaavien tietojen tuhoaminen	30
5.9	Asiakirjojen ja niitä vastaavien tietojen käsittely, suojaaminen ja turvaaminen	30
6	Tietosuojan ja tietoturvan toimintaohjeet	32
6.1	Tietoturvallisuus viranomaistoiminnassa	32
6.2	Tietosuojan ja tietoturvan seuranta	33
6.3	Tietosuojan ja tietoturvan arviointi.....	33
6.4	Tietosuojan ja tietoturvan kehittäminen ja ohjeistaminen	33
7	Määritelmät ja käsitteet	34
8	Tiedonhallinnan kansalliset toimijat ja keskeiset säädökset	41
9	Versiot ja voimaantulo	43

1 Tiedonhallintapolitiikka

1.1 Tiedonhallintapolitiikan tarkoitus ja soveltamisala

Mikkelin kaupungin tiedonhallintapolitiikka on Mikkelin kaupunginhallituksen, tiedonhallintayksikön johdon, strateginen kannanotto ja ohje tiedonhallinnan järjestämiseen, suunnitteluun, ylläpitoon ja kehittämiseen sekä tiedonhallinnan vastuita koskeva määräys, jolla kaupunginhallitus määrittää hallintosäännön 69 §:ssä tarkoitetut vastuut. Poliitiikka määrittelee kaupungin tiedonhallinnan periaatteet, tavoitteet, toimintatavat, vastuut ja valvonnan.

Mikkelin kaupungin tiedonhallinnan perustana on kaupunginhallituksen hyväksymä tiedonhallintapolitiikka ja sen pohjalta laaditut ohjeistukset. Poliitiikan toteuttaminen on edellytys tiedonhallinnan pitkäjänteiseen kehittämiseen. Tiedonhallinnan laadukkaan järjestämisen, suunnittelun, ylläpidon ja kehittämisen onnistuminen edellyttää johdon sitoutumisen tiedonhallintaa koskevan työn tukemiseen.

Tiedonhallintapolitiikka koskee koko Mikkelin kaupunkia ja sen henkilöstöä. Konserniyhteisöjä poliitiikka koskee niissä tapauksissa ja niiden tehtävien osalta, kun niihin sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) ja ne suorittavat kaupungin lukuun toimeksiantotehtävää tai julkista hallintotehtävää. Tämä poliitiikka koskee henkilötietojen käsittelyä silloin, kun kaupungin viranomaiset toimivat rekisterinpitäjinä. Samoin poliitiikka koskee sidosryhmiä, jotka käsittelevät henkilötietoja kaupungin rekisterinpitäjien lukuun ja ohjaamana.

Poliitiikka kattaa Mikkelin kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

1.2 Mikkelin kaupungin ja toimintaympäristön vaikutukset tiedonhallintaan

Mikkelin kaupungin toiminnan perustana ovat lakisääteiset tehtävät ja asukkaiden tarvitsemat palvelut. Toimintaa ohjaavat kaupunginvaltuuston kaupunkistrategiassa asettamat tavoitteet, joissa otetaan huomioon kaupungin asukkaiden hyvinvoinnin edistäminen, palvelujen järjestäminen ja tuottaminen, palvelutavoitteet, omistaja- ja henkilöstöpolitiikka, asukkaiden osallistumis- ja vaikuttamismahdollisuudet sekä elinympäristön ja alueen elinvoiman kehittäminen. Kaupungin toimintaa johdetaan valtuuston hyväksymän strategian mukaisesti.

Strategisten tavoitteiden toteuttaminen ja digitalisoituva toimintaympäristö ohjaavat kaupungin toimintaa ja palveluita verkottuneeseen, digitaalisuutta, verkkopalveluja ja digitaalisessa muodossa olevaa tietoa hyödyntävään toimintatapaan, jossa tiedonhallinnan suunnittelun, ylläpidon ja kehittämisen tarve ja merkitys korostuu.

Mikkelin kaupungin palvelut kattavat laajan maantieteellisen ja toiminnallisen alueen. Palvelujen toiminta perustuu pitkälti tieto- ja viestintätekniisiin järjestelmiin eli laitteisiin, verkkoihin ja sovelluksiin sekä niiden välisiin integraatioihin, jotka ovat tyypillisesti eri toimittajien hallussa ja siten

organisatorisesti ja maantieteellisesti hajautettuja. Näin ollen Mikkelin kaupungin tiedonhallinta ulottuu kaupungin organisaation ja maantieteellisen alueen ulkopuolelle.

1.3 Tiedonhallinta ja sitä koskeva sääntely

Tieto ja tietojenkäsittely ovat nykymuotoisen yhteiskunnan toiminnan tärkeä edellytys. Tämä edellyttää tieto- ja viestintätekniisten palvelujen laadukasta, tietoturvallista ja keskeytyksetöntä toimintaa. Digitalisaatio tuo tämän vaatimuksen ja yksityisyyden suojan vaatimukset uusille alueille. Tiedonhallintaan liittyvä osaaminen voi nousta tulevaisuudessa organisaation toiminnan menestystekijäksi. Oikein toteutettuna tiedonhallinta mukaan lukien tietosuoja ja tietoturva mahdollistavat muodostetun ja kerätyn tiedon aikaisempaa tehokkaamman hyödyntämisen ja kustannussäästöt.

Tiedonhallinnasta julkisissa organisaatioissa ja viranomaisissa säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019). Lain määritelmän mukaan tiedonhallinnalla tarkoitetaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvaluustoimenpiteitä viranomaisten tietoaaineistojen, niiden käsittelyvaiheiden ja tietoaaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaaineistojen tallentamistavasta ja muista käsittelytavoista.

Tiedonhallinta kohdistuu sekä digitaalisessa että analogisessa muodossa oleviin tietoaaineistojen tietoihin koko niiden elinkaaren ajan. Tietoaaineistojen tiedot ilmentyvät asiakirjoina, niiden rekisteröintitietoina, rekistereinä tai muina näitä vastaavina tietoina, jotka muodostuvat tehtävien ja toiminnan tuloksena. Tiedon elinkaaren vaiheisiin kuuluu tietoaaineistojen muodostaminen ja kerääminen, rekisteröinti ja talteenotto, säilyttäminen, jonka yhteydessä tapahtuu erityisesti tiedon käsittelyä, hyödyntämistä, luovuttamista, suojaamista ja turvaamista, sekä arkistointi tai tuhoaminen. Tietoaaineistojen arkistoinnin voidaan katsoa aloittavan niiden elinkaaren toisen vaiheen, jossa tärkeitä toimintoja ovat kulttuuriperinnöllisesti arvokkaiden aineistojen säilyttäminen sekä hyödyntäminen ja luovuttaminen tutkimustarkoituksia varten.

Tiedonhallinta on käsitteenä laaja ja sen voidaan katsoa pitävän sisällään asianhallinnan, asiakirjahallinnon ja arkistotoimen. Tietoaaineistot sisältyvät pääasiassa tietojärjestelmiin, joissa niitä myös käsitellään, jonka vuoksi tietojärjestelmien hallinta on osa tiedonhallintaa. Tietojärjestelmien ja niihin sisältyvien tietoaaineistojen tietoturvallisuuden varmistaminen kuuluu olennaisena osana tiedonhallintaan, jonka lisäksi analogisessa muodossa olevien tietoaaineistojen turvallisuudesta on huolehdittava. Tietoaaineistoissa olevat tiedot sisältävät usein henkilötietoja, joten myös henkilötietojen käsittely ja niiden tietosuojan varmistaminen kuuluvat osaksi tiedonhallintaa.

Asianhallinnasta säädetään tiedonhallintalaissa. Asianhallinnalla tarkoitetaan asioiden, asiankäsittelyvaiheiden ja niihin liittyvien asiakirjojen käsittelyn ohjaamista. Tiedonhallintayksikkö rekisteröi sillä käsittelyssä olevat asiat, asiankäsittelyä koskevat tiedot ja niihin liittyvät asiakirjat asiarekisteriin. Asiarekisteri on looginen kokonaisuus, joka muodostuu asianhallintajärjestelmässä, operatiivisissa tietojärjestelmissä sekä osittain manuaalisesti käsittelyssä olevista ja olleista asioista.

Asiakirjahallinnon järjestämisvelvoitteesta kunnissa säädetään kuntalaissa (410/2015). Asiakirjahallinnolla tarkoitetaan organisaation asiakirjojen ja asiakirjallisten tietojen hallintaa koko niiden elinkaaren ajan, jotta organisaatio pystyy toteuttamaan toimintaansa ja palvelemaan asiakkaitaan tehokkaasti sekä huolehtimaan sen oikeudellisista ja taloudellisista eduista, vastuista ja velvollisuuksista. Asiakirjahallinnon piiriin kuuluvat myös muut kuin asianhallinnan yhteydessä muodostuvat asiakirjat, kuten palvelujen tiedonhallinnan yhteydessä muodostuvat asiakirjat ja niitä vastaavat tiedot. Asiakirjahallinnon tärkeimpiin tehtäviin kuuluu asiakirjojen käytettävyyden eli saatavuuden ja käyttökelpoisuuden varmistaminen sekä asiakirjallisten tietojen säilyttäminen.

Arkistotoimesta säädetään arkistolaisissa (831/1994). Arkistotoimella tarkoitetaan asiakirjojen ja asiakirjallisten tietojen hallintaa niiden arkistoinnin jälkeen. Tiedon arkistoinnin tarkoituksena on jättää kattava ja luotettava aineisto tapahtuneesta toiminnasta ja yhteiskunnan ilmiöistä asiakirjallisena kulttuuriperintönä. Arkistoituja tietoja säilytetään ennen kaikkea myöhempiä tutkimustarkoituksia varten. Arkistotoimen tehtäviin kuuluu asiakirjojen käytettävyyden ja säilymisen varmistaminen, huolehtiminen arkistoituihin tietoihin liittyvästä tietopalvelusta, asiakirjojen säilytysarvon määrittely ja tarpeettoman aineiston hävittäminen. Asiakirjahallinnon ja arkistotoimen tehtävät ovat osittain samoja.

Tietojärjestelmien hallinnasta viranomaisissa ja ennen kaikkia niiden tietoturvallisuudesta sekä tietoaineistojen turvallisuudesta säädetään tiedonhallintalaissa. Tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä.

Tietoturva on tietojen suojaamista erilaisilta uhkatekijöiltä. Tietoturvalla tähdätään jatkuvuuden varmistamiseen ja toimintaan tai tietoihin, erityisesti henkilötietoihin, liittyvien riskien minimoimiseen. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Saatavuudella tarkoitetaan, että tieto on käyttökelpoisessa muodossa ja saatavilla silloin, kun sitä tarvitaan. Eheydellä tarkoitetaan tietojen suojausta siten, ettei niitä voida tahallisesti tai tahattomasta muuttaa niin, että niiden luotettavuus vaarantuu tai vähintäänkin sitä, että tallaiset muutokset ovat havaittavissa. Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeus. Tietoturvallisuuteen liittyy myös kiistämättömyys, jolla tarkoitetaan sitä, että tietoihin kohdistettavista toimenpiteistä jää jälki, jota muutoksen tekijä ei voi kiistää, tunnistus, jolla tarkoitetaan tietojärjestelmän käyttäjän liittämistä käyttäjätunnukseen sekä todennus, jolla tarkoitetaan käyttäjän luotettavaa tunnistamista luonnolliseksi henkilöksi tai oikeushenkilöksi.

Henkilötietojen käsittelystä ja tietosuojasta säädetään Euroopan unionin yleisessä tietosuojasetuksessa (2016/679) ja tietosuojalaissa (1050/2018). Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja ja niiden käsittelyllä toimintoa tai toimintoja, joita kohdistetaan niihin tai niitä sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen

tai sosiaalisen tekijän perusteella. Henkilötietojen käsittelyä on muun muassa henkilötietojen kerääminen, tallentaminen, säilyttäminen, hakeminen, poistaminen ja tuhoaminen. Tietosuojan tarkoituksena on määritellä säännöt henkilötietojen käsittelylle, jotta niitä käsiteltäessä luonnollisten henkilöiden perusoikeus yksityisyyden suojasta ei vaarannu. Henkilötietoja on suojattava organisatorisin ja teknisin menetelmin, ja niiden käsittelyn on oltava asian- ja tarkoituksenmukaista. Jokaisella henkilöllä on oikeus tutustua niihin tietoihin, joita hänestä on kaupungin henkilörekistereissä olemassa. Henkilöllä on tietyissä tilanteissa oikeus saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli lainsäädäntö sen mahdollistaa.

Tiedonhallintaan liittyy ja sitä sääntelevät useat erityislait, joissa säädetään muun muassa tietoaineistojen julkisuudesta, saavutettavuudesta ja avoimuudesta.

Viranomaisten toiminnan ja asiakirjojen julkisuudesta säädetään julkisuuslaissa ja erityislainsäädännössä. Julkisuuden tarkoituksena on lisätä avoimuutta viranomaisten toiminnassa, antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä sekä muodostaa vapaasti mielipiteensä, vaikuttaa julkisen vallan käyttöön sekä valvoa oikeuksiaan ja etujaan. Viranomaisten asiakirjat ovat lähtökohtaisesti julkisia ja kaikkien tahojen pyydettävissä, jonka vuoksi tiedonhallinta on suunniteltava siten että asiakirjojen julkisuus voidaan vaivatta toteuttaa. Henkilötietojen suojan lisäksi tiedonhallinnassa on huomioitava, että lailla tai lain nojalla salassa pidettäviksi säädetyt tai määrätyt tiedot on pystyttävä suojaamaan tietojärjestelmissä.

Viranomaisten digitaalisten palvelujen ja niissä olevien tietojen saavutettavuudesta säädetään laissa digitaalisten palvelujen tarjoamisesta (306/2019), jolla täytäntöön pannaan Euroopan unionin saavutettavuusdirektiivi (2016/2101). Saavutettavuudella tarkoitetaan periaatteita ja tekniikoita, joiden ansiosta digitaaliset palvelut ja niissä olevat tietoaineistot olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden saavutettavissa. Saavutettavuus edellyttää palvelujen ja tietoaineistojen hyvää havaittavuutta ja ymmärrettävyyttä. Tietoaineistojen saavutettavuudesta on huolehdittava, kun niitä esitetään tai tarjotaan yleisölle digitaalisissa palveluissa.

Tiedon avoimuus on otettava huomioon erityisesti arvokkaiden tietoaineistojen kohdalla, kun avointa dataa ja julkisen sektorin hallussa olevien tietojen uudelleen käyttöä koskeva Euroopan unionin direktiivi (2019/1024) on kansallisesti täytäntöön pantu.

2 Tiedonhallinnan periaatteet, tavoitteet ja riskienhallinta

2.1 Periaatteet ja tavoitteet

Tiedonhallinnan tarkoituksena on kaupungin toiminnan ja sen järjestämien palvelujen tukeminen. Tiedonhallinnan periaatteena on, että sillä edistetään ja mahdollistetaan tiedon hyödyntämistä päätöksenteossa, julkisuusperiaatteen ja avoimuuden toteutumista viranomaistoiminnassa, toiminnan ja palvelujen laadukkuutta, tehokkuutta ja tuloksellisuutta, tietoaineistojen käsittelyn sekä tieto- ja viestintätekniisten palvelujen turvallisuutta, henkilötietojen suojaa sekä kulttuuriperinnöllisesti ja tutkimusarvoltaan arvokkaiden tietoaineistojen säilymistä.

Tiedonhallintaan liittyvän työn tavoitteena on suunnitella, ylläpitää ja kehittää kaupungin omistaman tiedon käsittelyä mukaan lukien tiedon muodostamista, keräämistä, hyödyntämistä, julkaisemista, suojaamista, turvaamista, säilyttämistä ja arkistointia sekä parantaa toiminnan jatkuvuutta, laatua, luotettavuutta, tieto- ja viestintätekniisten palvelujen riskienhallintaa, tuloksellisuutta ja edistää tiedonhallinnan saattamista kiinteäksi osaksi kaupungin johtamista. Tavoitteina ovat myös kaupungin palvelujen käyttäjien, yhteistyökumppaneiden ja henkilöstön luottamus kaupungin palveluihin ja niiden tietosuojaan ja tietoturvaan sekä yhdenmukaisten ohjeiden ja toimintatapojen luominen.

Tietosuojan toteuttamisessa kaupungin tavoite on varmistaa tietosuojalainsäädännön ja toimialakohtaisen lainsäädännön vaatimusten toteutuminen käsiteltävien henkilötietojen koko elinkaaren ajan. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan.

Tiedonhallinnan kehittämisen painopisteitä ovat kokonaisvaltainen tiedolla johtaminen, tiedon hyödyntäminen toiminnassa ja kuntalaisille tarjottavissa palveluissa, tietoaineistojen säilyttämisen ja arkistoinnin varmistaminen, riskien tunnistaminen ja ennalta ehkäisy sekä tietojen, etenkin henkilötietojen suojaaminen ja turvaaminen.

Alla on taulukko, jossa esitetään yksityiskohtaisemmin tietosuoja- ja tietoturvatyön strategiset painopisteet, niiden tavoitteet sekä arvioinnin mittarit.

Strateginen painopiste	Tavoite	Arviointi ja mittarit
Tietosuojaan ja tietoturvaan kohdistuvien uhkatekijöiden tunnistaminen	<ul style="list-style-type: none"> Tuloksellinen ja kokonaisvaltainen riskienhallinta Tieto- ja viestintätekniisen varautumisen kehittäminen Tietosuojan varmistaminen tarvittaessa vaikutustesarvioinneilla 	<ul style="list-style-type: none"> Vakavien uhkatekijöiden tunnistaminen ja niihin liittyvät toimenpiteet Tehokas tietosuoja- ja tietoturvatyö ja raportointi Tietotilinpäätös

Strateginen painopiste	Tavoite	Arviointi ja mittarit
Palvelujen jatkuvuuden ja tietojen turvaaminen	<ul style="list-style-type: none"> • Luotettava tieto- ja viestintätekninen infrastruktuuri • Lakisääteisten velvoitteiden täyttäminen • Häiriötilanteiden hallinta ja tekniset ratkaisut • Häiriötilanteiden varautumis-, toipumis- ja viestintäsuunnitelmat 	<ul style="list-style-type: none"> • Tarpeiden mukaisesti mitoitettut palvelutasot ja tietoturvaratkaisut ovat käytössä • Palvelutasojen toteutuminen • Toimintamallien arviointi • Häiriötilanteiden määrä
Henkilöstön tietosuoja- ja tietoturvaosaamisen kehittäminen	<ul style="list-style-type: none"> • Positiivisen kulttuurin ja asenteiden kehittäminen • Selkeät vastuut, toimintamallit ja ohjeistukset • Yhtenäisten, tietoturvallisten toimintatapojen noudattaminen • Koulutus ja ohjeistus on ehdoton koskien työtehtäviä, joissa käsitellään salassa pidettäviä tietoja, henkilötietoja tai erityisiä henkilötietoja 	<ul style="list-style-type: none"> • Tiedonhallintapolitiikan ja tietosuoja- ja tietoturvaohjeiden noudattaminen • Tietosuoja- ja tietoturvakoulutusten kattavuus • Henkilöstön osaamismittarit
Tietosuoja ja tietoturva toiminnan kehittämisen mahdollistajana	<ul style="list-style-type: none"> • Ratkaisut mahdollistavat toiminnan turvallisen kehittämisen • Käyttötarkoituksenmukaisuus (paras mahdollinen tekninen ja organisatorinen riskiarvioon perustuva ratkaisu) ja kustannustehokkuus ohjaavat valintoja • Toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta • Ongelmanratkaisukyky 	<ul style="list-style-type: none"> • Tietosuojan ja tietoturvan kypsyys ja toteutuminen osana kokonaisarkkitehtuuria
Säädösten, määräysten ja suositusten mukainen toiminta	<ul style="list-style-type: none"> • Kaupungin tietosuoja ja tietoturva on kansallisesti hyvällä tasolla • Toiminnan dokumentointi on ajan tasalla 	<ul style="list-style-type: none"> • Toiminnan arviointi vasten kansallisia ja kansainvälisiä ohjeistuksia • Sopimusseuranta

Strateginen painopiste	Tavoite	Arviointi ja mittarit
	<ul style="list-style-type: none"> Sopimuksissa on ajan mukaiset tietosuoja- ja tietoturvasisällöt Kansallisten strategioiden, ohjeistusten ja hyvien käytäntöjen tehokas hyödyntäminen Kansainvälisten strategioiden, ohjeistusten ja hyvien käytäntöjen hyödyntäminen 	

2.2 Riskienhallinnan kehittäminen

Tiedon turvaaminen on merkittävä osa kaupungin toiminnan ja sen järjestämien palvelujen laatua, tieto- ja viestintäteknisten palvelujen riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa toimintaan kohdistuvat riskit, arvioida ne ja päättää tarvittavista toimenpiteistä. Tiedonhallintaan kohdistuvan riskienhallinnan toteuttaminen ja kehittäminen vaatii muun muassa seuraavien näkökulmien huomioon ottamista:

1. Tietoteknisestä näkökulmasta riskienhallinnan onnistuminen edellyttää tietojärjestelmäkokonaisuuden ja sen hallinnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä ja seuranta.
2. Organisatorisesta näkökulmasta riskienhallinnan onnistuminen edellyttää koko henkilöstön tiedonhallintaa, erityisesti tiedon elinkaarta, tietosuoja ja tietoturva koskevan osaamisen ja tietoisuuden lisäämistä kouluttamalla, ohjeistamalla ja viestimällä sekä yhteisesti sovittujen käytäntöjen ja ohjeiden noudattamisen valvontaa.
3. Asiakirjahallinnon, arkistotoimen ja tietosuojan näkökulmasta riskienhallinnan onnistuminen edellyttää, että asiakirjojen ja niitä vastaavien tietojen sekä henkilötietojen käsittely arvioidaan ja suunnitellaan palvelukehityksessä alusta alkaen.

Hyvä tietosuojan ja tietoturvan taso saavutetaan noudattamalla tiedonhallintapolitiikkaa ja sen pohjalta laadittuja ohjeita sekä ottamalla käyttöön erilaisia turvamekanismeja, joita hallitaan jatkuvan kehittämisen periaatteita noudattaen. Tietosuojariskien hallinta on osa kaupungin riskienhallintaprosessia. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on osa rekisterinpitäjien osoitusvelvollisuuden toteuttamista.

Tietosuojaan, tietoturvaan sekä tieto- ja viestintäteknisiin palveluihin liittyvästä riskienhallinnasta on ohjeistettu myös kaupungin sisäisen valvonnan ja riskienhallinnan ohjeessa.

3 Tiedonhallinnan vastuut

3.1 Kaupunginhallituksen ja kaupunginjohtoon vastuut

Mikkelin kaupunki on julkisen hallinnon tiedonhallinnasta annetussa laissa tarkoitettu tiedonhallintayksikkö. Mikkelin kaupunginhallitus toimii kaupungin hallintosäännön 69 §:n mukaisesti tiedonhallintayksikön johtona. Kaupunginhallituksen vastuulla on hallintosäännön mukaisesti huolehtia hyvän tiedonhallintatavan ja hyvän henkilötietojen käsittelyn toteuttamisesta sekä tiedonhallintapolitiikasta. Kaupunginhallitus vastaa yleisellä tasolla tiedonhallinnan järjestämisestä sekä määrittelee tiedonhallintaan liittyvät vastuut ja huolehtii siitä, että tiedonhallintalain mukaiset vaatimukset täyttyvät tiedonhallinnassa.

Kaupunginhallitus määrää hallintosäännön 69 §:n perusteella asiakirjahallintoa ja arkistotointa johtavan viranhaltijan ja valitsee hallintosäännön 56 §:n perusteella tietosuojavastaavan.

Kaupunginhallitus vastaa hallintosäännön 2 §:n ja 90 §:n mukaisesti sisäisen valvonnan ja riskienhallinnan järjestämisestä. Kaupunginhallitus vastaa edellä mainitun nojalla tiedonhallintaan liittyvän riskienhallinnan, erityisesti tietosuoja- ja tietoturvariskienhallinnan yleisestä järjestämisestä.

Hallintosäännön 2 §:n mukaisesti kaupunginhallituksen alaisena kaupungin hallintoa, taloutta ja toimintaa johtaa kaupunginjohtaja, joka omalta osaltaan vastaa kaupunginhallituksen tiedonhallintaa koskevien päätösten ja linjausten toimeenpanosta kaupungissa.

Kaupunginhallitus ja kaupunginjohtaja, kaupunginjohto sitoutuu tiedonhallinnan jatkuvaan suunnitteluun, ylläpitoon ja kehittämiseen sekä huolehtii viimekädessä resurssoinnin riittävydestä ja jatkuvuudesta.

3.2 Toimielinten vastuut

Kaupungin toimielimet vastaavat omalta osaltaan tiedonhallintaan liittyvien tehtävien hoitamisesta, jotka on säädetty kunnallisten viranomaisten vastuulle tiedonhallintalaissa tai muissa tiedonhallintaa koskevissa laeissa. Toimielimet ovat viranomaisen ominaisuudessaan arkistolaisissa tarkoitettuja arkistonmuodostajia ja Euroopan unionin yleisessä tietosuoja-asetuksessa tarkoitettuja rekisterinpitäjiä. Toimielimet vastaavat omassa ja niiden alaisten organisaatioyksiköiden toiminnassa muodostuvien asiakirjojen ja niitä vastaavien tietojen osalta arkistonmuodostajille kuuluvien tehtävien hoitamisesta. Toimielimet vastaavat myös omassa ja niiden alaisten organisaatioyksiköiden toiminnassa käsiteltävien henkilötietojen osalta rekisterinpitäjille kuuluvien tehtävien hoitamisesta.

Erityisesti lautakuntien ja liikelaitosten johtokuntien tulee kaupungin hallintosäännön 71 §:n mukaisesti vastata alaistensa organisaatioyksiköiden tiedonhallinnan sekä asiakirjojen ja niitä vastaavien tietojen hoitamisesta annettujen määräysten ja ohjeiden mukaisesti. Lautakuntien ja liikelaitosten johtokuntien tulee myös nimetä alaistensa organisaatioyksiköiden tiedonhallinnasta ja asiakirjahallinnasta vastaavat henkilöt. Lautakuntien ja liikelaitosten johtokuntien alaisten

organisaatioyksiköiden tiedonhallinnan ja asiakirjahallinnon vastuuhenkilöt määräytyvät tämän tiedonhallintapolitiikan mukaisesti, mikäli lautakunnat ja liikelaitosten johtokunnat eivät hallintosäännön perusteella muuta päätä.

Lautakuntien ja johtokuntien tulee hallintosäännön 91 §:n mukaisesti vastata omalla toimialallaan sisäisen valvonnan ja riskienhallinnan järjestämisestä, toimeenpanon valvonnasta ja tuloksellisuudesta. Lautakunnat vastaavat tämän nojalla myös tietosuojaan ja tietoturvaan liittyvästä riskienhallinnasta omalla toimialallaan.

Osallisuus- ja vaikuttamistoimielinten toiminnassa tapahtuvan tiedonhallinnan osalta tiedonhallintaan liittyvät viranomaisvastuut kuuluvat sille toimielimelle, jonka alaisuuteen osallisuus- ja vaikuttamistoimielimet organisatorisesti kuuluvat, silloin kun osallisuus- ja vaikuttamistoimielimet eivät toimi viranomaisina. Osallisuus- ja vaikuttamistoimielinten on noudatettava toiminnassaan kaupungin tiedonhallintapolitiikkaa.

3.3 Tiedonhallinnan asiantuntija- ja järjestämisvastuut

Asiakirjahallintoa ja arkistotointa johtavan viranhaltijan vastuulle kuuluu hallintosäännön 70 §:n mukaisesti asiakirjahallinnon ja arkistotoimen ohjaaminen ja kehittäminen osana tiedonhallintaa, arkistonmuodostussuunnitelmien ja tiedonohjaussuunnitelmien hyväksyminen sekä asiakirjahallinnon ja arkistotoimen koulutuksesta, ohjeistuksesta ja valvonnasta huolehtiminen. Näiden lisäksi tämä vastaa asiakirjoista, jotka tulee arkistolain nojalla säilyttää pysyvästi eli arkistoida sekä kaupungin keskusarkistosta.

Asiakirjahallintoa ja arkistotointa johtavan viranhaltijan tehtäviin kuuluu tämän lisäksi asianhallinnan, tietoaineistojen sähköiseen muotoon muuttamisen ja saatavuuden sekä tietoaineistojen säilyttämisen ohjeistaminen. Asianhallinnan ohjeistamisessa asiakirjahallintoa ja arkistotointa johtavaa viranhaltijaa avustaa ja tukee asianhallintatiimi silloin, kun asianhallinta tapahtuu kaupungin asianhallintajärjestelmässä. Silloin, kun asianhallinta tapahtuu muussa kuin asianhallintajärjestelmässä, ohjeistaa asianhallinnasta kyseisen tietojärjestelmän pääkäyttäjät asiakirjahallintoa ja arkistotointa johtavan viranhaltijan tukemana.

Kaupungin tietohallinnon ja erityisesti tietohallintopäällikön vastuulle kuuluu strategisten tieto- ja viestintäteknisten linjausten muodostaminen ja toteuttaminen, tieto- ja viestintäteknisten palvelujen järjestämisen ohjaaminen ja niihin liittyvä yleinen riskienhallinta sekä tietoturvan ja tietosuojaan kehittäminen ja hallinta. Tietohallinnon tehtävänä on ylläpitää tietoturvaan liittyviä ohjeistuksia, suorittaa tietoturvan valvontaa, seuranta ja arviointeja, välittää tietoa toimielimille, esimiehille ja muulle henkilöstölle tieto- ja viestintäteknisistä palveluista ja tietoturvallisuudesta sekä tarvittaessa järjestää koulutuksia ja jalkauttaa yhteisiä toimintatapoja. Tietohallinnon tietosuojaan ja tietoturvaan liittyvistä vastuista on ohjeistettu myös kaupungin sisäisen valvonnan ja riskienhallinnan ohjeissa.

Toimielimet ja esimiesviranhaltijat vastaavat näille määritellyn henkilöstöön ja talouteen liittyvän toimivallan puitteissa siitä, että niiden alaisilla organisaatioyksiköillä asianhallinta, palvelujen

tiedonhallinta sekä tietoaaineistojen sähköiseen muotoon muuttaminen, saatavuus, säilyttäminen ja arkistointi on järjestetty, ja että niiden toteuttamiseen on varattu riittävät henkilöstöresurssit. Toimielimiä ja esimiehiä ohjeistavat ja tukevat näissä tehtävissä asiakirjahallintoa ja arkistointia johtava viranhaltija, tietojärjestelmien pääkäyttäjät, tiedonhallintayhteyshenkilöt ja arkistovastaavat.

Toimielimet ja esimiesviranhaltijat vastaavat näille määritellyn henkilöstöön ja talouteen liittyvän toimivallan puitteissa siitä, että niiden alaisilla organisaatioyksiköillä on käytössä tarpeelliset tietoturvajärjestelyt, ja että tietojärjestelmien tietoturvallisuuteen mukaan lukien henkilötietojen suojaan, tietojärjestelmien toimintaan ja yhteentoimivuuteen sekä tietovarantojen yhteentoimivuuteen liittyvät seikat on otettu huomioon tietojärjestelmähankinnoissa ja tietojärjestelmiä koskevissa sopimuksissa. Toimielimiä ja esimiehiä ohjeistaa ja tukee näissä tehtävissä tietohallinto ja erityisesti tietohallintopäällikkö, tietojärjestelmien pääkäyttäjät ja tiedonhallintayhteyshenkilöt. Tietosuojaan liittyvissä asioissa toimielimiä ja esimiehiä ohjeistaa tietosuojavastaava.

Toimielimet ja esimiesviranhaltijat vastaavat näille määritellyn talouteen liittyvän toimivallan puitteissa siitä, että niiden alaisilla organisaatioyksiköillä on käytössään asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi.

3.4 Tietosuojavastaavan vastuut ja kaupunkikonsernin tietoturva- ja tietosuojatyöryhmä

Tietosuojavastaavan tehtävistä säädetään Euroopan unionin yleinen tietosuoja-asetuksen 39 artiklassa. Tietosuojavastaavan päätehtäviin kuuluu organisaation tietosuojan kehittäminen riskienhallinnan näkökulmasta ja organisaation tietosuojaosaamisen lisääminen muun muassa koulutuksia järjestämällä. Tietosuojavastaava toimii henkilökunnan ja tietosuojavaltuutetun yhteyshenkilönä. Tietosuojavastaava valvoo kaupunkikonsernissa tapahtuvaa henkilötietojen käsittelyä ja henkilötietojen suojan toteutumista sekä henkilötietojen tarkastuspyyntöihin vastaamista. Tietosuojavastaavan tehtävänä on ylläpitää tietosuoja koskevia ohjeistuksia. Asiakirjahallintoa ja arkistointia johtavan viranhaltijan ja tietohallintopäällikön ollessa esteellisiä, valvoo tietosuojavastaava myös muita tiedonhallinnan osa-alueita.

Kaupunkikonsernin tietosuoja- ja tietoturvatyötä ohjaa ja kehittää tietoturva- ja tietosuojatyöryhmä. Tietosuojavastaava toimii kaupunkikonsernin tietoturva- ja tietosuojatyöryhmän puheenjohtajana. Tietoturva- ja tietosuojatyöryhmässä on kaupungin tietosuojavastaavan lisäksi edustajat kaupunginhallituksen määrittämistä organisaatioyksiköistä sekä konserniyhteisöistä.

Organisaatioyksiköiden ja konserniyhteisöjen tietoturva- ja tietosuojayhteyshenkilöiden vastuulla on tuntee toimialansa erityispiirteet ja lainsäädäntö, seurata niiden kehittymistä ja kommunikoida niistä kaupungin tietohallinnolle sekä erityisesti tietohallintopäällikölle ja tietosuojavastaavalle. Yhteyshenkilöiden tehtävänä on valvoa tietosuojan ja tietoturvan toteutumista ja ohjeistuksen noudattamista sekä raportoida mahdollisista poikkeamista ja kehittämistarpeista.

3.5 Palvelualueiden vastuut ja tiedonhallintatyöryhmä

Palvelualueiden johtavat viranhaltijat vastaavat tiedonhallintapolitiikan ja erityisesti tietosuojaa ja tietoturva koskevien ohjeiden noudattamisesta omassa sekä alaisensa organisaatioyksiköiden toiminnassa.

Palvelualueiden johtavat viranhaltijat vastaavat hallintosäännön 92 §:n perusteella sisäisen valvonnan ja riskienhallinnan toimeenpanosta ja tuloksellisuudesta palvelualueillaan, ohjeistavat alaisiaan toimintayksiköitä ja raportoivat kaupunginhallituksen antamien ohjeiden mukaisesti. Tämän nojalla palvelualueiden johtajat vastaavat myös edellä mainituista asioista tiedonhallintaan liittyvän riskienhallinnan, erityisesti tietosuoja- ja tietoturvariskienhallinnan osalta. Edellä mainittu vastuu koskee hallintosäännön perusteella myös liikelaitosten johtajia ja tulosalueiden johtavia viranhaltijoita.

Tulosalueiden johtavat viranhaltijat ja tulosyksiköiden esimiehet vastaavat omien organisaatioyksiköidensä hallussa olevista asiakirjoista riippumatta niiden säilytysajoista ja -tavoista.

Tulosalueilla tulee olla tarpeellinen määrä tiedonhallintayhteyshenkilöitä. Tulosalueen johtavat viranhaltijat nimeävät tiedonhallintayhteyshenkilöt omilta tulosalueiltaan. Niillä palvelualueilla, joiden alaisilla organisaatioyksiköillä on analogisessa muodossa olevien asiakirjojen säilyttämistä varten lähiarkistoja, tulee olla tarpeellinen määrä arkistovastaavia. Tulosalueen johtavat viranhaltijat nimeävät arkistovastaavat omilta tulosalueiltaan. Tulosalueiden johtavien viranhaltijoiden on huolehdittava siitä, että näiden nimeämällä tiedonhallintayhteyshenkilöllä ja arkistovastaavilla on käytettävissään tarpeelliset aineelliset ja ajalliset resurssit tiedonhallinnan tehtävien hoitamiseen.

Kaupungin tiedonhallintaa ohjaa ja kehittää tiedonhallintatyöryhmä. Tiedonhallintatyöryhmään kuuluu asiakirjahallintoa ja arkistotointoa johtava viranhaltija, tietohallintopäällikkö, it-arkkitehdit ja tietosuojavastaava. Tiedonhallintatyöryhmä kokoontuu tarvittaessa sekä kiinnittää huomiota tapauskohtaisesti uusien tietojärjestelmien ja sovellusten suunnitteluun ja käyttöönottoon. Tiedonhallintatyöryhmä voi kutsua työryhmän kokouksiin tarpeellisen määrän tiedonhallintayhteyshenkilöitä sekä muita tarpeelliseksi katsomiaan henkilöitä. Tiedonhallintatyöryhmä raportoi toiminnastaan kaupunginjohtajalle tai tämän niin määrätessä kaupungin johtoryhmälle.

Tiedonhallintayhteyshenkilöiden ja arkistovastaavien vastuulla on tuntea toimialansa erityispiirteet ja lainsäädäntö, seurata niiden kehittymistä ja kommunikoida niistä tiedonhallintatyöryhmälle. Yhteyshenkilöiden ja arkistovastaavien tehtävänä on valvoa omalta osaltaan tiedonhallinnan toimintatapojen ja ohjeiden noudattamista sekä raportoida mahdollisista kehittämistarpeista. Arkistovastaavien tehtäviin kuuluu lisäksi omien organisaatioyksiköiden lähiarkistoista huolehtiminen. Tiedonhallintayhteyshenkilönä ja arkistovastaavana voi toimia sama henkilö, joka toimii tietoturva- ja tietosuojatyöryhmän edustajana.

3.6 Tietojärjestelmän omistajan ja pääkäyttäjän vastuut

Tietojärjestelmillä tulee olla yksilöidyt omistajat, jotka vastaavat tietojärjestelmien elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Tulosaluejohtajat toimivat lähtökohtaisesti tietojärjestelmien omistajina paitsi niissä tilanteissa, joissa tulosalueilla on tulosityksiköitä ja on tarkoituksenmukaista, että tietojärjestelmän omistajana toimii tulosityksikön esimies. Erityisestä syystä tietojärjestelmän omistajana voi toimia myös tulosityksikön muu viranhaltija kuin sen esimies, mikäli tällä on tarvittavat toimivaltuudet tehdä ratkaisuja tietojärjestelmän elinkaarta, tietosuoja- tai tietoturvaa koskevissa asioissa.

Tietojärjestelmän omistajan on huolehdittava tietojärjestelmässä tapahtuvan tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuotettava lakisääteiset seurantaraportit, mikäli tällaisia vaaditaan. Omistajan tulee kartoittaa yhteistyössä tietohallinnon, tietosuojavastaavan sekä palvelun- ja järjestelmätoimittajan kanssa tietojärjestelmään kohdentuvat riskitekijät, häiriötilanteiden toimintamallit ja varmistettava toiminnan jatkuvuus. Omistajan on huolehdittava, että tietojärjestelmästä on laadittu tietosuoja- ja tietoturvaohjeet tietojärjestelmän käyttäjille sekä siitä, että käyttäjät saavat niihin ja tietojärjestelmän käyttöön riittävän koulutuksen. Tietojärjestelmän omistajan tietosuojaan ja tietoturvaan liittyvistä vastuista on ohjeistettu myös kaupungin sisäisen valvonnan ja riskienhallinnan ohjeessa.

Tietojärjestelmillä tulee olla yksilöidyt pääkäyttäjät, joiden vastuulla on huolehtia tietojärjestelmän käyttöoikeuksista, ellei tietojärjestelmää koskevasta sopimuksesta muuta johdu. Pääkäyttäjältä edellytetään hyvää tietosuoja- ja tietoturvaosaamista. Tietojärjestelmän omistaja voi valtuuttaa tietojärjestelmän pääkäyttäjän huolehtimaan siitä, että tietojärjestelmälle laaditaan käyttöohjeita, tietosuoja- ja tietoturvaohjeet ja että tietojärjestelmän käytöstä pidetään tarvittaessa koulutuksia. Tietojärjestelmän omistajan on varattava pääkäyttäjälle tarvittavat ajalliset resurssit edellä mainittujen tehtävien hoitamiseen. Tietosuoja- ja tietoturvaohjeiden laatimisessa pääkäyttäjää avustaa ja tukee tietohallinto ja tietosuojavastaava.

3.7 Esimiehen yleiset vastuut

Tulosityksiköiden esimiehet vastaavat hallintosäännön 92 §:n perusteella yksiköidensä riskien tunnistamisesta, arvioinnista, riskienhallinnan toimenpiteiden toteutuksesta ja toimivuudesta sekä raportoivat kaupunginhallituksen antamien ohjeiden mukaisesti. Tämän nojalla tulosityksiköiden esimiehet vastaavat myös edellä mainituista asioista tiedonhallintaan liittyvän riskienhallinnan, erityisesti tietosuoja- ja tietoturvariskienhallinnan osalta.

Esimiesten vastuulla on omalta osaltaan huolehtia työnantajaa koskevien lakisääteisten tiedonhallintaa, erityisesti tietosuoja- ja tietoturvaa koskevien velvoitteiden toteuttamisesta ja noudattamisesta. Esimies, ja tietojärjestelmien käytön osalta pääkäyttäjät näin erikseen sovittaessa, huolehtivat palvelussuhteessa olevien henkilöiden riittävästä perehdytyksestä kaupungin tiedonhallintakäytänteisiin, erityisesti tietosuoja- ja tietoturvakäytänteisiin varmistaen, että jokainen ymmärtää niiden merkityksen työ- ja virkatehtävissään. Esimiesten tietosuojaan ja tietoturvaan liittyvistä vastuista on ohjeistettu myös kaupungin sisäisen valvonnan ja riskienhallinnan ohjeessa.

Henkilöstölle ja kaupungin lukuun toimiville on järjestettävä mahdollisuus saada riittävää koulutusta tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikössä laadituista ohjeista. Esimiehet kartoittavat yksikkönsä koulutustarpeet koulutus- ja henkilöstösuunnitelmaan. Koulutustarpeet tulee esittää joko henkilöstöpalveluille tai sille yksikölle, jolta koulutusta tarvitaan, koulutusten järjestämiseksi.

Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat palvelussuhteessa olevien henkilöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työ- ja virkatehtävien edellyttämässä laajuudessa. Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työ- ja virkatehtävien muutokset huomioidaan tietojärjestelmien käyttöoikeuksissa. Palvelussuhteen päättyessä esimiehen on huolehdittava, että palvelussuhteessa olevat henkilöt palauttavat kaiken työnantajalle kuuluvan omaisuuden. Esimiehen on myös ilmoitettava palvelussuhteen päättymisestä viivytyksettä tietohallinnolle ja tietojärjestelmien pääkäyttäjille käyttöoikeuksien poistamiseksi tai inaktivoimiseksi.

Esimiehiltä odotetaan esimerkillistä ja vastuullista tiedonhallintaan, erityisesti tietosuojaan ja tietoturvaan liittyvää käyttäytymistä. Esimiehillä on raportointivelvollisuus tietoturvapoikkeamista ja kehittämistarpeista tietohallintopäällikölle ja tietosuojavastaavalle. Esimiehillä on raportointivelvollisuus asiakirjahallintoon ja arkistotoimeen liittyvistä epäkohdista ja kehittämistarpeista asiakirjahallintoa ja arkistointia johtavalle viranhaltijalle.

3.8 Viranhaltijan ja työntekijän yleiset vastuut

Kaupungin viranhaltijoilla ja työntekijöillä on vastuu noudattaa hyväksytyjä tiedonhallintaohjeita mukaan lukien tietosuoja- ja tietoturvaohjeita sekä huolehtia päivittäisissä tehtävissään hyvän tiedonhallintatavan ja hyvän henkilötietojen käsittelyn käytänteistä. Viranhaltijoiden ja työntekijöiden velvollisuus on suorittaa hyväksytysti kulloinkin voimassa oleva tietosuoja- tai tietoturvakoulutus säännöllisin väliajoin. Viranhaltijoiden ja työntekijöiden tietoturvaan ja tietosuojaan liittyvistä vastuista on ohjeistettu myös kaupungin sisäisen valvonnan ja riskienhallinnan ohjeessa.

Viranhaltijat ja työntekijät ovat vastuussa näillä käsittelyssä ja hallussa olevista asiakirjoista ja asiakirjallisista tiedoista sekä niiden käytettävyyden ja säilymisen varmistamisesta. Jokaisella viranhaltijalla ja työntekijällä on vastuu asiakirjojen ja niitä vastaavien tietojen ohjeiden mukaisesta käsittelystä ja säilyttämisestä sekä talteenotosta tietojärjestelmiin tai sijoittamisesta arkistotiloihin. Viranhaltijan ja työntekijän vastuulla on huolehtia käsittelemänsä tiedon oikeellisuudesta, käytettävyydestä ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä ja tarpeen mukaan suojattuina, mikäli tietojen suojaaminen vaatii toimenpiteitä viranhaltijalta tai työntekijältä.

Viranhaltijoilla ja työntekijöillä on velvollisuus raportoida havaitsemistaan tietoturvapoikkeamista ja kehittämistarpeista esimiehilleen ja tietohallintoon. Viranhaltijoilla ja työntekijöillä on velvollisuus raportoida asiakirjahallintoon ja arkistotoimeen liittyvistä epäkohdista ja kehittämistarpeista esimiehilleen.

3.9 Tieto- ja viestintäteknisten palvelujen hankintoihin liittyvät vastuut

Mikkelin kaupunki voi ulkoistaa valitsemansa osan tieto- ja viestintäteknisestä palvelutuotannosta tai henkilötietojen käsittelystä sopimusperusteisesti lainsäädännön sallimissa rajoissa. Kaupungin tulee valita sopimuskumppaneikseen vain sellaisia tiedon ja henkilötietojen käsittelijöitä, jotka noudattavat hyvää tiedonhallintatapaa ja hyvää henkilötietojen käsittelytapaa.

Kaupungissa tulee huolehtia sopimuksin siitä, että palveluntuottajat järjestävät palvelut asianmukaisin sekä turvallisin teknisin ja organisatorisin toimenpitein sekä täyttävät tietosuojasetuksen vaatimukset henkilötietojen käsittelyssä ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta silloin kun palveluun sisältyy henkilötietojen käsittelyä. Silloin, kun hankittavaan palveluun sovelletaan tiedonhallintalakia, tulee kaupungin huolehtia sopimuksin siitä, että palveluntuottajat järjestävät palvelun tietoturvallisuuden ja tietoaineistojen turvallisuuden tiedonhallintalain edellyttämällä tavalla. Sopimuksin on lisäksi huolehdittava siitä, että palvelut täyttävät muut tiedonhallintalain ja muiden viranomaisten tiedonhallintaa koskevien säädösten edellyttämät vaatimukset, silloin kun hankittavaan palveluun näitä sovelletaan.

Tieto- ja viestintäteknisten palvelujen tietoturva, muusta turvallisuudesta, mukaan lukien henkilötietojen teknisestä suojaamisesta ja niihin liittyvästä ohjeistuksesta vastaavat palveluntuottajat. Palveluntuottajien tehtävänä on avustaa tietosuojaja- ja tietoturvaohjeiden laatimisessa ja ylläpidossa. Samoin heidän kuuluu raportoida ja tiedottaa merkittävistä tietoturvaan liittyvistä poikkeustilanteista ja riskeistä palvelun tilaajalle.

Palvelun tilaajan vastuulla on huolehtia, että tarjouspyyntöihin ja sopimukseen sisällytetään Mikkelin kaupungin tietohallinnon ylläpitämät tietosuojaja- ja tietoturva vaatimukset täydennettynä palvelua käyttävän organisaatioyksikön sekä palveluun itseensä mahdollisesti liittyvillä erityisvaatimuksilla. Lisäksi tarjouspyyntöihin ja sopimukseen on sisällytettävä palvelutaso, toiminta häiriötilanteissa ja vastuunjako koko arvoketjun läpi.

Rekisterinpitäjän vastuulla on huolehtia siitä, että henkilötietojen käsittely ja käsittelytoimet on kuvattu sopimuksessa. Tietosuojaja tulee huomioida hankintojen suunnitteluvaiheessa silloin, kun hankinnan kohde sisältää henkilötietojen käsittelyä. Vaatimukset lisätään osaksi tarjouspyyntöä. Rekisterinpitäjä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee teknisen ympäristön ja toimenpiteet halutun tason mukaan.

Asiakirjahallintoon ja arkistotoimeen liittyvät vaatimukset on huomioitava hankinnoissa ja sopimuksissa silloin, kun palvelussa muodostuu tai siinä käsitellään viranomaisten asiakirjoja tai niitä vastaavia tietoja. Tietojärjestelmissä tulee olla mahdollisuus arkistoitavien tietoaineistojen arkistointiin tai siirtämiseen arkistointivaatimukset täyttäviin tietojärjestelmiin ja määräajan säilytettävien asiakirjojen dokumentoituun tuhoamiseen. Asiakirjojen suojaamiseen ja salassapitoon liittyvät seikat on otettava huomioon tietojärjestelmiä ja muita palveluja koskevissa sopimuksissa.

Lokitietojen kerääminen, käsittely ja poistaminen on suunniteltava tieto- ja viestintäteknisten palvelujen hankinnoissa ja huomioitava niitä koskevissa sopimuksissa.

4 Tiedonhallinnan kuvaukset, tiedottaminen ja toiminta häiriötilanteissa

4.1 Tiedonhallintamalli

Tiedonhallintalain mukaisesti Mikkelin kaupungin tulee tiedonhallintayksikkönä ylläpitää sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia.

Tiedonhallintamallin on tiedonhallintalain mukaisesti sisällettävä vähintään tiedot toimintaprosessien nimikkeistä, prosesseista vastaavista viranomaisista sekä prosessien sidoksista muihin prosesseihin, tietovarantojen nimikkeistä, tietovarantojen sidoksista toimintaprosesseihin ja tietojärjestelmiin sekä yleisen tietosuojaa-asetuksen 30 artiklan 1 kohdan mukaisesta selosteen sisällöstä tai, jos selostetta ei tarvitse tietosuojalainsäädännön mukaan laatia, tietovarannosta vastaavasta viranomaisesta, tietovarannon käyttötarkoituksesta, keskeisistä tietoryhmistä tietoaaineistoissa, tietojen luovutuskohteista ja tietojen säilytysajoista, tietoaaineiston arkistoon siirtämisestä, arkistointitavasta ja arkistopaikasta tai tuhoamisesta, tietojärjestelmien nimikkeistä, tietojärjestelmästä vastaavasta viranomaisesta, tietojärjestelmän käyttötarkoituksesta, tietojärjestelmän liittymistä muihin tietojärjestelmiin ja liittymissä käytettävistä tiedonsiirtotavoista sekä tietoturvaluuostoimenpiteistä.

Tietoaaineistojen arkistoon siirtäminen, arkistointitapa ja arkistopaikka sekä tuhoaminen voidaan esittää arkistolain mukaisina arkistonmuodostussuunnitelmina tai tiedonohjaussuunnitelmina, jotka voidaan koota osaksi tiedonhallintamallia sen arkistonmuodostussuunnitelmaosaksi. Arkistonmuodostussuunnitelmissa on esitettävä arkistolain mukaisesti vähintään tiedot asiakirjojen säilytysajoista ja tavoista.

Toimintaprosessien kuvaamiseen voidaan käyttää kaupungilla käytössä olevia tehtäväluokituksia tai muita tarkoituksenmukaisia prosessikuvauksia. Tiedonhallintamallin arkistonmuodostussuunnitelmaosaa voidaan käyttää tietojärjestelmien, toimintaprosessien ja tietovarantojen välisten sidosten kuvaamiseen.

Tietojärjestelmien omistajuuteen ja pääkäyttäjäyteen liittyvät tiedot dokumentoidaan tiedonhallintamallin tietojärjestelmärekisteriosaan.

Tiedonhallintamalliin voidaan lisätä myös muita, kuin lain vaatimia tietoja, joista on hyötyä tiedonhallinnassa.

Tiedonhallintamallin laatii ja sitä ylläpitää tiedonhallintatyöryhmä. Kaupungin esimiehet ja henkilöstö ovat velvollisia antamaan työryhmälle sen tarvitsemat välttämättömät tiedot tiedonhallintamallin ylläpitämiseksi ja omalta osaltaan osallistumaan sen laadintaan. Tiedonhallintatyöryhmä voi käyttää tiedonhallintamallin laatimiseen ja ylläpitoon näkemyksensä mukaan tarkoituksenmukaisinta menetelmää tai välinettä.

Tiedonhallintamallin hyväksyy kaupunginjohtaja. Tiedonhallintamalli on tuotava kaupunginjohtajan hyväksyttäväksi vähintään kerran vuodessa ennen kalenterivuoden päättymistä. Mikäli

tiedonhallintamallin sisältöön tulee olennaisia muutoksia ennen tätä ajankohtaa, tulee tiedonhallintamalli tuoda kaupunginjohtajan hyväksyttäväksi tehtyjen muutosten jälkeen. Kaupunginjohtaja voi ennen tiedonhallintamallin hyväksymistä pyytää tekemään siihen tarpeelliseksi katsomiaan muutoksia.

Tiedonhallintamallin arkistonmuodostussuunnitelmaosan hyväksyy ja vahvistaa käyttöön asiakirjahallintoa ja arkistointia johtava viranhaltija.

Tiedonhallintatyöryhmä voi tehdä tiedonhallintamalliin muutoksia ilman kaupunginjohtajan hyväksyntää kesken kalenterivuoden, kunhan tiedonhallintamalliin ei lisätä tai siitä ei poisteta olennaista sisältöä.

4.2 Tiedonhallinnan muutosvaikutusten arviointi ja tietosuojaan vaikutustenarviointi

Tilanteissa, joissa kaupungin toimintaan on tulossa sellaisia hallinnollisia muutoksia tai keskeisten tietojärjestelmien hankintoja, vaihdoksia taikka käytöstä poistamisia, joilla on olennaista vaikutusta tiedonhallintaan, tulee tehdä tiedonhallinnan muutosvaikutusten arviointi.

Tiedonhallintalain mukaisesti arvioinnissa on tarkasteltava millä tavalla muutokset tulevat vaikuttamaan tiedonhallinnan vastuisiin, tietoturvallisuusvaatimuksiin ja -toimenpiteisiin, tietoaineistojen muodostamiseen ja luovutustapoihin, asianhallintaan ja palvelujen tiedonhallintaan sekä asiakirjojen säilyttämiseen, arkistointiin, tuhoamiseen, julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin. Arvioinnissa on otettava huomioon myös tietovarantojen yhteentoimivuus ja hyödynnettävyyys tietoaineistoja muodostettaessa ja käytettäessä.

Muutosvaikutusten arvioinnin tekemisestä vastaa hallinnollisesta muutoksesta tai tietojärjestelmämuutoksesta vastuussa olevan organisaatioyksikön esimies. Arvioinnissa apuna toimii pyydettyä tiedonhallintatyöryhmä. Arvioinnin tekijän on toimitettava arvioinnin tulos tiedonhallintatyöryhmälle tiedonhallintamalliin ja asiakirjajulkisuuskuvaukseen tehtävien muutosten toteuttamiseksi.

Tietosuojaan vaikutustenarviointi suoritetaan sellaisille henkilötietojen käsittelytoimenpiteille, joiden suunnitteluvaiheessa ilmenee, että toimenpiteisiin liittyy henkilön oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tekemisestä vastaa sen organisaatioyksikön esimies, jonka toiminnassa henkilötietojen käsittely tapahtuu. Tietosuojaan vaikutustenarvioinnit tehdään tietosuojavastaavan avustuksella.

4.3 Kuvaus asiakirjajulkisuuden toteuttamiseksi

Tiedonhallintalain mukaisesti Mikkelin kaupungin tulee tiedonhallintayksikkönä ylläpitää kuvausta sen hallinnoimista tietovarannoista ja asiarekisteristä julkisuusperiaatteen toteuttamista varten. Asiakirjajulkisuuskuvauksen on julkaistava yleisessä tietoverkossa siltä osin kuin sen tiedot eivät ole salassa pidettäviä.

Asiakirjajulkisuuskuvauksen on tiedonhallintalain mukaisesti sisällettävä tiedot tietojärjestelmistä, jotka sisältävät asiarekisteriin tai palvelujen tiedonhallintaan kuuluvia tietoja, asiarekisterin tai tietojärjestelmän sisältämien tietojen antamisesta päättävästä viranomaisesta ja sen yhteystiedoista tiedonsaantia koskevan pyynnön esittämiseksi, tietojärjestelmien sisältämistä tietoaineistoista tietoryhmittäin, hakutekijöistä, joilla asiakirjoja on mahdollista hakea teknisesti viranomaisen asiarekisteristä tai tietojärjestelmistä sekä tietoaineistojen saatavuudesta avoimesti teknisen rajapinnan avulla.

Kuvaukseen voidaan lisätä myös muita, kuin lain vaatimia tietoja, joilla on vaikutusta hallinnon asiakkaiden ja kuntalaisten tietoisuuden lisäämiseen kaupungin hallinnoimista tietovarannoista, kaupunginarkistosta, tietopalvelusta ja muista vastaavista asioista.

Asiakirjajulkisuuskuvauksen laatii ja sitä ylläpitää asiakirjahallintoa ja arkistointia johtava viranhaltija. Kaupungin esimiehet, henkilöstö, tietohallintopäällikkö, tietohallinto ja tietosuojavastaava ovat velvollisia antamaan kuvauksen laatijalle tämän tarvitsemat välttämättömät tiedot kuvauksen ylläpitämiseksi ja omalta osaltaan osallistumaan sen laadintaan liittyvään työhön sekä informoimaan kuvauksen ylläpitäjää hallinnollisista ja tietojärjestelmiin kohdistuvista muutoksista, joilla on vaikutusta kuvauksen sisältöön. Kuvauksen laatija ja ylläpitäjä voi käyttää sen laatimiseen ja ylläpitoon näkemyksensä mukaan tarkoituksenmukaisinta menetelmää tai välinettä.

4.4 Tietosuojaselosteet

Euroopan unionin yleisen tietosuojasetuksen III luvun 1 ja 2 jakson mukaisesti rekisterinpitäjän on ilmoitettava rekisteröityjä henkilötietojen käsittelystä mahdollisimman läpinäkyvästi.

Läpinäkyvän informoinnin toteuttamiseksi tulee kaupungin palveluista, joissa käsitellään henkilötietoja, laatia ja ylläpitää ajantasaisia tietosuojaselosteita, jotka pidetään nähtävillä yleisessä tietoverkossa tai palveluissa itsessään. Tietosuojaseloste voi olla useamman palvelun yhteinen, mikäli henkilörekisteri jakaantuu useampaan eri tietojärjestelmään tai manuaaliseen aineistoon. Tietosuojaselosteen tietosisällössä on otettava huomioon, mitä tietosuojasetuksen 12, 13 ja 14 artikloissa säädetään. Tietosuojavastaava antaa tarkempia ohjeita tietosuojaselosteiden laadinnasta, ylläpidosta ja tietosisällöstä.

Tietosuojaselosteen laatimisesta ja ajan tasalla pitämisestä vastaa palveluprosessin omistaja.

4.5 Tiedonohjaussuunnitelmat

Tietojärjestelmissä, joissa tapahtuu tiedonhallintalaissa tarkoitettua asianhallintaa, tulee pyrkiä ratkaisuihin, joissa niissä käsiteltäville asioille, asiankäsittelyvaiheille ja asiakirjoille voidaan asettaa mahdollisimman ennakkolisesti niiden käsittelyyn liittyviä metatietoja, erityisesti asiakirjojen säilytysaikoja koskevia metatietoja, joiden avulla asiakirjat ja niitä vastaavat tiedot voidaan tuhota niille asetettujen säilytysaikojen jälkeen ilman, että tämä vaatii erityisiä toimia käyttäjiltä tai palveluntuottajilta.

Asiakirjojen tuhoaminen on kuitenkin aina erikseen hyväksyttävä ja dokumentoitava 5.8 luvussa tarkoitetulla tavalla.

Tietoaineistojen metatietojen ennakkollisen määrittelyn mahdollistaminen on pyrittävä huomioimaan myös muissa tietojärjestelmissä, mikäli se on tarkoituksenmukaista tietojärjestelmän käytön kannalta.

Edellä tarkoitettu asioiden, asiankäsittelyvaiheiden ja asiakirjojen metatietojen ennakkollinen määrittely voidaan toteuttaa tiedonohjaussuunnitelmilla. Tiedonohjaussuunnitelmien rakenteessa on otettava huomioon, mitä niistä on erikseen määrätty tai suositettu. Tiedonohjaussuunnitelmissa toimintaprosessien määrittelyn pohjana tulee mahdollisuuksien mukaan käyttää jotain suositettua tai käytöltään vakiintunutta luokitusta.

Tiedonohjaussuunnitelmien laadinnasta ja ylläpidosta vastaavat tietojärjestelmien pääkäyttäjät. Tiedonohjaussuunnitelmien laadinnassa ja ylläpidossa pääkäyttäjät avustaa asiakirjahallintoa ja arkistointia johtava viranhaltija, joka myös hyväksyy ja vahvistaa ne käyttöön.

4.6 Tietotilinpäätös

Kaupunginhallitukselle tulee tuoda vuosittain tilinpäätöskäsittelyn yhteydessä tiedoksi tietotilinpäätös. Tietotilinpäätös on osa tiedolla johtamista ja antaa kokonaiskuvan organisaation tiedonhallinnan ja tietojenkäsittelyn sen hetkisestä tilasta. Raportti on tarkoitettu johdon työkaluksi sekä lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä käytetään yhtenä keinona Euroopan unionin yleisen tietosuojalain tarkoittaman osoitusvelvollisuuden toteuttamisessa.

Tietotilinpäätökseen kootaan edelliseltä kalenterivuodelta keskeisimmät havainnot, toteutumat ja arviot yleisesti tiedonhallinnasta, tieto- ja viestintäteknisistä palveluista, tietoturvallisuudesta, tietosuojasta, tietojenkäsittelystä sekä asianhallinnasta, asiakirjahallinnosta ja arkistotoimesta. Tietotilinpäätöksen kokoaa tietosuojavastaava. Tiedonhallintatyöryhmä avustaa tietosuojavastaavaa tarvittavien tietojen keräämisessä. Kaupungin esimiehet ja henkilöstö ovat omalta osaltaan velvollisia avustamaan tietosuojavastaavaa tietotilinpäätöksen kokoamisessa.

4.7 Tiedonhallinnasta tiedottaminen

Mikkelin kaupungin sisäisestä tiedottamisesta tiedonhallinnassa vastaavat asiakirjahallintoa ja arkistointia johtava viranhaltija, tiedonhallintayhteyshenkilöt, arkistovastaavat, tietojärjestelmien omistajat ja pääkäyttäjät, tietohallinto ja tietosuojavastaava yhteistyössä viestinnän kanssa. Palvelualueet ja liikelaitokset vastaavat lisäksi tiedon välittämisestä omien organisaatioyksiköidensä sisällä.

Tieto- ja viestintäteknisen palvelun tai tietojärjestelmän operatiivisista ongelmista ja häiriöistä tiedottaminen on kaupungin nimeämän omistajan, pääkäyttäjän tai sen sopimuksin valtuuttaman tahon vastuulla.

Ulkoisesta tiedottamisesta vastaa asiakirjahallintoa ja arkistotointa johtava viranhaltija, tietohallinto ja tietosuojavastaava yhdessä viestinnän kanssa.

4.8 Toiminta häiriötilanteissa

Mikkelin kaupungin toiminta kriisitilanteissa perustuu valmiuslain (1552/2011) mukaiseen valmiussuunnitteluun.

Mikkelin kaupunginvaltuusto hyväksyy Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa. Kaupungin tieto- ja viestintäteknisen infrastruktuurin tai tietojärjestelmien toimintaa, tietoturvaa tai tietosuojaa uhkaavissa tilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava tietohallintopäällikölle.

Tietoturva- ja tietosuojarikkomukset käsitellään tapauskohtaisesti. Tietohallintopäälliköllä tai tietohallinnon sopimuksin valtuuttamalla taholla on oikeus sulkea tietoliikenneyhteys, tietojärjestelmä, käyttäjätunnus tai laite uhkatilanteen vahinkojen minimoimiseksi. Tietohallintopäällikkö informoi asianosaisia suoritetuista toimenpiteistä ja mahdollisista jatkotoimenpiteistä mahdollisimman pian.

Henkilötietojen tietoturvaloukkauksen sattuessa kaupungin rekisterinpitäjillä on ilmoitusvelvollisuus valvontaviranomaiselle sekä rekisteröidylle. Valvontaviranomaiselle tehdään ilmoitus yleisen tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

5 Asiakirjahallinnon ja arkistotoimen toimintaohjeet

5.1 Asiakirjahallinnon ja arkistotoimen toimintaohjeiden tarkoitus ja soveltamisala

Tässä alaluvussa annetaan kaupunkia ja sen liikelaitoksia koskevat yleiset määräykset ja ohjeet asiakirjahallinnon ja arkistotoimen järjestämisestä ja suunnitelmallisesta hoidosta. Asiakirjahallintoa ja arkistotoimintaa johtava viranhaltija voi antaa näitä määräyksiä ja ohjeita täydentäviä määräyksiä ja ohjeita.

Asiakirjahallinnon ja arkistotoimen vastuista on määrätty kaupungin hallintosäännön 69–71 §:ssä ja tiedonhallintapolitiikan 3 luvussa, joiden mukaisesti asiakirjahallinnon ja arkistotoimen järjestämisestä vastaa kaupunginhallitus, jonka alaisuudessa sitä johtaa asiakirjahallintoa ja arkistotoimintaa johtava viranhaltija. Kaupungin toimielimet ovat viranomaisen ominaisuudessaan arkistolain tarkoittamia arkistonmuodostajia, joille kuuluvia käytännön tehtäviä hoitavat tulosaluejohtajat, tulosyksiköiden esimiehet, tiedonhallintayhteyshenkilöt ja arkistovastaavat. Jokaisella viranhaltijalla ja työntekijällä on vastuu asiakirjahallinnon ja arkistotoimen toimintaohjeiden noudattamisesta.

Asiakirjahallinnossa ja arkistotoimessa on näiden määräysten ja ohjeiden lisäksi huomioitava niitä koskevat ja niihin vaikuttavat säädökset, määräykset ja suositukset.

5.2 Asiakirjahallinnon ja arkistotoimen tehtävät ja tavoitteet

Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.

Asiakirjahallinnon ja arkistotoimen piiriin kuuluvat asiakirjat, jotka ovat saapuneet arkistonmuodostajalle sen tehtävien johdosta tai muodostuneet sen toiminnan yhteydessä.

Asiakirjahallinnon ja arkistotoimen tehtävänä on asiakirjojen ja asiakirjallisten tietojen säilytysarvon määrittely, niiden käytettävyydestä ja säilyvyydestä huolehtiminen niiden koko elinkaaren ajan ja tarpeettoman aineiston tuhoaminen asiakirjoille määriteltyjen säilytysaikojen päättymisen jälkeen. Edellä mainitun lisäksi arkistotoimen tehtäviin kuuluu arkistoitujen asiakirjojen tietopalvelusta huolehtiminen. Asiakirjahallinnon ja arkistotoimen tehtävänä on myös omalta osaltaan varmistaa asiakirjojen ja asiakirjallisten tietojen todistusvoimaisuus, joka mahdollistetaan huolehtimalla asiakirjojen ja asiakirjallisten tietojen käytettävyyden ja säilyvyyden lisäksi niiden alkuperäisyydestä ja eheydestä.

Asiakirjahallintoa ja arkistointia tulee hoitaa siten, että se:

1. tukee arkistonmuodostajan tehtävien suorittamista ja julkisuusperiaatteen toteutumista,
2. ottaa huomioon yksityisten ja yhteisöjen oikeusturvan ja tietosuojan,
3. mahdollistaa asiakirjallisen kulttuuriperinnön säilymisen ja sen käytön tutkimustarkoituksissa.

Asiakirjahallinnon ja arkistotoimen tavoitteiden saavuttaminen edellyttää pitkäjänteistä ja huolellista asiakirjojen ja asiakirjallisten tietojen elinkaaren suunnittelua, elinkaaren vaiheisiin liittyvien toimenpiteiden toteuttamista ja toiminnan jatkuvaa kehittämistä. Edellä mainittuihin sisältyy erityisesti asiakirjojen ja asiakirjallisten tietojen säilytysaikojen määrittely, digitaalisessa muodossa olevien asiakirjojen suunnitelmallinen rekisteröinti, talteenotto ja säilyttäminen, analogisessa muodossa olevien asiakirjojen säilyttäminen, järjestäminen, luettelointi ja kuvailu, määräajan säilytettävien asiakirjojen tuhoaminen sekä pysyvästi säilytettävien ja arkistoitavien asiakirjojen ja asiakirjallisten tietojen siirtäminen kaupunginarkistoon tai tietojärjestelmiin, jotka soveltuvat tietojen digitaaliseen pitkäaikaissäilytykseen.

5.3 Asiakirjojen ja niitä vastaavien tietojen säilytysarvon määrittäminen

Asiakirjoille ja niitä vastaaville tiedoille tulee määrittää säilytysarvo sekä säilytysajat ja -tavat.

Säilytysarvon määrittämisessä on otettava huomioon, onko asiakirjoja ja niitä vastaavia tietoja säädetty pysyvästi säilytettäväksi tai arkistoitavaksi taikka onko Kansallisarkisto määrännyt niitä arkistoitavaksi arkistolainsäädännön perusteella.

Niille asiakirjoille, joita ei ole säädetty tai määrätty pysyvästi säilytettäväksi tai arkistoitavaksi, tulee määrittellä mahdollisimman konkreettiset säilytysajat. Säilytysaikojen määrittämisessä on tiedonhallintalain mukaisesti otettava huomioon, mitä tietoaineistojen säilytysajoista on erikseen säädetty tai määrätty, tietoaineistojen alkuperäisen käyttötärpeen mukainen tarpeellisuus viranomaisen toiminnassa, luonnollisten henkilöiden tai oikeushenkilöiden etujen, oikeuksien, velvollisuuksien ja oikeusturvan toteutuminen ja todentaminen, sopimusten tai muiden yksityisoikeudellisten oikeustoimien oikeusvaikutukset sekä vahingonkorvausoikeudelliset ja rikosoikeudelliset vanhentumisajat. Määräajan säilytettävien asiakirjojen säilytysaikojen päättymisen jälkeen asiakirjat ja niitä vastaavat tiedot tulee tuhota niin, että tietosuoja ja tietoturva on varmistettu.

Asiakirjojen ja niitä vastaavien tietojen säilytysajat ja -tavat merkitään tiedonhallintamallin arkistonmuodostussuunnitelmaosaan. Arkistonmuodostussuunnitelmat laaditaan yhteistyössä arkistonmuodostajan alaisen organisaatioyksikön esimiehen, tiedonhallintayhteyshenkilöiden, arkistovastaavien, tarvittaessa muun henkilöstön sekä asiakirjahallintoa ja arkistointia johtavan viranhaltijan kanssa. Tiedonhallintayhteyshenkilöt ja arkistovastaavat vastaavat omien organisaatioyksiköidensä arkistonmuodostussuunnitelmien laatimisesta ja ylläpitämisestä. Asiakirjahallintoa ja arkistointia johtava viranhaltija avustaa ja antaa ohjeistusta arkistonmuodostussuunnitelmien laadinnassa.

Mikäli tietojärjestelmissä on käytössä tiedonohjaussuunnitelmia, tulee tietojärjestelmän sisältämien tietoaineistojen osalta säilytysaika koskevat tiedot merkitä myös niihin.

Tiedonohjaussuunnitelmia voidaan käyttää arkistonmuodostussuunnitelmien sijasta tässä alaluvussa kuvatussa tarkoituksessa.

5.4 Asianhallinta ja palvelujen tiedonhallinta

Mikkelin kaupungin viranomaisille käsiteltäväksi saapuneet tai niiden itsensä laatimat asiakirjat tulee rekisteröidä viipymättä asiarekisteriin. Asiarekisteriin rekisteröidään asiaa, asiantkäsittelyä ja asiakirjoja koskevat tiedot siten kuin tiedonhallintalaissa ja erityislainsäädännössä säädetään. Rekisteröitävien tietojen osalta tulee myös ottaa huomioon, mitä niistä on määrätty tai suositettu.

Asiarekisteri on looginen kokonaisuus, joka muodostuu asianhallintajärjestelmässä, operatiivisissa tietojärjestelmissä sekä osittain myös manuaalisesti käsittelyssä olevista asioista.

Asiarekisteröintiin käytetään ensisijaisesti kaupungin asianhallintajärjestelmää. Käsittelyyn tulleet tai otetut asiat avataan asianhallintajärjestelmään kaupungin kirjaamossa. Kirjaamo rekisteröi ja tallentaa kaupungille saapuneet asiakirjat asianhallintajärjestelmään. Mikäli asiakirjat saapuvat suoraan muuhun organisaatioyksikköön kuin kirjaamoon, tulee asiakirjat vastaanottaneen organisaatioyksikön rekisteröidä ja tallentaa asiakirjat asianhallintajärjestelmään. Organisaatioyksiköt voivat sopia kaupungin kirjaamon kanssa myös toisenlaisesta työnjaosta. Viranhaltijoiden ja työntekijöiden tulee rekisteröidä ja tallentaa laatimansa asiakirjat asianhallintajärjestelmään niitä koskeville asioille, ellei työnjaosta asiakirjojen rekisteröinnissä ja tallentamisessa ole kaupungin kirjaamon kanssa toisin sovittu.

Asianhallintajärjestelmässä asioiden luokittelussa käytetään kaupungin tehtäväluokitusta. Asianhallintajärjestelmän pääkäyttäjä vastaa luokituksen ylläpidosta ja kehittämisestä yhdessä asiakirjahallintoa ja arkistointia johtavan viranhaltijan kanssa.

Asiarekisteröinti voi tapahtua myös muussa, kuin asianhallintajärjestelmässä, mikäli kaupungilla on jotain tiettyä tehtävää tai palvelua varten käytössä oleva tietojärjestelmä, jota käytetään asiantkäsittelyyn. Operatiivisen tietojärjestelmän käyttö asiarekisteröinnissä on näissä tapauksissa oltava tarkoituksenmukaista verrattuna asianhallintajärjestelmän käyttöön. Operatiivisissa tietojärjestelmissä tapahtuvassa asiarekisteröinnissä asiat avataan ja asiakirjat rekisteröidään ja tallennetaan tietojärjestelmään sen omistavan organisaatioyksikön ohjeiden ja käytänteiden mukaisesti siten, että niissä otetaan huomioon asiakirjahallinnon ja arkistotoimen vaatimukset.

Asioiden, asiantkäsittelyvaiheiden ja asiakirjojen rekisteröinnissä on käytettävä mahdollisimman selkeitä nimeämiskäytäntöjä ja vältettävä moninkertaista rekisteröintiä ja tietojen tallentamista.

Asianhallinnan lisäksi muiden kuin asiantkäsittelyn yhteydessä muodostuvien asiakirjojen ja niitä vastaavien tietojen saatavuudesta on huolehdittava siten kuin tiedonhallintalaissa ja erityislainsäädännössä säädetään. Palveluja tuotettaessa muodostuvat asiakirjat ja niitä vastaavat

tiedot on rekisteröitävä viipymättä siten, että niiden muodostuminen voidaan jälkikäteen todentaa. Palvelujen tiedonhallinnassa asiakirjat rekisteröidään ja tallennetaan tietojärjestelmään sen omistavan organisaatioyksikön ohjeiden ja käytänteiden mukaisesti siten, että niissä otetaan huomioon asiakirjahallinnon ja arkistotoimen vaatimukset.

5.5 Asiakirjojen ja niitä vastaavien tietojen säilyttäminen

Asiakirjoja ja niitä vastaavia tietoja, jotka ovat muodostuneet 1.1.2022 alkaen, säilytetään tiedonhallintalain mukaisesti lähtökohtaisesti sähköisessä muodossa. Tätä ajankohtaa aikaisemmin muodostuneet asiakirjat ja niitä vastaavat tiedot säilytetään siten kuin ne ovat muodostuneet tai kuten kaupungin arkistonmuodostussuunnitelmissa tai muissa ohjeissa on määrätty, jollei niitä myöhemmin muuteta digitaaliseen muotoon.

Digitaalisessa muodossa olevia asiakirjoja säilytetään lähtökohtaisesti niissä kaupungin tietojärjestelmissä, joissa ne muodostuvat tai joihin ne on tallennettu taikka digitoitu osana asianhallinnan tai palvelujen tiedonhallinnan toteuttamista. Edellytyksenä tietoaineistojen digitaaliselle säilyttämiselle on, että tietojärjestelmät täyttävät tiedonhallintalain mukaiset tietoturvaluusvaatimukset. Mikäli tietojärjestelmä ei täytä näitä vaatimuksia tai tietojärjestelmän muusta seikasta johtuen asiakirjojen ja niitä vastaavien tietojen luotettava säilyttäminen ei ole mahdollista, tulee kaupungissa tehdä tarvittavat järjestelyt tietojen siirtämiseksi tietojärjestelmään, joka soveltuu kyseisten tietojen digitaaliseen säilyttämiseen.

Asiankäsittelyä tai palvelujen tiedonhallintaa varten 1.1.2022 alkaen kaupungille saapuneet tai kaupungissa muodostetut analogiset asiakirjat tulee digitoida sellaiseen tietojärjestelmään, jossa asiakirjaan liittyvää asiaa käsitellään. Digitoinnista voidaan poiketa tiedonhallintalaissa säädetyin perustein. Digitoituja asiakirjoja säilytetään ensisijaisesti digitaalisessa muodossa. Digitoinnin jälkeen määräajan säilytettävien asiakirjojen analogiset versiot voidaan tuhota tietoturvallisesti, kunhan ensin niiden luotettavuus ja eheys on varmistettu ja ne on tallennettu tiedonhallintalain mukaiset tietoturvaluusvaatimukset täyttävään tietojärjestelmään.

Mikäli määräajan säilytettävillä asiakirjoilla on niiden analogisessa muodossa rahallista arvoa, ne ovat yksityisoikeudellisesti sitovia ja niissä on asiakirjojen todistusvoimaisuuteen vaikuttavia merkintöjä, kuten allekirjoituksia tai jos niiden muuhun luonteeseen liittyvän tekijä niin edellyttää, tulee tällaiset asiakirjat säilyttää edelleen myös analogisessa muodossa. Asiakirjahallintoa ja arkistointia johtava viranhaltija antaa tarkentavia ohjeita digitoitujen asiakirjojen tuhoamisesta.

Asiakirjojen tuhoamisesta on oltava aina erikseen yhteydessä asiakirjahallintoa ja arkistointia johtavaan viranhaltijaan, mikäli niiden tuhoamisesta ei ole annettu ennakkoon ohjeistusta.

Määräajan säilytettävien asiakirjojen analogisia versioita, jotka ovat saapuneet tai muodostuneet ennen 1.1.2022, ja jotka myöhemmin muutetaan digitaaliseen muotoon, ei saa tuhota ennen kuin asiakirjahallintoa ja arkistointia johtava viranhaltija on antanut tähän luvan.

Analogisessa muodossa olevia määräajan säilytettäviä asiakirjoja säilytetään lähtökohtaisesti organisaatioyksiköiden lähiarkistotiloissa.

Arkistovastaavien tehtävänä on järjestää ja pitää järjestyksessä organisaatioyksiköidensä lähiarkistot. Organisaatioyksikön muu henkilöstö on velvollinen noudattamaan asiakirjojen järjestämisessä ja lähiarkistoon siirtämisessä arkistovastaavan, organisaatioyksikön esimiehen sekä asiakirjahallintoa ja arkistointia johtavan viranhaltijan antamia ohjeita. Mikäli organisaatioyksikössä on epäjärjestykseen joutuneita asiakirjoja, on ne järjestettävä tai palautettava alkuperäiseen järjestykseen lähiarkistossa.

5.6 Asiakirjojen ja niitä vastaavien tietojen pitkäaikaissäilyttäminen ja arkistointi

Asiakirjoja ja niitä vastaavia tietoja, jotka ovat muodostuneet 1.1.2022 alkaen ja jotka on säädetty tai määrätty pysyvästi säilytettäväksi tai arkistoitavaksi, säilytetään tiedonhallintalain mukaisesti lähtökohtaisesti sähköisessä muodossa, ellei toisin ole säädetty tai määrätty. Kansallisarkiston arkistolain nojalla pysyvästi säilytettäväksi eli arkistoitaviksi määräämien digitaalisessa muodossa olevien asiakirjojen kohdalla on huomioitava, että tietojärjestelmät, joissa arkistoitavia asiakirjoja pitkäaikaissäilytetään tai johon ne siirretään pitkäaikaissäilytystä varten, täyttävät tiedonhallintalain mukaisten tietoturvasuoritusvaatimusten lisäksi viranomaisia koskevat arkistointivaatimukset.

Kansallisarkiston arkistolain nojalla pysyvästi säilytettäväksi eli arkistoitaviksi määräämiä asiakirjoja ja niitä vastaavia tietoja voidaan säilyttää yksinomaan digitaalisessa muodossa lähtökohtaisesti kaupungin asianhallintajärjestelmässä ja sähköisessä arkistossa taikka muussa viranomaisia koskevat arkistointivaatimukset täyttävissä tietojärjestelmissä. Muissa kuin edellä mainituissa tietojärjestelmissä olevien arkistoitavien asiakirjojen kohdalla tulee tietojärjestelmien kehittämiseen varattujen määrärahojen puitteissa kehittää ratkaisuja, joilla arkistoitavaksi määrättyt asiakirjat ja niitä vastaavat tiedot voidaan siirtää arkistointivaatimukset täyttäviin tietojärjestelmiin. Arkistoitavien tietoaineistojen talteenotto sähköiseen arkistoon tai muuhun arkistointivaatimukset täyttävään tietojärjestelmään tulee huomioida ja toteuttaa tietojärjestelmän elinkaaren mahdollisimman varhaisessa vaiheessa, mutta viimeistään silloin, kun tietojärjestelmän käytöstä ollaan luopumassa.

Sähköiseen arkistoon voidaan tehdä myös muiden kuin arkistoitavaksi määrättyjen tietoaineistojen siirtoja, jos tietoaineistoihin sisältyviä asiakirjoja ja niitä vastaavia tietoja tulee säilyttää pitkäaikaisesti, ne ovat kaupungille ja sen toiminnalle arvokkaita, niiden alkuperäinen tietojärjestelmä ei täytä tiedonhallintalain mukaisia tietoturvasuoritusvaatimuksia tai niihin kohdistuu säädettyjä tai määrättyjä erityisvaatimuksia, joiden vuoksi niiden käytettävyys ja säilyminen on erityisesti turvattava.

Asiakäsittelyä tai palvelujen tiedonhallintaa varten 1.1.2022 alkaen kaupungille saapuneet tai kaupungissa muodostetut analogiset asiakirjat, jotka on säädetty tai määrätty pysyvästi säilytettäväksi tai arkistoitaviksi tulee digitoida sellaiseen tietojärjestelmään, jossa asiakirjaan liittyvää asiaa käsitellään. Digitoinnista voidaan poiketa tiedonhallintalaissa säädettyin edellytyksin. Digitoituja asiakirjoja säilytetään ensisijaisesti digitaalisessa muodossa. Digitoinnin jälkeen pysyvästi

säilytettävien ja arkistoitavien asiakirjojen analogiset versiot voidaan tuhota tietoturvallisesti, kunhan ensin niiden luotettavuus ja eheys on varmistettu ja ne on tallennettu tiedonhallintalain mukaiset tietoturvaluusvaatimukset täyttävään tietojärjestelmään, ellei toisin ole säädetty tai määrätty.

Mikäli pysyvästi säilytettävillä tai arkistoitavilla asiakirjoilla on niiden analogisessa muodossa kulttuuriperinnöllistä, tutkimuksellista tai rahallista arvoa, ne ovat yksityisoikeudellisesti sitovia ja niissä on asiakirjojen todistusvoimaisuuteen vaikuttavia merkintöjä, kuten allekirjoituksia tai jos niiden muuhun luonteeseen liittyvän tekijä niin edellyttää, tulee tällaiset asiakirjat säilyttää edelleen myös analogisessa muodossa. Asiakirjahallintoa ja arkistointia johtava viranhaltija antaa tarkentavia ohjeita digitoitujen asiakirjojen tuhoamisesta.

Asiakirjojen tuhoamisesta on oltava aina erikseen yhteydessä asiakirjahallintoa ja arkistointia johtavaan viranhaltijaan, mikäli niiden tuhoamisesta ei ole annettu ohjeistusta.

Pysyvästi säilytettävien ja arkistoitavien asiakirjojen analogisia versioita, jotka ovat saapuneet tai muodostuneet ennen 1.1.2022 tai 1.1.2015 alkaen saapuneita tai muodostuneita pysyvästi säilytettävien ja arkistoitavien asiakirjojen analogisia versioita, joita ei ole digitoitu asianhallintajärjestelmään tai sähköiseen arkistoon, ja jotka muutetaan myöhemmin digitaaliseen muotoon, ei saa tuhota.

Mikäli edellä mainittujen arkistolain nojalla pysyvästi säilytettävien eli arkistoitavien asiakirjojen analogiset versiot halutaan tuhota niiden digitoinnin jälkeen, on digitoinnissa noudatettava hävittämiseen tähtäävän digitoinnin vaatimuksia, jonka lisäksi analogisten versioiden tuhoamista varten on anottava tuhoamislupaa Kansallisarkistolta arkistolain mukaisesti. Hakemuksen voi tehdä asiakirjahallintoa ja arkistointia johtava viranhaltija. Mikäli Kansallisarkisto myöntää tuhoamisluvan, ratkaisee kaupunginhallitus päätöksellään, tuhotaanko aineistot luvan mukaisesti.

Analogisessa muodossa olevat pysyvästi säilytettävät ja arkistoitavat asiakirjat tulee siirtää organisaatioyksiköistä kaupunginarkistoon, kun organisaatioyksiköt eivät enää aktiivisesti tarvitse niitä tehtäviensä hoidossa. Organisaatioyksiköiden esimiehet, arkistovastaavat ja asiakirjahallintoa ja arkistointia johtava viranhaltija voivat sopia ajankohdasta, jolloin siirto toteutetaan. Organisaatioyksiköiden hallussa olevia pysyvästi säilytettäviä ja arkistoitavia asiakirjoja voidaan säilyttää pidempään yksiköissä, mikäli yksiköillä on niihin kohdistuvaa jatkuvaa tarvetta tehtäviensä hoidossa ja yksiköillä on käytössään riittävän turvalliset lähiarkistotilat asiakirjojen säilyttämistä varten.

Kaupunginarkistoon voidaan ottaa säilytykseen myös pitkäaikaisesti säilytettäviä asiakirjoja tai asiakirjoja, jotka ovat kaupungille ja sen toiminnalle arvokkaita, mikäli kaupunginarkiston tilat riittävät näiden säilyttämiseen. Kaupunginarkistoon ei kuitenkaan lähtökohtaisesti siirretä säilytettäväksi alle kymmenen vuotta säilytettäviä asiakirjoja.

Organisaatioyksiköiden esimiesten, arkistovastaavien tai muiden asiakirjoja kaupunginarkistoon siirtävien tahojen tulee ennen siirtoa varmistaa asiakirjahallintoa ja arkistointia johtavalta

viranhaltijalta, että kaupunginarkistolla on mahdollisuus ottaa asiakirjat vastaan ja sopia tämän kanssa siirron käytännön järjestelyistä.

Asiakirjat tulee siirtää kaupunginarkistoon valmiiksi järjestettyinä, koteloituina ja nimiöityinä. Järjestämisestä, koteloinnista, nimiöinnistä ja siirtämisestä vastaa luovutuksen tekevä organisaatioyksikkö.

Kaupunginarkistoon siirrettävistä asiakirjoista laaditaan luovutusluettelo, johon merkitään arkistoyksikön tarkkuudella luovutettavat asiakirjat. Luovutusluettelon laatii asiakirjat siirtävä organisaatioyksikkö, ja sen hyväksyy asiakirjahallintoa ja arkistointia johtava viranhaltija.

5.7 Kaupunginarkisto

Mikkelin kaupunginarkiston tehtävänä on säilyttää kaupungin toiminnassa muodostuneet analogiset asiakirjat, jotka tulee arkistolain nojalla säilyttää pysyvästi eli arkistoida tai erityislainsäädännön nojalla arkistoida.

Kaupunginarkisto säilyttää Mikkelin kaupungin arkiston lisäksi Mikkelin kaupunkiin liitettyjen kuntien eli Anttolan kunnan, Haukivuoren kunnan, Mikkelin maalaiskunnan, Ristiinan kunnan ja Suomenniemen kunnan arkistot sekä Mikkelin seudun terveydenhuollon kuntayhtymän arkiston hallinnolliset asiakirjat.

Kaupunginarkistoon siirrettyjen ja siellä säilytyksessä olevien asiakirjojen järjestyksen säilymisestä on huolehdittava, ja niistä tulee laatia ja ylläpitää arkistoluetteloita. Arkistoluetteloiden lisäksi tulee, käytettävissä olevien henkilöstöresurssien puitteissa, laatia arkistokokonaisuuksista kuvailut, joissa esitetään tarkemmin arkistokokonaisuuksien tietosisältö.

Mikäli kaupunginarkistosta siirretään lainsäädännön mukaisesti tai sen salliessa asiakirjoja muun arkistonmuodostajan arkistoon tai arkistoinstituutioon niiden pysyvää säilyttämistä tai arkistointia varten, tulee asiakirjojen luovuttamisesta laatia luovutusluettelo, johon merkitään arkistoyksikön tarkkuudelle luovutettavat asiakirjat. Luovutusluettelon hyväksyy asiakirjahallintoa ja arkistointia johtava viranhaltija.

Kaupunginarkiston tietopalvelu palvelee kuntalaisia, hallinnon asiakkaita, tutkijoita, yrityksiä, yhteisöjä, kaupungin henkilökuntaa ja muita asiakkaita. Kaupunginarkistossa olevan aineiston tietopalvelua voi hoitaa muunkin organisaatioyksikön kuin kaupunginarkiston henkilöstö, mikäli tämä on aineiston ja toiminnan kannalta tarkoituksenmukaista. Kaupunginarkistosta tutkittavaksi tai tutustuttavaksi annettujen asiakirjojen käsittelyssä on noudatettava kaupunginarkiston antamia ohjeita.

Kaupunginhallitus huolehtii viimekädessä siitä, että kaupunginarkistolla on riittävät aineelliset ja ajalliset resurssit sekä henkilöstöresurssit kaupunginarkiston hoitamiseen ja siellä säilytyksessä olevien asiakirjojen järjestämiseen, luettelointiin, kuvailuun ja tietopalvelun tarjoamiseen.

5.8 Asiakirjojen ja niitä vastaavien tietojen tuhoaminen

Määräajan säilytettävät asiakirjat tulee tiedonhallintalain ja arkistolain mukaisesti tuhota viipymättä tietoturvalisella tavalla sen jälkeen, kun niiden säilytysaika on päättynyt. Pysyvästi säilytettäviä tai arkistoitavia asiakirjoja ei saa tuhota, vaan ne säilytetään pysyvästi.

Analogisessa muodossa olevat määräajan säilytettävät asiakirjat, jotka ovat salassa pidettäviä tai sisältävät henkilötietoja, tulee tuhota tietoturvalisesti käyttäen kaupungille hankittuja tuhoamispalveluja tai muita tietoturvalisia tuhoamistapoja.

Analogisessa muodossa olevien määräajan säilytettävien asiakirjojen tuhoamisesta niiden säilytysaikojen päättymisen jälkeen huolehtivat organisaatioyksiköiden arkistovastaavat. Kaupunginarkistoon siirrettyjen määräajan säilytettävien asiakirjojen tuhoamisesta niiden säilytysaikojen päättymisen jälkeen huolehtii kaupunginarkiston henkilöstö.

Tuhottavista asiakirjoista tulee laatia hävittämisluekkelo. Hävittämisluekkelo laaditaan yli kymmenen vuotta säilytettävistä asiakirjoista ja kaikista kirjanpidon asiakirjoista. Hävittämisluekkelon laatii tuhoamisen suorittanut henkilö, jonka tämä tai tämän tulosalueen johtava viranhaltija hyväksyy asiakirjahallintoa ja arkistointia johtavan viranhaltijan kanssa. Kaupunginarkistosta tuhottavien määräajan säilytettävien asiakirjojen hävittämisluekkelon hyväksyy asiakirjahallintoa ja arkistointia johtava viranhaltija. Hävittämisluekkelo tai vastaava asiakirja tulee laatia myös digitaalisessa muodossa olevista asiakirjoista, mikäli tietojärjestelmässä ei ole tuhoamistoiminnallisuutta, jossa hävittämisluekkelo muodostuu automaattisesta asiakirjojen ja niitä vastaavien tietojen tuhoamisen yhteydessä.

5.9 Asiakirjojen ja niitä vastaavien tietojen käsittely, suojaaminen ja turvaaminen

Asiakirjoja ja niitä vastaavia tietoja on käsiteltävä ja säilytettävä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä. Asiakirjoja ja niitä vastaavia tietoja ei saa oikeudettomasti hävittää, ottaa haltuun, vahingoittaa, vääristää tai tehdä muutoin käyttökelvottomiksi.

Pysyvästi säilytettävät ja arkistoitavat asiakirjat tulee laatia ja tiedot tallentaa pitkäaikaista säilytystä kestäviä materiaaleja ja säilyvyyden turvaavia menetelmiä käyttäen. Analogisessa muodossa olevien arkistoitavien asiakirjojen kohdalla on huomioitava, mitä Kansallisarkisto on arkistolain nojalla materiaaleista määrännyt. Digitaalisessa muodossa olevien asiakirjojen kohdalla on huomioitava, mitä tiedonhallintalaissa on säädetty tietoaineistojen turvallisuudesta sekä mitä siitä on erikseen suositettu. Arkistoitavien digitaalisessa muodossa olevien asiakirjojen kohdalla on lisäksi huomioitava, mitä Kansallisarkisto on niiden säilyttämisestä arkistolain nojalla määrännyt ja ohjeistanut.

Kaupungin materiaalihankinnoissa, erityisesti toimistotarvikehankinnoissa on huomioitava, että arkistokelpoisia materiaaleja, kuten laatuvaatimukset täyttävää paperia ja suojakoteloita, on aina saatavilla.

Arkistoitavia analogisessa muodossa olevia asiakirjoja tulee säilyttää sellaisissa arkistotiloissa, jotka täyttävät Kansallisarkiston arkistolain nojalla antamat arkistotilamääräykset. Määräajan säilytettäviä analogisessa muodossa olevia asiakirjoja tulee säilyttää turvallisissa lähiarkistotiloissa, mikäli niitä ei siirretä kaupunginarkiston keskusarkistotiloihin pitkäaikaissäilytettäväksi. Keskusarkistotiloja rakennettaessa tai korjattaessa on otettava huomioon arkistotilamääräykset.

Viranomaisten asiakirjat ovat julkisuuslain perusteella lähtökohtaisesti julkisia. Niiden käsittelyssä on kuitenkin otettava huomioon henkilötietojen suojaan liittyvät vaatimukset silloin, kun ne sisältävät henkilötietoja. Erityistä huolellisuutta on noudatettava käsiteltäessä salassa pidettäviä asiakirjoja ja asiakirjoja, jotka sisältävät arkaluontoisia henkilötietoja.

Viranhaltijat, työntekijät ja luottamushenkilöt eivät saa paljastaa sivullisille salassa pidettäviä tietoja, jotka nämä ovat saaneet tietoonsa tehtäviensä johdosta. Salassapito- ja vaitiolovelvollisuus koskee myös harjoittelijoita, toimeksiantotehtävän saaneita tahoja sekä luvan tai asianosaisaseman nojalla salassa pidettäviä tietoja saaneita tahoja.

Kaupungin toiminnan jatkumisen sekä kulttuuriperinnön ja tutkimuksen kannalta tärkeät tietoaaineistot on turvattava myös poikkeusoloissa. Poikkeusolojen suojaamistarpeita varten asiakirjat ryhmitellään kolmeen suojeluluokkaan:

1. I Toiminnan jatkumisen kannalta välttämättömät asiakirjat
2. II Tutkimuksellisista, juridisista tai taloudellisista syistä suojeltavat asiakirjat
3. III Muut asiakirjat

Analogisessa muodossa olevia asiakirjoja, jotka kuuluvat suojeluluokkaan I tai II, tulee säilyttää arkistotiloissa, jotka täyttävät Kansallisarkiston arkistotilamääräykset tai niiden on oltava siirrettävissä tällaisiin tiloihin lyhyellä varoitusajalla poikkeusolojen tullessa voimaan. Digitaalisessa muodossa olevia asiakirjoja, jotka kuuluvat suojeluluokkaan I tai II, tulee säilyttää sellaisissa tietojärjestelmissä, jotka täyttävät tiedonhallintalain mukaiset tietoturvasuoritusvaatimukset, jonka lisäksi tällaisia asiakirjoja sisältävien tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

6 Tietosuoja ja tietoturvan toimintaohjeet

6.1 Tietoturvallisuus viranomaistoiminnassa

Tiedonhallintayksikön ja siinä toimivien viranomaisten on huolehdittava, että sen omistamien tai hankkimien tietojärjestelmien ja tietoaisteiden tietoturvallisuus varmistetaan tiedonhallintalain 4 luvun vaatimusten mukaisesti. Tietoturvallisuudessa on huomioitava myös, mitä erityislainsäädännössä siitä säädetään.

Tiedonhallintayksikössä on seurattava toimintaympäristön tietoturvallisuuden tilaa ja varmistettava tietoaisteiden ja tietojärjestelmien tietoturvallisuus sekä selvittävät olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti. Toimintaympäristön tietoturvallisuuden tilan seurannan ja riskienhallinnan vastuut on määritelty luvussa 3.

Tietojärjestelmistä vastaavien viranomaisten on huolehdittava, että toiminnan kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys testataan riittävän säännöllisesti. Tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojen käsittely on suunniteltava siten, että asiakirjojen julkisuus ja salassapito voidaan vaivatta toteuttaa.

Tietojärjestelmistä ja tietoaisteista vastaavien viranomaisten on huolehdittava, että tietoaisteiden muuttumattomuus, suojaus teknisiltä ja fyysisiltä vahingoilta, alkuperäisyys, ajantasaisuus, virheettömyys, saatavuus sekä käyttökelpoisuus on varmistettu tarpeellisilla tietoturvaluustoimenpiteillä. Lisäksi tietoturvaluustoimenpitein on varmistettava, että tietoaisteiden saatavuutta rajoitetaan vain, jos tiedonsaantia ja käsittelyoikeuksia on laissa erikseen rajoitettu ja, että tietoaisteitot voidaan tarvittavilta osin arkistoida. Tietoaisteitot on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaisteiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien tietoturvaluustovaatimusten toteuttamiseksi riittävän turvallisia.

Tietojärjestelmistä vastaavien viranomaisten on huolehdittava, että tietojärjestelmien käyttöoikeudet on määritelty siten, että ne perustuvat on käyttäjien tehtäviin liittyviin käyttötarpeisiin. Käyttöoikeudet on pidettävä ajan tasalla.

Tietojärjestelmistä vastaavien viranomaisten on huolehdittava, että tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

Salassa pidettävien tietojen siirto yleisessä tietoverkossa tulee toteuttaa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä. Salassa pidettävien tietojen vastaanottaja on myös varmistettava tai tunnistettava riittävän tietoturvallisesti ennen kuin tämä pääsee käsittelemään kyseisiä tietoja.

Tiedonhallintayksikössä on tunnistettava tehtävät, joiden suorittaminen edellyttää palvelussuhteessa olevilta erityistä luotettavuutta, ja otettava tämä huomioon henkilöstön rekrytoinnissa.

6.2 Tietosuoja ja tietoturvan seuranta

Kaupunkikonsernin tietoturva- ja tietosuojatyöryhmään nimettyjen edustajien tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä sekä tietohallinnolle että tieto- ja viestintätekniisten palvelujen tuottajille.

Tieto- ja viestintätekniisten palvelujen tuottajien tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä sekä tietohallinnolle että kaupungin nimeämälle tietojärjestelmän omistajalle tai pääkäyttäjälle.

Tietohallinto ylläpitää kokonaiskuvaa tietoturvasta ja siihen liittyvistä riskeistä ja raportoi siitä osana sisäisen tarkastuksen prosessia.

Tietosuojavastaava ylläpitää kokonaiskuvaa tietosuojasta ja siihen liittyvistä riskeistä ja raportoi siitä osana sisäisen tarkastuksen prosessia.

6.3 Tietosuoja ja tietoturvan arviointi

Tietohallinnon tehtävänä on arvioida tietoturvaa säännöllisesti tietojärjestelmäkohtaisesti ja kokonaisuutena. Arvioinnit voivat kohdistua sekä kaupungin ja sen sidosryhmien että tieto- ja viestintätekniisten palvelujen palveluntuottajien toimintaan. Arvioinnin kohteena on tietoturvan kolmen pääkäsitteen, saatavuuden, eheyden ja luottamuksellisuuden, toteutuminen ja tavoitteena on tunnistaa niihin liittyviä riskejä ja kehittämiskohteita. Tietohallinto priorisoi arviointikohteet. Priorisointiperusteena on tietojärjestelmän tai palvelun vaikutus kaupungin palvelutuotantoon.

Tietosuoja toteutumisen arviointi lisätään osaksi sisäisen tarkastuksen toimintaa vuosittain toteutuvaksi. Tietosuoja vaikutustenarviointien tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa.

6.4 Tietosuoja ja tietoturvan kehittäminen ja ohjeistaminen

Tietohallinto tarkentaa tietoturvan ja tietosuoja kehittämisen tavoitteet vuosittain tavoitteiden pohjalta huomioiden sekä seurannan että arviointien tuottaman tiedon. Tietohallinto huomioi kehittämistavoitteet Mikkelin kaupungin kokonaisarkkitehtuurin kehittämisen yhteydessä.

Tietohallinto voi antaa näitä ohjeita täydentäviä ohjeita tietoturvasta sekä tieto- ja viestintätekniisistä palveluista. Tietosuojavastaava voi antaa näitä ohjeita täydentäviä ohjeita tietosuojasta.

7 Määritelmät ja käsitteet

Alla esitetään neljä taulukkoa tiedonhallintaa koskevista keskeisistä määritelmistä ja käsitteistä.

Tiedonhallinnan yleiset määritelmät ja käsitteet	
Kuvaus asiakirjajulkisuuden toteuttamiseksi	Tiedonhallintayksikön ulkoinen kuvaus hallinnon asiakkaille ja julkiselle yleisölle, joka pitää sisällään tiedot tietojärjestelmistä, jotka sisältävät asiarekisteriin kuuluvia tai palvelujen tiedonhallinnan tietoja, tietoaineistojen antamisesta päättävistä viranomaisista ja näiden yhteystiedoista, tietoaineistojen tietoryhmistä, hakutekijöistä, joilla tietoja voi hakea tietojärjestelmästä sekä tieto siitä ovatko tietoaineistot saatavilla avoimesti teknisten rajapintojen avulla.
Koneluettava muoto	Tiedostomuoto, jonka rakenne mahdollistaa sen, että ohjelmistot pystyvät helposti yksilöimään, tunnistamaan ja poimimaan siitä tietoaineistoja, yksittäisiä tietoja sekä niiden rakenteita.
Tekninen rajapinta	Sähköisen tietojenvaihdon mahdollistama tiedonsiirtoratkaisu kahden tai useamman tietojärjestelmän välillä.
Tiedon elinkaari	Tiedon olemassaolon aikaiset vaiheet, joihin kuuluu tietoaineistojen muodostaminen ja kerääminen, rekisteröinti ja talteenotto, säilyttäminen, jonka yhteydessä tapahtuu erityisesti tiedon käsittelyä, hyödyntämistä, luovuttamista, suojaamista ja turvaamista, sekä arkistointi tai tuhoaminen.
Tiedonhallinnan muutosvaikutusten arviointi	Hallinnollisten tai tietojärjestelmiin kohdistuvien muutosten tiedonhallintaan vaikuttavien tekijöiden arviointi.
Tiedonhallinta	Viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvat toimet ja tietoturvallisuustoimenpiteet viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista.
Tiedonhallintayksikkö	Viranomaisorganisaatio, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti.
Tiedonhallintamalli	Tiedonhallintayksikön sisäinen kuvaus sen tiedonhallinnasta, joka pitää sisällään tiedot organisaation toimintaprosesseista, tietovarannoista ja niiden käyttötarkoituksesta, tietoryhmistä, luovutuskohteista ja säilytysajoista, tietoaineistojen arkistoinnista ja tuhoamisista, tietojärjestelmistä ja niiden käyttötarkoituksista ja liittymistä, tietoturvallisuustoimenpiteistä sekä vastuuviranomaisista.

Tiedonhallinnan yleiset määritelmät ja käsitteet	
Tietojärjestelmä	Tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely.
Tietoaineisto	Asiakirjoista ja muista vastaavista tiedoista muodostuva tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus.
Tietovaranto	Viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettävä tietoaineistoja sisältävä kokonaisuus, jota käsitellään tietojärjestelmien avulla tai manuaalisesti.
Yhteentoimivuus	Tietojen hyödyntäminen ja vaihto eri tietojärjestelmien välillä siten, että tietojen merkitys ja käytettävyys säilyvät.

Asiakirjahallinnon ja arkistotoimen määritelmät ja käsitteet	
Analoginen säilytysmuoto	Asiakirjan säilytysmuoto, jossa tietoa säilytetään moniarvoisessa muodossa, kuten paperiasiakirjoina tai mikrofilmillä.
Arkistointi	Asiakirjojen ja niitä vastaavien tietojen säilyttäminen yleisen edun mukaisia tarkoituksia, kuten kulttuuriperintö- ja tutkimustarkoituksia varten niiden säilytysajan päättymisen jälkeen. Kaikkia asiakirjoja ei arkistoida, vaan arkistointi perustuu sitä koskevaan sääntelyyn.
Arkistonmuodostaja	Viranomaisen, jonka tehtävänä on järjestää arkistotoimi arkistolain vaatimusten mukaisesti.
Arkistonmuodostussuunnitelma (AMS)	Arkistonmuodostajan laatima ja ylläpitämä sisäinen määräys, jossa määritellään vähintään asiakirjojen säilytysajat ja -tavat.
Arkistotoimi	Organisaation toimi, jonka tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeeton aineisto.
Asiakirja	Kirjallisen ja kuvallisen esityksen lisäksi sellainen käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuva tietty kohde tai asiaa koskeva viesti, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.
Asiakirjahallinto	Organisaation toimi, jonka tehtävänä on asiakirjojen hallintaprosessien ohjaaminen ja valvonta sekä asiakirjojen elinkaaren vaiheiden toimenpiteiden suorittamisen tehokas ja systemaattinen ohjaaminen ja valvonta, jotta organisaatio pystyy toteuttamaan toimintaansa ja palvelemaan asiakkaitaan tehokkaasti sekä huolehtimaan sen oikeudellisista ja taloudellisista eduista.

Asiakirjahallinnon ja arkistotoimen määritelmät ja käsitteet	
Asianhallinta	Viranomaisen käsittelemien asioiden, asiakäsittelyvaiheiden ja niihin liittyvien asiakirjojen rekisteröiminen ja käsittelyn ohjaaminen niiden koko elinkaaren ajan.
Digitaalinen säilytysmuoto	Asiakirjan säilytysmuoto, jossa tieto säilytetään täsmällisesti rajattuina arvoina, kuten binäärimuotoisena datana. Dataa säilytetään esimerkiksi optisilla tai sähkömagneettisilla tallennusvälineillä.
Digitointi	Analogisessa muodossa olevien asiakirjojen muuttaminen digitaaliseen muotoon tähän tarkoitetuilla teknisillä apuvälineillä.
Pysyvä säilyttäminen	Asiakirjojen säilyttäminen pysyvästi niiden alkuperäistä käyttötarkoitusta varten. Asiakirjojen pysyvistä säilyttämisestä säädetään lailla.
Säilyttäminen	Asiakirjojen säilyttäminen määräajan niiden alkuperäistä käyttötarkoitusta varten.
Tehtäväluokitus	Organisaation lakisäätöisten tehtävien sekä tuki- ja ylläpitotehtävien hierarkkinen luettelo, jota käytetään apuna toimintaprosessien määrittämiseen sekä asioiden ja asiakirjojen luokitteluun niiden käytettävyyden parantamiseksi.
Tiedonohjaussuunnitelma (TOS)	Arkistonmuodostussuunnitelman tietojärjestelmässä oleva ilmentymä. Tiedonohjaussuunnitelman avulla, jota hallitaan joko tietojärjestelmän toiminnallisuuksilla tai erillisellä tiedonohjausjärjestelmällä (TOJ), pystytään tietojärjestelmään määrittelemään erilaisia toimintaprosessien ja asiakirjojen metatietoja, kuten säilytysaikatietoja.
Tuhoaminen	Asiakirjojen ja niitä vastaavien tietojen hävittäminen siten, että niitä ei voida enää käsitellä tai palauttaa käsiteltävään muotoon. Tuhoaminen voidaan toteuttaa, säilytysmuodosta riippuen, esimerkiksi silppuamalla, polttamalla tai ylikirjoittamalla.
Viranomaisen asiakirja	Viranomaisen hallussa oleva asiakirja, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka asiakirja, joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa sekä asiakirja, joka on laadittu viranomaisen antaman toimeksiannon johdosta tai, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten.

Tietosuojan ja tietoturvan määritelmät ja käsitteet	
Anonymisointi	Henkilötietojen käsitteleminen siten, että tunnistettavuus poistetaan lopullisesti. Yhdistäminen rekisteröityyn ei tämän jälkeen ole enää mahdollista.
Biometrinen henkilötieto	Luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvä teknisellä käsittelyllä saatu henkilötieto, esim. sormenjälkitieto, joka mahdollistaa tunnistamisen tai sen varmistamisen.
Eheys	Tietoturvallisuuden osa-alue, jolla tarkoitetaan sitä, että tieto on suojattu tahalliselta tai tahattomalta muuttamiselta siten, että sen luotettavuus ei vaarannu.
Eriytyinen henkilötieto	Eriyisiä henkilötietoja ovat rotu, etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, joita käytetään henkilön tunnistamiseksi, terveyttä koskevat tiedot sekä luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.
Geneettinen henkilötieto	Luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia koskevat henkilötiedot, jotka on saatu erityisesti kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla.
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
Henkilötietojen käsittelijä	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.
Henkilötietojen käsittely	Toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä on esimerkiksi henkilötietojen kerääminen, tallentaminen, muokkaaminen, haku, käyttö, luovuttaminen tai saattaminen muutoin saataville, yhdistäminen, rajoittaminen tai poistaminen.
Henkilötietojen käsittelyn lainmukaisuus	Henkilötietojen käsittelyn edellytys, joka toteutuu kun henkilötietojen käsittelyyn on rekisteröidyn suostumus, käsittely on määritelty sopimuksessa, käsittely kuuluu rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseen, käsittely on tarpeellista elintärkeiden etujen suojaamiseksi, käsittely tapahtuu yleistä etua

Tietosuojan ja tietoturvan määritelmät ja käsitteet	
	koskevan tehtävä suorittamiseksi tai julkisen vallan käyttämiseksi taikka jos käsittelyn perusteena on rekisterinpitäjän oikeutettu etu.
Henkilötietojen käsittelyn rajoittaminen	Tallennettujen henkilötietojen merkitseminen tarkoituksena rajoittaa niiden myöhempää käsittelyä.
Henkilötietojen tietoturvaloukkaus	Tietoturvaloukkaus, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen käsittely tai pääsy tietoihin.
Henkilötietojen vastaanottaja	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu toimielin, jolle luovutetaan henkilötietoja.
Kolmas osapuoli	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu toimielin, jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.
Kiistämättömyys	Tietoturvallisuuteen liittyvä vaatimus siitä, että tietoihin kohdistetuista toimenpiteistä jää jälki, jota muutoksen tekijä ei voi kiistää.
Lasten henkilötietojen käsittely	Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta.
Luottamuksellisuus	Tietoturvallisuuden osa-alue, jolla tarkoitetaan sitä, että tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeus.
Osoitusvelvollisuus	Rekisterinpitäjän velvollisuus osoittaa, että se on noudattanut henkilötietojen käsittelyssä tietosuojaperiaatteita.
Profilointi	Henkilötietojen automaattista käsittelyä, jossa arvioidaan luonnollisen henkilön ominaisuuksia tai ennakoidaan luonnollisen henkilön eri toimintoihin liittyviä piirteitä.
Pseudonymisointi	Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää luonnolliseen henkilöön käyttämättä lisätietoja. Edellyttää tietojen säilyttämistä erillään ja sen varmistamista, ettei yhdistämistä luonnolliseen henkilöön tapahdu.
Rekisteri	Mikä tahansa jäseneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein.
Rekisterinpitäjä	Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
Rekisteröity	Luonnollinen henkilö, jonka henkilötietoja käsitellään.

Tietosuojan ja tietoturvan määritelmät ja käsitteet	
Saatavuus	Tietoturvallisuuden osa-alue, jolla tarkoitetaan sitä, että tieto on käyttökelpoisessa muodossa ja saatavilla silloin, kun sitä tarvitaan.
Sisäänrakennettu ja oletusarvoinen tietosuoja	Tietosuojaperiaatteiden sisällyttäminen henkilötietojen käsittelyn osaksi koko toimintaketjussa. Periaatteiden huomioiminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä siten, että varmistetaan käsittelyn vastaavuus tietosuoja-asetuksen vaatimusten kanssa. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, joilla taataan rekisteröityjen oikeuksien toteutuminen, tietosuoja-asetuksen vaatimusten toteutuminen koko henkilötietojen käsittelyn elinkaaren ajan, määrittelyvaiheesta hävitykseen, että kerätään vain henkilötietoja, jotka ovat käyttötarkoituksen mukaan välttämättömiä ja tarpeellisia, että tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on käyttötarkoituksen mukaan tarpeellista ja, että huolehditaan, että tiedot ovat käytettävissä asetuksen mukaisissa rajoissa.
Suostumus	Vapaaehtoinen ja yksiselitteinen tahdonilmaus, jolla luonnollinen henkilö hyväksyy henkilötietojensa käsittelyn.
Terveystieto	Luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyvät henkilötiedot, jotka ilmaisevat hänen terveydentilaansa.
Tietosuoja	Toimenpiteet, joilla taataan yksityisyydensuoja ja tietosuojaperiaatteiden toteutuminen henkilötietojen käsittelyssä.
Tietosuojan vaikutustenarviointi	Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin. Jos käsittelytoimet todennäköisesti aiheuttavat yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä riskienhallinnan toimenpiteet. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.
Tietosuojan valvontaviranomainen	Euroopan unionin jäsenvaltion yleisen tietosuoja-asetuksen 51 artiklan perusteella perustama riippumaton viranomainen.
Tietosuojaperiaatteet	Toimenpiteet, joilla taataan henkilötietojen käsittelyssä tietojen lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, säilytyksen rajoittaminen, eheys ja luottamuksellisuus sekä täsmällisyys.

Tietosuojan ja tietoturvan määritelmät ja käsitteet	
Tietosuojaseloste	Asiakirja, joka kuvaa henkilötietojen käsittelyn helposti ymmärrettävässä ja tiiviissä muodossa. Rekisterinpitäjän tulee laatia tietosuojaselosteet ja pitää ne yleisesti saatavilla.
Tietosuojavastaava	Tietosuoja-asetuksessa määritelty rooli, joka rekisterinpitäjän ja henkilötiedon käsittelijän on perustettava, jos tietojenkäsittelyä suorittaa viranomaisen tai julkishallinnon elin pois lukien tuomioistuinin, organisaation ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen laajamittaista säännöllistä ja järjestelmällistä seuranta, organisaation ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin. Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan. Yritysryhmä voi nimittää yhden tietosuojavastaavan samoin kuin yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.
Tietotilinpäätös	Kuvaus, joka on osa tietojohdantamista ja antaa kokonaiskuvan organisaation tietojenkäsittelyn ja tiedonhallinnan nykytilasta. Raportti on tarkoitettu johdon työkaluksi sekä lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa.
Tietoturva	Toimenpiteet, joilla taataan tiedon saatavuus, luottamuksellisuus, eheys ja kiistämättömyys toimintaympäristössä. Sisältää toimenpiteet tietojenkäsittelyn turvaamiseen uhkatekijöiltä ja tietoturvalliset tunnistautumiskäytännöt
Tietoturvallisuustoimenpide	Tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistava hallinnollinen, toiminnallinen ja tekninen toimenpide.
Todennus	Tietoturvallisuuteen liittyvä vaatimus siitä, että käyttäjä voidaan luotettavasti tunnistaa luonnolliseksi henkilöksi tai oikeushenkilöksi.
Tunnistus	Tietoturvallisuuteen liittyvä vaatimus siitä, että tietojärjestelmän käyttäjä liitetään käyttäjätunnukseen.

8 Tiedonhallinnan kansalliset toimijat ja keskeiset säädökset

Alla esitetään taulukko julkisen hallinnon tiedonhallintaa ohjaavista keskeisistä kansallisista toimijoista ja näiden rooleista.

Tiedonhallinnan kansallinen toimija	Rooli
Digi- ja väestötietovirasto	Valtiovarainministeriön hallinnonalaan kuuluva virasto, joka edistää yhteiskunnan digitalisaatiota, turvaa tietojen saatavuutta ja tarjoaa palveluja asiakkaiden elämäntapahtumiin sekä tuottaa julkisen hallinnon tiedonhallintalautakunnalle asiantuntijapalveluita tiedonhallinnan ja tietoturvallisuuden menettelyjen kehittämistä.
Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI)	Valtiovarainministeriön asettama digitaalisen turvallisuuden kehittämistä ja ohjausta tekevä yhteistyö-, valmistelu- ja koordinaatioelin.
Julkisen hallinnon tiedonhallintalautakunta	Valtiovarainministeriössä toimiva asiantuntijaviranomainen, joka ohjaa ja valvoo julkisen hallinnon tiedonhallintaa ja arvioi julkisten toimijoiden tiedonhallintalain mukaisten velvoitteiden toteutumista ja noudattamista.
Kansallisarkisto	Opetus- ja kulttuuriministeriön hallinnonalaan kuuluva virasto, jonka päätehtävänä on kansalliseen kulttuuriperintöön kuuluvien asiakirjojen ja niihin sisältyvien tietojen pysyvän säilymisen ja saatavuuden varmistaminen sekä käytön edistäminen. Toimii arkistoitavien asiakirjojen ja arkistotoimen asiantuntijaviranomaisena.
Kyberturvallisuuskeskus	Liikenne- ja viestintäministeriön hallinnonalaan kuuluvassa Liikenne- ja viestintävirastossa toimiva keskus, joka tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä.
Tietosuojavaltuutettu ja tietosuojavaltuutetun toimisto	Oikeusministeriön yhteydessä toimiva riippumaton tietosuoja-asetuksessa tarkoitettu kansallinen valvontaviranomainen, joka valvoo tietosuoja-asetuksen toteutumista luonnollisten henkilöiden perusoikeuksien ja vapauksien suojaamiseksi henkilötietojen käsittelyssä ja henkilötietojen vapaan liikkuvuuden helpottamiseksi unionissa.

Alla esitetään taulukko julkisen hallinnon tiedonhallintaa säätelevistä ja siihen vaikuttavista keskeisistä säädöksistä erityisesti kaupungin näkökulmasta.

Tiedonhallintaan vaikuttavat keskeiset säädökset
Arkistolaki (831/1994)
Euroopan unionin direktiivi avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (2019/1024)
Euroopan unionin yleinen tietosuoja-asetus (2016/679)
Hallintolaki (434/2003)
Kuntalaki (410/2015)
Laki digitaalisten palvelujen tarjoamisesta (306/2019)
Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Laki sähköisen viestinnän palveluista (917/2014)
Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
Laki viranomaisten toiminnan julkisuudesta (621/1999)
Laki yksityisyyden suojasta työelämässä (759/2004)
Rikoslaki (39/1889)
Suomen perustuslaki (731/1999)
Tietosuojalaki (1050/2018)

9 Versiot ja voimaantulo

Alla esitetään taulukko tämän tiedonhallintapolitiikan versioista ja voimaantulosta.

Versio	Sisältö
6.4.2018	Luonnos. Esitellään seudun tietosuojatyöryhmälle 5/2018.
29.8.2018	Lisätty liitteet: käsitteet ja määritelmät. Poistettu linkit lainsäädäntöön. Johtoryhmäkäsittelyyn 3.9.2018. YT-neuvottelukunta 12.9.2018.
9.10.2018	Ei tekstimuutoksia. Kaupunginhallituksen 15.10.2018 käsittelyyn.
1.2.2021	Muutettu versio luonnoksesta tietoturva- ja tietosuojapolitiikasta tiedonhallintapolitiikaksi esitetty tietosuojavastaavalle.
16.2.2021	Luonnos tiedonhallintapolitiikasta annettu tietohallinnon kommentoitavaksi.
26.3.2021	Luonnos tiedonhallintapolitiikasta annettu hallintojohtajan, talousjohtajan, HR-päällikön ja viestintäpäällikön kommentoitavaksi.
7.5.2021	Luonnos tiedonhallintapolitiikasta annettu pääluottamusmiesten ja työsuojeluvaltuutettujen kommentoitavaksi.
9.11.2022	Luonnos tiedonhallintapolitiikasta käsitelty YT-neuvottelukunnassa.
21.11.2022	Tiedonhallintapolitiikka käsitelty kaupunginhallituksessa.