



MYNÄMÄEN KUNNAN
TIETOTILINPÄÄTÖS
2024

Sisällys

Sisällys.....	1
1 Tietotilinpäätöksen tarkoitus	2
2 Tietosuoja-asioiden vastuunjako	3
2.1 Kunnanhallitus.....	3
2.2 Tietosuojavastaava	3
2.3 Tietosuojaa koskevat vastuut toimialaloilla.....	3
2.4 Tietoturva- ja tietosuojaryhmä	3
2.5 Ulkoistetut kunnan ICT- palvelut	3
3 Tietojen käsittelyyn vaikuttava lainsäädäntö.....	4
3.1 Tietosuojaa määrittelevä keskeinen lainsäädäntö	4
3.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset.....	4
4 Keskeiset toimenpiteet ja muutokset 2024.....	5
5 Rekisteröityjen oikeudet ja niiden toteuttaminen	5
6 Rekisterinpitäjän vastuut ja velvoitteet.....	6
6.1.1 Osoitusvelvollisuus.....	6
6.1.2 Käsittelyn oikeusperusta	6
6.1.3 Tietosuojavastaava	6
6.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja	7
6.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista.....	7
7 Kunnan henkilötietorekisterit ja keskeiset tunnusluvut	7
7.1 Kunnan rekisterinpitäjät	8
8 Tiedon hallinta	9
8.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma.....	9
8.2 Asiakirjajulkaisuuskuvaus.....	9
8.3 Keskeiset tietojärjestelmät.....	9
9 Dokumentaatio ja koulutus	9
10 Rekisterinpitäjän ja -käsittelijän väliset sopimukset	10
11 Tietosuojauksen periaatteet	11
11.1 Suurimmat uhkatekijät	11
11.2 Taphtuneet tietoturvaloukkaukset.....	11
12 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2025.....	12
Liite 1 Kunnan henkilötietoja sisältävien rekisterien luettelo	12
Liite 2 Tietovirroissa hyödynnettävät tietojärjestelmät.....	20

1 Tietotilinpäätöksen tarkoitus

Tietotilinpäätöksen tavoitteena on rakentaa avoimuutta ja luottamusta siihen, että organisaatiossa noudatetaan organisaation luomia tietoturva- ja tietosuojaperiaatteita ja käsitellään henkilötietoja niiden mukaisesti.

Tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja toimenpiteitä. Julkaistavalla tietotilinpäätöksellä halutaan lisätä johdon, luottamushenkilöiden, henkilöstön ja suuren yleisen tietoisuutta tietosuojasta ja tietoturvasta sekä saada näkyvyyttä näiden asioiden eteen tehdystä työstä.

Tietotilinpäätös on keskeinen osa tietosuojan toteutumisen seuranta ja EU:n yleisen tietosuoja-asetuksen (EU 2016/679, jäljempänä tietosuoja-asetus) määrittelemää osoitusvelvollisuutta (5 artikla). Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.

Tietotilinpäätöksen koonnista vastaa kunnan tietosuojavastaava yhdessä hallintojohtajan kanssa. Tietotilinpäätös käsitellään kunnanhallituksessa 17.3.2025.

Tietosuojan toteuttaminen

Tietosuojan toteuttaminen edellyttää jatkuvaa tietosuojaseikkojen huomioimista sekä koko organisaation läpäisevää tietosuojakulttuuria. Käytännön toteutuksen kannalta ensisijaisen tärkeää on johdon tuki tietosuojan edistämisessä.

Kunnan luottamushenkilöt ja henkilökunta ovat sitoutuneet tietosuojan huomioivaan toimintaan ja noudattamaan tietosuojalain mukaisia tietosuojaperiaatteita, jonka mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa
- epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin
- on tarpeen tietojenkäsittelyn tarkoitusten toteutumista varten.

2 Tietosuoja-asioiden vastuunjako

2.1 Kunnanhallitus

Hallintosäännön 8 luvun 1 §:n 5-kohdan mukaisesti kunnanhallitus vastaa siitä, että kunta täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista.

2.2 Tietosuojavastaava

Tietosuoja-asetus velvoittaa kaikkia julkishallintoon kuuluvia organisaatioita nimittämään tietosuojavastaavan. Tietosuojavastaavan tehtäviin kuuluu organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä, tietosuoja-asetuksen noudattamisen valvonta mukaan lukien tähän liittyvät tarkastukset, yhteistyö valvontaviranomaisen kanssa ja rekisteröityjen oikeuksien toteuttamisen tukeminen.

2.3 Tietosuojaa koskevat vastuut toimialaloilla

Jokainen toimiala vastaa siitä, että tietosuoja- ja turva-asiat hoidetaan asetusten ja lakien mukaisesti omalla toimialalla.

Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen, ohjeistus ja asianmukaiset työkalut tietoturvan ja tietosuojan mukaiseen tietojenkäsittelyyn. Heidän tehtävänä on valvoa tietoturvan ja tietosuojan toteutumista omalla toimialallaan ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta.

2.4 Tietoturva- ja tietosuojaryhmä

Kunnan tietosuoja ja –tietoturvatyöryhmänä toimii johtoryhmä. Johtoryhmä käsittelee yleisiä ja koordinoivia vaativia tietosuojaan, tietoturvaan, tiedonhallintaan, riskienhallintaan ja varautumiseen liittyviä asioita. Tarvittaessa johtoryhmän kokouksiin osallistuu tietohallintopäällikkö, tietosuojavastaava ja tarpeen mukaan muita asiantuntijoita eri toimialoilta. Tarvittaessa asiat viedään päätettäväksi ja hyväksyttäväksi kunnanhallitukselle tai lautakuntiin.

2.5 Ulkoistetut kunnan ICT- palvelut

Kunnan tietoturvatyötä tehdään kiinteässä yhteistyössä ulkopuolisen operaattorin kanssa, joka toimittaa kunnan verkkoyhteyden sekä palomuuritoiminnot.

Kunnan tietohallinto vastaa yhdessä toimialojen kanssa tietojärjestelmien toipumis-, varautumis- ja valmiussuunnitelmista.

3 Tietojen käsittelyyn vaikuttava lainsäädäntö

Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista. Tietosuoja-asetuksessa (GDPR) on keskeisenä teemana tietosuojariskien hallinta ja rekisterinpitäjän tilintekokykyisyys-periaate. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation sopimuksissa ja alihankinnoissa on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjän tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat riskit.

3.1 Tietosuojaan määrittelevä keskeinen lainsäädäntö

- Perustuslaki (731/1999)
- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n yleinen tietosuoja-asetus EU 679/2016
- Tietosuojalaki 5.12.2018/1050
- Tiedonhallintalaki (906/2019)
- Arkistolaki (831/1994)
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13
- Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
- Työsopimuslaki (55/2001)
- Rikoslaki (39/1889)

Lisäksi on olemassa runsaasti toimialakohtaista erityislainsäädäntöä, joissa tietojen käsittelyä on säädelty.

3.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset

Muutokset tietosuojalakiin ja rikosasioiden tietosuojalakiin tulivat voimaan 1.1.2024. Muutoksessa selkeytetään henkilötunnuksen käsittelyä koskevaa sääntelyä. Henkilön tunnistamiseen ei saa käyttää yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää.

Euroopan unionin verkko- ja tietoturvadirektiivi eli NIS2-direktiivi astui EU:ssa voimaan 14.12.2023. Hallituksen esitys HE 57/2024 eduskunnalle kyberturvallisuudsdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi on vielä kesken. Hallituksen esityksen perusteella vaikutukset koskevat useita kansallisia lakeja, joista keskeisimpinä ovat uusi kyberturvallisuuslaki sekä uusi tiedonhallintalain (906/2019) 4 a luku.

4 Keskeiset toimenpiteet ja muutokset 2024

1. Julkisten työvoimapalveluiden järjestämisvastuu siirtyi valtiolta kuntien muodostamille työllisyysalueille vuoden 2025 alusta. Mynämäen kunta kuuluu Turun työllisyysalueeseen. Työnhakijoiden, työttömien ja muiden työvoimapalveluja tarvitsevien palvelut tuottaa lähipalveluna Raision kaupungin työllisyyspalvelut. Mynämäen kunnassa toimii työllisyysohjaajan asiointipäivystys. Palvelussa käytössä olevasta Työmarkkinatori järjestelmästä vastaa rekisterinpitäjänä KEHA-keskus. Turun kaupunki ja Raision kaupunki toimivat henkilötietojen käsittelijänä rekisterissä olevien asiakastietojen osalta.
2. Ostolaskujen julkaisu tapahtuu nyt Avoindata.fi-palvelussa. Kunnan vuoden 2024 alkupuoliskon (1–6 kk) laskut on julkaistu ja tästä eteenpäin ostolaskut julkaistaan puolivuositain syksyllä ja keväällä.

Aineistosta on poistettu tietosuojalainsäädännön edellyttämällä tavalla mm. yksityiset henkilöt ja toiminimiyritykset, koska heillä toiminimi on pääsääntöisesti oma nimi. Tiedot on julkaistu Kuntaliiton ohjeistuksen mukaisella tavalla ja tasolla. Palvelussa on julkaistu myös muiden kuntien ostolaskuja.
3. Kaksivaiheisen tunnistautumisen käyttöönotto.
4. Loppuvuonna 2024 otettiin käyttöön Julius –tilavarausjärjestelmä, jolla kunnan toimitilojen (mm. koulujen liikuntatilat) käyttäjät tekevät itse tilavaraukset.

5 Rekisteröityjen oikeudet ja niiden toteuttaminen

EU:n yleinen tietosuoja-asetus sisältää useita artikloja, jotka säätävät rekisteröidylle kuuluvia oikeuksia henkilötietojen käsittelyyn liittyen. Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus:

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy henkilötietoihin
- oikaista henkilötietoja
- poistaa henkilötietoja
- rajoittaa henkilötietojen käsittelyä
- siirtää henkilötiedot järjestelmästä toiseen
- vastustaa henkilötietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisterinpitäjän on toimitettava rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Tiedot on annettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Rekisteröidyllä on oikeuksia liittyen omiin henkilötietoihinsa ja niiden käsittelyyn. Rekisteröidyllä on muun muassa oikeus tietää, käsitelläänkö hänen henkilötietojaan ja mitä henkilötietoja käsitellään sekä pyytää häntä koskevat tiedot itselleen. Lisäksi rekisteröidyllä on oikeus vaatia virheelliset henkilötiedot oikaistavaksi. Muita rekisteröidyn oikeuksia sovelletaan eri tavoin riippuen siitä, mikä on henkilötietojen käsittelyn oikeusperuste. Esimerkiksi oikeutta tietojen poistamiseen ei sovelleta lakisääteisiin rekistereihin.

Tietosuojaselosteet ja tietopyyntölomakkeet löytyvät osoitteesta:

<https://www.mynamaki.fi/kunta-ja-hallinto/paatoksenteko/rekisteriselosteet-ja-tietosuoja/>

Rekisteröidyn pyyntöön vastaus toimitetaan ensisijaisesti sähköisessä muodossa. Rekisteröity voi myös noutaa pyytämänsä tiedot kunnan virastolta tai tiedot voidaan toimittaa hänelle postitse. Asiakkaan henkilöllisyys varmennetaan ennen tietojen antamista.

Rekisteröidyiltä tulleiden pyyntöjen määrä 1.1.2024 – 31.12.2024 välisenä aikana.
Hallinnon toimiala

- tietosuoja-asetuksen mukaiset tietopyynnöt 11 kpl.
- julkisuuslain mukaiset tietopyynnöt 4 kpl.

6 Rekisterinpitäjän vastuut ja velvoitteet

6.1.1 Osoitusvelvollisuus

Tietosuoja-asetus velvoittaa kuntaa osoittamaan noudattavansa tietosuoja-asetusta esimerkiksi dokumentoimalla henkilötietojen käsittelyyn liittyvät prosessit ja muut käytännön tietosuojatoimenpiteet. Osoitusvelvollisuus merkitsee käytännössä sitä, että vain riittävällä ja asianmukaisella dokumentaatiolla ja koulutuksella kunta voi osoittaa toimivansa asetuksen mukaisesti.

6.1.2 Käsittelyn oikeusperusta

Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittelylle on aina nimetty oikeusperusta. Rekisterinpitäjän tulee huolehtia, että henkilötietoja käsitellään vain asianmukaisin edellytyksin ja että tietojenkäsittelyn tarkoitus määritellään jo ennen kuin tietoja ryhdytään käsittelemään.

Tietosuoja-asetuksessa on kuusi eri perustetta, joilla henkilötietojen käsittely on mahdollista:

- rekisteröidyn suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleistä etua koskeva tehtävä tai julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

6.1.3 Tietosuojavastaava

Kunnalla on nimetty tietosuojavastaava, jonka tehtävänkuvaan kuuluu seurata organisaation tietojenkäsittelyyn liittyviä toimintatapoja ja huolehtia, että ne vastaavat asetuksessa tai muualla erityislainsäädännössä säädettyä. Hän myös ohjaa ja auttaa organisaatiota tietosuojaperiaatteiden ja vaatimusten toteuttamisessa, sekä antaa pyydettyä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta. Lisäksi tietosuojavastaava toimii kontaktipisteenä sekä valvontaviranomaiseen että rekisteröityihin.

6.1.4 Sisäänrakennettu ja oletusarvoinen tietosuojaja

Tietosuojaja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta alkaen koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojajan velvollisuuksista voidaan huolehtia, kunnan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

6.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Kunta tekee ilmoituksen henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Tapauksen niin vaatiessa ilmoitus tehdään myös kyberturvallisuuskeskukselle ja poliisille.

Kunnan tulee ilmoittaa rekisteröidylle, jos hänen henkilötietonsa ovat vuotaneet ulkopuolisille luvottomasti. Ilmoitus on tehtävä, jos tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille. Kunnan on tällöin ilmoitettava asiasta ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua mahdollisia tapauksesta koituvia uhkia vastaan.

7 Kunnan henkilötietorekisterit ja keskeiset tunnusluvut

Koko kunnan henkilötietoja sisältävien rekisterien määrä on 53.

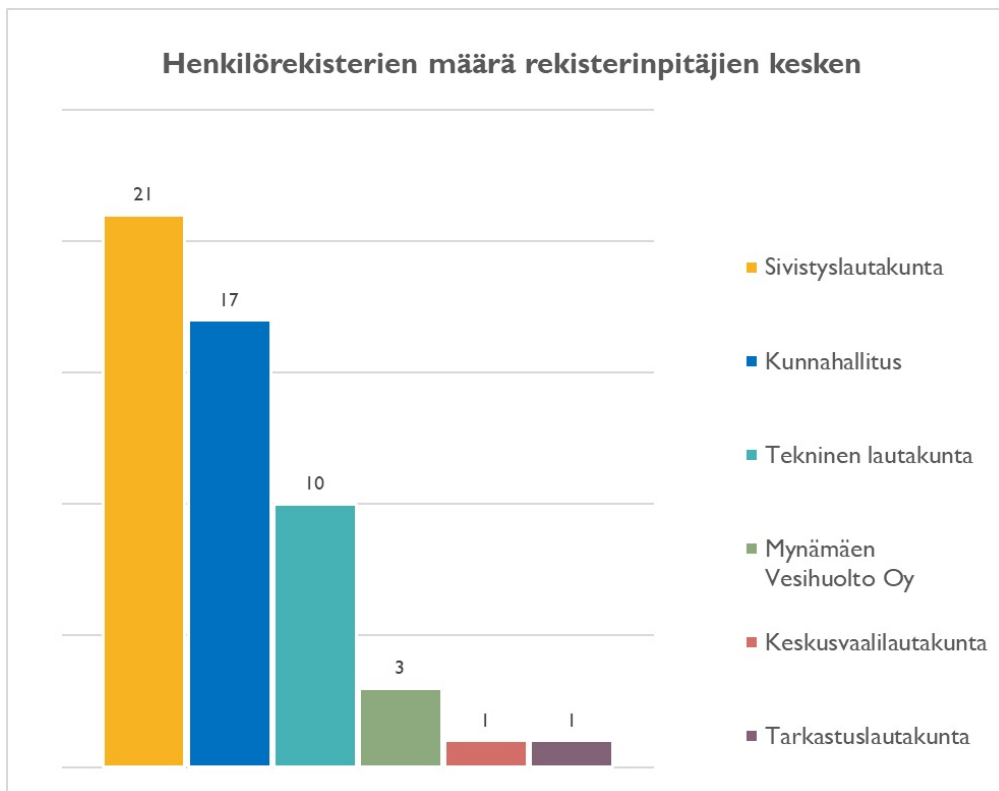
Kunnan henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Kuntalaisten tietoja sisältäviä lakisääteisiä henkilötietorekistereitä kunnassa on 29 kappaletta.
2. Kuntalaisten tietoja sisältäviä rekisteröidyn suostumukseen perustuvia henkilötietorekistereitä kunnassa on 16 kappaletta.
3. Kunnan henkilökuntaa koskevia henkilötietorekistereitä kunnassa on 8 kappaletta.

Kunnan henkilötietoja sisältävien rekisterien luettelo, katso Liite1

7.1 Kunnan rekisterinpitäjät

Rekisterivastuut jakautuvat kunnanhallituksen ja lautakuntien välillä seuraavasti:



Kukin rekisterinpitäjä huolehtii henkilötietojen käsittelystä EU:n tietosuoja-asetuksen ja lainsäädännön vaatimusten mukaisesti. Lisäksi kunnanhallitus velvoittaa kaikkia rekisterinpitäjiä huolehti maan tarvittavasta tietosuojakoulutuksesta ja -ohjeistuksesta.

8 Tiedon hallinta

Tiedonhallinnalla tarkoitetaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaisteistojen, niiden käsittelyvaiheiden ja tietoaisteistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaisteistojen tallentamistavasta ja muista käsittelytavoista. Mynämäen kunnassa tiedonhallintaa kuvataan ja ohjataan tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksella.

8.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma

Tiedonhallintamallissamme kuvataan tiedonhallintayksikön eli Mynämäen kunnan toiminta, tietopääoma ja tietojärjestelmät.

Tiedonohjaussuunnitelmassamme kuvaamme kunnan tehtävät ja käsittelyprosessit, tehtävien hoidossa syntyvän asiakirjallisen tiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat.

Tiedonhallintamallin ja tiedonohjaussuunnitelman ylläpito on jatkuva prosessi, jota päivitetään tehtävien muuttuessa.

8.2 Asiakirjajulkisuuskuvaukset

Asiakirjajulkisuuskuvauksemme antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoja lakisääteisissä tehtävissämme. Asiakirja julkisuuskuvaukset toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön sekä opastaa tietoaisteistojen omatoimisessa haussa ja käytössä.

Asiakirjajulkisuuskuvaukset on saatavilla <https://www.mynamaki.fi/kunta-ja-hallinto/paatoksenteko/asiakirjajulkisuuskuvaukset/>

8.3 Keskeiset tietojärjestelmät

Kunnalla on sekä keskitettyjä koko konsernin tietojärjestelmiä että toimialakohtaisia järjestelmiä. (katso Liite2)

9 Dokumentaatio ja koulutus

Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuojasetusta. Organisatorisiin toimenpiteisiin sisältyvät muun muassa koulutukset ja ohjeistukset, jota kaupungin henkilötietoja käsitteleville työntekijöille annetaan.

Kunnan tietosuojaohjaavana dokumenttina toimii kunnan laatima tietosuojaohjekäsikirja. Tietosuojaohjekäsikirjaa päivitetään säännöllisesti tietosuojaavasta toimesta. Käsikirja sisältää kunnan tietosuojoinen, rekisterikuvaukset, tietosuojan vaikutustenarvioinnit, kriisiviestinnän ohjeet, tietosuojoinen ja tietosuojaavasta tehtävänkuvan.

Kunnan ohjeena on, että kaikkien työntekijöiden, sekä uusien että vanhojen, tulee käydä läpi eOppiva- koulutusympäristön kurssimateriaali. Kurssin lopussa testataan opitun materiaalin ymmärtäminen testillä.

Mynämäen kunnan henkilöstölle järjestettiin vuoden aikana kaksi tietosuojakoulutusta. 7.8.2024 järjestetty koulutus oli suunnattu opettajille ja 18.9.2024 järjestettiin koulutus koko henkilöstölle. Koulutuksen tavoite oli perustiedon jakaminen ja osaamisen kasvattaminen.

Yleisen tietosuojakoulutuksen lisäksi Tietosuojavastaava julkaisee henkilöstölle joka toinen viikko ilmestyvän uutiskirjeen kunnan intranetissä. Uutiskirjeissä on mm. ajankohtaisia tietosuojaan ja -turvaan liittyviä asioita ja vastauksia kunnissa esiin tulleisiin konkreettisiin kysymyksiin.

10 Rekisterinpitäjän ja -käsittelijän väliset sopimukset

Tietosuoja-asetus asettaa velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella, kun joku muu (kuten kunnan palveluntuottaja) käsittelee tietoja rekisterinpitäjän (kunta) puolesta. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään. Tietosuoja-asetuksessa säädetään sopimisvelvoitteen lisäksi tietosuojaa koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia.

Rekisterinpitäjän ja -käsittelijän välisellä sopimuksella (DPA) varmistetaan, että käsittelijä käsittelee henkilötietoja ainoastaan sopimuksessa sovittujen ehtojen mukaisesti.

Sopimuksen tila toimittajakohtaisesti:

Rekisterien määrä	Toimittaja	Vastuutaho kunnassa	Status
8	CGI	kaikki osastot	valmis
2	Google	hallinto-osasto sivistysosasto	valmis
2	THV Turvapalvelut	tekninen osasto	valmis
1	Basware	hallinto-osasto	valmis
1	Microsoft	hallinto-osasto	valmis
1	Innofactor	hallinto-osasto	valmis
1	FCG Finnish Consulting Group Oy	kaikki osastot	valmis
Useita	Useita sähköisiä oppimis-ympäristöjä	sivistysosasto	valmis
1	Visma	sivistysosasto	valmis
1	Anvia Securi	hallinto-osasto	valmis
1	Project-TOP Solutions Oy	hallinto-osasto	valmis
1	Finna	sivistysosasto	valmis
1	Webropol Oy	hallinto-osasto	valmis
1	Pusatec Oy	sivistysosasto	valmis
1	Loihde Trust	hallinto-osasto	valmis
1	3StepIT	hallinto-osasto	valmis
1	Edita Publishing	sivistysosasto	valmis
1	Talent Oy	sivistysosasto	valmis

1	Cloudpermit Oy	tekninen osasto	valmis
1	Oy Matkahuolto Ab	hallinto-osasto	valmis
1	Posti	hallinto-osasto	valmis
1	Tiera/Atea	hallinto-osasto	valmis

11 Tietosuojauksen periaatteet

Mynämäen kunta suhtautuu asiakkaidensa tietojen suojaamiseen sekä tietoturvaan vakavasti.

Tiedon luottamuksellisuus, virheettömyys ja käytettävyys varmistetaan huolellisella käsittelyllä. Henkilötiedot suojataan asianmukaisia teknisiä ja organisatorisia suojakeinoja käyttämällä. Tällaisia keinoja ovat muun muassa palomuurien, salaustekniikoiden ja turvallisten laitetilojen sekä kulunvalvonnan ja turvallisuusjärjestelmien käyttö. Suojakeinoja ovat lisäksi hallittu käyttöoikeuksien myöntäminen ja seuranta, henkilötietojen käsittelyyn osallistuvan henkilöstön osaamisen varmistaminen sekä alihankkijoiden huolellinen valinta.

Tietosuojan keskeinen ohjausdokumentti on kunnan tietosuojakäsikirja, jossa on kuvattu muun muassa vastuut, tietosuojavastaavan rooli, henkilörekisterit tietosuojaselosteineen, toimintaympäristö, rekisteröidyn oikeuksien toteuttaminen ja rekisterinpitäjän sopimusasiat.

11.1 Suurimmat uhkatekijät

Käyttäjätunnuksien kalasteluun tähtäävien viestine määrä on edelleen kasvanut. Tavat, joilla käyttäjätunnuksia yritetään saada haltuun ovat monipuolistuneet ja huijausviestejä tulee sähköpostien, sosiaalisen median ja puheluiden kautta. Uhkaa lisää rikollisten lisääntyvä tekoälyn käyttö, jota voidaan käyttää hyökkäysten automatisointiin ja vakuuttavampien kalastelukampanjoiden luomiseen. Yhtenä suojaavana tekijänä, kunta otti käyttöön kaksivaiheisen tunnistautumisen.

Helmikuussa 2024 nähtiin Suomessa joukko palvelunestohyökkäyksiä, joiden kohteina olivat kotimaiset organisaatiot. Totutusta poiketen mukana oli uusia kohteita esimerkiksi kunta- ja koulutussektorilta. Palvelunestohyökkäykset eivät yleensä riko mitään, mutta kunnan verkkosivusto voi olla hetkellisesti saavuttamattomissa. Kunnan tulee huomioida tämä uusi kuntiin kohdistuva uhka ja varautua palvelunestohyökkäyksiin.

Verkon reunalla sijaitsevien laitteiden haavoittuvuudet, puutteet prosesseissa ja konfiguraatiovirheet altistavat organisaatiot hyökkääjille. Rikolliset havaitsevat ja hyödyntävät haavoittuvuuksia yhä nopeammin. Esimerkiksi etätyön mahdollistava VPN-ratkaisu on yksi kriittisimmistä palveluista, joka kiinnostaa myös rikollisia. Tärkeää onkin huolehtia näiden laitteidentietoturvasta ja pitää päivitykset ajan tasalla.

Riskien osalta yhtenä haavoittuvuutena on poikkeamat, jotka johtunut inhimillisestä virheestä joko järjestelmäasetuksissa, prosessissa tai yksittäisen henkilön työtehtävissä.

11.2 Tapahtuneet tietoturvaloukkaukset

Vuoden 2024 aikana ei tapahtunut yhtään tietosuojaloukkausta, joka olisi vaatinut raportointia tietosuojavaltuutetun toimistolle.

Vuoden 2024 aikana ei myöskään tapahtunut yhtään tietosuojarikkomusta, josta olisi laadittu sisäinen dokumentti tietosuojapoikkeamasta.

12 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2025

1. Kunta tekee selvitystä siirtymisestä Google Workspace -ympäristöstä Microsoft 365 -ympäristöön. Jos siirtyminen Microsoft 365 -ympäristöön hyväksytään, niin työ voidaan aloittaa 2025 aikana.
2. Kunta seuraa NIS2-direktiivin kansallista toteutusta. Hallituksen esityksen ja Kuntaliiton asiantuntijalausunnon mukaan kunnan ei kriittiset toiminnot ovat rajattu direktiivissä julkishallinnon ulkopuolelle. NIS2-direktiivi tulee vaikuttamaan hallituksen esityksen perusteella kansallisesti useihin lakeihin, joista keskeisimpinä ovat uusi kyberturvallisuuslaki sekä uusi tiedonhallintalain (906/2019) 4 a luku.
3. Jatkuvana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.
4. Varhaiskasvatus on ottamassa vuonna 2025 käyttöön toiminnanohjausjärjestelmää, joka yhdistää varhaiskasvatuksen hallinnon, toimintayksiköt ja asiakkaat samaan järjestelmään.