



MYNÄMÄEN KUNNAN
TIETOTILINPÄÄTÖS
2023

Sisällys

Sisällys.....	1
1 Tietotilinpäätöksen tarkoitus	2
2 Tietojen käsittelyyn vaikuttava lainsäädäntö	3
2.1 Tietosuoja määrittelevä keskeinen lainsäädäntö	3
2.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset.....	3
3 Keskeiset toimenpiteet ja muutokset 2023.....	4
4 Rekisteröityjen oikeudet ja niiden toteuttaminen	4
5 Rekisterinpitäjän vastuut ja velvoitteet.....	5
5.1.1 Osoitusvelvollisuus.....	5
5.1.2 Käsittelyn oikeusperusta	5
5.1.3 Tietosuojavastaava	5
5.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja	6
5.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista	6
6 Kunnan henkilötietorekisterit ja keskeiset tunnusluvut	6
6.1 Kunnan rekisterinpitäjät	7
7 Tiedon hallinta	8
7.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma.....	8
7.2 Asiakirjajulkisuuskuvaukset.....	8
7.3 Keskeiset tietojärjestelmät.....	8
8 Dokumentaatio ja koulutus	8
9 Rekisterinpitäjän ja -käsittelijän väliset sopimukset	9
10 Tietosuojauksen periaatteet	10
10.1 Suurimmat uhkatekijät	10
10.2 Tapahtuneet tietoturvaloukkaukset	10
11 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2024.....	11
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 tietosuojaan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja toimenpiteitä. Julkaistavalla tietotilinpäätöksellä halutaan lisätä johdon, luottamushenkilöiden, henkilöstön ja suuren yleisön tietoisuutta tietosuojasta ja tietoturvasta sekä saada näkyvyyttä näiden asioiden eteen tehdystä työstä.

Tietotilinpäätöksen laatiminen ja julkaisu on linjassa tietosuojavaltuutetun suositusten kanssa, joiden mukaan tietotilinpäätöksen laatiminen on yksi tapa toteuttaa tietosuojalainsäädännön edellyttämää rekisterinpitäjän osoitusvelvollisuutta. 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 11.3.2024.

Tietosuojaan toteuttaminen

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

Kunnan luottamushenkilöt ja henkilökunta ovat sitoutuneet tietosuojaan 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 Tietojen käsittelyyn vaikuttava lainsäädäntö

Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista. Tietosuoja-asetuksessa (GDPR) on keskeisenä teemana tietosuariskien 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.

2.1 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.

2.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset

Laki julkisen hallinnon tiedonhallinnasta (906/2019) astui voimaan 1.1.2020. Yleislakina tiedonhallintalaki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteen toimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.

Tiedonhallintalain siirtymäsäännösten mukaan neljäs siirtymäaika päättyi 31.12.2023 seuraaville lain kohdille:

- Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä (22 §)
- Katseluyhteyden avaaminen viranomaiselle (23§)
- Tietoaineistojen luovuttaminen teknisen rajapinnan avulla muille kuin viranomaisille (24§)

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.

3 Keskeiset toimenpiteet ja muutokset 2023

1. Vastuu sosiaali- ja terveydenhuollon ja pelastustoimen järjestämisestä siirtyi 1.1.2023 Varsinais-Suomen hyvinvointialueelle (Varha). Siirron vaikutus henkilötietorekisterien osalta oli pieni, koska suurimaksi osaksi henkilörekistereistä ennen siirtoa vastasi kuntayhtymä Ptky Akseli. Siirron myötä Mynämäen kunnalta poistui 1 henkilörekisteri.
2. Ison haasteen 2023 aiheutti opiskeluhuollon järjestämisen kannalta välttämättömien tietojen luovuttaminen Varhalle, mikä pitkälti johtui kansallisen ohjeistuksen puutteesta. Oppilas- ja opiskelijahuollon tietojen luovuttaminen tai käyttöoikeuksien antaminen mm. Wilmaan nousivat puheenaiheeksi valtakunnallisesti. Käytännön ratkaisut olivat eriäviä kuntien kesken, tämä aiheutti hämmennystä ja epätietoisuutta aina marraskuulle 2023 saakka, jolloin OPH julkaisi ohjeistusta liittyen tietojen luovutukseen koulutuksesta opiskeluhuoltopalveluille. Ohjeistus selvensi käytänteitä, mutta ei poistanut epäselvyyksiä kaikilta osin.
3. Tietosuoja-asetuksen 35. artikla velvoittaa tekemään vaikutuksenarvioinnit (PIA/DPIA) ja ennakko kuulemiset sellaisille prosesseille, joissa henkilötietojen käsittelyyn liittyy riskejä. Kansallinen tietosuojavaltuutetun toimisto on julkaissut vuonna 2021 viralliset ohjeistukset ja työkalut vaikutuksenarvioinnin tekemiseen. 2023 alkuvuodesta valmistui Ilmoituskanavan vaikutuksenarviointi ja sitä päivitetään tarpeen mukaan.
4. Mynämäen kunta osallistui Digi- ja väestötietoviraston TAISTO23 –harjoitukseen 23.11.2023. Taisto on tietosuoja- ja tietoturvaloukkauksia simuloiva valtakunnallinen harjoitus, jossa häiriö- ja poikkeamatilanteissa toimimista harjoitellaan kuvitteellisten häiriötilanteiden kautta, tämä oli toinen kerta, kun Mynämäen kunta osallistui Taisto harjoitukseen.

4 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

Rekisteröityjen informointi on toteutettu kunnan internet-sivuilla löytyvien tietosuojaselosteiden avulla.

Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön rekisterinpitäjälle ensisijaisesti sähköisellä tietojenpyyntö lomakkeella, vapaamuotoisella sähköpostilla tai asioiden henkilökohtaisesti.

Tietosuojaselosteet ja tietopyyntölomakkeet löytyvät osoitteesta:

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

Jos rekisteröity esittää pyynnön sähköisesti, tiedot toimitetaan yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää. Asiakas voi tulla noutamaan pyytämänsä tiedot kunnan virastolta. Tiedot voidaan toimittaa hänelle myös postitse.

Ennen tietojen luovutusta, tietosuojaoikeuksiaan käyttävän rekisteröidyn henkilöllisyys on pystyttävä vahvistamaan.

Rekisteröidyiltä tulleiden pyyntöjen määrä 1.1.2023 – 31.12.2023 välisenä aikana.

Kaikki toimialat

- tietosuoja-asetuksen mukaiset tietopyynnot yhteensä 1
- julkisuuslain mukaiset tietopyynnot 21

5 Rekisterinpitäjän vastuut ja velvoitteet

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 Sisäänrakennettu ja oletusarvoinen tietosuojaja

Tietosuojaja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta alkaen koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojaan 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.

5.1.5 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 tietosuojavaikuttetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaikuttetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.

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.

6 Kunnan henkilötietorekisterit ja keskeiset tunnusluvut

Koko kunnan henkilötietoja sisältävien rekisterien määrä on 48.

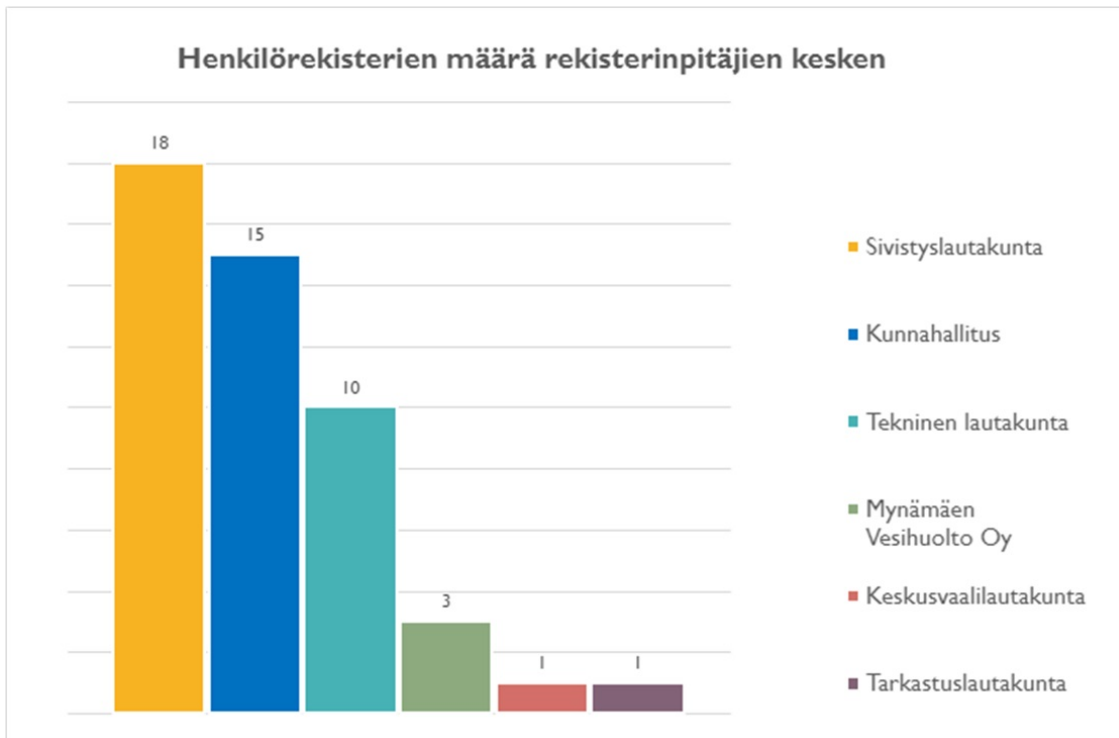
Kunnan henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Kuntalaisia koskevat lakisääteiset henkilörekisterit
Tämä ryhmä sisältää isoimman osat rekistereistä (25 kpl) ja kyseisiä rekistereitä on kaikilla kunnan toimialoilla.
2. Kuntalaisia koskevat rekisteröidyn suostumukseen perustuvat henkilörekisterit
Näitä rekistereistä kunnassa on (17 kpl) ja kyseisiä rekistereitä on usealla kunnan toimialalla.
3. Kunnan henkilökuntaa koskevat rekisterit
Näitä rekistereistä kunnassa on (6 kpl) ja kyseisiä rekistereitä on usealla kunnan toimialoilla.

Kunnan henkilötietoja sisältävien rekisterien luettelo, katso Liite1

6.1 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.

7 Tiedon hallinta

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

7.1 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.

7.2 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 tietojärjestelmien omatoimisessa haussa ja käytössä.

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

7.3 Keskeiset tietojärjestelmät

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

8 Dokumentaatio ja koulutus

Kunnalla on tietosuojakäsikirja, jota päivitetään säännöllisesti tietosuojavastaavan toimesta. Käsikirja sisältää esimerkiksi kunnan tietosuojapolitiikan, rekisterikuvaukset, kriisiviestinnän ohjeet, tietosuojaselosteet ja tietosuojavastaavan tehtävänkuvaukset.

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 tietosuojakoulutus 9.3.2023. Koulutuksen tavoite oli perustiedon jakaminen ja osaamisen kasvattaminen.

Kunnassa työskenteleville työntekijöille järjestetään tarpeen mukaan lisäkoulutusta.

Yleisen tietosuojakoulutuksen lisäksi Tietosuojavastaava julkaisee henkilöstölle joka toinen viikko ilmestyvän uutiskirjeen kunnan intranetissä.

9 Rekisterinpitäjän ja -käsittelijän väliset sopimukset

Tietosuojasetus 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. Tietosuojasetuksessa säädetään sopimisvelvoitteen lisäksi tietosuoja 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	valmis
		sivistysosasto	
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 oppimisympäristöjä	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

10 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, henkilörekisteritietosuojaselosteineen, toimintaympäristö, rekisteröidyn oikeuksien toteuttaminen ja rekisterinpitäjän sopimusasiat.

10.1 Suurimmat uhkatekijät

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.

Erilaiset käyttäjätunnusten kalastelu viestit tulevat pysymään myös vuoden 2024 yhtenä suurimpana jatkuvana uhkana. Uhkaa lisää rikollisten lisääntyvä tekoälyn käyttö, jota voidaan käyttää hyökkäysten automatisointiin ja vakuuttavampien phishing-kampanjoiden luomiseen.

Etätyöskentely on tullut jäädäkseen, vaikka huippulukemat ovatkin jo takanapäin. Hakerit kohdistavat hyökkäyksiään etätyöinfrastruktuureihin hyödyntämällä VPN:ien ja pilvipalveluiden haavoittuvuuksia. Tyypillisesti nämä hyökkäykset johtavat luvattomaan pääsyyn arkaluonteisiin yritysverkkoihin ja -tietoihin ja toimivat siten ransomware-hyökkäysten ensimmäisinä vaiheina. Työntekijöiden ohjeistus tietosuojasta ja tietoturvasta huolehtimiseen tulee pysymään tärkeässä roolissa.

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

10.2 Tapahtuneet tietoturvaloukkaukset

Vuoden 2023 aikana ei tapahtunut yhtään tietosuojaloukkausta, joka olisi vaatinut raportointia tietosuojavaltuutetun toimistolle.

Vuoden 2023 aikana ei myöskään tapahtunut yhtään tietosuojarikkomusta, josta olisi laadittu sisäinen dokumentti tietosuojapoikkeamasta.

11 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2024

1. TE-palvelut 2024-uudistus, jossa työllisyyspalvelut siirtyvät kuntien hoidettaviksi uudistuksen sisällön mukaisesti 1.1.2025 lukien. Tämä uudistus tuo tullessaan merkittäviä tiedonhallinnan kysymyksiä. Mynämäen kunta kuuluu Turun työllisyysalueeseen. Työllisyysalue vastaa tiedonhallinnan asianmukaisesta järjestämisestä. Työllisyysalueelle muodostetaan pienempiä toiminta-alueita. Toiminta-alueiden muodostaminen ja niiden tehtävien määrittely valmistellaan kevään 2024 aikana.
2. Kunta seuraa NIS2-direktiivin kansallista toteutusta. Julkishallinnon osalta soveltamisalaan kuulumista tullaan tarkentamaan tiedonhallintalaissa. NIS2-direktiivi on EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö. Siinä esimerkiksi kiinnitetään huomiota hallinnolliseen tietoturvaan sekä organisaation tietoturvakäytäntöihin ja politiikoihin, kuten kunnan henkilökunnalle suunnattuihin tietoturvaohjeistuksiin ja käytäntöihin. NIS2-direktiivin soveltaminen alkaa 18.10.2024.
3. Jatkovana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.