Tietotilinpäätös 2023

Kunnanhallitus x.x.2024

Sisällysluettelo

1 JOHDANTO 2
1.1 Tietotilinpäätöksen tarkoitus 2
1.2 Organisaation kuvaus 2
2 TIETOVARANNOT 3
2.1 Tiedonhallinta 4
2.2 Tietosuojaselosteet 5
2.3 Seloste käsittelytoimista 5
2.4 Henkilötietojen käsittely 6
2.4.1 Yleisiä käsitteitä 6
2.4.2 Käsittelyperuste 6
3 TIETOJENKÄSITTELYN NYKYTILA KUNNASSA 7
3.1 Kuntalaisille tiedottaminen ja johdolle raportointi 7
3.2 Koulutukset ja tiedottaminen henkilöstölle 7
3.3 Tietosuoja luottamushenkilöille 8
4 TIETOSUOJAN JA TIETOTURVAN TOTEUTUMINEN 8
4.1 Organisaatio ja vastuut 8
4.2 Whistleblowing -ilmoituskanava 9
4.3 Tietoturvan kehittäminen 10
4.4 Tietosuojatyöryhmä 10
4.4.1 Tietosuojavastaava 10
5 TIETOSUOJAN PROSESSIT JA VALVONTA 11
5.1 Tietojen tarkistaminen, korjaaminen ja poistaminen 11
5.2 Tietosuojan toteutuminen 11
5.3 Tietoturvaloukkaus 12
6 TIETOJEN KÄSITTELYN JA TIETOSUOJAN KEHITTÄMINEN 12

1 JOHDANTO

Tietotilinpäätös kuvaa tietovarantoihin, tietojenkäsittelyyn ja tietoturvallisuuteen liittyviä toimintaperiaatteita sekä toteutumia Joutsan kunnassa. Kuntalaki (410/2015) painottaa julkisuusmyönteisyyttä, mutta se ei tarkoita sitä, että kaikkia asioita voidaan käsitellä julkisesti. Kuntalaki säätelee myös luottamushenkilöiden tiedonsaantioikeutta, joka kunnassa on huomioitava.

Kunnan tiedonhallintaa ohjaavat useat eri lait, kuten Laki julkisen hallinnon tiedonhallinnasta (906/2019). Henkilötiedon käsittelyä sääntelee ensisijaisesti EU:n yleinen tietosuoja-asetus (GDPR, EU 680/2016) ja kansallinen Tietosuojalaki (1050/2018) sekä useat toimialakohtaiset erityislait sekä Laki yksityisyyden suojasta työelämässä (759/2004). Asiakirjajulkisuutta sääntelee puolestaan Laki viranomaisten toiminnan julkisuudesta eli niin kutsuttu julkisuuslaki (621/1999) ja sektorikohtainen lainsäädäntö.

EU:n tietosuoja-asetus (GDPR) soveltaminen astui voimaan 25.5.2018 kaikissa EU-maissa ja kansallinen tietosuojalaki Suomessa 1.1.2019.

1.1 Tietotilinpäätöksen tarkoitus

Vuosittain laadittava Joutsan kunnan tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa, arvioi tietosuojan ja tietoturvan toteutumista, tarkastelee tietosuojan valvontaa ja esittelee kehityskohteita. Tietotilinpäätös on kunnan johdolle tarkoitettu tietosuojan seurannan ja kehittämisen työkalu ja sitä voidaan käyttää sisäisen ja ulkoisen valvonnan apuvälineenä.

Tietotilinpäätöksen koonnista vastaa tietosuojavastaava yhdessä tietosuojatyöryhmän kanssa. Tietotilinpäätöstä laadittaessa on huomioitu tietosuojavaltuutetun toimiston ohjeistus sekä kunnan tietosuojavastaavan saama koulutus. Tietotilinpäätöksen hyväksyy kunnanhallitus.

Joutsan kunnan ensimmäinen tietotilinpäätös tehtiin vuodesta 2017, jolloin tietotilinpäätös keskittyi pääasiassa kehittämiskohteisiin. Tämän jälkeen tietotilinpäätöksissä on päästy yhä enemmän tarkastelemaan toimenpiteitä, joita tietosuoja-asetuksen eteen on tehty.

1.2 Organisaation kuvaus

Joutsan kunnan työntekijät joutuvat käsittelemään henkilötietoja työssään useissa tietojärjestelmissä, henkilörekistereissä ja asiakaspalvelussa. Suurin osa henkilötietojen käsittelystä kunnassa perustuu lakiin sekä yleistä etua koskevaan etuun tai julkiseen valtaan.

Viimekädessä vastuu lainmukaisuudesta sekä tietosuojan ja tietoturvan toteutumisesta on organisaation johdolla. Joutsan kuntaan on nimetty tietosuojatyöryhmä, joka omalta osaltaan valvoo tietosuojan toteutumista sekä kehittää tietosuojatyötä. Tietosuojatyöryhmään kuuluvat on alusta asti kuulunut tietosuojavastaava ja tietoturvavastaava sekä johtoryhmän edustajana talous- ja hallintojohtaja. Aiemmin tietosuojatyöryhmässä oli edustaja perusturvasta, mutta perusturvan siirtyessä hyvinvointialueelle oli tarkoituksenmukaista valita tietosuojatyöryhmään edustaja hyvinvointi- ja sivistysosastolta. Kunnanhallitus nimesi uudeksi jäseneksi tietosuojatyöryhmään 8.5.2023 § 95 apulaisrehtori Matti Miettisen.

Tietosuojavastaava toimii mm. yhdyshenkilönä henkilötietojen käsittelijöille (kunnan työntekijät), rekisteröidyille (kuntalaiset) ja valvontaviranomaiselle (tietosuojavaltuutetun toimisto). Tietosuojavastaavan tehtäviin kuuluu myös asiantuntijana ja tiedottajana toiminen, tietosuoja-asetuksen ja –lain noudattamisen valvominen sekä kouluttajana ja neuvonantaja toimiminen. Tietosuojavastaava raportoi säännöllisesti kunnan johdolle tietosuojan toteutumisesta kunnassa.

2 TIETOVARANNOT

Kunnan tietovarannot muodostuvat kunnan lakisääteisten ja kunnan itselleen ottamien tehtävien hoidon eri vaiheista. Tietovarannot löytyvät kunnassa vuonna 2021 käyttöön otetusta tiedonohjaussuunnitelmasta (TOS) ja tämän mukaan kunnan tehtäviä ovat mm.

- Hallintoasia kuten hallintoasioiden ohjaus (mm. vaalien järjestäminen), toiminnan suunnittelu, järjestäminen, toteuttaminen ja kehittäminen, johtaminen ja päätöksenteko, tarkastustoimi ja kotimainen yhteistyö
- Henkilöstöasiat kuten henkilöstöasioiden ohjaus, palvelussuhdeasiat, palkan, palkkioiden ja korvausten maksaminen, osaamisen kehittäminen ja työhyvinvoinnin edistäminen
- Talousasiat, verotus ja omaisuuden hallinta kuten talousasioiden ohjaus, talouden suunnittelu ja seuranta, verotus, rahoitus ja varainhallinta, kirjanpito ja maksuliikenne, omaisuuden hallinta, hankintatoimi ja omien palvelujen ja tavaroiden myynti
- Lainsäädäntö ja lainsäädännön soveltaminen
- Ulkopolitiikka ja kansainvälinen toimista kuten maahanmuuttopolitiikka ja kansainväliseen toimintaan osallistuminen
- Sosiaalihuolto kuten sosiaalihuollon yleinen järjestäminen, ikäihmisten, työikäisten ja lapsiperheiden palvelut, lastensuojelu, päihdehuolto ja vammaispalvelut
- Terveydenhuolto kuten terveydenhuollon yleinen järjestäminen
- Tiedonhallinta ja viestintäpalvelut kuten tiedonhallinnan ja viestintäpalveluiden ohjaus, viestintä ja tiedottaminen sekä tietojärjestelmien kehittäminen ja ylläpito
- Liikenne kuten liikenteen suunnittelu ja kehittäminen sekä liikennepalvelut
- Turvallisuus ja yleinen järjestys kuten väestönsuojelu ja poikkeusoloihin varautuminen
- Maankäyttö, rakentaminen ja asuminen kuten maankäytön, rakentamisen ja asumisen ohjaus sekä kaavoitus
- Ympäristöasiat kuten ympäristöasioiden ohjaus, suunnittelu ja kehittäminen, ympäristövalvonta, ympäristöterveydenhuolto, vesi- ja jätevesihuollon järjestäminen, toteuttaminen ja toiminta sekä jätehuollon järjestäminen ja toteuttaminen

- Opetus- ja sivistystoimi kuten opetus- ja sivistystoimen yleinen järjestäminen, ohjaus ja organisointi, oppilasasiat, opetuksen toteuttaminen, kirjasto- ja kulttuuripalvelut, liikunta- ja vapaa-ajanpalvelut, nuorisoasioiden palvelut sekä varhaiskasvatus ja vapaa sivistystyö
- Tutkimus- ja kehittämistoiminta, niiden suunnittelu, järjestäminen ja toteuttaminen
- Elinkeino- ja työvoimapalvelut kuten elinkeino- ja työvoimapalveluiden ohjaus, yritystoiminnan ja matkailun edistäminen sekä työvoimapalvelut

2.1 Tiedonhallinta

Kunnassa aloitettiin tiedonohjaussuunnitelman (TOS) laatiminen syksyllä 2020, joka saatiin valmiiksi keväällä 2021. Vuonna 2019 asetettu laki julkisen hallinnon tiedonhallinnasta (906/2019) määrittelee tarkoituksen seuraavasti:

- varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi
- mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hallinnon asiakkaille hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti
- edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta.

Asiakirjahallinnon ja arkistotoimen päätehtäviä ovat aineistojen säilyttäminen, käytettävyys ja todistusvoima. Sähköisen toimintaympäristön tiedonhallintaa ohjataan tiedonohjaussuunnitelmalla (TOS). Tiedonohjaussuunnitelma tulee laatia silloin kun siirrytään sähköisiin käsittelyprosesseihin, tietojärjestelmiin halutaan toteuttaa asiakirjallisten tietojen hallinnan automaattinen ohjaus ja kun organisaatio haluaa tietojärjestelmiensä täyttävän asiakirjallisten tietojen osalta laatuvaatimukset.

Hyvä tiedonhallintatapa edellyttää, että organisaatio arvioi asiakirjojen ja tietojärjestelmiin tallennettujen tietojensa merkityksen lainsäädännön, oman toimintansa ja tutkimuksen tietotarpeiden näkökulmasta. Asiakirjojen hallintaa ohjaa kunnassa virallisesti vahvistetun arkistonmuodostussuunnitelman (AMS). Tiedonohjaussuunnitelmassa pystytään määrittelemään mm. asiakirjatyypit, niiden luonne ja säilytysajat. Säilytysajat ovat aina vähimmäissäilytysaikoja, joita ei saa alittaa. Asiakirjoja ei myöskään saa hävittää ennen kuin asia, johon ne liittyvät, on käsitelty loppuun. Hävittämiselle pitää löytyä aina perusteet. Tässä tulee huomioida mm. tietosuoja-asetus (5 artikla), joka määrittelee, ettei esim. henkilötietoja sisältäviä asiakirjoja tai rekistereitä ei tule säilyttää pidempää aikaa kuin on niiden käytön kannalta tarpeen.

Joutsan kunnan asiakirjajulkisuuskuvaus löytyy kunnan nettisivuilta, jossa osana on kunnan tietovarannot ja rekisterit.

2.2 Tietosuojaselosteet

Joutsan kunnan tietovarannot koostuvat mm. useista rekistereistä. Kunnassa päivitettiin vanhat rekisteriselosteet tietosuojaselosteiksi vuonna 2018, jonka jälkeen niitä on päivitetty aina tarpeen tullen. Tietosuojaselosteet tarkistetaan vähintään kerran vuodessa tietosuojavastaavan toimesta. Selosteiden tarkistamisen käytännön työn on tehnyt yhteistyössä tietosuojavastaava aina kyseisen tietosuojalosteen rekisterin pääkäyttäjän, osastopäällikön ja esihenkilön kanssa.

Tietosuoja-asetuksen 12 artiklan mukaan henkilötietojen käsittelijän tulee esittää käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tietosuojaselosteet on tallennettu kunnan verkkolevylle ja intraan, josta kunnan työntekijä voi ne tarvittaessa tarkistaa ja tulostaa. Tietosuojaselosteen voi pyytää nähtäväksi kunnan asiointipisteeltä (Länsitie 5) tai pyytää sähköpostitse kirjaamosta (kirjaamo@joutsa.fi). Tietosuojaselosteet on laadittu tietosuojavaltuutetun toimiston ohjeiden mukaan.

Tietosuojaselosteet ovat osa kunnan informointivelvollisuutta. Rekisteröidyillä on oikeus tietää, mihin tarkoitukseen hänen henkilötietojaan kerätään sekä miten niitä käsitellään. Tietosuojaselosteesta käy ilmi mm. henkilötietojen käsittelyn tarkoitus, rekisterin tietosisältö, tietolähteet ja tietojen säilyttäminen, suojauksen periaatteet sekä rekisteröidyn oikeudet. Tietosuojaselosteet ovat julkisia asiakirjoja. Työntekijöiden tulee pystyä vastaamaan rekisteröidyille rekisteriin liittyviin kysymyksiin, jolloin hän voi apuna käyttää tietosuojaselostetta tai olla tarvittaessa yhteydessä kunnan tietosuojavastaavaan.

Tietosuojavastaava on laatinut kunnalle yleisen pohjan tietosuojaselosteelle, jolloin uusista rekistereistä on helppo tehdä tietosuojaselosteet. Uusin rekistereihin tietosuojaselosteet laativat rekisterin pääkäyttäjä yhdessä tietosuojavastaavan kanssa.

2.3 Seloste käsittelytoimista

Seloste käsittelytoimista on kirjallinen kuvaus organisaation tekemästä henkilötietojen käsittelystä. Kunnassa on tietosuoja-asetuksen 30 artiklan määrittelemä velvollisuus laatia seloste käsittelytoimista. Asetuksen mukaan selosteen on sisällettävä mm. rekisterinpitäjän ja tietosuojavastaavan yhteystiedot, käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja kuvaus teknisistä ja organisatorisista turvatoimista.

Seloste käsittelytoimista on kunnan omaan käyttöön laadittu sisäinen asiakirja. Se edistää kunnan osoitusvelvollisuuden toteutumista. Selostetta voidaan käyttää rekisteröidyille suunnatun informaation tuottamiseen, vaikka sitä suoraan ei ole tarkoitettu rekisteröidyn informointiin. Joutsan kunnassa rekisteröidyn informointiin käytetään ensi sijassa tietosuojaselosteita. Seloste käsittelytoimista voidaan tarvittaessa toimittaa valvontaviranomaiselle.

Tietosuojavastaava on laatinut Joutsan kunnalle selosteen käsittelytoimista. Seloste on tallennettu kunnan verkkolevylle sekä intranettiin työntekijöiden saataville. Seloste käsittelytoimista on päivitetty syksyllä 2023 ja sen päivittämisestä huolehtii tietosuojavastaava.

2.4 Henkilötietojen käsittely

2.4.1 Yleisiä käsitteitä

Tietosuoja-asetuksen 4 artiklassa on määritelty tietosuoja-asetuksessa käytettäviä käsitteitä. Asetuksen mukaan henkilötietona pidetään merkintää, jonka perusteella henkilö voidaan tunnistaa. Henkilö voidaan tunnistaa suoraan tai epäsuorasti eli myös tietoja yhdistelemällä. Henkilötunnus on tehty henkilön yksilöintiin eikä henkilötunnusta yksinään voida pitää henkilön tunnistamiseen riittävänä.

Henkilötietojen käsittelynä pidetään kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin, kuten henkilötietojen kerääminen, tallettaminen, käyttäminen, muuttaminen ja poistaminen. Henkilörekisteri on henkilötietoja sisältävät tietojoukko, teknisesti esim. paperinen nimilista tai asiakastietojen hallintaan käytettävä ohjelmisto. Joutsan kunnalla on myös yhteisrekistereitä, jolloin samaa rekisteriä käyttää esim. palvelun tarjoaja ja palveluntuottaja. Kunnalla on yhteisrekisteri mm. Keski-kirjastojen kanssa sekä Joutsan seurakunnan kanssa yhtenäiskoulun iltapäiväkerhon asiakkaista.

Tietosuoja-asetuksessa on määritelty erityiset henkilötiedot, joiden käsittely saattaa aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja –vapauksille ja johtaa syrjintään. Kunnassa erityisiä henkilötietoja käsitellään etenkin perusturvaosastolla. Lisäksi tietosuoja-asetus antaa erityistä suojaa lasten henkilötiedoille. Tietosuojalain § 5:ssä on määritellyt Suomessa lapsen iäksi 13-vuotta, jolloin alle 13-vuotiaan henkilötietoja ei saa käsitellä ilman huoltajan suostumusta.

2.4.2 Käsittelyperuste

Henkilötietojen käsittelyperusteet on määritelty tietosuoja-asetuksen 6 artiklassa. Kunnassa henkilötietojen käsittely perustuu usein lakisääteisen velvoitteen noudattamiseen tai yleiseen etuun ja julkiseen valtaan. Kunnalla on monissa tapauksissa tehtävään perustuva oikeus henkilötietojen käsittelyyn eli laissa määrätyn tehtävän hoitaminen edellyttää henkilötietojen käsittelyä. Yleistä etua koskevaa käsittelyä kunnassa käytetään mm. tilastointiin. Yleistä etua koskeva tehtävä tai julkinen valta on täytynyt antaa lailla tai muulla oikeudellisella säännöksellä.

Työntekijöillä on oikeus käsitellä vain työssään välttämättömiä henkilötietoja. Esihenkilöt myöntävät työntekijöille käyttöoikeudet niihin tietojärjestelmiin, joita he työssään tarvitsevat. Kunnan henkilöstön koulutuksissa on painotettu sitä, että työntekijän tulee kiinnittää huomiota miten ja missä henkilötietoja käsittelevät, mitä tietoja käsittelevät sekä kenelle henkilötietoja luovuttavat.

Työntekijöiden tulee huomioida henkilötietoja käsitellessään laki viranomaisen toiminnan julkisuudesta (621/1999) ja sieltä etenkin salassapitoon liittyvät § 22-25. Työntekijöiden tulee huolehtia salassapito- ja vaitiolovelvollisuudesta käsitellessään erityisiä henkilötietoja tai muutoin salaisiksi määriteltyä tietoja.

Kunnan luottamushenkilöt, kuten valtuutetut, joutuvat myös käsittelemään tehtävässään henkilötietoja tai muita luottamuksellisia tietoja. Luottamustoimen vastuullinen hoitaminen tarkoittaa sitä, että kaikessa toiminnassa noudatetaan lakeja, määräyksiä, kunnan hallintosääntöä ja muita organisaation ohjeita, täysin samoin kuin kunnan työntekijät ja viranhaltijatkin. Julkishallinnon organisaatioiden luottamushenkilöillä on lisäksi poliittinen ja eettinen vastuu toiminnastaan. Luottamushenkilönä toimit virkavastuun alla ja vastaavat näin itsenäisesti myös tietosuojalakien noudattamisesta.

3 TIETOJENKÄSITTELYN NYKYTILA KUNNASSA

Kunnalla on julkisena toimijana lakisääteinen velvollisuus nimetä tietosuojavastaava (tietosuoja-asetus 37 artikla). Kunnanhallituksen päätöksen mukaisesti (khall 29.1.2018 § 15) kunnan tietosuojavastaavana toimii Liisa Alfthan. Kunnan tietosuojatyöryhmässä tietosuojavastaavan lisäksi ovat tietoturvavastaava eli ICT-asiantuntija, johtoryhmän edustajana talous- ja hallintojohtaja (khall 13.8.2018 § 175) ja hyvinvointi- ja sivistysosaston edustajana apulaisrehtori Matti Miettinen (khall 8.5.2023 § 95).

3.1 Kuntalaisille tiedottaminen ja johdolle raportointi

Kunnan nettisivuilla (https://www.joutsa.fi/kunta-ja-hallinto/tietosuoja/) tiedotetaan kuntalaisia mm. heidän tarkastusoikeudestaan omiin tietoihin. Omien henkilötietojen tarkastus, korjaamis- ja poistamispyyntöihin löytyy sähköiset lomakkeet kunnan nettisivuilta.

Kunnan tietosuojavastaavan työpiste on kunnan virastotalolla, joten hän on helposti myös kuntalaisten tavoitettavissa. Kunnan verkkosivuilla on tietosuojavastaavan yhteystiedot.

Kunnanhallitus hyväksyi kokouksessaan 8.5.2023 § 96 tietotilinpäätöksen vuodelta 2022.

3.2 Koulutukset ja tiedottaminen henkilöstölle

Kunnan työntekijät on koulutettu ja ohjeistettu henkilötietojen käsittelystä. Rekrytointisuunnitelmassa, joka otettiin kunnassa käyttöön vuonna 2020, on liitetty tietosuoja, tietoturva ja henkilötietojen käsittelyn ohjeistus uudelle työntekijälle. Myös henkilöstöoppaassa on koottuna tärkeimmät huomiot niin tietoturvasta kuin henkilötietojen käsittelystäkin. Näin jokainen kunnassa aloittava työntekijä saa perustiedot tietosuojaan liittyen.

Kunnan intrasta löytyy työntekijöille tietosuojaselosteiden ja käsittelytoimien selosteen lisäksi perehdytykseenkin liittyvä ohjeistus henkilötietojen käsittelystä sekä tietosuojaan ja –turvaan liittyvät ohjeistukset. Intraan lisätään tietosuojan ajankohtaiset asiat.

Kunnan toimipisteillä on vuosittain mahdollista pyytää tietosuojavastaava pitämään henkilöstölle tietosuojakoulutusta. Marraskuussa 2023 pidettiin henkilöstölle kaksi samansisältöistä sisäistä tietosuojakoulutusta henkilötietojen käsittelystä Teams-yhteydellä. Koulutuksen materiaali on henkilöstön käytettävissä intrassa.

Kunnan tietosuojavastaava osallistui aktiivisesti tietosuojavastaavien verkoston Teams-kokouksiin ja keskusteluin.

3.3 Tietosuoja luottamushenkilöille

Kunnan tietosuojavastaava oli kevään 2021 mukana tietosuojavastaavien verkoston yhteisissä Teams-palavereissa, joissa suunniteltiin tietosuojaohjeistusta luottamushenkilöille. Tämän pohjalta tietosuojavastaava laati uusille valtuutetuille ja muille luottamushenkilöille tietosuojaohjeen jaettavaksi syksyllä 2021.

Kunnassa on tehty päätös hankkia kaikille valtuutetuille ja lautakuntien varsinaisille jäsenille tabletit sekä @joutsa.fi -sähköpostiosoitteet. Näin luottamushenkilöille pystyttiin takaamaan henkilökohtainen ja turvallinen työväline luottamustehtävän hoitamiseen. Luottamushenkilöiden saaneen ohjeistuksen mukaan näitä tulee käyttää vain kyseisen tehtävän hoitamiseen eikä laitteisiin saa asettaa esim. henkilökohtaisia sähköposteja tai muita ohjelmia.

4 TIETOSUOJAN JA TIETOTURVAN TOTEUTUMINEN

4.1 Organisaatio ja vastuut

Tietoturvaa ja tietosuojaa johtaa ja valvoo kunnanhallitus. Kunnanhallitus nimeää tietoturvavastaavan, tietosuojavastaavan ja tietosuojatyöryhmän.

Tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta kunnassa sekä raportoinnista vastaa kunnan johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa tietoturvavastaava. Hän vastaa myös tietoturva-asioiden tiedottamisesta kunnan ulkopuolelle ja kunnan sisällä yleisellä tasolla. Tietosuojavastaava seuraa henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet sekä toimii valvontaviranomaisen sekä rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietoturva- ja tietosuoja-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esihenkilö yhdessä tietoturvavastaavan ja tietosuojavastaavan avustuksella. Jokainen kunnan työntekijä, luottamushenkilö, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan ja –suojan toteuttamisesta sekä niihin liittyvien ohjeiden noudattamisesta. Työntekijät ovat velvollisia ilmoittamaan tietoturvaan liittyvistä uhista ja poikkeamista esihenkilölleen tai tietoturvavastaavalle.

Käyttöoikeudet järjestelmiin annetaan työtehtävän mukaan ja esihenkilö määrittelee työntekijälle annetut oikeudet. Järjestelmien pääkäyttäjät huolehtivat, että työntekijällä on oikeudet työssään tarpeellisiin tietoihin. Työntekijän tulee huomata, että käyttöoikeus ei anna oikeutta käsitellä tietoa, jota ei työssään tarvitse, vaikka tietoon pääsisikin käsiksi.

4.2 Whistleblowing -ilmoituskanava

Ilmoittajansuojelulaki eli laki Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta on astunut voimaan 1.1.2023 ja sen soveltaminen tuli ottaa kunnissa käyttöön 17.12.2023 mennessä. Joutsan kunnassa whistleblowing-ilmoituskanava otettiin käyttöön henkilöstölle 5.10.2023 ja se löytyy helposti intran etusivulta oman painikkeen takaa.

Ilmoittajansuojaa koskevan lainsäädännön tarkoituksena on varmistaa, että henkilö, joka työnsä yhteydessä havaitsee tai epäilee yleisen edun vastaista toimintaa erikseen määritellyillä EU:n oikeuden aloilla, voi ilmoittaa asiasta turvallisesti ilman pelkoa ilmoituksen takia häneen kohdistuvista mahdollisista seuraamuksista. Väärinkäytösten ilmoituskanava on eettisten periaatteiden ja luottamuksen ylläpitämiseen sekä väärinkäytösepäilyistä ilmoittamiseen tarkoitettu kanava.

Ilmoituskanavan soveltamispiiriin kuuluvat lain laiminlyönnit mm. julkisista hankinnoista, rahanpesusta, liikenneturvallisuudesta, ympäristönsuojelusta, elintarviketurvallisuudesta, kuluttajansuojasta ja yksityisyyden ja henkilötietojen suojasta sekä verkko- ja tietojärjestelmien turvallisuudesta. Tehty ilmoitus antaa kunnalle mahdollisuuden selvittää ja korjata epäkohtia.

Whistlebowing-kavanalla ilmoittajan suojelun edellytyksenä on, että ilmoitus koskee tekoa tai laiminlyöntiä, jotka on säädetty rangaistaviksi, joista voi seurata rangaistusluonteinen hallinnollinen seuraamus, tai jotka voivat vakavasti vaarantaa lainsäädännön yleisen edun mukaisten tavoitteiden toteutumista. Ilmoittaminen koskee sekä kansallisen että EU-lainsäädännön rikkomista. Muista rikkomuksista tai laiminlyönneistä ilmoittaminen ei ole ilmoittajansuojelulain piirissä.

Ilmoituskanava ei ole palautekanava vaan tarkoitettu väärinkäytösepäilyistä ilmoittamiseen. Esimerkiksi henkilöstöasioiden tai henkilötietojen käsittelyyn liittyviä ilmoituksia ei hoideta ilmoituskanavan kautta, koska työ- ja virkasuhteita koskevan lainsäädännön ja virka- ja työehtosopimusten asiat eivät ole ilmoittajansuojelulain piirissä. Kaikissa henkilöstöasioita koskevissa tilanteissa, esimerkiksi epäasiallista toimintaa ja työturvallisuutta koskevat ilmoitukset, tulee ilmoittaa muita kunnan henkilöstölle tarkoitettuja kanavia pitkin. Näitä ovat muun muassa Ilmoitukset työsuojelulle -lomakkeet tai yhteydenotto tietosuoja- tai työsuojeluvaltuutetuille.

Ilmoittajansuojakanavaa ei ole tarkoitettu myöskään laskutukseen tai sopimusehtoihin liittyvän asiakas- tai toimittajapalautteen antamiseen. Tahallisten väärien ilmoitusten tekeminen on kiellettyä ja ne voivat johtaa oikeudellisiin seuraamuksiin.

Kunnan työntekijä voi jättää ilmoituksen joko omalla nimellä tai anonyymisti. Kaikki ilmoitukset käsitellään luottamuksellisesti eikä ilmoituksen tekijää voi jäljittää. Kunnassa ilmoituskanavaan tulleet ilmoitukset tulevat tietosuoja- ja tietoturvavastaavalle sekä viestintäsuunnittelijalle. Vähintään kaksi heistä käsittelee jokaisen ilmoituksen ja tekee tarvittavat toimenpiteet. Vuoden 2023 aikana ilmoituskanavaan tuli kaksi ilmoitusta, joista kumpikaan ei kuulunut whistleblowing-ilmoituskanavaan, mutta ne käsiteltiin siirtämällä palaute oikeaan kanavaan.

Kuntalaiset ja kunnan luottamushenkilöt eivät voi ilmoittaa kunnan sisäisen ilmoituskanavan kautta, mutta he voivat tehdä ilmoituksen oikeuskanslerinviraston keskitettyyn ilmoituskanavaan.

4.3 Tietoturvan kehittäminen

Lisääntyneiden riskien vuoksi tietoturva on aktiivisen kehittämisen kohteena. Tämä koskee niin päätelaitteita kuin järjestelmiäkin. Laitteiden etähallittavuuden kehittämistä on jatkettu vuonna 2023.

Eurooppalainen kyberturvallisuusdirektiivi NIS2 tulee voimaan syksyllä 2024 ja se vaatii menettelytapojen luomista, dokumentointia ja tiedottamista. Direktiivi pyrkii siihen, että yhteiskunnan kannalta kriittiset organisaatiot ovat valmistautuneita kyberrikollisten mahdollisesti aiheuttamiin häiriöihin.

Tekoäly tulee muuttamaan lähivuosina ennennäkemättömällä tavalla tietotyötä. Tekoälyyn käyttöönottoon on alettu valmistautumaan tekemällä tietotekniseen infrastruktuuriin tarvittavat muutokset. Tekoälyn käyttöön tulee luoda politiikat ja toimintamallit sekä testata työkalut ennen laajempaa käyttöönottoa.

Tietojenkalastelu on päivittäistä ja sitä voidaan tukea tekoälyllä. Kun tekoälyä käytetään tällaiseen, onnistumisprosentilla ei ole merkitystä, kunhan yksikin käyttäjä saadaan lankeamaan. Tekoälyn tuottamaan tietojenkalasteluun voidaan vastata vain tekoälyllä, joka tunnistaa tällaiset kampanjat. Tällaisten tietojärjestelmien rakentaminen on yksittäiselle pienelle kunnalle täysin mahdotonta ja vaatii palveluostoja eri kokoluokan toimittajilta.

Deepfake-tyyppiset kampanjat ovat lisääntymässä. Deepfakella voidaan tuottaa puhetta, videota tai muuta tuotosta, joka matkii taitavasti alkuperäistä tuotosta, mutta tarkoitus on vahingollinen. Näiden välttäminen vaatii mm. maksatusprosessien lähikäyntiä.

4.4 Tietosuojatyöryhmä

Tietosuojatyöryhmän tehtävänä on tietoturvan ja tietosuojan kehittämiseen liittyvät linjaukset ja ohjeistukset ennen kuin ne esitellään johdolle hyväksyttäväksi. Lisäksi tietosuojatyöryhmä käsittelee kokouksissaan mm. tietoturvaloukkaukset ja niihin liittyvät toimenpiteet sekä muut tietosuojaan ja –turvaan liittyvät ajankohtaiset asiat.

Tietosuojatyöryhmä on kokouksissaan käynyt läpi tietosuojan toteutumista kunnassa, koulutusten materiaalia sekä tietopyyntöihin ja tietosuojarikkomuksiin liittyviä tilanteita. Tietosuojavastaava kirjaa muistion kaikista tietosuojatyöryhmän kokoontumisista.

4.4.1 Tietosuojavastaava

Kunnanhallituksen kokouksessa 29.1.2018 § 15 tietosuojavastaavaksi nimitettiin Liisa Alfthan.

Tietosuojavastaava toimii kokoonkutsujana tietosuojatyöryhmän kokouksissa sekä kirjoittaa muistion niistä. Kunnan johto antaa tietosuojavastaavalle riittävät resurssit tehtävän hoitamiseen. Tietosuojavasta toimii kunnassa tietosuojan asiantuntijana, kouluttajana ja neuvonantajana, valvojana sekä yhdyshenkilönä niin henkilötietojen käsittelijöille, rekisteröidyille kuin valvontaviranomaiselle.

5 TIETOSUOJAN PROSESSIT JA VALVONTA

5.1 Tietojen tarkistaminen, korjaaminen ja poistaminen

Rekisteröidyillä on oikeus saada pääsy tietoihin sekä oikaista ja poistaa henkilötietojaan rekisteristä tietyissä tapauksissa. Rekisteröityä koskevat virheelliset ja epätarkat henkilötiedot on mahdollista korjata rekisteröidyn pyynnöstä. Lisäksi on mahdollista, että asiakkaan puuttuvia henkilötietoja lisätään tai virheellisiä tietoja poistetaan. Oikeus tulla unohdetuksi eli henkilötietojen poistaminen rekisteristä on joissakin tilanteissa mahdollista. Rekisteröidyllä ei kuitenkaan ole oikeutta saada tietojaan pois rekisteristä, jos tietojen käsittely perustuu esim. lakiin.

Tietosuojatyöryhmä on laatinut tietojen tarkastamiseen, korjaamiseen ja poistamiseen prosessikaavion. Kuntaan laadittiin myös omat lomakkeet tietopyyntöjä varten. Lomakkeet löytyvät kunnan nettisivuilta (https://www.joutsa.fi/kunta-ja-hallinto/tietosuoja/) sekä kunnan asiointipisteeltä (Länsitie 5). Kunnan nettisivuilla on myös ohjeistettu kuntalaisia, kuinka tietopyyntö kuntaan tulee jättää. Tietopyyntö jätetään kunnan tietosuojavastaavalle osoitettuna. Tietopyynnön vastaanottajan tulee varmistaa tietopyynnön jättäjän henkilöllisyys.

Kunta vastaa rekisteröityjen tietopyyntöihin asetuksen määrittämässä ajassa eli kuukauden sisällä. Tietyissä tapauksissa kunnalla on mahdollisuus kieltäytyä tietojen antamisesta, jolloin kieltäytymisen tulee perustua lakiin ja siitä tulee antaa rekisteröidylle kirjallinen tieto. Mikäli rekisteröidyn tietopyyntö on vaativa ja monimutkainen, voi kunta ilmoittaa pyytäjälle perusteluineen käsittelyn kestävän pidempään kuin 30 pv, jatkoaika on kuitenkin enintään kaksi kuukautta.

Tietojen pyytäminen on pääsääntöisesti maksutonta, mutta kunnanhallituksen päätöksen (§ 113/2018) mukaan jatkuvista ja työllistävistä tietopyynnöistä kunta perii 100 € käsittelymaksun.

Tietosuojavastaava kirjaa kaikki tietopyynnöt ja niihin liittyvät toimet on Dynasty-asiakirjahallintaohjelmaan. Tietopyynnöissä sovelletaan tietosuoja-asetusta ja lakia sekä pyynnöstä riippuen myös muita lakeja, esim. hallintolakia (434/2003) ja lakia potilaan asemasta ja oikeuksista (785/1992).

Vuoden 2023 aikana ei tullut yhtään tietosuoja-asetuksen mukaista tietopyyntöä. Asiakirja- ja tietopyynnöissä tulee erottaa muut kuin tietosuoja-asetuksen mukaiset tietopyynnöt, joita kuntaan tulee runsaasti. Tietosuojavastaava osallistui vuoden 2023 aikana yhden asiakirjapyynnön prosessiin asiakirjojen arkuuden vuoksi.

5.2 Tietosuojan toteutuminen

Jokainen kunnan työntekijä on vastuussa omalta osaltaan tietosuojan toteutumisesta ja noudattamisesta. Tietosuojavastaava ohjaa ja valvoo tietosuoja-asetuksen ja lain noudattamista. Tärkeä osa tietosuojan toteutumista on ollut henkilöstölle suunnatut koulutuksen henkilötietojen käsittelystä. Tietosuojan toteutumisessa korostuu käytännön ohjeet, joita jokaisen kunnan työntekijän tulee noudattaa omassa työssään ja ilmoittaa, mikäli huomaa niissä puutteita tai korjattavaa.

5.3 Tietoturvaloukkaus

Tietosuojatyöryhmä on laatinut prosessikaavion tietoturvaloukkauksien hoitamiseen. Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esihenkilölleen tai tietoturvavastaavalle. Tietoturvavastaava yhdessä esihenkilön ja tarvittaessa tietosuojavastaavan kanssa arvioi ja selvittää tilanteen sekä suorittaa tarvittavat toimenpiteet vahinkojen minimoimiseksi. Tarvittaessa tietoturvavastaava kutsuu tietosuojatyöryhmän sekä muut mahdolliset henkilöt koolle ja tehdään päätös tiedottamisen laajuudesta. Kaikki tietoturvaepäilyt ja niihin kohdistetut toimenpiteet kirjataan tiedostoon kunnan verkkolevylle.

Yksikön esihenkilön tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään. Tietoturvavastaavan tehtävänä on seurata ja valvoa Joutsan kunnan tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

Muuttunut maailmantilanne on johtanut siihen, että tietojen kalastelu on päivittäistä. Loppukäyttäjiä on informoitu säännöllisesti, mikäli laajempia hyökkäyksiä on menossa. Tarvittaessa on etsitty myös sähköpostin lokitiedostoista viestejä, jotka viittaavat tietojen kalasteluun ja varoitettu näitä käyttäjiä henkilökohtaisesti. Varsinaisia tietovuototapauksia on ilmoitettu tämän lisäksi vuoden aikana kaksi kappaletta. Ne ovat johtuneet virheelliseen osoitteeseen lähetetyistä sähköposti- tai muista viesteistä. Näissä tapauksissa on menetelty tietosuojatyöryhmän laatiman tietoturvaloukkauksien hoitamisohjeen mukaisesti.

6 TIETOJEN KÄSITTELYN JA TIETOSUOJAN KEHITTÄMINEN

Vuoden 2024 aikana kunnassa tullaan ottamaan käyttöön sähköisen arkistointi. Sähköisen arkisto otetaan käyttöön asteittain niin, että ensimmäisenä arkistoidaan Dynasty-asiahallintajärjestelmän asiat. Myöhemmin sähköinen arkistointi tullaan laajentamaan muihin asiakirjoja sisältäviin järjestelmiin ja viime vaiheessa paperiarkiston siirto sähköiseksi. Sähköisen arkistoinnin avulla pystytään aiempaa helpommin varmistamaan mm. asiakirjojen säilytysajat arkisto- ja tietosuojalakien mukaisesti. Lisäksi tiedonhallintamalli tullaan ottamaan vahvemmin haltuun.

Tekoäly tekee tuloaan vauhdilla eikä sen tulemista kuntapuolelle voi estää. Tärkeätä on huomioida tietoturvallinen ja tietosuojan huomioiva käyttöönotto tekoälyssä ja valmistautua tekoälyn hallittuun käyttöönottoon.

Vuonna 2024 tullaan huomioimaan NIS2 direktiivin vaatimusten täyttäminen. Myös valmistautuminen mahdollisiin poikkeusoloihin on huomioitava tulevina vuosina huolellisesti myös tietosuojan ja -turvan puolella. Kehittämiskohteena huolehditaan lisäksi hyökkäysrajapinnan kaventaminen entisestään ja hyökkäysrajapinnan entistä tiukempi puolustaminen.