Puumala
SAIMAAN KAUNEIN

PUUMALAN KUNNAN
TIETOTILINPÄÄTÖS 2023

Sisällys

1 Tietotilinpäätöksen tarkoitus

Puumalan kunnan tietotilinpäätös laaditaan osana tilinpäätöstä ja sen tarkoitus on kuvata ja arvioida tietosuojan ja tietoturvan tilannetta Puumalan kunnassa. Se toimii sisäisen ja ulkoisen valvonnan raporttina, johdon työvälineenä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan. Tietotilinpäätöksellä vastataan EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, Rekisterinpitäjän vastuu). Organisaation tulee osoittaa noudattavansa asetusta, lakia ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä. Rekisterinpitäjä vastaa osoitusvelvollisuuden toteuttamisesta.

Puumalan kunnan organisaatiossa noudatetaan kunnanhallituksen 2.12.2021 hyväksymää tietosuoja- ja tietoturvapolitiikkaa. Tietosuojan koordinointi ja kehittäminen toteutuvat alueellisessa ja Puumalan kunnan omassa tietosuojatyöryhmässä.

Tietotilinpäätöksen laatimisesta vuoden 2023 osalta on vastannut hallintopäällikkö ja se on ollut kommentoitavana Puumalan kunnan tietosuojatyöryhmässä. Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä.

2 Tietosuojan ja tietoturvallisuuden toteuttaminen

Suomessa kansallisena valvontaviranomaisena toimii tietosuojavaltuutettu. Toiminnassaan tietosuojavaltuutettu on itsenäinen ja riippumaton. Tietosuojavaltuutettu on Euroopan tietosuojaneuvoston jäsen.

Mikkelin alueella toimii alueellinen tietosuojatyöryhmä, johon kuuluu Hirvensalmi, Juva, Kangasniemi, Mikkeli, Mäntyharju, Pertunmaa, Pieksämäki ja Puumala. Alueen yhteisenä tietosuojavastaavana toimii Päivi Malinen Mikkelin kaupungista.

Puumalan kunta ottaa huomioon toiminnassaan tietosuojavaatimukset perustuen EU:n yleiseen tietosuoja-asetukseen (GDPR). Velvoitteiden mukaisesti kuntaan on perustettu tietosuojatyöryhmä, jossa on edustus jokaiselta toimialalta. Työryhmä ei kokoontunut vuonna 2023.

Puumalan kunnan tietoturvaa ja tietosuojaa ohjaa kunnanhallituksen 2.12.2021 (§ 217) hyväksymä tietoturvapolitiikka, joka on laadittu keskeisen lainsäädännön mukaisesti.

Tietoturvapolitiikka sisältää:

- Tietoturvan ja tietosuojan periaatteet
- Tietoturva
    - Tietojärjestelmä
    - Tietoturvan hallinnolliset periaatteet
    - Henkilöstöturvallisuus
    - Fyysinen tietoturva
    - Tietoaineistoturvallisuus

    - Laitteistoturvallisuus
    - Ohjelmistoturvallisuus
    - Tietoliikenneturvallisuus
    - Käyttöturvallisuus
    - Liikkuva työ
    - Seuranta, valvonta ja raportointi
- Tietosuoja
    - Henkilötietojen kerääminen ja käsittely
- Tietoturvariskeihin varautuminen
    - Riskien arviointi
    - Tietoturvapoikkeamat
    - Tietoturvarikkomusten seuraamukset
        - Vakava rikkomus
        - Rikkomus
        - Lievä rikkomus
        - Vastuut ja organisointi
- Vastuut ja organosointi

Tietoturvapolitiikka tukee Puumalan kunnan strategian mukaisesti palvelujen tuottamista asukaslähtöisesti, tehokkaasti ja turvallisesti. Henkilötietojen käsittelyä ohjaa **sisäänrakennetun tietosuojan periaate** edellyttäen, että tietosuojaperiaatteet ovat osana henkilötietojen käsittelyä niiden kaikissa vaiheissa.

Kunnantalon monitoimilaitteissa on käytössä turvatulostus, jolloin tulostetut asiakirjat saa tulostimelta vain tunnisteen kanssa. Kunnantalon turvatulostimen toiminnassa oli häiriöitä useampaan kertaan vuoden aikana. Tietoon ei kuitenkaan tullut tapauksia, joissa tietosuoja olisi vaarantunut. Koululla ja päiväkodilla on käytössä suojattu tulostus, jota käytetään tarpeen vaatiessa. Tällä estetään, ettei arkaluontoisia asiakirjoja jää kopiokoneeseen ilman valvontaa.

Lukolliset tietoturva-astiat ovat olleet käytössä koululla ja kunnantalolla. Kaikki arkaluonteinen asiakirjamateriaali laitetaan tietoturva-astioihin tai asiakirjasilppureihin. Tietoturva-astioiden tyhjennyksestä ja materiaalin tietoturvallisesta hävittämisestä vastaa Itä-Suomen Ekoyhtiö Oy. Tuhoamisprosessi varmistaa, ettei arkaluontoinen tieto päädy vääriin käsiin.

Puumalan kunnan henkilökunnan ja luottamushenkilöiden Office 365 -tileissä on käytössä monivaiheinen tunnistautuminen. Monivaiheinen tunnistautuminen (MFA, engl. multifactor authentication, suom. myös monivaiheinen todentaminen) on käyttäjän tunnistamiseen käytettävä tapa, jossa käytetään kahta tai useampaa keinoa tunnistaa käyttäjä tämän kirjautuessa tiettyyn järjestelmään tai palveluun.

Outlook -sähköpostissa on käytössä Microsoft 365 salattu sähköposti niillä henkilöillä, jotka työssään käsittelevät arkaluontoisia tietoja. Pääsääntönä voidaan ajatella, että sähköposti pitää salata aina kun se sisältää arkaluontoista tietoa.

2.1 Henkilöstön koulutus

Kunnan henkilökunta sekä luottamushenkilöt on velvoitettu suorittamaan vuosittain tietoturva ja tietosuoja -koulutus Navisec Flex -koulutusjärjestelmässä. Järjestelmässä on yhteensä neljä eri koulutusaluetta; ”Henkilöstön tietosuoja”, ” Opetustoimen tietoturva ja tietosuoja”, ” Varhaiskasvatuksen tietoturva ja tietosuoja” ja ” Luottamushenkilöiden tietoturva ja tietosuoja”. Henkilökunta suorittaa vähintään ”Henkilöstön tietosuoja” -osion. Lisäksi tehdään omaan toimialaan liittyvä koulutusosio. Koulutuspaketti päivitettiin 8.6.2023.

Vuosina 2020-2023 testin suorittanut henkilöstö koulutusosioittain:

	2020	2021	2022	2023
Henkilöstön tietosuoja	69%	64%	**46%**	**73%**
Opetustoimen tietoturva ja tietosuoja	64%	78%	90%	**60%**
Varhaiskasvatuksen tietoturva ja tietosuoja	54%	63%	69%	**91%**
Luottamushenkilöiden tietoturva ja tietosuoja	33%	23%	55%	50%

Kunnan poikkeusolojen johtoryhmä osallistui Digi- ja väestöviraston (DVV) järjestämään Digitaalisen turvallisuuden Taisto-harjoitukseen 23.11.2023. Suomen suurin digitaalisen turvallisuuden harjoitus Taisto järjestettiin kuudetta kertaa. Taisto on kaikille julkisen sektorin organisaatioille avoin ja maksuton harjoitus, jossa organisaatiot pääsivät valmiiseen harjoitukseen testaamaan ja kehittämään omia toimintatapojaan kuvitteellisten häiriötilanteiden kautta. Harjoituksessa käsiteltiin teemoja, jotka liittyivät tietoturvakäytäntöihin, tietojenkalasteluun ja hybridivaikuttamiseen. Harjoituksessa näyttäytyi myös tekoäly ja sen mukanaan tuomat haasteet. Harjoitus tarjosi tilaisuuden oppia ja kehittää kriittistä ajattelua, riskienhallintaa, tietoturvareaktiivisuutta ja häiriötilanteiden viestintää. Kokemukset harjoituksesta olivat tietoa lisäävät ja hyödylliset.

Henkilöstöä on informoitu sähköpostitse erilaisten huijausviestien yleistymisestä ja toimintatavoista viestien kanssa.

2.2 Tietosuojaohjeet

Puumalan kunnan tietosuoja- ja tietoturvaa ohjaa tietosuojan ja tietoturvaan liittyvien lakien lisäksi paikalliset ohjeet ja säännöt:

- Puumalan kunnan tietosuoja- ja tietoturvapolitiikka
- Puumalan kunnan asiakirjajulkisuuskuvaus
- eri tietojärjestelmäkohtaiset ohjeet

Yleisiä tietosuojaohjeita löytyy Navisec Flex oppimisympäristöstä koko henkilökunnan ja luottamushenkilöiden luettavissa.

- Tietoturvapolitiikka
- Asianhallinta ja tietojen käsittelyohje
- Henkilöstön tietoturvaohje

- Tietosuoja-asetuksen koulutusmateriaali
- Tietoturva- ja tietosuojasitoumus

3 Tiedonhallinta, tietovarannot ja tietovirrat

Puumalan kunnan tiedonhallinnan, tietovarantojen sekä niihin liittyvien tietovirtojen kokonaistilanteen kuvausta ei ole laadittu, mutta järjestelmäluettelo on ja sitä on hyödynnetty henkilötietojen kartoituksessa.

Puumalan kunnassa oli vuonna 2023 käytössä seuraavat tietojärjestelmät, joissa käsitellään henkilötietoja:

- AD (hallinnon verkon käyttöoikeudet)
- Asteri (isännöinnin kirjanpito)
- CaseM (asianhallintaohjelma)
- CGI HR po, Populus (palkkahallinto)
- CGI, Nessos (verkkolaskupalvelu)
- CGI, ProEconomica Premium (taloushallinto)
- Digital Booker (varausjärjestelmä)
- DNA puhelinvaihde
- Facta kuntarekisteri (rakennusvalvonnan toiminnanohjaus)
- Flexim (työajanseuranta), 28.8.2023 alkaen Navisystem työajanseuranta
- Hellewi (kansalaisopisto toiminnanohjaus)
- Intrum, luottotieto- ja perintäpalvelu
- It’s learning (oppimisympäristö)
- Kartturi (peltokarttaohjelma)
- Kulkuri (urheiluhallin avainkorttijärjestelmä)
- Lyyti (kysely- ja tapahtumatyökalu)
- Lupapiste (rakennusvalvonnan toiminnanohjaus)
- Opinsys (perusopetuksen käyttöjärjestelmä)
- Otava (opetusohjelma)
- PARENT -tilastointi (etsivä nuorisotyö)
- Primus, Kurre, Wilma (opetuksen ja varhaiskasvatuksen toiminnanohjaus)
- Puumalan kunnan ilmoituskanava (whistleblower)
- Sanoma Pro (opetusohjelma)
- Sympa HR (henkilöstöhallinta)
- Sähköpostijärjestelmä (Microsoft Office 365)
- Titania (työvuorosuunnittelu)
- Työterveysportaali, Pihjalalinna
- Unes isännöinti
- Varda (varhaiskasvatuksen kansallinen tietovaranto)
- VINGO (jätehuollon rekisteri)
- Wintie (yksityisteiden hallinta)
- WordPress (verkkosivut)
- Xerox tulostusjärjestelmä

3.1 Tietojärjestelmien käyttöoikeudet

Henkilöstön tietojärjestelmien käyttöoikeuksia ja järjestelmärooleja on päivitetty tarpeen mukaan henkilöstön tai työtehtävien vaihtuessa. Osa kunnan IT-palveluista siirrettiin MarskiDatan ylläpitämäksi ja tuolloin tarkastettiin kaikki tietojärjestelmien ylläpitoroolit. Kaikkien käytössä olevien tietojärjestelmien ohjattua käyttöoikeuksien katselmointia ei ole vuoden 2023 aikana suoritettu.

3.2 Kunnan hankkeiden ja kaavojen julkaisujen automatisointi

Puumalan kunta oli mukana Porin kaupungin vetämässä ”Hankkeiden ja kaavojen käsittely ja julkisuus asianhallinnassa (HAKA)” -hankkeessa. Hankkeen tuloksena saatiin kaavojen ja merkittävimpien hankkeiden käsittelyvaiheet ja niihin liittyvien asiakirjojen julkaisu Tiera CaseM asianhallinta -järjestelmästä suoraan verkkoon.

3.3 Puumalan kunnan ilmoituskanava

1.1.2023 voimaan tullut EU:n whistleblower-direktiiviin mukainen ilmoittajansuojelulaki velvoittaa yritykset ja organisaatiot tarjoamaan anonyymin kanavan väärinkäytösepäilyjen ilmoittamiseen.

Laki edellyttää, että vähintään 50 henkilöä työllistävät organisaatiot ottavat käyttöön kanavan, jonka kautta on mahdollista tehdä ilmoituksia havaitsemistaan väärinkäytöksistä ja epäkohdista organisaatiossa.

Direktiivin tarkoituksena on varmistaa, että ilmoittaja, joka havaitsee työssään EU-oikeuden rikkomuksia, voi ilmoittaa asiasta joutumatta negatiivisten toimenpiteiden kohteeksi.

Ilmoituksia seuraavia asioita koskien:

- julkiset hankinnat
- rahoituspalvelut, -tuotteet ja -markkinat sekä rahanpesun ja terrorismin rahoituksen ehkäiseminen
- tuoteturvallisuus ja vaatimustenmukaisuus
- liikenneturvallisuus
- ympäristönsuojelu
- säteilyturva ja ydinturvallisuus
- elintarvikkeiden ja rehujen turvallisuus sekä eläinten terveys ja hyvinvointi
- kansanterveys
- kuluttajansuoja
- yksityisyyden ja henkilötietojen suoja sekä verkko- ja tietojärjestelmien turvallisuus.

Puumalan kunnassa sisäinen ilmoituskanava WB otettiin käyttöön maaliskuussa 2023. Ilmoituksen voi jättää nimettömänä sähköisesti kanavalla tai kirjeitse kunnantalon pääoven vieressä sijaitsevaan postilaatikkoon.

4 Rekisteröidyn oikeudet ja niiden toteutuminen

Puumalan kunta noudattaa henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kunnan nettisivuilta (artiklat 13 ja 14). Aiemmin tehdyt rekisteriselosteet löytyvät kunnan verkkolevyltä (K-asema).

Puumalan kunnan nettisivuille on avattu tietosuojasivusto asian tiedottamista varten. Nettisivuilta löytyvät tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16). Kuntaan ei tullut vuoden 2023 aikana yhtään tietopyyntöä henkilötietojen käsittelystä.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa 72 tunnin kuluessa tietosuojavastaavalle, mikäli loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä silloin kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietosuojavastaavan harkinnan mukaan. Tietoon ei ole tullut yhtään tietoturvaloukkausta vuoden 2023 aikana.

4.1 Seuranta ja mittaaminen

Henkilökunnan tietosuojakouluttautumista Navisec Flex -koulutusympäristössä seurataan säännöllisesti ja tarvittaessa muistutetaan testin suorittamisesta. Henkilökunnalle annetaan ohjeita henkilötietojen käsittelystä ja niiden noudattamista seurataan. Tietojärjestelmien pääkäyttäjät huolehtivat, että henkilöstön käyttövaltuudet ohjelmissa pidetään ajan tasalla.

Tietosuojavastaava pitää kirjaa tietopyynnöistä ja tietosuojapoikkeamista. Tietojen kalasteluviestejä tulee aika ajoin sähköpostiin. Niistä on varoitettu henkilökuntaa sekä annettu tarvittaessa toimintaohjeita.

Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

5 Arviointi ja kehittäminen

Vuosien 2021 ja 2022 välillä henkilökunnan tietosuoja- ja tietoturvakoulutusten ”Henkilöstön tietosuoja” suoritusprosenteissa oli huolestuttava 18%:n lasku. Tilanne korjaantui paremmaksi vuonna 2023, testien suoritusprosentin ollessa peräti 73%. Suunta on hyvä, mutta parannettavaa on vielä. Esihenkilöitä velvoitetaan edelleen valvomaan, että jokainen suorittaa koulutuksen vuosittain vuoden loppuun mennessä.

Käyttäjiä muistutetaan edelleen ottamaan huomioon tietosuoja- ja tietoturvalliset toimintatavat työskentelyssään. Henkilötietoja sisältäviä papereita ei saa jättää pöydälle työpaikalta poistuttaessa niin, että niihin pääsee asiaankuulumattomat käsiksi. Työhuoneiden ovet on pidettävä lukittuina, kun työhuoneesta poistutaan. Lähetettäessä sähköpostissa salassa pidettävää tietoa, on käytettävä viestin salausta.

1.1.2020 voimaan astunut tiedonhallintalaki velvoittaa organisaatioilta tiedon elinkaarenhallinnan perusvaatimusten kuvantamista ja julkistamista yhtenäisenä kokonaisuutena. Kehitetään asianhallintaa niin, että CaseM asianhallintajärjestelmään kirjataan kaikki saapuneet asiakirjat. Asianhallintajärjestelmään kirjataan myös kaikki henkilötietojen käsittelyihin liittyvät tietopyynnöt niin, että jokainen tietopyyntö käynnistää uuden aktin eli asian. Kaikki ko tietopyyntöön liittyvät asiakirjat liitetään asiaan. Samalla käynnistetään yhteisen K-verkkolevyn tiedostojen seulonta niin, että vanhentuneet tiedostot poistetaan eikä verkkolevyä pidetä arkistona vaan kaikki asiakirjat kirjataan CaseM -asianhallintaan.

Luottamushenkilöiden CaseM asianhallinnan kokoustyötilan käyttöönottoa jatketaan ja tarvittaessa järjestetään koulutustilaisuus.

Tiedonhallintalain vaatimusten mukaisia toimenpiteiden toteuttamista jatketaan vuonna 2024.

Seudullinen tietosuojatyöryhmä kokoontuu joka toinen kuukausi käsittelemään ajankohtaisia tietosuoja- ja tietoturva-asioita. Kokouksissa saadaan ajankohtaista tietoa ja käsitellään yhdessä mahdollisia tietoturvapoikkeamia.

Kunnan oma tietosuojatyöryhmä kokoontuu tarvittaessa ja pohtii tietosuojan kehittämistä eri toimialoille. Laaditaan tarvittaessa paikallisia tietosuoja ja tietoturvaohjeita, joita lähetetään sähköpostitse henkilöstölle tietoiskuina sekä kirjataan CaseM asianhallintajärjestelmään.

Osallistutaan Tieran koordinoimaan asianhallinnan kehitystyöryhmään.

Osallistutaan DVV järjestämään Taisto-harjoitukseen vuonna 2024.