Kunnanhallitus 30.3.2020 § 43 liite nro 1
Valtuusto 22.6.2020 § 18 liite nro 1

TIETOTILINPÄÄTÖS 2019

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 valtuuston helmikuussa 2017 hyväksymää tietoturvapolitiikkaa sisältäen tietoturvan ja siinä kuvattua tietosuojan organisaatiorakennetta. Tietosuojan koordinointi ja kehittäminen toteutuvat alueellisessa ja Puumalan kunnan omassa tietosuojatyöryhmässä.

Tietotilinpäätöksen laatimisesta on vastannut hallintopäällikkö Annakaisa Arilahti ja ICT-tuki Anne Valtonen ja se on käsitelty Puumalan kunnan tietosuojatyöryhmässä.

Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä.

2 Tietosuojan – ja tietoturvallisuuden toteuttaminen

Puumalan kunta valmistautui tietosuoja- ja tietoturvan toteuttamiseen ja EU:n yleisen tietosuoja-asetuksen velvoitteisiin perustamalla tietosuojatyöryhmän ja kouluttamalla henkilökunnan tietosuoja-asetuksen periaatteisiin syksyllä 2018. Kunnan tietosuojatyöryhmään kuuluu edustus hallinto-, hyvinvointi- ja teknisten palvelujen toimialalta, puheenjohtajana toimii hallintopäällikkö. Lisäksi työryhmään kuuluu IT-asiantuntija.

Mikkelin alueelle perustettiin seudullinen tietosuojatyöryhmä syksyllä 2017. Ryhmään kuuluu Hirvensalmi, Juva, Kangasniemi, Mikkeli, Mäntyharju, Pertunmaa, Pieksämäki ja Puumala. Alueen yhteisenä tietosuojavastaavana toimii Päivi Malinen Mikkelin kaupungista.

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

Puumalan kunnan tietoturvaa ja tietosuojaa ohjaa valtuuston 20.2.2017 (§37) hyväksymä tietoturvapolitiikka, joka on laadittu keskeisen lainsäädännön mukaisesti.
Tietoturvapolitiikka sisältää:

1. Tietoturvan tavoitteet
2. Keskeiset käsitteet ja sanasto
3. Tietoturvatehtävät ja tietoturvatyön organisointi
4. Tietoturvallisuuden seuranta

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.

Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjä oletusarvoisesti käsittelee vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste ja henkilöstön tulee olla tietoisia siitä missä kaikkialla henkilötietoja sijaitsee ja miten niitä käytetään.

Tietosuoja-asetuksen informointivelvoite (artiklat 13 ja 14) edellyttävät organisaatiota informoimaan läpinäkyvästi sen toteuttamasta henkilötietojen käsittelystä. Puumalan kunnan henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet.

Tietosuojaselosteita on tallennettu kunnan nettisivuille, jossa ne toimivat asiakkaiden informaatioasiakirjoina.

Henkilötietojen käsittelyn kartoitus on nyt tehty keskeisten henkilötietoa sisältävien tietojärjestelmien osalta ja kuvattu lähinnä järjestelmäkohtaisesti.

Tietosuoja- ja tietoturvatyön organisointi ja tietosuojavastaavan rooli on merkittävä tekijä myös tietoturvan kannalta. Ennen kaikkea pitäisi muistaa, ettei tietosuojaa ole olemassa ilman tietoturvaa.

Rekisterinpitäjä on tietosuoja-asetuksen (artikla 24) mukaan vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia.

Henkilöstön koulutus

Syksyllä 2018 koko henkilökunnalle ja luottamushenkilöille pidettiin koulutusta EU:N tietosuoja-asetuksen vaatimuksista. Syksyllä 2019 kuntaan hankitiin Navisec Flex -koulutusjärjestelmä, jonka avulla lisättiin henkilökunnan tietosuoja- ja tietoturvatietämystä. Lisäksi pidettiin valtuustosalissa kaksi tilaisuutta, jossa käsiteltiin tietosuoja- ja tietoturva-asioita.

Kunnan henkilöstöstä Navisec Flex –oppimisympäristön suoritti vuoden 2019 loppuun mennessä yhteensä 74 henkilöä eli n. 93% koko henkilöstöstä. Oppimisympäristö pitää sisällään opetusvideoita ja testejä eri tietosuojan ja tietoturvan osa-alueista. Jatkossa kaikki työntekijät tekevät nettitestin vuosittain. Vuodesta 2020 alkaen myös luottamushenkilöt käyvät läpi oppimisympäristön.

Kunnantalon henkilökunnalle otettiin käyttöön henkilökortit.

Kuntalain 29 §:n mukaan kunnan on huolehdittava, että asioiden valmistelusta annetaan riittävästi tietoja yleisessä tietoverkossa. Verkossa tiedottaminen tuo haasteita asiakirjahallintoon erityisesti henkilötietojen käsittelyn suhteen, sillä henkilötietoja tulee viedä verkkoon harkitusti eikä niitä saa pitää siellä tarpeettomasti. Asianhallintaohjelmassa on otettu käyttöön vaihtoehtoinen teksti, jonka avulla henkilötiedot voidaan peittää julkaistuista asiakirjoista oikaisuvaatimusajan jälkeen automaattisesti.

Tietosuojaohjeet

Tietosuojaohjeita löytyy Navisec Flex oppimisympäristöstä koko henkilökunnan ja luottamushenkilöiden luettavissa.
- Tietoturvapolitiikka
- Asianhallinta ja tietojen käsittelyohje
- Henkilöstön tietoturvaohje

- Tietosuoja-asetuksen koulutusmateriaali
- Tietoturva- ja tietosuojasitoumus

Fyysinen suojaus

Ovien lukitusjärjestelmä uusittiin koulussa ja päiväkodissa syksyllä 2018 ja kunnantalolla keväällä 2019. Samalla tarkistettiin henkilökunnan tarvitsemat kulkuoikeudet.
Palvelukeskuksessa on ulko-ovissa ja sisäovessa otettu käyttöön ovikoodilukot, lähinnä asiakasturvallisuuden vuoksi. Lisäksi hissi kulkee alaspäin vain avaimella.
Kunnantalon monitoimilaitteissa otettiin käyttöön turvatulostus, eli tulostetut asiakirjat saa tulostimelta tunnisteen kanssa. Tällä estetään, ettei arkaluontoisia asiakirjoja jää kopiokoneeseen ilman valvontaa. Koululla on rehtorin ja erityisopettajan käytössä turvatulostus.
Koululla on tallentava kameravalvonta.

Riskiperusteinen lähestymistapa

EU:n yleisessä tietosuojavelvoitteessa edellytetään, että riskit on otettava huomioon sisäänrakennettuna ja oletusarvoista tietosuojaa toteutettaessa (artikla 25). Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Velvoitteet ja suojatoimet on suhteutettava tietokäsittelyjen aiheuttamaan riskiin (artikla 32). Korkeamman riskin henkilötietojen käsittely edellyttää enemmän panostamista teknisiin ja hallinnollisiin toimenpiteisiin, kun taas vähäisen riskin toiminta ei aiheuta merkittävää uhkaa rekisteröidyn yksityisyyden suojalle. (Korpisaari, Pitkänen ja Warma-Lehtinen, 2018.)

Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä hallitaan järjestelmällisesti ja ennakoivasti. Riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarvioinnin sekä tarvittaessa ennakkokuulemisen tulisi tehdä sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.

Tietosuojaan ja yksilön vapauksiin suunniteltuja henkilötietojen käsittelytoimien vaikutustenarviointia (PIA/DPIA) sekä ennakkokuulemista (artikla 35 ja 36) ei ole vielä toteutettu.

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 on käytössä seuraavat tietojärjestelmät, joissa käsitellään henkilötietoja:
- Kulkuri (urheiluhallin avainkorttijärjestelmä)
- Primus, Kurre, Wilma (opetuksen ja varhaiskasvatuksen toiminnanohjaus)
- It’s learning (oppimisympäristö)
- Sanoma Pro (opetusohjelma)
- Näppistaituri (opetusohjelma)
- Opinsys (perusopetuksen käyttöjärjestelmä)
- Elisa Ring (puhelinvaihde)
- WordPress (verkkosivut)
- KuntaZef (kyselytyökalu)
- CaseM (asianhallintaohjelma)

- ProEconomica Premium (taloushallinto)
- Pegasos (palkanlaskenta)
- Sympahr (henkilöstöhallinta)
- Flexim (työajanseuranta)
- ProConsona (päivähoito)
- Titania (työvuorosuunnittelu)
- Facta kuntarekisteri (rakennusvalvonnan toiminnanohjaus)
- Lupapiste (rakennusvalvonnan toiminnanohjaus)
- Unes isännöinti
- JHLWin (jätehuollon rekisteri)
- Wintie (yksityisteiden hallinta)
- Hellewi (kansalaisopisto toiminnanohjaus)
- AD (hallinnon verkon käyttöoikeudet)
- Sähköpostijärjestelmä
- Xerox tulostusjärjestelmä

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 K-asemalta ja paperitulosteet asiointipisteestä.

Puumalan kunnan nettisivuille on avattu tietosuojasivusto asian tiedottamista varten. Nettisivuilta löytyvät tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16). Kuntaan tuli vuoden 2018 aikana yksi tietopyyntö henkilötietojen käsittelystä, vuonna 2019 ei yhtään.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa 72 tunnin kuluessa tietosuojavastaavalle, jos 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 2019 aikana.

5 Seuranta ja mittaaminen

Henkilökunnan tietosuojakouluttautumista oppimisympäristössä seurataan säännöllisesti ja tarvittaessa muistutetaan testin suorittamisesta. Henkilökunnalle annetaan ohjeita henkilötietojen käsittelystä ja niiden noudattamista seurataan. Ohjelmien pääkäyttäjät huolehtivat, että henkilöstön käyttövaltuudet ohjelmissa pidetään ajan tasalla.
Tietosuojavastaava pitää kirjaa tietopyynnöistä ja tietosuojapoikkeamista.
Tietojen kalasteluviestejä tulee aika ajoin sähköpostiin ja niistä on varoitettu henkilökuntaa ja annettu ohjeita, miten toimia, jos on antanut niihin tietojaan.
Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

Pelastus- ja turvallisuussuunnitelmat on päivitetty koulussa ja päiväkodissa 2017 ja virastotalolla 2019.

Tilinpäätöksessä on tehty tietojärjestelmien riski- ja vaikutustenarviointi.

6 Arviointi ja kehittäminen

EU Yleinen tietosuoja-asetus on otettu organisaatiossamme vastaan hyvin ja organisaatio pyrkii vastaamaan asetuksen tuomiin haasteisiin, joskin monella osa-alueella on vielä kehitettävää. Myös ilmoituskäytännön hiominen tietosuojavaltuutetulle on tärkeää.

Kunnan oma tietosuojatyöryhmä kokoontuu tarvittaessa ja pohtii tietosuojan kehittämistä eri toimialoille.

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

Asianhallintajärjestelmää kehitetään yhteistyössä eri kuntien kanssa kiinnittäen huomiota erityisesti henkilötietojen käsittelyyn.