Puumala
SAIMAAN KAUNEIN

PUUMALAN KUNNAN
TIETOTILINPÄÄTÖS 2021

Sisällys

1 Tietotilinpäätöksen tarkoitus

Tieto on keskeisessä roolissa organisaatioiden toiminnassa ja palvelutuotannossa. Tiedon tulee olla hyödynnettävissä tarpeen mukaisesti ja tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys ovat tärkeitä toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Tietosuoja suojaa ihmisten yksityisyyttä. Inhimillisenä toimintana tietojenkäsittelyyn liittyy aina riskejä, joita pyritään minimoimaan ohjeistuksilla, koulutuksella ja teknisillä ratkaisuilla. Tietoturvariskeistä pystytään minimoimaan teknisin ratkaisuin vain osa, tärkeintä ovat päivittäisessä tietojenkäsittelyssä tehdyt ratkaisut ja toimenpiteet.

Tietoturva suojaa henkilötietoja ja muita tietoja luvattomalta käytöltä. Se käsittää keskeisiin toimintoihin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti uhkia ja tarvittaessa sietää niiden vaikutuksia. Riskien tunnistamisen ja hallinnan sekä vaikutusten minimointi on osa organisaation aktiivista tietoturvan toteuttamista.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla, jonka on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös organisaation toimintakykyyn. Lisäksi lainsäädäntö edellyttää tietoturvan asianmukaista hoitamista. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen. Tietoturvan ja tietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvonantajina.

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 joulukuussa 2021 hyväksymää tietosuoja- ja tietoturvapolitiikkaa. Tietosuojan koordinointi ja kehittäminen toteutuvat alueellisessa ja Puumalan kunnan omassa tietosuojatyöryhmässä.

Tietotilinpäätöksen laatimisesta vuoden 2021 osalta on vastannut hallintoasiantuntija Mervi Kelloniitty ja se on käsitelty 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 Etelä-Savon tietoturva- ja 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 kunnassa toimii tietosuojatyöryhmä, johon kuuluu edustus hallinto-, hyvinvointi- ja teknisten palvelujen toimialalta sekä IT-asiantuntija. Ryhmän puheenjohtajana toimii hallintopäällikkö.

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

Tietosuoja- ja tietoturvapolitiikka sisältää:

1. Tietoturvan ja tietosuojan periaatteet
2. Tietoturva
3. Tietosuoja
4. Tietoturvariskeihin varautuminen
5. Vastuut ja organisointi

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 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.

Heinäkuussa 2021 Windows Print Spoolerista eli taustatulostuspalvelusta löytyi kriittinen haavoittuvuus CVE-2021-34527, joka mahdollisti esimerkiksi toimialueen haltuunoton. Haavoittuvuudelle ei ollut muuta korjausvaihtoehtoa tiedossa, kuin ”Print Spooler” -palvelun sammuttaminen ja käytöstä poistaminen. Se tarkoitti sitä, että tulostus ei toimi, kunnes Microsoft tekee tietoturvapäivityksen palveluun ja se päivitetään työasemille. Etelä-Savon tietosuojavaltuutetun pyynnöstä palvelu poistettiin käytöstä alueen kaikissa kunnissa. Microsoft julkaisi 12.7.2021 korjaavan päivityksen haavoittuvuuteen, mutta se ei palauttanut turvatulostusta täysin kaikille käyttäjille vaan tulostamaan pääsi vain, jos työasemaan oli järjestelmänvalvojan oikeudet. Microsoft julkaisi 14.9.2021 korjaukset kaikkiin tunnettuihin Print Spooler -haavoittuvuuksiin.

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.

Vuosina 2021-2022 testin suorittanut henkilöstö koulutusosioittain:

	2020	2021
Henkilöstön tietosuoja	69%	64%
Opetustoimen tietoturva ja tietosuoja	64%	78%
Varhaiskasvatuksen tietoturva ja tietosuoja	54%	63%
Luottamushenkilöiden tietoturva ja tietosuoja	33%	23%

Tietosuojasta ja tietoturvallisista toimintatavoista työpaikalla sekä etätyöskentelyn osalta on henkilöstöä muistutettu tietoiskun omaisilla sähköpostiviesteillä.

Kunta osallistui Digi- ja väestöviraston (DVV) järjestämään Taisto2021 -harjoitukseen. Julkishallinnolle suunnatussa tietosuoja- ja tietoturvaloukkauksien hallinnan harjoituksessa organisaatiot harjoittelivat toimintamalleja ja prosesseja erilaisten häiriötilanteiden varalle. Pääpaino harjoituksessa oli kehittää digitaalisen turvallisuuden häiriötilanteiden hallintaa ja organisaatioiden omien prosessien, ohjeiden ja toimintamallien kehittäminen. Kokemukset harjoituksesta olivat tietoa lisäävät ja hyödylliset.

Henkilöstölle on pidetty koulutusta Teams -ohjelman käytöstä maalis-huhtikuussa 2021. Samalla on muistutettu myös tietoturvasta ja tietosuojasta etätyössä ja sähköisissä kokouksissa.

Henkilöstöä on muistutettu säännöllisesti sähköpostitse, tekstiviestitse ja puhelimitse tulevista huijaus- ja kalasteluyrityksistä ja annettu toimintaohjeita, jos on tietojaan antanut.

2.2 Tietosuojaohjeet

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

- Tietoturvapolitiikka
- Asianhallinta ja tietojen käsittelyohje
- Henkilöstön tietoturvaohje
- Tietosuoja-asetuksen koulutusmateriaali
- Tietoturva- ja tietosuojasitoumus

Etätyöstä on kunnanhallituksen kirjallinen ohjeistus ja etätyösopimuspohja.

2.3 Fyysinen suojaus

Ovien lukitusjärjestelmät ovat käytössä koululla, päiväkodilla ja kunnantalolla. Palvelukeskuksen ulko- ja sisäovissa on käytössä ovikoodilukot asiakasturvallisuuden vuoksi. Palvelukeskuksen hissi kulkee alaspäin vain avaimella.

Kunnantalon monitoimilaitteissa on käytössä turvatulostus, jolloin tulostetut asiakirjat saa tulostimelta vain tunnisteen kanssa. Koululla rehtorin ja erityisopettajan käytössä on turvatulostus. Tällä estetään, ettei arkaluontoisia asiakirjoja jää kopiokoneeseen ilman valvontaa.

Koululla, jäteasemalla ja kunnantalon sisääntuloaulassa, hissitornissa, keskusvarikolla, urheiluhallilla, terveysaseman vastaanotollla ja poukamassa on tallentava kameravalvonta.

Lukolliset tietoturva-astiat ovat käytössä koululla, päiväkodilla, ruokahuollossa 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 Office 365 -tilien turvallisuutta parannetaan käyttämällä monivaiheista tunnistautumista. 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. Monivaiheinen tunnistautuminen on käytössä kirjauduttaessa kunnan Office 365 -palveluihin.

Outlook -sähköpostissa on käytössä Microsoft 365 salattu sähköposti. Pääsääntönä voidaan ajatella, että sähköposti pitää salata aina kun se sisältää arkaluontoista tietoa.

2.4 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 vaikutustenarviointi sekä tarvittaessa ennakkokuuleminen 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

1.1.2020 voimaan astunut tiedonhallintalaki velvoittaa organisaatioilta tiedon elinkaarenhallinnan perusvaatimusten kuvantamista ja julkistamista yhtenäisenä kokonaisuutena. Eri velvollisuuksien täyttämiseen on olemassa siirtymäaikoja.

Puumalan kunnan tiedonhallintamallin koostaminen on käynnistetty ja sen päivittäminen on jatkuvaa.

Tiedonhallintamalli on sisältää tiedot ja kuvaukset:

- Toimintaprosesseista
- Tietovarannoista
- Tietoaineistoista
- Tietojärjestelmistä
- Tietoturvajärjestelyistä

Puumalan kunnan asiakirjajulkisuuskuvaus on hyväksytty kunnanhallituksessa 2.12.2021. Kuvaus on julkaistu kunnan verkkosivulla.

Asiakirjajulkisuuskuvauksen tarkoituksena on antaa kuntalaisille ja hallinnon asiakkaille yleinen kuva siitä, millaisia tietovarantoja kunnalla on ja miten ne liittyvät kunnan asiarekisteriin, millaisia tietoaineistoja tietovarannot sisältävät, missä tietojärjestelmissä tietoaineistot ovat ja kuka

päättää tietojen antamisesta. Kuvaus sisältää myös esimerkkejä hakutekijöistä, joilla asiakirjoja tai niitä vastaavia tietoja voi hakea tietojärjestelmistä sekä tiedon, jos tietoaineistot ovat saatavilla avoimesti teknisten rajapintojen avulla. Lisäksi kuvaus sisältää yleisiä ohjeita tietopyyntöjen tekemiseksi sekä tietoa kunnan päätearkistosta, asiakirjoista perittävistä maksuista ja tietojen käyttöön liittyvistä vastuista.

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 nettisivuilla on tietosuojasivusto asian tiedottamista varten. Nettisivuilta löytyvät tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16). Kuntaan ei tullut vuoden 2021 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 2021 aikana.

5 Seuranta ja mittaaminen

Henkilökunnan tietosuojakouluttautumista Navisec -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. Niistä on varoitettu henkilökuntaa sekä annettu tarvittaessa toimintaohjeita.

Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

6 Arviointi ja kehittäminen

Tiedonhallintalain velvoitteiden mukaisten tiedonhallinta- ja digiturvamallien laatiminen jatkuu.

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.

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 paikallisia tietosuoja ja tietoturvaohjeita, joita lähetetään sähköpostitse henkilöstölle tietoiskuina sekä tallennetaan kunnan verkkolevylle (K-asema).

Osallistutaan asianhallintajärjestelmän kehittämiseen yhteistyössä eri kuntien kanssa kiinnittäen huomiota erityisesti henkilötietojen käsittelyyn.

Käynnistetään vuosittain suoritettava tietojärjestelmien käyttöoikeuksien katselmointi ICT-asiantuntijan organisoimana.

Velvoitetaan jokainen poistamaan omalta O-levyltä sekä yhteiseltä K-levyltä kaikki omat tarpeettomat tiedostot.

CaseM kokoushallinnan käyttö laajennetaan valtuuston ja lautakuntien käyttöön.

Osallistutaan Digi- ja väestöviraston (DVV) järjestämään Taisto2022 -harjoitukseen.

Koulun, päiväkodin ja kunnantalon lukitusjärjestelmien kulkuoikeudet tarkistetaan ja päivitetään.