TIETOTILINPÄÄTÖS 2020

Sisällys

2 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 vuoden 2020 osalta on vastannut hallintoasiantuntija Mervi Kelloniitty ja se on käsitelty Puumalan kunnan tietosuojatyöryhmässä. Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä.

3 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. Työryhmään kuuluu edustus hallinto-, hyvinvointi- ja teknisten palvelujen toimialalta sekä IT-asiantuntija. Ryhmän puheenjohtajana toimii hallintopäällikkö.

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 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.

Kunnan verkkosivuille kohdistui kyberhyökkäys heinäkuussa 2020. Hyökkäyksestä ei kuitenkaan koitunut haittaa eikä tietosuoja ja tietoturvallisuus vaarantunut. Hyökkäyksen johdosta kaikki sivuston ylläpitäjät vaihtoivat salasanansa.

3.1 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.

Vuoden 2020 aikana testin suorittanut henkilöstö koulutusosioittain:

Henkilöstön tietosuoja	69%
Opetustoimen tietoturva ja tietosuoja	64%
Varhaiskasvatuksen tietoturva ja tietosuoja	54%
Luottamushenkilöiden tietoturva ja tietosuoja	33%

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

Hallintopäällikkö Annakaisa Arilahti ja ICT-tuki Anne Valtonen osallistuivat Innowisen järjestämään Tietosuojavastaavan peruskoulutusohjelmaan sekä FCG Finnish Consulting Group Oy:n Kyperturvalllisuuspäiville 22.-23.9.2020. Tietosuojavastaavan koulutuspakettia on jaettu eteenpäin ja sitä on hyödynnetty paikallisessa ohjeistuksessa.

Kunta osallistui Digi- ja väestöviraston (DVV) järjestämään Taisto2020 -harjoitukseen. Julkishallinnolle suunnatussa tietosuoja- ja tietoturvaloukkauksien hallinnan harjoituksessa organisaatiot harjoittelivat toimintamalleja ja prosesseja erilaisten häiriötilanteiden varalle. Kokemukset harjoituksesta olivat tietoa lisäävät ja hyödylliset. Henkilöstölle on järjestetty harjoituksen jälkeen yksi koulutustilaisuus aiheena; “Näin pidät huolta tietoturvasta kotona ja työpaikalla”.

Henkilöstöä on sähköpostitse ohjeistettu Teamsin käytöstä, salatun sähköpostin lähettämisestä ja vastaanottamisesta.

3.2 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

3.3 Fyysinen suojaus

Ovien lukitusjärjestelmät on uusittu koulussa ja päiväkodissa syksyllä 2018 sekä kunnantalolla keväällä 2019. Henkilökunnan kulkuoikeudet on tarkistettu samanaikaisesti. Palvelukeskuksen ulko- ja sisäovissa on käytössä ovikoodilukot asiakasturvallisuuden vuoksi. 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 vastaanotolla ja Poukamassa on tallentava kameravalvonta.

Lukolliset tietoturva-astiat ovat käytössä koululla, ruokahuollossa ja kunnantalolla. Kaikki arkaluonteinen asiakirjamateriaali laitetaan tietoturva-astioihin tai asiakirjasilppureihin. Tietoturva-astioiden tyhjennyksestä ja materiaalin tietoturvallisesta hävittämisestä vastaa Itä-Suomen Ekoyhtiö Oy. Tuhousprosessi 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.

3.4 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 vaikutustenarvioinnin sekä tarvittaessa ennakkokuulemisen tulisi tehdä sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.

4 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:

- AD (hallinnon verkon käyttöoikeudet)
- Asteri (isännöinnin kirjanpito)
- CaseM (asianhallintaohjelma)
- Elisa Ring (puhelinvaihde)
- Facta kuntarekisteri (rakennusvalvonnan toiminnanohjaus)
- Flexim (työajanseuranta)
- Hellewi (kansalaisopisto toiminnanohjaus)
- It’s learning (oppimisympäristö)
- VINGO (jätehuollon rekisteri)
- Kulkuri (urheiluhallin avainkorttijärjestelmä)

- KuntaZef (kyselytyökalu)
- Lupapiste (rakennusvalvonnan toiminnanohjaus)
- Näppistaituri (opetusohjelma)
- Opinsys (perusopetuksen käyttöjärjestelmä)
- Otava (opetusohjelma)
- Pegasos (palkanlaskenta)
- Primus, Kurre, Wilma (opetuksen ja varhaiskasvatuksen toiminnanohjaus)
- ProConsona (päivähoito)
- ProEconomica Premium (taloushallinto)
- Sanoma Pro (opetusohjelma)
- Sympahr (henkilöstöhallinta)
- Sähköpostijärjestelmä (Microsoft Office 365)
- Titania (työvuorosuunnittelu)
- Unes isännöinti
- Wintie (yksityisteiden hallinta)
- WordPress (verkkosivut)
- Xerox tulostusjärjestelmä

5 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 2020 aikana yhtään tietopyyntö 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 2020 aikana.

6 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. Niistä on varoitettu henkilökuntaa sekä annettu tarvittaessa toimintaohjeita.

Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

Pelastus- ja turvallisuussuunnitelmat on päivitetty koulussa ja päiväkodissa vuonna 2020 ja virastotalolla 2019. Koulussa on suoritettu turvallisuusharjoitus vuonna 2020.

Tilinpäätöksessä on tehty tietojärjestelmien riski- ja vaikutustenarviointi.

7 Arviointi ja kehittäminen

1.1.2020 voimaan astunut tiedonhallintalaki velvoittaa organisaatioilta tiedon elinkaarenhallinnan perusvaatimusten kuvantamista ja julkistamista yhtenäisenä kokonaisuutena. Eri velvollisuuksien täyttämiseen on olemassa siirtymäaikoja. Ensimmäisenä valmiina tulee olla tiedonhallintamalli 1.1.2021 mennessä.

Tiedonhallintamallin on sisällettävä vähintään seuraavat tiedot ja kuvaukset:

- Toimintaprosesseista
- Tietovarannoista
- Tietoaineistoista
- Tietojärjestelmistä
- Tietoturvajärjestelyistä

Tiedonhallintalain velvoitteiden mukaisesti tiedonhallinta- ja digiturvamallien laatiminen käynnistetään kevään 2021 aikana.

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).

Puumalan kunnan Tietoturvapolitiikka päivitetään vuoden 2021 aikana.

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

Aloitetaan toimenpiteet turvatulostuksen käyttöönottoon koululla koko henkilökunnan osalta, ettei arkaluontoisia asiakirjoja jäisi monitoimilaitteeseen.

Etätyöskentelyn lisääntyessä ohjeistetaan henkilöstöä ottamaan tietosuoja ja tietoturvallisuus huomioon työskenneltäessä muualla kuin työpaikalla.

Käynnistetään vuosittain suoritettava tietojärjestelmien käyttöoikeuksien katselmointi tietosuojavastaavan organisoimana.

Osallistutaan Digi- ja väestöviraston (DVV) järjestämään Taisto2021 -harjoitukseen.