27.4.2022

Tietojenkäsittely pilvipalveluissa

Yleistä pilvipalveluista

Tämän ohjeen tarkoituksena on kertoa yleisesti huomioitavat asiat, kun kaupungin toiminnassa syntyviä tietoja tallennetaan ja käsitellään erilaisissa pilvitallennustiloissa ja -palveluissa. Ohjeen on laatinut Savonlinnan kaupungin tietohallintopäällikkö/tietoturvavastaava ja tietosuojavastaava.

- Valtiovarainministeriö julkaisi linjaukset julkisen hallinnon pilvipalveluista 18.1.2019. Linjaukset määrittävät, miten julkisen hallinnon organisaation omistamaa tietoa voidaan käsitellä pilvipalveluissa. Linjausten tavoitteena on tukea valtion, maakuntien ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita. Linkki julkaisuun: https://vm.fi/-/linjaukset-julkisen-hallinnon-pilvipalveluista-julkaistu
- Traficomin Kyberturvallisuuskeskus julkaisi Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) 29.5.2019. PiTuKri:n tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta. Linkki julkaisuun: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri
- Pilvipalvelussa (esim. Microsoft 365, jäljempänä M365 sekä Googlen Classroom/G Suite for Education koulujen pilvipalvelut), tiedostot ja palvelimet sijaitsevat palveluntarjoajan konesaleissa (fyysisesti usein ulkomailla ja tietojenkäsittelyä/ylläpitoa tehdään ja siten myös tietoja luovutetaan EU-ETA maiden ulkopuolelle ja noudatetaan ko. yhtiöiden tietosuojasopimusliitteittä (DPA) sekä kyseisten maiden lakeja.
- Jos käyttämäsi päätelaite rikkoontuu, niin pilvipalvelimiin siirtämäsi tiedot eivät katoa. Savonlinnan kaupungin ATK-palvelukeskus ei varmista pilvipalveluiden dataa pilvien ulkopuolelle vaan jatkuvuuden osalta ollaan palveluntuottajan peruspalvelusopimusten palvelutasojen alaisia, jotka pääsääntöisesti ei anna takeita datan säilyvyydestä. Tämänkin vuoksi kriittiset tiedot tulee aina tallentaa kaupungin operatiivisiin järjestelmiin tai tiedostopalvelimiin (ns. O/M-levyt).
- Pilvipalveluita käytettäessä on noudatettava annettuja ohjeita, jotta esim. rajatulle joukolle tarkoitettu aineisto ei joudu sivullisten haltuun.
- Pilvipalvelut jaetaan yksityisiin pilvipalveluihin ja julkisiin.
    1. **Yksityiset pilvipalvelut**, joilla tarkoitetaan esimerkiksi:
        - Toimialojen hankkimia ja atk-palvelukeskuksen hyväksymiä eri palveluntuottajien pilvestä tarjoamia SaaS-palveluita ja -ohjelmistoja (esim. Facta, Primus, Vesikanta, Intime, Personec F/ESS/OSS jne.). **Näiden osalta tietojenkäsittelyohjeet annetaan aina tapauskohtaisesti tiedon omistajan, rekisterinpitäjän ja pääkäyttäjien toimesta.**
        - Kaupungin hankkimia globaaleja pilvipalveluita, kuten esimerkiksi Microsoft M365 ja Google Education-pilvipalvelut. **Huomioi, että näissä ns. kolmansia maita koskevissa pilvipalveluissa ei saa toistaiseksi käsitellä kaupungin salassa pidettäviä tietoja (Julkisuuslaki, linkki) tai laajoja henkilötietoja sopimusteknillisistä syistä (GDPR, linkki).** Tarvittaessa tapauskohtaisesti

toteutetaan GDPR:n mukaisia vaikutustenarviointeja ja tietosuojasopimuksia tarkentavia ohjeistuksia. Varmista oikea toimintamalli esihenkilöltäsi sekä tiedon omistajalta sekä tietohallintopäälliköltä ja tietosuojavastaavalta.

2. **Julkisia pilvipalveluita** ovat esim. sosiaalisen median palvelut (Facebook, Twitter jne.), yleiset sähköpostipalvelut (Outlook.com, Gmail.com jne.) sekä julkiset tiedostojen välityspalvelut (Dropbox.com jne.). **Savonlinnan kaupungin tietoja ei saa käsitellä kuin työnantajan määräämissä työhön tarkoitetuissa tietojärjestelmissä ja ohjelmissa.**

Sähköisen tietojenkäsittelyn tietoturvalliset periaatteet

EU:n yleinen tietosuoja-asetus (GDPR) ja Tiedonhallintalaki edellyttävät, että kuntien vastuulla olevat tiedot on suojattu ja että niihin rajataan pääsy työtehtävien mukaisesti. Jokainen työntekijä on vastuussa tietoturvan ja tietosuojan toteuttamisesta omalta osaltaan. Jokainen työntekijä vastaa siitä, että henkilötietoja käsitellessään noudattaa niitä koskevia lakeja ja annettua ohjeistusta. Esimiehen tehtävä on huolehtia siitä, että työntekijällä on työtehtävän mukaiset käyttöoikeudet tietojärjestelmiin ja tietoaineistoihin. Esihenkilö vastaa myös siitä, että käyttöoikeudet lakkautetaan, kun työntekijä poistuu organisaation palvelusta.

Tietojenkäsittely käytännössä

Kaupungin vastuulla ja omistuksissa olevat tiedot pitää tallentaa ja ylläpitää niiden käyttöön suunnitelluissa ja hankituissa järjestelmissä, laitteissa ja ohjelmistoissa (esim. Effica, Wilma, Facta) riippumatta siitä käytetäänkö palvelua pilvipalvelusta (SaaS) vai ei. **Salassa pidettävän tiedon sekä laajoja henkilötietoja sisältävän tiedon osalta pitää aina erityisesti huolehtia ja arvioida lain mukaisuus ennen käyttöä.** Esihenkilö, johto, tietohallinto ja tietosuojavastaava auttavat tämän arvioinnissa. Henkilötietojen käsittelyn osalta vastuu on aina viime kädessä rekisterinpitäjällä, jolta pitää pyytää lupa henkilötietojen käsittelyyn ja mahdollisuus muutoksiin käytetyissä välineissä.

Esimerkiksi **Savonlinnan kaupungin Microsoft 365-pilvipalveluihin** (Sähköposti/Outlook, OneDrive, Teams, Sharepoint jne M365 sovellukset) **ei saa tallentaa ja käsitellä salassa pidettävää eikä laajoja henkilötietoja, vaan tiedot on tallettava ja käsiteltävä muilla soveltuvilla välineillä** kuten esim. Turvaposti, ATK-palvelukeskuksen henkilöstön Suomessa ylläpitämät tiedostopalvelimet (M:- ja O:-levy). Kysy aina tarvittaessa apua esihenkilöltäsi, rekisterinpitäjältä sekä IT Helpdeskistä ja/tai tietosuojavastaavalta oikean tietojenkäsittelyn varmistamiseksi. Tietoja ei saa käsitellä tai säilyttää tarpeettomasti.

Microsoft 365 mahdollistaa työtiedostojen käsittelyn myös muualla kuin kaupungin verkossa kuten esimerkiksi kotilaitteilla. Työtiedostoja ei saa tallentaa kotikoneelle ja on myös huolehdittava, että on varmasti kirjautunut ulos työympäristöstä, kun poistuu yhteiskäyttöiseltä koneelta. Kotikoneen suojaus haittaohjelmia vastaan on pidettävä ajan tasalla. Kotikonetta tai muuta ”ei Savonlinnan IT:n hallitsemaa laitetta” käytettäessä, käyttäjän tulee hyväksyä ja käyttää Savonlinnan IT:n määrittelemiä tietoturvasääntöjä ja -ohjeita, ja näiden käyttöä ja toiminnallisuuksia voidaan rajoittaa Savonlinnan kaupungin tietojenkäsittelyn osalta teknisillä rajoitteilla (esim. ulkomailla työskentely estetty).

Arkistoitavien tietojen osalta pitää noudattaa arkistonmuodostussuunnitelmia. Arkistoon siirtäminen pitää tehdä mahdollisimman pian asiakirjojen käsittelyn päätyttyä.

Julkisten tietojen käsittely

Julkisia tietoja voidaan tallentaa ja käsitellä kaupungin hankkimissa pilvipalveluissa. Julkisia henkilötietoja (esim. nimitiedot) tulee kuitenkin käsitellä harkiten ja perustellusti. Tietojen julkisuus ja niiden julkaiseminen ovat kaksi eri asiaa. **Julkisia tietoja voidaan käsitellä avoimesti ja tallentaa pilvipalveluihin, mutta julkaisemisessa ja jakamisessa pitää käyttää harkintaa ja noudattaa lainsäädäntöä.**

Kotihakemiston käsittely

Savonlinnan kaupungin työskentely-ympäristöön kuuluu jokaisen käyttäjän *henkilökohtainen käyttäjähakemisto M-levy*, jonne on käyttöoikeus vain käyttäjällä itsellään. M-levyt sijaitsevat kaupungin tiedostopalvelimella, josta ATK-palvelukeskus ottaa varmuuskopioita palvelunsa mukaisesti. **Tallenna ja käsittele täällä kaikki tärkeä, salainen ja henkilötietoja sisältävät tiedostot, mitkä eivät voi olla suoraan niihin hankituissa operatiivisissa tietojärjestelmissä (kuten Wilma, Primus, Facta jne).** Huomioi säilytysajat erityisesti henkilötietojen säilytyksissä. Tiedot tulee poistaa heti, kun niitä ei enää tarvita.

M365-ympäristön palveluihin kuuluu mm. *henkilökohtainen OneDrive-tallennuspalvelu*. Noudata pilvipalvelun osalta em. tietojenkäsittelyohjetta. OneDriven tietojenkäsittelyyn liittyy lisäksi huomioon otettavia seikkoja.

- Työsuhteen päättyessä sähköpostiosoite ja -laatikko, M-levyasema ja henkilökohtainen OneDrive poistetaan, ellei erillisellä valtakirjalla ole sovittu siirrosta toiselle henkilölle.
- Siirrä tarvittaessa käsittelyä edellyttävä työpostisi työnantajan käyttöön omatoimisesti tai anna erillinen valtakirja edellä mainittujen henkilökohtaisten työkalujen (sähköposti) ja tietojen (M-levyasema ja OneDrive) siirtoon toiselle henkilölle (esihenkilö tai joku muu nimetty henkilö). Poista mahdolliset henkilökohtaiset viestit – noudata annettua ohjeistusta. (Yhteistyötoimikunta xx.x.2022, §xx)

Edellä mainitut seikat on otettava huomioon erityisesti tietosuojan näkökulmasta. OneDrivella ei tule säilyttää mitään tarpeetonta aineistoa ja ennen työsuhteen päättymistä se on tyhjennettävä sellaisesta aineistosta, jota ei ole tarkoitus valtakirjalla määritellyn henkilön käyttöön.

Esihenkilön tehtävä on huolehtia siitä, että atk-palvelukeskus saa tiedon työsuhteessa tapahtuvista muutoksista, jotta järjestelmässä säilyy ajantasainen tieto työntekijän käyttöoikeuksista. Työntekijällä on oltava käyttöoikeudet vain siihen aineistoon, mitä hän tarvitsee työtehtävissään.