

Julkisen sektorin AI-akatemia – tekoälyn tietosuoja ja tietoturva

Tekoälysovellukset ja tietoturvallisuus

- Markkinoilla on paljon eri tekoälysovelluksia joiden tietosuojakäytännöt vaihtelevat ohjelmistokohtaisesti
- Laveasti jaoteltuna on olemassa **kuluttajakäyttöön** tehtyjä tekoälysovelluksia sekä **organisaatiokohtaisia** tekoälyratkaisuja
- Tekoälyn turvallinen käyttö ja vastuulliset käyttötarkoitukset saattavat siis olla hyvinkin erilaisia eri ratkaisujen välillä.
- **Hyödynnä aina ensisijaisesti organisaatiosi valitsemaa tekoälysovellusta**

Kuluttajakäyttöön tehty ratkaisu	Organisaatiokohtainen ratkaisu
Tietojen hyödyntäminen • Kuluttajakäyttöön tehtyt, usein ilmaiset ratkaisut hyödyntävät lähtökohtaisesti käyttäjän tekoälylle syöttämiä tietoja mallin kehittämiseen tai niitä voidaan käyttää yleisissä tietokannoissa • Kaikki tieto jonka tekoälylle syötät voi siis päätyä kolmansien osapuolien käsiin Turvallisen käytön peruseriaatteet • Kysy vain yleisiä ja "fiktiivisiä" kysymyksiä • Käytä syötteissä anonymisoitua tietoa, muista että tekoäly lukee myös kuvien tiedot • Käytä vain julkisesti saatavilla olevaa tietoa • Älä syötä tekijänoikeudellisesti suojattua sisältöä • Älä syötä toisen tietoa ilman lupaa tai tietoa johon sinulla ei kuuluisi olla pääsyä	Tietojen hyödyntäminen • Organisaatiokohtaisessa ratkaisussa puolestaan toimitaan usein suljetussa ympäristössä, jossa tiedon käsittelylle on erilaiset käytännöt. • Esimerkiksi Microsoft Copilot ei luovuta tietoja eteenpäin eikä hyödynnä niitä mallin kehittämisessä Turvallisen käytön peruseriaatteet • Kaikki tieto organisaation sisällä ei kuulu kaikille - kiinnitä siis huomiota siihen minkälaisilla käyttöoikeuksilla jaat organisaation sisällä tietoa ja mihin tietoon kuka tahansa pääsee tekoälyn avulla käsiksi • Myös tekoälyn tuottama tieto, jonka lähdeaineistona on käytetty rajattua tietolähdettä on pidettävä salassa niiltä joilla ei pitäisi olla pääsyä tietoon

Muista siis nämä!

Tarkista aina tiedon luokittelu ja sen asettamat lähtökohdat tekoälyn käytölle

- Jo Julkinen tieto – esim. tiedote
- Sisäinen – esim. sähköposti
- Luottamuksellinen – esim. Sisäinen raportti
- Salassapidettävä – esim. turvallisuusasiakirja



Tarkkana verkossa

- Tekoälysovelluksiin liittyvät huijaukset ovat yleisiä ja sovelluksia on tarjolla paljon
- Ole tarkkana vaikkapa verkko-osoitteiden kanssa ja noudata erityisesti kuluttajaversioiden sivuilla asioidessa yleistä valvutuneisuutta

Sallitut sovellukset ja käyttötarkoitukset

- Organisaatiossa on eri käytäntöjä tekoälytyökalujen käytön suhteen
- Tarkista siis aina suositellut työkalut kuhunkin käyttötarkoitukseen organisaatiosi tietosuoja- tai tekoälyvastaavalta

Jos väärinkäytös tai virhe on päässyt tapahtumaan

- Keskeytä työ ja estä leviäminen
- Pyri poistamaan tieto palvelusta jos mahdollista
- Ilmoita tietosuojavastaavalle