

12.9.2023

TEKOÄLY JA HENKILÖTIETOJEN TIETOSUOJA

Tekoälyllä tarkoitetaan tietokoneen tai tietokoneohjelman kykyä käyttää perinteisesti ihmisen älyyn liitettyjä taitoja. Näitä taitoja ovat mm. päättely, oppiminen, suunnitteleminen tai luominen. Tekoäly voi auttaa sinua työssäsi, mutta huomioi sen käytössä erityisesti seuraavat tietosuojan ja -turvaan liittyvät asiat.

Tekoälypalvelujen käytössä on huomioitava GDPR:n eli EU:n yleisen tietosuoja-asetuksen vaatimuksia. **Älä koskaan syötä julkisiin tekoälypalveluihin (esim. Chat GPT, Google Bard, Bing Chat) mitään henkilötietoja.** Älä myöskään syötä palveluun salassa pidettävää tai turvaluokiteltua tietoa, asiakastietoja, arkaluonteisia tietoja, järjestelmä-, tietokanta- tai salasanatietoa tai organisaatioon liittyvää tunnistettavaa tietoa. Julkiseen tekoälypalveluun voit siis laittaa vain julkisia tietoja.

Jos teet tutkimusta, älä lataa tekstiäsi verkossa oleviin julkisiin tekoälypalveluihin. Suojele omaa julkaisematonta työtäsi, varsinkin jos siinä on salassa pidettävää tai arkaluonteista tietoa. Julkisten tekoälypalvelujen käytössä on huomioitava, että tekoäly hyödyntää syötettyjä kysymyksiä oppimiseen ja jakaa eteenpäin niissä saatua tietoa.

Muista tarkistaa tekoälypalvelun tuottamat tulokset ennen niiden julkaisemista tai muuta hyödyntämistä. Tekoäly voi hallusinoita eli "keksiä" tietoa ja silloin tekoäly tuottaa virheellistä tietoa. Tekoälyjärjestelmät eivät myöskään osaa erotella puolueellista tietoa puolueettomasta tiedosta. Tekoäly vaatii aina ihmisen valvontaa.

Tekoälyjärjestelmät ovat tietojärjestelmiä. Kaikissa tietojärjestelmissä voi olla tietoturvaheikkouksia, joita voidaan käyttää pahoihin tarkoituksiin

12.9.2023

(kyberrikollisuus). Riskejä voidaan ehkäistä erilaisin teknisin ratkaisuin (esim. salausten menetelmät).

Henkilötietojen tietosuojan yleisiä perusteita

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.

Tietosuojaperiaatteita on noudatettava aina kun henkilötietoja käsitellään.

Sinun on myös pystyttävä osoittamaan, että noudatat periaatteita.

Tietosuoja turvaa myös sinun oikeutesi henkilötietoja käsiteltäessä.

Tietosuojaperiaatteiden mukaan henkilötietoja on

- käsiteltävä lainmukaisesti (käsittelyperuste löydyttävä), asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (kerro käsittelystä selkeästi ja ymmärrettävästi)
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten (käyttötarkoitussidonnaisuus)
- kerättävä vain ja ainoastaan tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden (tietojen minimointi)
- päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä (tietojen täsmällisyys)
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (hävittäminen tai anonymisointi heti kun ei tarvita)
- käsiteltävä luottamuksellisesti ja turvallisesti (riskien arviointi ja suojaustoimet).

Kaikki henkilötietoihin kohdistuvat toimenpiteet suunnittelusta keräämiseen, käsittelyyn ja henkilötietojen poistamiseen ovat henkilötietojen käsittelyä. Tietosuojaperiaatteita on noudatettava koko henkilötietojen käsittelyn elinkaaren ajan.

12.9.2023

Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Perusteet ovat rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleistä etua koskeva tehtävä tai julkinen valta sekä rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Säätelyä

Tekoälyteknologiaa käytetään maailmassa koko ajan enemmän ja se vaatii yhteisten pelisääntöjen kehittämistä. EU:ssa on valmisteilla tekoälyasetus eli Artificial Intelligence Act (AIA). Sen tarkoituksena on varmistaa, että tekoälyn käyttö olisi turvallista ihmisille ja organisaatioille. Ehdotettu EU:n tekoälyasetus perustuu riskipohjaiseen lähestymistapaan, jossa asiaa tarkastellaan ihmisten terveyden, turvallisuuden ja perusoikeuksien kautta. Säätelyn haasteena on tekoälyteknologian nopea kehitystahti.

Kansallisessa jo voimassa olevassa lainsäädännössä tulee noudatettavaksi mm. Julkisuuslain (621/1999) 22 § Asiakirjasalaisuus.

”Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi.”

Mervi Hätinen, Hallinnon suunnittelija / tietosuojavastaava
tietosuojavastaava@savonia.fi