Tekoäly, tietosuoja ja yksityisyys

Sekä uhkia, että mahdollisuuksia

Tietosuojavastaava, väitöskirjatutkija Ilona Sidoroff 6.3.2025

Miten tietosuoja-asiantuntija suhtautuu tekoälyyn?

Neutraalisti

Muista tietosuojaperiaatteet

Läpinäkyvyys → kerro asiakkaille, mitä heidän tiedoillaan tehdään
Lainmukaisuus → noudata lakia tietojen käsittelyssä
Asianmukaisuus → käsittelytoimien ja –tarkoituksen tasapaino
Täsmällisyys → tietojen pitää olla oikeita, päivitys ja virheiden korjaus tarvittaessa
Käyttötarkoitussidonnaisuus → tietoja saa käyttää vain ilmoitettuun tarkoitukseen
Tietojen minimointi → tietoja ei saa käsitellä yli tarpeen
Säilytyksen rajoittaminen → tietoja ei saa säilyttää pidempään kuin tarve vaatii
Luottamuksellisuus → ulkopuoliset eivät pääse käsiksi tietoihin

Lisätietoa tietosuojaperiaatteista

https://tietosuoja.fi/tietosuojaperiaatteet

Muutama nosto

Käyttötarkoitussidonnaisuus → muuta tarkoitusta varten kerättyjä tietoja ei saa käyttää esim. tekoälyn kouluttamiseen

Asianmukaisuus → tarvitaanko tekoälyä? Älä ammu kärpästä tykillä

Luottamuksellisuus → älä myöskään vie norsua posliinikauppaan, ts. arkaluonteisia tietoja järjestelmään, jossa ne eivät ole turvassa

Luottamuksellisuus, käyttötarkoitussidonnaisuus, avoimuus...

Uutinen

Työntekijät vuotavat asiakastietoja ChatGPT:hen – Näin paljon salassa pidettävää tietoa päätyy tekoälylle

Suvi Korhonen 20.1.2025 11:47 | päivitetty 20.1.2025 11:47 TEKOÄLY TIETOSUOJA

Kielimalleille jaettujen tietojen määristä on nyt tehty tutkimusta.

Tivi 20.1.2025

Teknologia

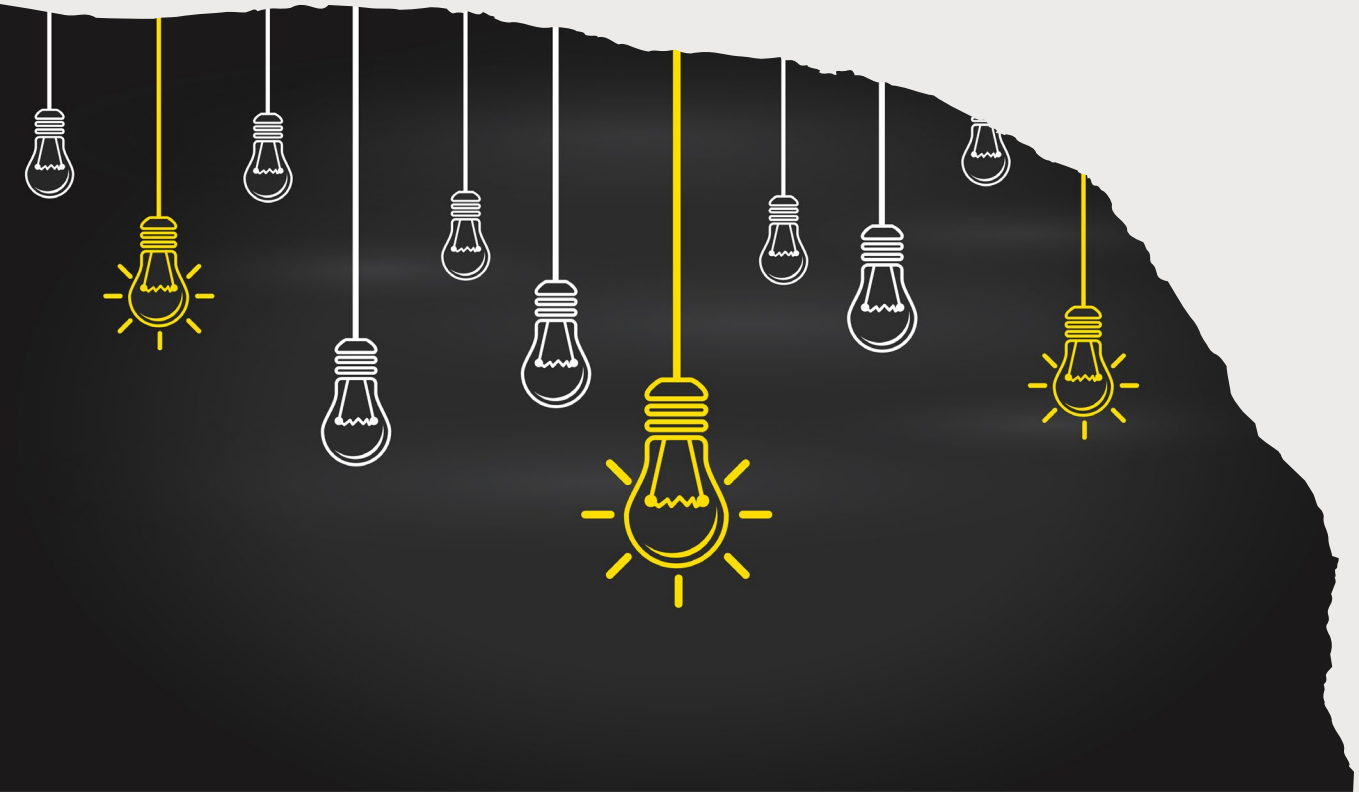
Meta ruokkii pian teköälyään käyttäjiensä kuvilla ja teksteillä, eikä kysy siihen lupaa

Facebookin eurooppalaiset käyttäjät ovat alkaneet saada viestejä, joissa kerrotaan päivityksistä yksityisyysasetuksiin. Viesteissä palvelut omistava Meta kertoo kouluttavansa tekoälymalleja käyttäjien sisällöillä.

Yle 9.6.2024

Tietosuoja vaatii tiedonhallintaa

Tietosuojan hallinta



- ROPA (record of processing activities) eli seloste käsittelytoimista
  - Pakollinen kaikille organisaatioille
  - Organisaation sisäinen dokumentti, tarvittaessa valvovalle viranomaiselle annettava
  - Sisältää tiedot kaikista organisaation käsittelytoimista = tiedonhallintaa
- Tietosuojaseloste
  - Asiakkaan informointia eli viestintää
- Tietosuojan vaikutustenarviointi
  - Tarvittaessa korkea riskin käsittelystä tehtävä arviointi

Tärkeintä olisi tietosuojan perusasiat

Dokumentointivelvoite: mitä tietoja käsittelet, miksi, miten, missä, kenellä on pääsy, miten toteutatte tietosuojaperiaatteet, rekisteröityjen oikeudet jne.

Tietosuojan vaikutustenarvioinnit: korkean riskin käsittelyssä on arvioitava vaikutukset rekisteröidylle (ihminen, asiakas)

Riskiarviointi: mitä riskejä käsittelyyn liittyy, miten ne taklataan → tehtävä aina, kun käsitellään henkilötietoja tekoälyllä

Riskeistä

- Yleisesti käytössä oleva tekoälyjärjestelmä, kuten ChatGTP
- Tekoäly integroituna esim. laskutusjärjestelmään; suljettu järjestelmä

→ Erilaiset riskit, mm. käsitelläänkö asiakasdataa, miten kontrolloidaan sitä, mitä dataa järjestelmä käyttää, minne data menee, käytetäänkö sitä koulutukseen

→ Erilaiset riskit vaativat erilaiset hallintakeinot

Tunne datasi, jotta
voit hallita sitä

Hallitse datasi:
missä se on, kuka
pääsee käsiksi?

Muutamia järjestelmiä

- Excell, word tms. ihan hyvä, jos kyse on hyvin pienestä yrityksestä, joka ei käsittele paljon henkilötietoa, esim. kampaaja
- PrivacyDesigner tätä käytän itse, innovatiivinen ja monipuolinen, sisältää myös tekoälyn hallintamallin, suosittelen isommalle organisaatiolle tai paljon henkilötietoja käsitteleville
- Easy GDPR (D-Fence), helppo ja edullisempi pk-yritykselle
- Privaon

Tekoälyn mahdollisuudet?

- Voisiko tunnistaa esim. vanhentuneen tiedon ja kehottaa poistamaan sen?
- Voisiko tunnistaa päällekkäisiä järjestelmiä?
- Voisiko varmistaa paremmin tiedon oikeellisuuden?
- Voisiko poimia laajasta datamassasta oleellisen → mahdollisuus poistaa epäolennainen data?

Teknologia

Tekoäly tarkkailee liikkeitäsi K-kaupoissa ja yrittää tunnistaa myymälävarkaat – tällaiset liikkeet ovat epäilyttäviä

Järjestelmä lähettää tapahtumasta videon kauppiaan puhelimeen, jos se tulkitsee valvontakamerassa näkyvän toiminnan epäilyttäväksi.

Yle 27.12.2024

Tekoäly ei ole pelkkä uhka, kun tietosuojan perusasiat ovat kunnossa