Opas tekoälyn turvalliseen käyttöön

TyhyTeko-hanke

Euroopan unionin osarahoittama
Elinvoimakeskus
SEAMK Seinäjoen ammattikorkeakoulu
LAPIN AMK Lapland University of Applied Sciences
SAVONIA
Tampereen ammattikorkeakoulu
XAMK
jamk

Turvallinen tekoälyn käyttö

Turvallinen tekoälyn käyttö syntyy tiedosta ja yrityksen tekemistä päätöksistä. Yrityksen on päätettävä, miten tekoälyä käytetään, kuka käytöstä vastaa ja millaista tietoa tekoälylle ei saa syöttää. Ilman näitä päätöksiä tekoälyn käyttö on epävarmaa, hallitsematonta ja altistaa yrityksen tietoturva- ja maineriskeille.

Jotta tekoälyn käyttö on turvallista, **yrityksen tulee määritellä vähintään:**

- mitä tekoälytyökaluja käytetään ja mitkä ovat kiellettyjä
- missä ympäristöissä tekoälyä käytetään ja miten niihin kirjaudutaan
- mitä tietoa tekoälyyn saa syöttää ja mitä ei
- mitkä tekoälyn tuottamat sisällöt tarkistetaan ennen käyttöä
- kuka vastaa tekoälyn käytöstä, seurannasta ja auditoinnista
- miten toimitaan tilanteissa, joissa tekoälyn käyttöön liittyy virhe tai tietoturvariski

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Turvallinen tekoälyn käyttö

- Tekoälyn käyttöön liittyvä vastuu on aina ihmisellä. Tekoäly on työväline, ja yritys sekä sen työntekijät vastaavat loppukädessä kaikesta tekoälylle syötetyn sisällön ja aineiston käytöstä sekä tekoälyn tuottaman tiedon hyödyntämisestä ja julkaisemisesta.
- Tekoälyn tuottamat sisällöt on tarkistettava ennen niiden lähettämistä, julkaisemista tai käyttöä.
- Yrityksen tulee seurata ja arvioida tekoälyn käyttöä säännöllisesti. Hyvää on määritellä selkeä toimintamalli tilanteisiin, joissa tapahtuu tietoturvan rikkoutuminen tai arkaluonteista tietoa päätyy tekoälyn käyttöön. Tällaisia tilanteita voivat olla esimerkiksi asiakastietojen syöttäminen tekoälyyn, tietovuoto tai sopimusrikkomus.

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

EU AI Act, mitä se tarkoittaa käytännössä?

EU:n tekoälyasetus (AI Act) on EU:n yhteinen sääntely, joka määrittää, miten tekoälyä saa kehittää ja käyttää. Sen tavoitteena on varmistaa, että tekoäly on turvallista, läpinäkyvää ja kunnioittaa ihmisten oikeuksia. **Asetus koskee kaikkia yrityksiä, jotka hyödyntävät tekoälyä toiminnassaan**. Se ei kiellä tekoälyn käyttöä, vaan ohjaa käyttämään sitä vastuullisesti. Yritykselle tämä tarkoittaa käytön tunnistamista, riskien ymmärtämistä ja vastuun kantamista.

- Yritys vastaa käytöstä ja lopputuloksista, ei vain teknisestä työkalusta
- Yrityksen on pystyttävä näyttämään tarvittaessa toteen, miten se on tekoälyä käyttänyt
- Asetus myös mahdollistaa luottamuksen rakentamisen ja kilpailuedun, kun tekoälyä käytetään avoimesti esimerkiksi markkinoinnissa.

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Tietosuoja ja vastuullinen käyttö

Muista nämä:

- Älä syötä tekoälyyn: **henkilötietoja, arkaluonteista tietoa, liikesalaisuuksia**
- Tekoäly toimii **työn tukena**, ei itsenäisenä päätöksentekijänä
- Noudata **GDPR:ää ja yrityksen omia tietosuojakäytäntöjä**
- Älä käytä tekoälyä kiellettyihin tarkoituksiin esim. manipulointi, arviointi ilman perusteita
- Tunnista missä tekoälyä käytetään yrityksessä (työkalut, automaatio, chatbotit), ja kerro avoimesti, kun asiakas asioi tekoälyn kanssa
- **Hyvä sääntö:** Jos et voi jakaa tietoa sähköpostitse, älä syötä sitä myöskään tekoälylle!

Esimerkki tietosuojalausekkeesta:

"Hyödynnämme tekoälyä työn tukena esimerkiksi tekstien luonnostelussa ja tiedon jäsentelyssä. Tekoälyyn ei syötetä henkilötietoja ilman perusteltua tarvetta, ja kaikkia tietoja käsitellään voimassa olevan tietosuojalainsäädännön (GDPR) mukaisesti."

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Mitä tekoälytyökalut osaavat (myös ilmaisversiossa)?

- Kirjoittaa ja ehdottaa tekstiä
- Vastata kysymyksiin ja kysyä jatkokysymyksiä
- Hakea ajankohtaista tietoa netistä
- Tutkia kuvia ja tiedostoja (esim. Reseptit, dokumentit, menut, esitteet…)
- Tehdä ja muokata kuvia
- Analysoida dataa ja asiakirjoja
- Tuottaa videoita ja audiota
- …ja paljon muuta – työkalut kehittyvät ja laajenevat huimalla vauhdilla.

Muista tämä:

- Tekoäly ei ajattele tai tiedä asioita kuten ihminen.
- Se ennustaa parhaan mahdollisen vastauksen, perustuen valtavaan tietomäärään, ajankohtaiseen tiedonhakuun ja todennäköisyyslaskentaan.
- Sitä kannattaa ajatella fiksuna työparina, ei erehtymättömänä asiantuntijana.

- **Ihminen on aina vastuussa tiedon tarkistamisesta ja käyttämänsä/ julkaisemansa materiaalin oikeellisuudesta!**

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Tekoäly osana TyhyTeko-kokeilua

TyhyTeko-kokeilu ei vaadi maksullisia lisenssejä

- Matalan kynnyksen käyttöönotto, ilman lisäkuluja tai kytköksiä yrityksen muuhun IT-ympäristöön.
- Sopii hyvin osaamisen kehittämiseen ja käytön opetteluun.
- Mahdollisuus vertailla eri työkaluja ja saada arvokasta käyttäjäkokemusta ennen mahdollista lisenssin hankintapäätöstä.

Ilmaisversioiden rajoitteita

- Rajalliset ominaisuudet verrattuna maksullisiin lisensseihin
- Ei integrointia yrityksen järjestelmiin (tiedostoihin, sähköposteihin ym.)
- Rajoitetut käyttömäärät (promptit eli kehotteet per päivä)
- Hitaampi vasteaika ruuhka-aikoina

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Tekoäly osana TyhyTeko-kokeilua

Tekoälyn ”pelisäännöt” kokeilun aikana

- Älä anna tekoälylle mitään henkilötietoja.
- Älä anna tekoälylle mitään ainoastaan yrityksen sisäiseen käyttöön tarkoitettuja dokumentteja tai liikesalaisuuksia.
- Sen sijaan julkisesti kenen tahansa saatavilla olevat tiedot, esim. yrityksen verkkosivut ja somekanavat voidaan antaa tekoälylle taustatietoina linkkeinä.
- Tutustu aina ennen työkalun testausta AI-oppaisiin ja tekoälyn turvallisuuteen

Työkaluja saatavilla selaimen kautta (tai sovelluksena):

- https://copilot.microsoft.com
- https://chatgpt.com
- https://gemini.google.com/ (vaatii Google-kirjautumisen)
- https://claude.ai/
- https://grok.com/
- https://www.deepseek.com/en/

→ Seuraavalla sivulla eri työkalujen vertailua

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Ominaisuus	ChatGPT (ilmainen)	Microsoft Copilot (ilmainen)	Google Gemini (ilmainen)	Claude (ilmainen)	Grok (ilmainen/X)	DeepSeek (ilmainen)
Peruskäyttö	Chat, kirjoittaminen, ideointi	Chat, haku, Office-työ	Chat, kirjoittaminen	Pitkät tekstit, analyysi	Ajankohtainen keskustelu, some	Koodi, analyysi
Käytön helppous	Erittäin helppo	Helppo Microsoftissa	Helppo Google-tilillä	Selkeä mutta pelkistetty	Vaatii X-tilin	Vaihtelee, teknisempi
Mallin taso	Hyvä yleismalli	Hyvä + hakupainotus	Hyvä, nopea	Erittäin hyvä tekstissä	Vaihtelee, joskus epätarkka	Yllättävän vahva, etenkin koodissa
Käyttörajat	Rajoitettu	Rajoitettu	Päivärajoja	Tiukat rajat ilmaisessa	Riippuu käytöstä	Usein väljempi
Vaste ruuhkassa	Voi hidastua	Voi hidastua	Voi hidastua	Usein rajoittaa käyttöä	Vaihtelee paljon	Voi hidastua
Tiedostojen käsittely	Rajattu	Rajallinen	Rajallinen	Hyvä tekstille	Heikko	Hyvä teknisessä
Kuvien / multimodaali	Rajattu	Rajattu	Parempi kuvissa	Rajattu	Heikko	Rajattu
Oma data	Ei pääsyä	Ei pääsyä	Ei pääsyä	Ei pääsyä	Ei pääsyä	Ei pääsyä
Integraatiot	Ei suoria	Microsoft-ekosysteemi	Google-ekosysteemi	Ei juuri	X-alusta	Ei
Yritystason tietosuoja	Ei	Ei	Ei	Ei	Ei	Ei
Soveltuvuus työhön	Yleiskäyttö	Toimisto- ja haku	Google-työ	Syvä ajattelu, tekstit	Ajankohtainen sisältö	Koodaus, analyysi
Paras käyttötapa	Kirjoittaminen, ideointi	Tiedonhaku + Office	Arjen tehtävät	Pitkät sisällöt	Trendit, nopea reagointi	Tekniset tehtävät

Päivitetty 04/2026

Microsoft Copilot - Tietosuoja

Tietojen käyttö ja säilytys

- Microsoft Copilot toimii Microsoft 365 –ympäristössä.
- Kevyempi versio Copilot Chat mahdollisesti käytössä yritystilillä ilman lisämaksua.
- Maksullisella yrityslisenssillä on mahdollisuus käyttää organisaation sisäisiä tietoja ja dokumentteja osana työskentelyä.
- Tällöin käyttäjän syöttämät kehotteet ja Copilotin vastaukset pysyvät Microsoftin *sopimuksen* mukaisesti Microsoft 365 -palvelun rajojen sisällä. *Sopimus*, joka on tehty sitoo siihen, että tietoja ei käytetä Microsoftin tekoälyn kouluttamiseen.

Tietosuoja ja vaatimustenmukaisuus

- Microsoft Copilot noudattaa GDPR:ää ja muita tietosuojalakeja.
- Lisenssillä kirjautuneen käyttäjien kehotteet ja Copilotin vastaukset tallennetaan käyttäjän Copilot-toimintahistoriaan, ja nämä tiedot salataan sekä säilytyksen aikana että siirron aikana.

Tietojen sijainti ja käsittely

- Microsoft Copilot reitittää LLM-kutsut lähimpiin alueellisiin palvelinkeskuksiin (EU), mutta kapasiteetin mukaan niitä voidaan käsitellä myös muilla alueilla.
- EU:n käyttäjille on lisäsuojakeinoja EU:n tietorajan noudattamiseksi, ja EU:n liikenne pysyy EU:n tietorajojen sisällä.

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

OpenAI ChatGPT - Tietosuoja

Tietojen käyttö ja säilytys

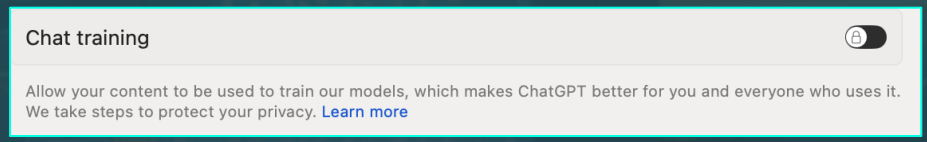
- OpenAI tarjoaa lisenssiasiakkailleen mahdollisuuden tehdä tietojenkäsittelysopimuksen (**D**ata **P**rocessing **A**ddendum, DPA) tukemaan GDPR:n ja muiden tietosuojalakien noudattamista.
- ChatGPT Enterprise- ja ChatGPT Edu -palvelut kuuluvat SOC 2 Type 2 -raportin piiriin, mikä tarkoittaa, että riippumaton kolmas osapuoli on arvioinut niiden tietoturvakontrollit.

Tietosuoja ja vaatimustenmukaisuus

- OpenAI tukee asiakkaidensa GDPR:n ja muiden tietosuojalakien noudattamista tarjoamalla DPA:n.
- API-, ChatGPT Enterprise-, ChatGPT Team- ja ChatGPT Edu -tuotteet kuuluvat SOC 2 Type 2 -raportin piiriin, mikä tarkoittaa, että riippumaton kolmas osapuoli on arvioinut niiden kontrollit varmistaakseen niiden vastaavan alan tietoturva- ja luottamuksellisuusstandardeja.

OpenAI ChatGPT - Tietosuoja

Käyttäjän oikeudet ja tietojen poistaminen



- ChatGPT Free- ja Plus-käyttäjät voivat valita, haluavatko osallistua tulevien mallien parantamiseen asetuksissaan.
- ChatGPT:ssä “Temporary Chats” -toiminto ei käytä keskusteluja mallien kouluttamiseen, mutta ei myöskään tallennu käyttäjän viestihistoriaan.
- API-, ChatGPT Enterprise- ja ChatGPT Team -asiakkaiden dataa ei käytetä mallien kouluttamiseen oletusarvoisesti.

Tietojen sijainti ja käsittely

- OpenAI käsittelee henkilötietoja eri lainkäyttöalueilla, mukaan lukien Yhdysvalloissa sijaitsevilla palvelimilla.
- Vaikka tietosuojalait vaihtelevat maittain, OpenAI soveltaa tässä käytännössä kuvattuja suojatoimia henkilötietoihisi riippumatta siitä, missä niitä käsitellään, ja siirtää tietoja vain laillisesti pätevien siirtomekanismien mukaisesti.

Google Gemini – Tietosuoja 1/2

Tietojen käyttö ja säilytys

- **Tietojenkäsittelysopimus (DPA):** Google tarjoaa asiakkailleen Cloud Data Processing Addendum -sopimuksen, joka tukee GDPR:n ja muiden tietosuojalakien noudattamista. Tämä sopimus määrittelee Googlen ja asiakkaan vastuut henkilötietojen käsittelyssä.
- **Tietoturvasertifikaatit:** Google Cloudin palvelut, mukaan lukien Gemini, ovat saaneet useita tietoturvasertifikaatteja, kuten ISO 27001, ISO 27017, ISO 27018 ja ISO 27701. Lisäksi Google on saanut SOC 2 Type 2 -raportin, joka osoittaa riippumattoman kolmannen osapuolen arvioineen sen tietoturvakontrollit.
- **Tietojen säilytys:** Asiakkaat voivat valita, missä heidän tietonsa säilytetään. Google sitoutuu säilyttämään tiedot asiakkaan valitsemassa sijainnissa, mikä tukee tietosuojalainsäädännön vaatimuksia.

Tietosuoja ja vaatimustenmukaisuus

- **GDPR:n noudattaminen:** Google tukee asiakkaidensa GDPR:n ja muiden tietosuojalakien noudattamista tarjoamalla DPA:n. Lisäksi Google auttaa asiakkaita suorittamaan tietosuojaan liittyviä vaikutustenarviointeja (DPIA) tarjoamalla ohjeita ja resursseja.
- **Tietojen käsittely:** Gemini ei käytä asiakkaiden syötteitä tai vastauksia mallien kouluttamiseen ilman asiakkaan suostumusta. Tämä koskee erityisesti Gemini Code Assist Standard- ja Enterprise-versioita.

Lähteet: https://cloud.google.com/terms/data-processing-addendum; https://business.safety.google/compliance

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Google Gemini – Tietosuoja 2/2

Käyttäjän oikeudet ja tietojen poistaminen

- **Tietojen hallinta:** Asiakkaat voivat hallita ja poistaa tietojaan Google Cloudin hallintatyökaluilla. Tämä mahdollistaa tietojen poistamisen pyynnöstä, mikä tukee GDPR:n mukaisia oikeuksia.
- **Tietojen käyttö mallien koulutuksessa:** Google ei käytä asiakkaiden syötteitä tai vastauksia mallien kouluttamiseen ilman asiakkaan suostumusta. Tämä koskee erityisesti Gemini Code Assist Standard- ja Enterprise-versioita.

Tietojen sijainti ja käsittely

- **Tietojen sijainti:** Google tarjoaa asiakkaille mahdollisuuden valita, missä heidän tietonsa säilytetään. Tämä sisältää vaihtoehtoja Euroopassa, kuten Alankomaissa, Ranskassa, Saksassa, Belgiassa ja Isossa-Britanniassa ja **Suomessa**.
- **Koneoppimisen käsittely:** Kun asiakkaat valitsevat tietojen säilytyssijainnin, Google sitoutuu suorittamaan koneoppimisen käsittelyn samassa sijainnissa. Tämä tarkoittaa, että sekä tietojen säilytys että käsittely tapahtuvat asiakkaan valitsemassa alueella, mikä tukee tietosuojavaatimuksia.

Lähteet: https://cloud.google.com/terms/data-processing-addendum; https://business.safety.google/compliance

Tekoälyn hyödyntäminen käytettävän työkalun toiminnassa ja tietosuojassa

- Anna kehote käyttämällesi tekoälylle:
  - *Kertoisitko, millainen tietosuoja tässä käyttämässäni Copilotissa/ChatGPT:ssä/Geminissä on? Miten antamiani prompteja ja dokumentteja käytetään esimerkiksi kielimallin opettamiseen?*

- Jos tekoäly vastaa esimerkiksi linkillä palvelun tietosuojaselosteeseen, niin jatka kehotteella:
  - *Tee tiivistelmä tietosuojan pääkohdista, käyttäen antamaasi tietosuojaselostetta (+ lisää linkki).*

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko

Kysymys	ChatGPT (OpenAI)	Microsoft Copilot	Google Gemini	Claude (Anthropic)	Grok (xAI)	DeepSeek
Omistajuus tuotokseen	Käyttäjällä	Käyttäjällä	Käyttäjällä	Käyttäjällä	Käyttäjällä	Käyttäjällä
Tekijänoikeussuoja tuotokselle	Mahdollinen, jos ihmisen panos riittävä	Sama periaate	Sama periaate	Sama periaate	Sama periaate	Sama periaate
Vastuu tekijänoikeusloukkauksista	Käyttäjällä, OpenAI voi tarjota suojaa maksullisissa	Käyttäjällä, Microsoftilla rajattu suoja yrityksille	Käyttäjällä	Käyttäjällä	Käyttäjällä	Käyttäjällä
Koulutusdata sisältää suojattua sisältöä	Kyllä, osittain	Kyllä (OpenAI + Microsoft data)	Kyllä, osittain	Kyllä, mutta painottaa “turvallista käyttöä”	Todennäköisesti kyllä	Kyllä, epäselvää mitä tarkalleen
Käytetäänkö syötettyä dataa mallin koulutukseen	Voi käyttää, ellei estetty (asetuksista / sopimuksella)	Voi käyttää, riippuu palvelusta	Voi käyttää	Ei oletuksena Claude-chatissa, mutta vaihtelee	Voi käyttää, sidottu X-dataan	Epäselvää, riski suurempi
Läpinäkyvyys datasta	Kohtalainen	Kohtalainen	Kohtalainen	Parempi kuin monilla	Heikompi	Heikko
Yritystason tietosuoja	Ei ilmaisessa	Ei ilmaisessa	Ei ilmaisessa	Ei ilmaisessa	Ei	Ei

Tekijänoikeudet eri kielimalleissa. Päivitetty 04/2026

1. Tavoite - Mikä on tehtävän tai kysymyksen päämäärä?	2. Konteksti – Missä tilanteessa ja kenelle?	3. Odotukset – Millainen vastaus olisi hyödyllinen?	4. Lähde – Onko jotain, mihin vastauksen tulisi perustua?
Selkeä, tarkka ja tarkoituksenmukainen pyyntö tekoälylle. Promptin (kehotteen) laadulla on valtava vaikutus siihen, kuinka hyödyllisen ja oikeansuuntaisen vastauksen tekoäly antaa. Voit antaa tekoälylle roolin, missä se toimii.	**Kerro lyhyesti taustasta tai kohderyhmästä.** Esimerkiksi perustiedot yrityksestä (kahvila / leipomo), asiayhteys, kohderyhmä tms. Mitä enemmän taustatietoa, sen parempi vastaus.	**Toivottu muoto:** lista, taulukko, luonnos, valmis teksti, pidempi blogikirjoitus? **Pituus:** lyhyt yhteenveto vai yksityiskohtainen selostus? **Kieli/tyyli:** rennosti vai virallisesti? Suomeksi vai englanniksi…?	Voit liittää mukaan tietoa, verkkosivun, kuvan, aikaisemman tekstin tai dokumentin. Tekoäly voi hyödyntää tätä lähteenä ja jatkaa sen pohjalta. **Huomioi dokumentin sisältö, älä lähetä henkilötietoja tai arkaluontoista sisältöä!**
“Olet ravintolatoiminnan ja perehdytyksen asiantuntija…” “Laadi minulle…” “Anna 5 ideaa…”	“Olen laatimassa perehdytysopasta… haluaisin huomioida erityisesti uudet osa-aikaiset työntekijät, jotka työskentelevät opintojen ohessa…”	“Kirjoita oppaaseen sopivalla tavalla…” “Luo taulukkomuodossa…” “Tee tästä blogikirjoitus, joka käyttää yrityksemme viestintätyyliä…”	“Käytä lähteenä tätä verkkosivua ja sen alasivuja…” “Käytä pohjana tätä dokumenttia…” “Ota huomioon tämä nykyinen versio ja ehdota parannuksia…”

Tämä opas tekoälyn turvalliseen käyttöön on koottu osana TyhyTeko-hanketta, lue lisää hankkeesta: www.jamk.fi/TyhyTeko