

# Tekoälyn reilut säännöt



[www.eoppiva.fi](http://www.eoppiva.fi)

Koulutus koostuu neljästä osiosta. Niiden tekeminen vaatii yhteensä noin 90 minuuttia. Käytä koulutukseen kuitenkin juuri sen verran aikaa kuin tarvitset. Meistä jokainen oppii omalla tyylillään ja omaan tahtiinsa, joten voit tarvittaessa keskeyttää osion, palata taaksepäin ja liikkua osioiden välillä vapaasti.

Kun olet suorittanut kaikki osiot, pääset antamaan palautetta ja tilaamaan todistuksen.



Tervetuloa reilun tekoälyn maailmaan



Arvioi tekoälyn riskitaso



Näin kehität suuririskistä tekoälyä



Näin hankit ja otat käyttöön tekoälyä



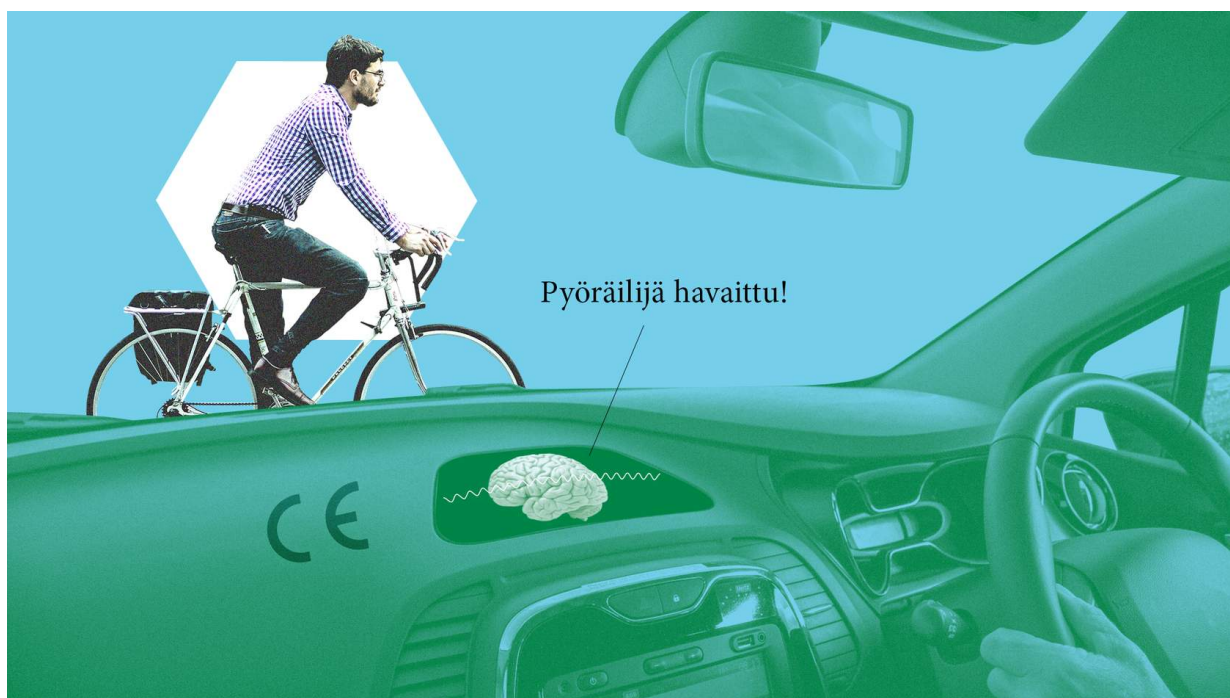
Palaute ja itsearviointi



Todistus ja suorituksen kirjaaminen

# Tervetuloa reilun tekoälyn maailmaan

---



---

**Tekoälyn merkitys yhteiskunnassa kasvaa kasvamistaan. Euroopan unionin tekoälyasetus varmistaa, että tekoälyjärjestelmät on tehty huolellisesti ja niiden aiheuttamat riskit on minimoitu.**

Tekoälyn käyttö ja kehittäminen EU:ssa on edelleen sallittua ja siihen myös kannustetaan.

Tekoälyasetus sallii valtaosan tekoälyn käyttötavoista ilman sen suurempia velvoitteita. Vain jos tekoäly voi aiheuttaa suuria riskejä, on sitä kehitettävä ja otettava se käyttöön erityisen huolellisesti, riskit minimoiden.

Tämä koulutus avaa tekoälyasetuksen käytännön seuraukset tekoälyn kehittäjille ja käyttönottajille.

Myös yksityishenkilöt, jotka usein ovat tekoälyn kohteena, saavat tietoa uusista oikeuksistaan.

## Mitä tekoäly on?

### *Testaa tietosi*

Mitkä seuraavista ovat mielestäsi esimerkkejä tekoälyn käytöstä?

---

☐

A) Chattibotti

☐

B) Kännykän kameran tarkennus ihmisen kasvoihin kuvaa otettaessa

☐

C) Kaistavahti tai sopeutuva vakionopeudensäädin autossa

☐

D) Lentokoneen automaattipilotti

☐

E) Some-palvelun suosittelualgoritmi

SUBMIT

Vaikka tekoäly nousi yleiseksi puheenaiheeksi vuonna 2022, on tekoäly jo vuosikymmenet vauhdittanut yhteiskunnan toimintoja, kansainvälisestä logistiikasta aina roskapostisuodattimiin ja sosiaalisen median algoritmeihin. Tekoälyn rooli yhteiskunnassa ei ainakaan vähene, joten ymmärrys tekoälystä, sen mahdollisuuksista ja sen riskeistä on uusi kansalaistaito. Yhtä tärkeää on myös lainsäädännöllä sanoa, mikä on sallittua ja mikä ei.

Tekoäly-sanaa käytetään arkikielessä eri yhteyksissä eri tavoin, joten on hyvä ymmärtää sen eri merkityksiä:



**AUTOMAATIO**

**Organisaation prosessien automatisointia, mahdollisesti tekoälyä käyttäen, mutta monesti yksinkertaisempien ohjelmoitujen sääntöjen perusteella.**





## **"PERINTEINEN" TEKOÄLY**

**tekee johtopäätöksiä aineistosta. Tällainen tekoäly on ollut olennainen osa yhteiskuntaamme jo pari vuosikymmentä. Ilman sitä meillä ei olisi esimerkiksi toimivia roskapostisuodattimia, sosiaalisen median algoritmeja, toimivaa sähköverkkoa tai tehokasta**



## **GENERATIIVINEN TEKOÄLY**

**Tekoälyratkaisu, joka tuottaa uutta aineistoa sille annetun koulutusaineiston perusteella. Syötetty ja tuotettu aineisto voi olla tekstiä, kuvia, ääntä, videota, organisaation omia tietoja tai teoriassa mitä tahansa.**



## **TEKOÄLY- JÄRJESTELMÄ**

**Toimiva palvelu tai tuote,  
joka hyödyntää tekoälyä.**



## **TEKOÄLYMALLI**

**Datalla koulutettu malli,  
joka toimii  
tekoälyjärjestelmän  
moottorina.**



# YLEISKÄYTTÖINEN TEKOÄLYMALLI

**Yleisluontoinen malli,  
joka voi suorittaa  
monenlaisia eri tehtäviä ja  
jota voidaan hyödyntää  
erilaisissa  
järjestelmissä.**

## *Esimerkiksi*

Yleiskäyttöinen tekoälymalli on tyypillisesti koulutettu laajalla kieliaineistolla ja se pystyy vastaamaan hyvin monenlaisiin kysymyksiin chatbot-tyyppisenä palveluna. Rajoitetumpi tekoälymalli voisi olla koulutettu vaikkapa sosiaalisen median palvelun käyttäjien käyttäytymisdatalla ja sitä voi hyödyntää käyttäjiä kouluttavan sisältösyötteen muodostamiseen, mutta ei juurikaan muuhun.

## **Muutamia teknisiä käsitteitä tekoälyyn liittyen**

- **Algoritmi:** Tietojärjestelmän toimintaohje. Algoritmi voi olla kokonaan ihmisen kirjoittama tai se voi sovittaa toimintaansa sille annetun aineiston pohjalta.
- **Koneoppiminen:** Aineiston pohjalta koulutettu päättelyjärjestelmä. Yksinkertaisessa tapauksessa puhutaan tilastollisesta analyysistä, monimutkaisemmassa tapauksessa tekoälystä.
- **Neuroverkko:** Informaation käsittelyn, matematiikan tai laskennan malli, joka jäljittelee ihmisen aivojen toimintaa ja kykyä oppia.
- **Syväoppiminen:** Koneoppimisen alalaji, jossa koulutus tallentuu neuroverkkotyyppiseen rakenteeseen

- **Suuret kielimallit** (engl. large language model, LLM): Yleistermi generatiivisen tekoälyn yleiskäyttöisille malleille, jotka perustuvat luonnolliseen kirjoitettuun tai puhuttuun kieleen.
- **Muut suuret mallit**: Mikäli suuren mallin aineisto ei ole kieltä, tulisi käyttää eri termiä kuin kielimalli, mutta monesti LLM-lyhennettä väärinkäytetään myös tällöin. Suuri malli voidaan rakentaa vaikkapa terveyden, liikenteen, säähavaintojen, some-profilien, molekyylibiologian tai minkä tahansa aineiston pohjalta.

Tekoälyn toiminta ei ole tarkalleen ennalta määrätty, vaan perustuu sille annettuun koulutusaineistoon. Tekoäly toimii siis osin ennakoimattomalla tavalla ja sen toiminta muuttuu aineiston päivittyessä. Edes tekoälyn kehittäjät eivät aina tiedä, miten se käyttäytyy jokaisessa yksittäisessä tilanteessa.

Koska tekoälyn tuloksia ei voida täysin varmasti ennakoida, on luotettavan tekoälyn kehittäminen erityisen vaikeaa. EU pyrkii varmistamaan lainsäädännöllä, että tekoälyjärjestelmiä kehitetään mahdollisimman laadukkaasti ja luotettavasti. Tekoälyasetus (AI Act) ottaakin huomioon tekoälyn koko tuotantoketjun alkaen sen koulutukseen käytettävistä data-aineistoista ja päättyen vuorovaikutukseen loppukäyttäjän kanssa. Tekoälyasetuksessa tekoälyjärjestelmällä tarkoitetaan

*"konepohjaista järjestelmää, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättelee vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin."*

## Millainen on reilu tekoäly?

### *Pohdittavaksi*

Mitä mieleesi tulee, kun ajattelet reilua tekoälyä? Mikä taas tuntuisi epärealulta?

Videolla samaan kysymykseen vastaa joukko asiantuntijoita, jotka työskentelevät tekoälyn parissa eri rooleista käsin.



Reilu tekoäly voidaan ymmärtää monella tavalla, mutta ehkä voimme olla samaa mieltä siitä, että tekoäly ei saisi aiheuttaa haittaa ihmisille tai yhteiskunnalle. Reilun tekoälyn pitäisi olla sekä eettisesti että oikeudellisesti kunnossa. Esimerkit epärealista tekoälystä voivat auttaa hahmottamaan reilua:



Tekoälyä koulutetaan ilman lupaa taiteilijoiden taideteoksilla siten, että tekoäly voi imitoida näiden tyyliä.

- Tekoäly ohjaa autoa liikennesäännöistä välittämättä.
- Keskusteleva tekoäly lisää keskusteluun salakavalasti tietyn valtion propagandaa.
- Tekoäly tekee yrityksessä palkkauspäätöksiä ja hylkää tietyn vähemmistön työhakemukset syrjivästi.
- Tekoäly käyttää valtavasti energiaa tuottaakseen vähäarvoista viihdettä.
- Tekoäly auttaa rikollisia tekemään huijauksia verkossa.
- Tekoäly tuottaa sosiaalisen median palveluihin syväväärennöksiä ja väärää tietoa ja vaikuttaa näin eduskuntavaalien tulokseen tai lietsoo kapinaa tai väkivaltaisuuksia.

EU:ssa halutaan varmistaa, että tekoälyjärjestelmät toimivat luotettavasti eivätkä aiheuta hallitsemattomia riskejä ihmisille tai yhteiskunnalle. Yksilön näkökulmasta EU:ssa laillisesti tarjotut tekoälyjärjestelmät ovat siis turvallisia käyttää. Yritysten vastuulla on kehittää ja tuoda markkinoille vain turvallisia järjestelmiä. Tämä on EU:n tekoälyasetuksen tavoite.

Katso video, jossa Sitran vanhempi neuvonantaja Reijo Aarnio avaa tekoälyasetuksen tavoitteita ja kuvaa teknologia-alan sääntelyn tulevaisuutta.



## Riskitasot

Tekoälyä arvioidaan Euroopassa sen mahdollisten riskien perusteella. Suurin osa tekoälyjärjestelmistä on täysin sallittuja. Riskit jaetaan neljään tasoon:

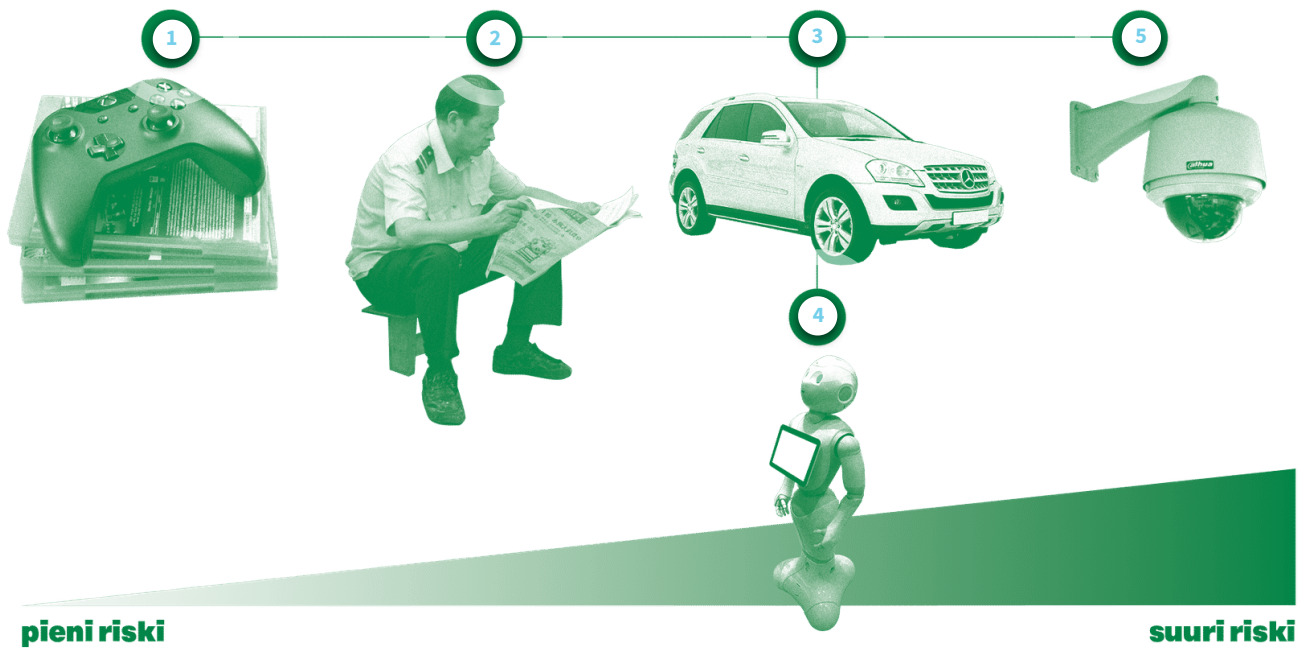
- 1 Vähäinen riski:** Tässä ryhmässä ovat täysin vaarattomat järjestelmät, kuten sähköpostin suodattimet tai videopeleiden tekoälygeneraattorit. Näitä voi kehittää ja käyttää vapaasti ilman, että käyttäjälle tarvitsee erikseen kertoa niiden olemassaolosta.
- 2 Rajoitettu riski:** Valtaosa tekoälyjärjestelmistä kuuluu tähän ryhmään. Esimerkkejä ovat tekoälyavustajat, chattibotit ja kuvageneraattorit. Ainoa vaatimus on, että palvelun käyttäjät ymmärtävät olevansa tekemisissä tekoälyn kanssa.
- 3 Suuri riski:** Tässä ryhmässä tekoäly voi mahdollisesti aiheuttaa merkittävää haittaa. Tekoäly on kehitettävä ja testattava huolellisesti, mahdolliset riskit minimoiden ja se on dokumentoitava tarkasti. Tekoälyn ohkeen lisätään CE-merkintä.

a. Jos tekoälyjärjestelmä liittyy ihmisiä liikuttaviin koneisiin, lääkinnällisiin laitteisiin, leluihin tai muihin tuotesääntelyn piirissä oleviin tuotteisiin, kuuluu se tähän ryhmään. Tiedät kyllä, jos nykyinen toimintasi on tuotesääntelyn alaista.

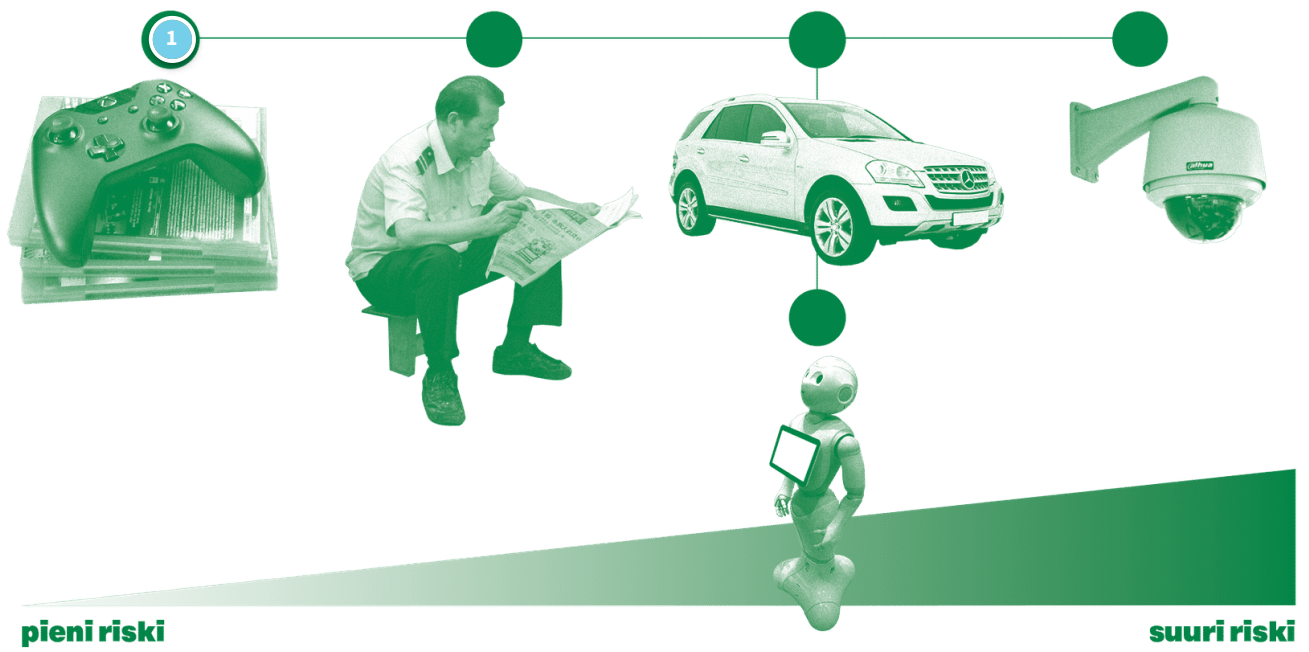
b. Mikäli tekoälyjärjestelmäsi aiheuttaa merkittävän vahingon riskin terveydelle, turvallisuudelle tai perusoikeuksille, kuuluu se tähän ryhmään. Perusoikeuksia ovat esimerkiksi oikeus opiskeluun, työhön ja itseilmaisuu.

4

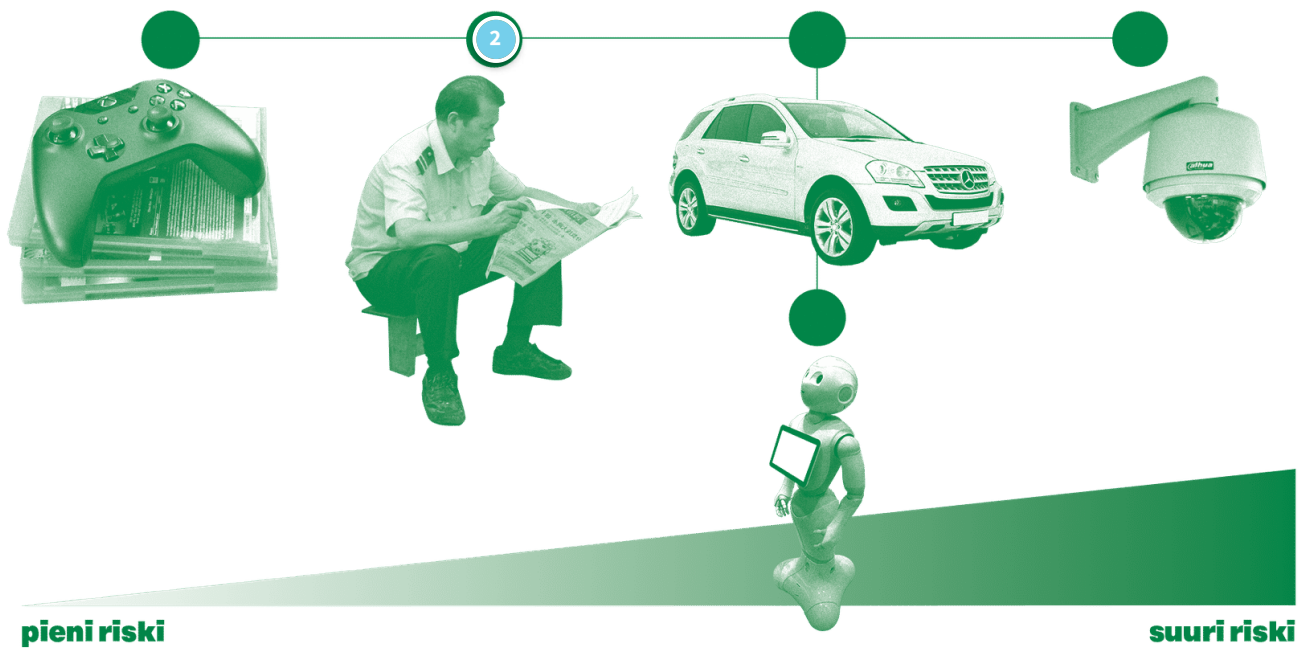
**Kestämätön riski:** Tietty tekoälyjärjestelmien käyttötavat ovat kokonaan kielletty. Nämä loukkaavat ihmisoikeuksia räikeästi. Kiellettyä on esimerkiksi ihmisten reaaliaikainen tunnistaminen valvontakameroista tai sosiaalinen pisteytys eri tietokantoja yhdistelemällä. Lainvalvontatarkoituksiin on tähän liittyviä poikkeuksia.



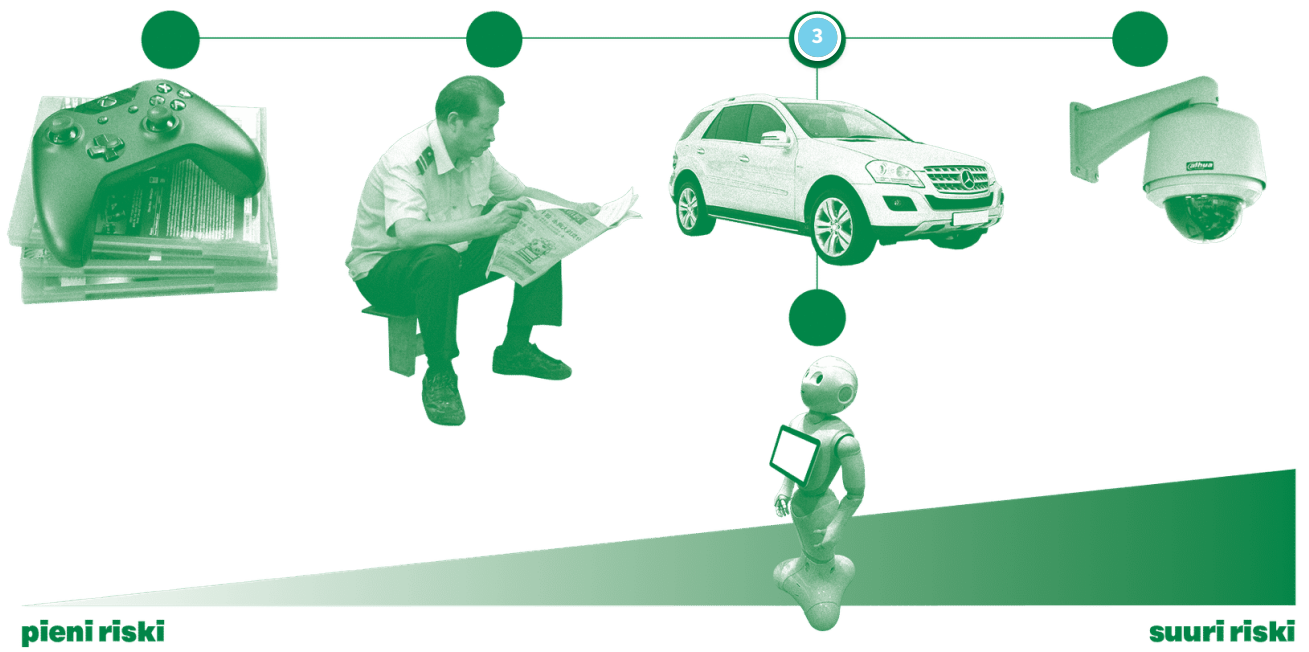




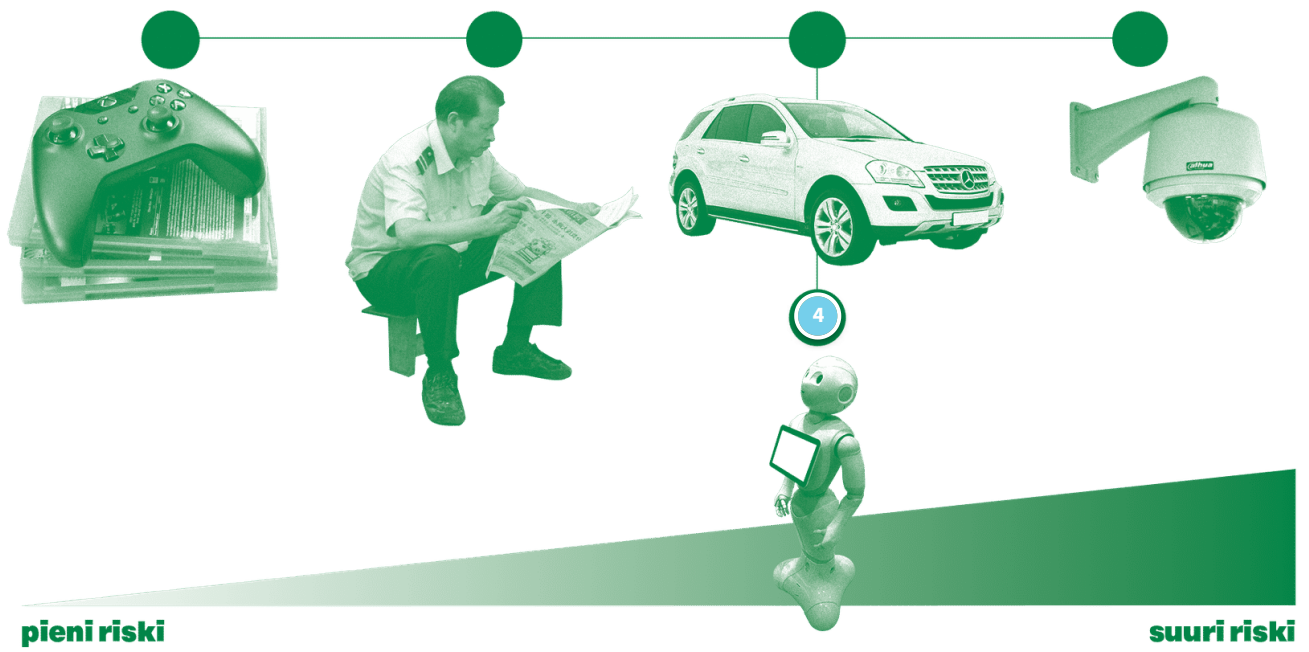
Täysin riskittömistä järjestelmistä kuten tekoälyä käyttävästä spämmisuodattimesta ei tarvitse edes kertoa käyttäjälle.



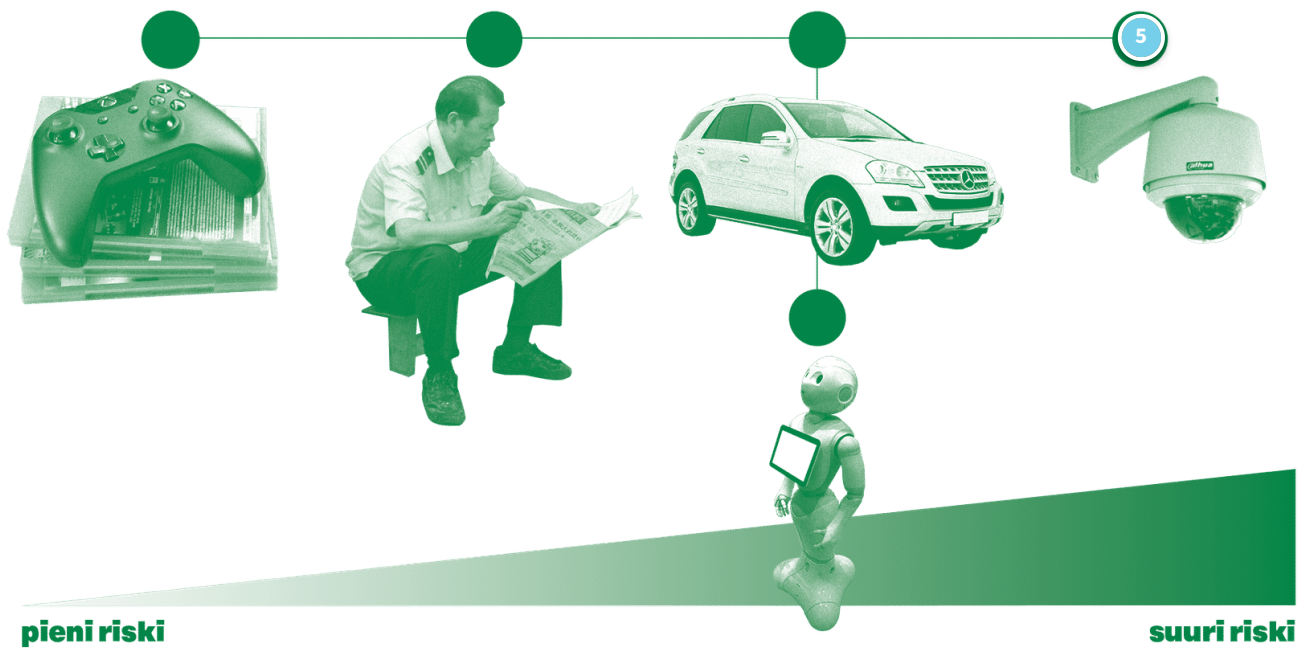
Tekoälyn tuottaessa synteettistä sisältöä on yleisölle kerrottava, että tekoäly on tuottanut sisällön.



Ihmisiä liikuttavat koneet sekä muut tuoteturvallisuuden piirissä olevat laitteet ovat suuririskisiä, joten niiden tekoäly on tehtävä huolellisesti riskejä minimoiden.



Ihmisten perusoikeuksille riskin muodostavat järjestelmät, kuten rekrytointipäätöksiä tekevä tekoäly, ovat samoin suuririskisiä.



Jotkin äärimmäiset käyttötavat on kokonaan kielletty, kuten ihmisten reaaliaikainen tunnistaminen valvontakameroista julkisilla paikoilla.

Nämä riskitasot huomioiden tekoälymallien koulutus sekä tekoälyjärjestelmien kehittäminen, tarjoaminen ja käyttö on sallittua EU:ssa. On kuitenkin tärkeää muistaa, että kaikki lait ovat voimassa samanaikaisesti. Tekoälyjärjestelmän on siis tekoälyasetuksen lisäksi noudatettava myös tietosuojalakeja (engl. General Data Protection Regulation, GDPR), kyberturvallisuussäädöksiä, toimialakohtaisia määräyksiä sekä muita sen toimintaan liittyviä lakeja ja sääntöjä.

## **EU:ssa on runsaasti sääntelyä, joka tekoälyn kehittämisessä on huomioitava**

Alla olevaa luetteloa ei tarvitse opetella, mutta se tarjoaa (epätäydellisen) kuvan sääntelyn kokonaisuudesta tekoälyasetuksen lisäksi

- **Yleinen tietosuojalaki, GDPR:** Henkilötietojen suojaaminen ja hyödyntäminen esimerkiksi tekoälyn kouluttamisessa
- **Digipalveluasetus tai digipalvelusäädös (Digital Services Act, DSA):** Digitaalisten palvelujen avoimuus, luotettavuus ja turvallisuus sekä käyttäjien toimijuuden

vahvistaminen

- **Data-asetus tai datasäädös (Data Act):** Älylaitedatan ja pilvipalveluiden tehokkaampaa käyttöä muun muassa tekoälyn hyödyntämiseksi
- **Avoimen datan direktiivi (Open Data Directive):** Arvokkaan julkisen sektorin datan uudelleenkäyttö
- **Asetus datan vapaasta liikkuvuudesta (Free Flow of Non-Personal Data Regulation):** Datan vapaa liikkuvuus ja siirtäminen ammattikäyttäjille
- **Tuotevastuudirektiivi:** Vastuu vahingosta, joka koituu viallisista tuotteista, mukaan lukien tekoälyjärjestelmät
- **EU:n tekijänoikeuslainsäädännön paketti, johon lukeutuu 13 direktiiviä ja kaksi asetusta:** Tekijöiden, esittäjien, tuottajien ja muiden oikeudet
- **Sekä laaja joukko tuotesäätelyä,** esimerkiksi direktiivi lelujen turvallisuudesta, direktiivi hisseistä ja niiden turvakomponenteista, direktiivi köysiratalaitteistoista ja asetus lääkekinnäisistä laitteista.

## Koulutuksessa esiintyvien yritystarinoiden kuvitteelliset yritykset ja henkilöt

Voit käydä tätä koulutusta läpi yksityishenkilönä tai yrittäjänä tai edustamasi yrityksen edustajana. Tällä kursilla kuvitteelliset esimerkkihenkilöt ja -yritykset havainnollistavat uusien sääntöjen merkitystä käytännössä ja arjessa.



## **Lumi Valkamo**

Putsis Oy:n  
toimitusjohtaja.

## **Putsis Oy**

Vantaalainen  
siivousfirma, jossa  
digitalisaatiota on  
otettu käyttöön  
melkoisen runsaasti  
eikä tekoäly pelota.



**Sari Hyvärinen**



**Atte Torney**

## **Sari Hyvärinen**

Hyvinvointialueen  
hallintojohtaja.

## **Atte Torney**

Teknologiaan  
erikoistunut  
freelancer-juristi.



## *Yritystarina*

### **Meillä on tekoälyä ja dataa**

*Vantaalainen siivousfirma Putsis Oy on ylpeä pitkälle kehittyneestä työnteon järjestely- ja hallintajärjestelmästään:*

*Työvuorolistat laaditaan taulukkolaskentaohjelmalla. Putsis Oy tarjoaa työntekijöilleen työmatkaliput julkiseen liikenteeseen, kannustaa heitä käyttämään niitä ja pyrkii minimoimaan hiilijalanjälkensä, joten työvuorot kootaan työntekijöiden työvuorotoiveiden ja algoritmiavusteisen navigointi- ja liikennesovelluksen ehdotusten perusteella. Sovellus yhdistää työntekijän valitseman "kotipysäkin" ja asiakasta lähinnä olevan pysäkin sekä mahdolliset useammat asiakkaat ja kotiinpaluun siten, että valinnat minimoivat työmatkojen aiheuttamat päästöt.*

*Positiivisuus on Putsis Oy:n keskeinen arvo, sekä sisäisesti että ulkoisesti. Reiluna työnantajana yhtiö seuraa työntekijöidensä suoriutumista positiivisuuteen keskittyvällä ohjelmalla, joka päivittäin kerää työsuorituksen*



liittyviä tietoja ja ehdottaa työntekijän suoriutumisdatan perusteella ylennyksiä ja palkankorotuksia. Iloinen asiakaspalvelu on osa Putsis Oy:n brändiä, minkä vuoksi järjestelmän tietokonenäkö poimii asiakasyritysten kameravalvontavirrasta kappalemäärätiedon työpaidan perusteella putsislaisiksi tunnistettujen iloisista tervehdyksistä asiakkaille ja lisää automaattisesti tämän tiedon osaksi työntekijän suoriutumisdataa.

Asiakkailleen Putsis Oy haluaa olla avoin ja saavutettavissa, minkä vuoksi sen kielimalliperusteinen chatbot on koulutettu käyttämään järjestelmään kirjattua siivousdataa. Botti on aina valmiina vastaamaan kaikkiin siivoukseen liittyviin kysymyksiin (esim. milloin viimeksi siivottu, mitä puhdistusaineita käytetty, ovatko puhdistusaineet kotimaisia ja ekologisia).

Kaikki nämä toiminnot on integroitu osaksi yhtä TAP-nimistä tietojärjestelmää, johon kaikki yhtiön työntekijät kirjautuvat töiden ajaksi eri käyttäjäprofileilla ja erinäköisten käyttöliittymien kautta.

#### **Pohdittavaksi**

Mitä ajattelet Putsis Oy:n järjestelmistä? Mitkä niistä ovat arveluttavia vaikkapa tietosuojan, eettisyyden tai turvallisuuden näkökulmasta?

#### **Testaa tietosi**

Mitkä seuraavista Putsis Oy:n järjestelmistä sisältävät tekoälyä?

☐

A) Työvuorojärjestelmä

☐

B) Positiivisuusmittari

☐

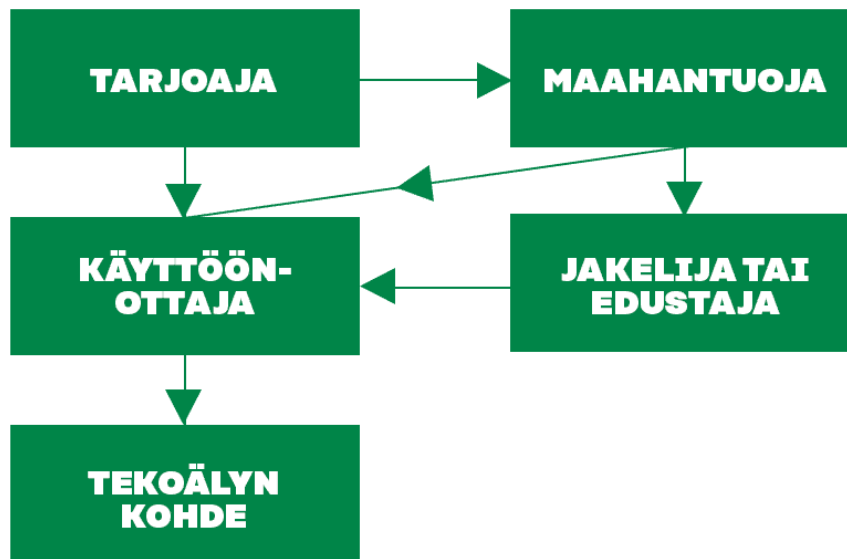
C) Chatbot

SUBMIT

## Tunnista oma roolisi

Tekoälyn tuottaminen muistuttaa monin tavoin perinteistä palveluliiketoimintaa. Alihankintakehittäjä luokitteluun useita rooleja, joista palveluntarjoaja koostaa valmiin ratkaisun ja tuo sen markkinoille.

Käyttöönottaja hankkii palvelun ja ottaa sen käyttöön, jolloin tekoäly alkaa vaikuttaa käyttöönottajien asiakkaiden, työntekijöiden tai muiden sidosryhmien arkeen. Todennäköisesti tunnistat itsesi jostakin seuraavista rooleista. Yritys voi hyvin toimia useassa roolissa.



Tarjoaja kehittää tekoälymallin tai -järjestelmän. Käyttöönottaja tuo tekoälyjärjestelmän markkinoille tai ottaa muuten käyttöön, jolloin se alkaa vaikuttaa kohteisiinsa. Osan vastuista voivat hoitaa tarjoajan valtuuttamat maahantuojat, jakelijat tai edustajat.

### *Esimerkiksi*

Microsoft on yhdysvaltalainen yritys, joka tarjoaa Copilot-tekoälyjärjestelmää yritysasiakkaille.

Microsoftilla on toimipisteitä EU:ssa, joten se ei tarvitse erillistä maahantuoja. Monesti asiakasyritykset ostavat palvelun kotimaiselta edustajalta. Yritysasiakkaat ovat siten Copilotin käyttöönottajia ja tekoälyn kohteena ovat yrityksen työntekijät, niiden asiakkaat ja sidosryhmät.

Bytedance on kiinalainen yritys, jonka Tiktok-alustalla on tekoälypohjainen suositteualgoritmi, jonka kohteina ovat EU:ssa olevat yksityishenkilöt. Bytedance on tekoälyn tarjoaja ja käyttöönottaja. Vuoden 2025 alussa sillä ei ollut toimistoa EU:ssa. Bytedancen on siis vuoden 2026 elokuuhun mennessä perustettava toimisto EU-alueelle tai valtuutettava maahantuoja, joka hoitaa tarvittavat velvoitteet tekoälyyn liittyen.

## **Roolien tarkemmat kuvaukset**

- **Loppukäyttäjä tai tekoälyn kohde:** Yksittäinen henkilö, joka on tekemisissä tekoälyn kanssa tai johon tekoälyn toiminta vaikuttaa. (Ei velvoitteita tekoälyasetuksesta, mutta sitäkin enemmän oikeuksia, joista on hyvä olla tietoinen.)
- **Käyttöönottaja:** Organisaatio, joka ottaa (toisen tuottaman) tekoälyjärjestelmän käyttöön esimerkiksi sisäisissä prosesseissa, omien työntekijöiden parissa tai asiakkaiden tai kumppanien kanssa. (Tekoälyasetuksesta tulee joitain velvoitteita käyttöönottajille, varsinkin, jos käyttöönottaja on julkisen sektorin toimija ja kyseessä on suuririskistä tekoälyä.)
- **Tarjoaja:** Organisaatio, joka kehittää ja asettaa tekoälyjärjestelmän tai yleiskäyttöisen tekoälymallin EU:n markkinoille. (Tekoälyasetuksesta tulee pääosin velvoitteita tarjoajille, varsinkin, jos kyseessä on suuririskistä tekoälyä.)
- **Maahantuoja:** Organisaatio, joka tuo EU:n ulkopuolella kehitetyn tekoälyjärjestelmän tai tekoälymallin EU:n markkinoille, vastaa sen laillisuudesta. (Tekoälyasetuksesta tulee joitain velvoitteita maahantuojoille, varsinkin, jos kyseessä on suuririskistä tekoälyä.)
- **Valtuutettu edustaja:** EU:n ulkopuolella olevan toimijan edustaja. (Tekoälyasetuksesta tulee joitain velvoitteita edustajille, varsinkin, jos kyseessä on suuririskistä tekoälyä.)
- **Jakelija:** Muu organisaatio kuin maahantuoja tai edustaja, joka asettaa tekoälyä markkinoille. (Tekoälyasetuksesta tulee joitain velvoitteita jakelijoille, varsinkin, jos kyseessä on suuririskistä tekoälyä.)

Lopulta kyse on tuoteturvallisuudesta. Tekoälyjärjestelmän käyttöönottajien vastuulla on varmistaa, että järjestelmä ei riko mitään lakeja. Etenkin tuoteturvallisuuden osalta tehtävä helpottuu, kun tekoälyjärjestelmän tarjoaja huolehtii siitä, että järjestelmä noudattaa tekoälyasetuksen vaatimuksia. Käyttämällä luotettavan tarjoajan tekoälyratkaisua voit nojautua tarjoajan vakuutuksiin ja selvityksiin siitä, että järjestelmä täyttää siihen soveltuvat tekoälyasetuksen vaatimukset. Riittää, että tarkistat omat käytäntösi.

Tulevaisuudessa suuririskisen tekoälyn, joka täyttää EU:n vaatimukset, tunnistaa sähkölaitteista tutusta CE-merkinnästä.

Tekoälyn turvallisuutta voi tarkastella myös maahantuonnin näkökulmasta. Henkilön tai tahon, joka tuo tekoälyjärjestelmän EU:n markkinoille, on varmistettava sen laimukaisuus.



## Kuka toimiikaan maahantuojana?

*Putsis Oy:n käyttämän järjestelmän on alun perin kehittänyt TAP US Ltd, joka on tunnettu Amazonin tehokkaana järjestelmätoimittajana. Yhdysvaltalaisyhtiön valtuutettu edustaja Euroopassa on TAP Europe GmbH, ja järjestelmän on tuonut maahan Tukiälypalvelut Oy, jolla on yksinoikeus toimittaa järjestelmää suomalaisille toimijoille. Siivousfirma Putsis Oy on hankkinut järjestelmän kotimaiselta Tukiälypalvelut Oy:ltä.*

*Vuonna 2027 kansallinen markkinavalvontaviranomainen (tietosuojavaltuutettu) ottaa yhteyttä Putsis Oy:n toimitusjohtaja Lumi Valkamoon. Viranomainen kertoo, että Putsis Oy:n TAP-järjestelmästä on tehty valitus, jonka mukaan järjestelmää epäillään suuririskiseksi. Käsitelläkseen asian viranomainen pyytää Putsis Oy:tä toimittamaan dokumentaation siitä, että TAP-järjestelmä tekoälyjärjestelmänä täyttää EU-oikeuden vaatimukset.*

*Toimitusjohtaja Lumi kauhistuu – järjestelmän hankinnasta on jo aikaa. Sen tarjoaja TAP US Ltd ja sen edustaja ovat menneet konkurssiin jo vuosi sitten. Mistä Lumi voi nyt hankkia tarvittavat tiedot? Tuskastuneena Lumi soittaa Atte Torneylle.*

### PUTSIS OY

Atte rauhoittelee Lumia: "Tekoälyasetuksen 71 artiklan mukaan tarjoajalla ja sen valtuutetulla edustajalla on ollut velvollisuus rekisteröidä asetuksen liitteen VII:n edellyttämät tiedot EU:n suuririskisiä tekoälyjärjestelmiä koskevaan tietokantaan – myös silloin, kun järjestelmää pidetään ei-suuririskisenä. Tiedoista löytyy muun muassa asetuksen 47 artiklan mukainen tekoälyjärjestelmän vaatimusten mukaisuusvakuutus. Lisäksi maahantuojalla on asetuksen 23(5) artiklan mukaan velvollisuus säilyttää tarvittavia dokumentteja 10 vuotta järjestelmän markkinoille asettamisesta tai käyttöönottamisesta."

"Dokumentointi kyllä löytyy", rauhoittelee Atte. Lisäksi Atte kehottaa Lumia kertomaan viranomaiselle, että tiedustelun voi ohjata maahantuojalle, Tukiälypalvelut Oy:lle.

"On tämäkin, että pitää selvittää nyt jo vanhentuneen järjestelmän tietoja – kun ei sitä ole edes vuosiin päivitetty tarjoajan konkurssin takia", puuskahtaa Lumi.

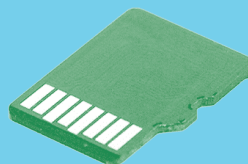
Atte Torney havahtuu ja kysyy: "Milloin järjestelmä on otettu käyttöön ja milloin sitä viimeksi on merkittävästi muutettu?"

"Käyttöön 2023 ja viimeisin kunnon päivitys 2025", vastaa Lumi.

"Jos on näin", toteaa Atte, "eikä tekoälyjärjestelmäänne sisälly kiellettyjä käyttötarkoituksia, asetuksen ajallinen soveltamisala ei ulotu tilanteeseen: se ei koske Putsis Oy:n hankkimaa TAP-järjestelmää tai sen käyttöä, jos järjestelmä oli ennen 2.8.2026 markkinoille saatettu tai käyttöön otettu – eikä järjestelmään ole sittemmin tehty merkittäviä muutoksia, jotka edellyttäisivät uutta vaatimusten mukaisuuden arviointia."

"Mitä jos on tarpeen tehdä merkittäviä muutoksia tekoälyjärjestelmään?" kysyy Lumi. "Siis oletetaan, että teidän pitää merkittävästi muuttaa käyttämäännne suuriskistä tekoälyjärjestelmää ja voitte niin sopimustenne pohjalta tehdä", aloittaa Atte, "niin silloin te tuotte sen markkinoille tai otatte käyttöön uutena järjestelmänä ja tarjoajana arvioitte, että järjestelmä on tekoälyasetuksen vaatimusten mukainen ja vastaatte sen vaatimusten mukaisuudesta. Tai voitte te pyytää kolmattakin osapuolta suorittamaan vaatimusten mukaisuuden arvioinnin puolestanne."

"Ei kuulosta lainkaan mahdottomalta. Kiitos, Atte", sanoo Lumi.



**Muista ainakin nämä**

1

Suurin osa tekoälyjärjestelmistä ei ole suuririskisiä, joten niitä voi varsin vapaasti kehittää ja käyttää.

2

Suuririskiset tekoälyjärjestelmät on kehitettävä ja käyttöön otettava vaatimusten mukaisesti huolellisesti dokumentoiden ja riskit minimoiden. Niihin on liitettävä CE-merkintä.

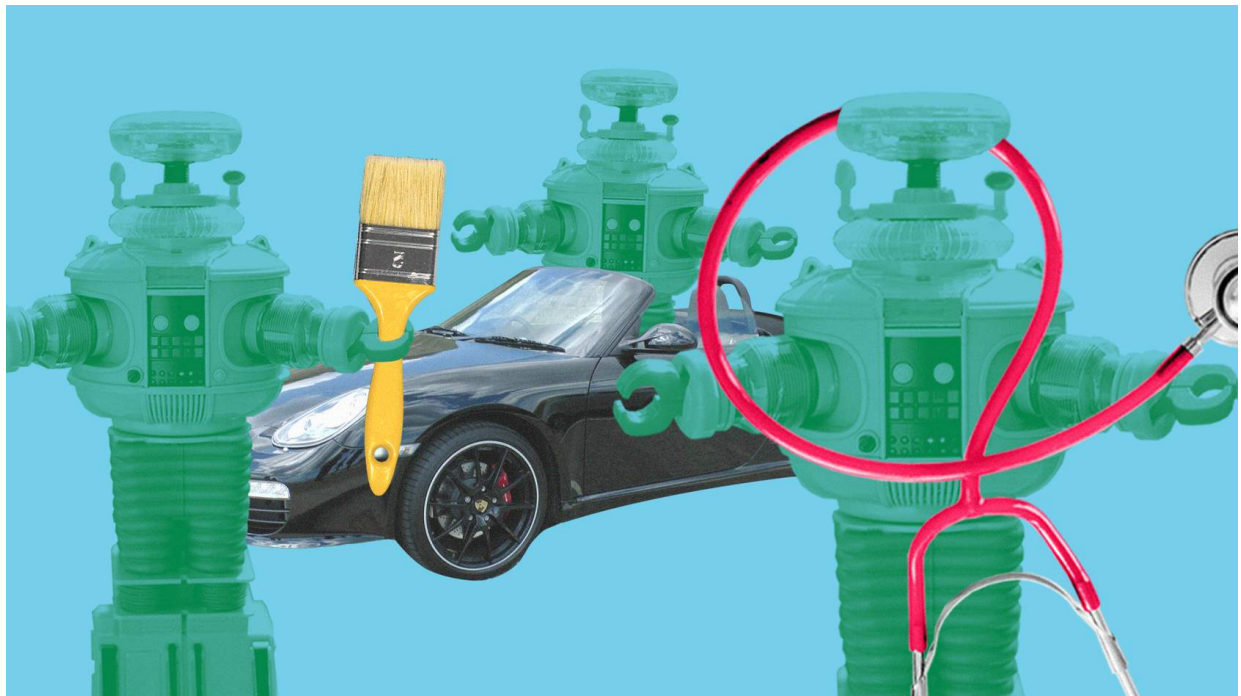
3

Suuririskisyys ei tarkoita, että tekoäly olisi kielletty tai sellaisen kehittämistä tulisi välttää.

**Jatka seuraavaan osioon**

# Arvioi tekoälyn riskitaso

---



---

**Mitä suurempia tekoälyn riskit ovat, sitä huolellisemmin se on valmistettava ja otettava käyttöön.**

Jos tekoälyjärjestelmällä on riski aiheuttaa merkittävää haittaa, nämä haitat on minimoitava huolellisesti. Vastuu kuuluu ensisijaisesti tekoälyn kehittäjälle eli tarjoajalle. Käyttöönottajien tehtävänä on puolestaan



käyttää järjestelmää käyttötarkoituksen mukaisesti, noudattaa kehittäjän antamia ohjeita ja varmistaa, että omassa toiminnassa ei synny tilanteita, jotka vaarantaisivat riskienhallinnan.

## Arvioi tekoälyn riskitaso

### Testaa tietosi

Mitä tiedät ennestään tekoälyn riskitason arvioinnista? Kokeile ja valitse ne väittämät, jotka ovat oikein.

---

- ☐ A) Riskitaso määräytyy yksinomaan tekoälyn kehittäjän arvion perusteella
- ☐ B) Käyttöönottajän valitsema käytötapa voi nostaa tai laskea tekoälyjärjestelmän riskitasoa
- ☐ C) CE-merkintä on pakollinen kaikille tekoälyjärjestelmille riskitasosta riippumatta
- ☐ D) Suuririskiset tekoälyjärjestelmät edellyttävät tiukempia vaatimuksia ja huolellista dokumentaatiota
- ☐ E) Jos tekoälyjärjestelmä on alun perin arvioitu matalariskiseksi, sitä ei voida missään tilanteessa pitää suuririskisenä
- ☐ F) Yleiskäyttöinen tekoälyjärjestelmä voi muuttua suuririskiseksi riippuen

käyttötarkoituksesta

SUBMIT

EU:n markkinoille tuotavien tekoälyjärjestelmien riskitaso on arvioitava jo ennen sen markkinoille saattamista tai käyttöönottoa tekoälyasetuksen mukaisin kriteerein. Arvioinnin ensisijainen vastuu kuuluu tekoälyn kehittäjille eli tarjoajille, mutta myös käyttöönottajien on tarkasteltava riskitasoa, sillä käyttötavat voivat vaikuttaa merkittävästi riskeihin – joko kasvattaa tai pienentää niitä.

#### *Esimerkiksi*

Yrityksen kehittämä ja tarjoama yleiskäyttöinen chattibotti ei itsessään ole suuririskinen. Sairaala päättää kuitenkin käyttää tätä chattibottia potilaskäyntien keskustelujen tiivistämiseen, mikä tekee sen käytöstä todennäköisesti suuririskisen.

Toinen yritys taas kehittää itseajavan auton, jonka tekoäly kuuluu suuririskisiin järjestelmiin. Autokouluyritys käyttää kuitenkin tätä tekoälyä ajosimulaattorissaan, jolloin riski on huomattavasti pienempi, eikä käyttöä todennäköisesti pidettäisi suuririskisenä.

Suurimassa osassa tekoälyjärjestelmiä riskit ovat vähäisiä, eikä niille aseteta merkittäviä velvoitteita. Sen sijaan suuririskisissä järjestelmissä noudatetaan tiukkoja vaatimuksia ja ne on dokumentoitava huolellisesti. Niihin liitetty CE-merkintä osaltaan kertoo, että ne noudattavat asetuksen vaatimuksia.

Oikean riskitason selvittäminen ei ole aivan suoraviivaista. Kysymyksiä, poikkeuksia ja yksityiskohtia on monia. Arviossa kannattaa tukeutua valmiisiin ohjeisiin tai hakea asiantuntija-apua. Kehitteillä on lukuisia ohjesivustoja ja teknisiä ratkaisuja riskiarvion tekemiseen.

**Tutustu Sitran ja Teknologiateollisuuden rahoittamaan työkaluun, joka purkaa riskiarvion joukoksi kysymyksiä, joihin vastaamalla saat tuntuman yksittäisen ratkaisun riskitasosta sekä siihen kohdistuvista vaatimuksista. Työkalu on veloituksetta käytettävissä ainakin vuoden 2025 ajan.**

#### LISÄTIETOJA

Videolla AI Finlandin operatiivinen johtaja Iida Lähde määki kertoo tarkemmin riskiluokittelusta ja sen vaikutuksista yritysten toimintaan.



## **Kokonaan sääntelyn ulkopuolella olevat tekoälyn käyttökohteet**

Seuraavat käyttökohteet on erikseen rajattu tekoälyasetuksen ulkopuolelle. On toki hyvä muistaa, että muut lait ovat voimassa normaalisti.

## Henkilökohtaista käyttöä ei säännellä

Mikäli otat tekoälyä käyttöön puhtaasti henkilökohtaisessa toiminnassasi, ei sitä rajoiteta mitenkään. Osa omasta toiminnastasi voi kuitenkin olla ammattitoimintaa, vaikkapa yksityisyrittäjän tapauksessa. Ammattitoiminta ei ole henkilökohtaista.

## Avoimesti lisensoituja tekoälymalleja ei säännellä

Mikäli yleiskäyttöinen tekoälymalli julkaistaan avoimesti lisensoituna, uudelleenkäytettävänä työkaluna, ei tällainen tekoälymalli lähtökohtaisesti ole sääntelyn piirissä.

Jos tällaisesta mallista kehitetään markkinoille tekoälyjärjestelmä, koskevat tätä järjestelmää tekoälyasetuksen vaatimukset normaaliin tapaan, mutta velvoitteet ovat tämän järjestelmän kehittäjällä, ei avoimen tekoälymallin julkaisijalla.

## Tutkimuskäyttöä ei säännellä, eikä kehittämistä ennen käyttöönottoa

Tekoälyn kehittämiselle ei ole rajoituksia. Vasta kun tekoälyä saatetaan markkinoille tai otetaan käyttöön, on sen oltava sääntelyn mukainen.

Puhtaasti tieteelliseen tutkimukseen suunnattua tekoälyä tai sen tuloksia ei säännellä.

## Puolustuskäyttöä tai kansallisen turvallisuuden tarkoituksia ei säännellä

Mikäli tekoälyjärjestelmää käytetään sotilaallisia, puolustuksen tai kansallisen turvallisuuden tarkoituksia varten, ei tekoälyasetus rajoita sitä mitenkään.

### *Testaa tietosi*

Millä seuraavista aloista tekoälyasetusta ei sovelleta?

---

- ☐ A) Henkilökohtainen käyttö
- ☐ B) Avoimen lähdekoodin tekoäly, kun se julkaistaan avoimesti lisensoituna työkaluna
- ☐ C) Tekoälyjärjestelmien kaupallinen käyttöönotto
- ☐ D) Tutkimuskäyttö ja kehittäminen ennen markkinoille saattamista
- ☐ E) Puolustuskäyttö ja kansallisen turvallisuuden tarkoitukset

SUBMIT

**Kestämättömän riskin tekoälyratkaisut**

Joillakin tekoälyn käyttötavoilla rikotaan niin selkeästi ihmisoikeuksia ja EU:n perusarvoja vastaan, että ne ovat täysin kiellettyjä EU:ssa. Näihin kieltoihin voi liittyä joitakin tarkoin määriteltyjä poikkeuksia. Kaikki muut käyttötavat ovat sallittuja, kunhan ne noudattavat voimassa olevaa sääntelyä.

## **Harhaanjohtava manipulointi on kiellettyä**

Ihmisten alitajuinen (sublimaalinen) tai tarkoituksellinen manipulointi tai harhautus tekemään merkittävästi haitallisia päätöksiä on kielletty.

## **Haavoittuvien henkilöiden tai henkilöryhmien hyväksikäyttö on kiellettyä**

Henkilöryhmä voi olla haavoittuvaa iän, vamman tai erityisen sosiaalisen tai taloudellisen tilanteen perusteella. Tekoälyjärjestelmä on kielletty, jos sen seurauksena tällaisen henkilöryhmän tai yksittäisen henkilön päätöksenteko voi vääristyä ja se voi aiheuttaa heille merkittävää haittaa.

## **Henkilöiden haitallinen tai epäedullinen kohtelu sosiaalisen pisteytyksen avulla on kielletty**

Sosiaalinen pisteytyks on kiellettyä, jos pisteytyksen dataa kerätään eri tilanteista, mutta pisteytys voi johtaa henkilöille epäedulliseen kohteluun toisessa tilanteessa.

## **Rikosprofilointi persoonallisuuspiirteiden perusteella on kielletty**

Ihmisten todennäköisyyttä syyllistyä rikoksiin ei saa tekoälyllä arvioida pelkästään profilointiin tai persoonallisuuspiirteisiin perustuen. Mikäli rikoksesta on jo tietoa, voidaan kuitenkin tukea ihmisarvointia henkilön osallistumisen todennäköisyydestä.

## **Laaja-alaiset kasvojentunnistustietokannat on kielletty**

Kasvojentunnistustietokantojen luonti tai laajentaminen netistä tai valvontakamerakuvista kerätyillä kasvokuvilla on kiellettyä.

## **Tunteiden tunnistus työpaikoilla tai oppilaitoksissa on kielletty**

Henkilöiden tunteiden päättelyä tekoälyn avulla työpaikalla tai oppilaitoksissa ei sallita. Ainoastaan lääketieteeseen tai turvallisuuteen liittyvä käyttö on sallittua.

## **Ihmisten luokittelu biometristen tietojen tai arkaluontoisten tietojen perusteella on kielletty**

Henkilöitä ei saa luokitella biometrisesti rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella.

Laillisesti hankittujen biometristen tietojen käsittely lainvalvonnassa on kuitenkin sallittua.

## **Reaaliaikainen biometrinen etätunnistaminen julkisissa tiloissa on kielletty**

Henkilöiden tunnistaminen tekoälyllä biometrisesti esimerkiksi valvontakameroista ei ole sallittua, paitsi seuraavissa lainvalvonnan tilanteissa:

- kaappaukset ja ihmiskauppa
- henkeen kohdistuva merkittävä ja välitön uhka tai terrori-iskun ehkäiseminen
- tietyistä vakavista rikoksista epäillyn henkilön paikantaminen tai tunnistaminen.

Mikäli tekoälyjärjestelmän käyttö ei kuulu mihinkään yllä kuvatuista kielletyistä käyttötavoista, on se sallittu EU:ssa.

### *Testaa tietosi*

Mitkä seuraavista tekoälyn käyttötavoista ovat pääsääntöisesti kiellettyjä?

---

- ☐ A) Subliminaalinen manipulointi ihmisten päätöksenteon ohjaamiseksi heille haitallisella tavalla
- ☐ B) Ihmisten luokittelu biometristen tietojen perusteella rodun tai uskonnon mukaan
- ☐ C) Lainvalvonnan reaaliaikainen biometrinen etätunnistaminen julkisissa tiloissa ilman poikkeuksia
- ☐ D) Tekoälyn käyttö henkilön emotionaalisten reaktioiden arviointiin työpaikalla tai oppilaitoksessa
- ☐ E) Rikosten ennustaminen analysoimalla persoonallisuuspiirteitä yhdistettynä rikostietoihin

SUBMIT



## Suuririskiset tekoälyratkaisut

Kun tekoälyyn liittyvät riskit ovat suuria, järjestelmää ei saa tuoda markkinoille ilman, että se täyttää riskejä vähentävät vaatimukset. Suuririskistä tekoälyä ei siis kielletä, mutta sen kehittäminen ja käyttö edellyttävät huolellista suunnittelua ja toteutusta, jotta riskit pysyvät hallinnassa.

Seuraavassa osiossa käydään läpi, miten tekoäly voidaan kehittää ja ottaa käyttöön asianmukaisesti. Tässä osiossa tarkastellaan ensin niitä tilanteita, joissa tekoäly voi aiheuttaa merkittäviä riskejä.

### Tuoteturvallisuuden piirissä olevat tuotteet ovat suuririskisiä

Tiettyt tuotteet voivat huonosti suunniteltuina tai toteutettuina olla vaarallisia, kuten terveysteknologian laitteet, lelut, autot, hissit, moottorit ja junat. Näitä tuotteita säätelee toimialakohtainen tuoteturvallisuuslainsäädäntö, ja niiden markkinoille saattaminen edellyttää CE-merkintää. Joillain aloilla CE-merkintä edellyttää ulkopuolista tarkastusta. Jos tuote ei kuulu tuoteturvallisuuden piiriin, olet varmasti tietoinen vaatimuksista.

Tekoälyjärjestelmä voi itsessään olla tuoteturvasäännelty tuote, kuten syöpäseulontaa kuva-aineistosta tekevä järjestelmä. Usein tekoäly kuitenkin toimii osana tuoteturvasäänneltyä tuotetta, esimerkiksi auton ohjauksessa turvakomponenttina.

Lienee selvää, että jos tekoäly ajaa autoa tai ohjaa sairaalan kirurgista laitetta, huonosti tehty tekoäly on iso riski. Tuoteturvallisuuden piirissä oleviin tuotteisiin turvakomponenttina lisätty tekoäly onkin tekoälyasetuksen myötä automaattisesti suuririskistä.

### Ihmisten perusoikeuksia vaarantavat käyttötilanteet ovat suuririskisiä

Mikäli tekoälyjärjestelmä voi aiheuttaa merkittävän vahingon riskin ihmisten terveydelle, turvallisuudelle tai perusoikeuksille, sitä pidetään lähtökohtaisesti suuririskisenä. Tekoälyasetuksen liitteessä III on lueteltu

tällaisista käyttötilanteista, mutta Euroopan komissiolla on valtuudet täydentää luetteloa tulevaisuudessa. Tämä luettelo on siis lähtökohta:

- **Koulutus:** opiskelijoiden valinta oppilaitoksiin, oppimistulosten arviointi, tulevien oppimispolkujen arviointi, opiskelijoiden tarkkailu ja vilpin havaitseminen.
- **Työelämä:** rekrytointi, urakehitys ja irtisanomiset. Henkilöstön suorituksen ja käyttäytymisen arviointi.
- **Yhteiskunnan välttämättömät palvelut:** palvelujen myöntäminen, peruminen tai pääsy niihin.
- **Poliittinen prosessi:** vaalitulosten tai äänestyskäyttäytymisen manipulointi.
- **Talous:** luottokelpoisuuden arviointi (ei koske talouspetosten havaitsemista), sairaus- ja henkivakuutusten saajien riskiarviointi.
- **Biometriset järjestelmät:** ihmisten etätunnistaminen, luokittelu tai tunteiden tunnistaminen.
- **Kriittiset infrastruktuurit:** turvakomponentit, kuten vesi-, sähkö-, tie- ja tietoliikenneverkostojen hallinta.
- **Hätäpalvelut:** luokittelu ja priorisointi
- **Lainvalvonta:** uhririskiarviot, valheenpaljastus, todistusaineiston luotettavuuden arviointi, rikosuusimisriskin arviointi ja ihmisten profilointi.
- **Rajavalvonta:** valheenpaljastus, maahanmuuttajien turvallisuusriskien arviointi, turvapaikka-, viisumi- ja oleskelulupahakemusten käsittely, ihmisten tunnistaminen (ei koske matkustusasiakirjojen tarkastusta).
- **Oikeusjärjestelmä:** lainsäädännön tai tosiseikkojen tutkiminen ja tulkinta.

## **Tekoälyn roolia rajaamalla perusoikeudet eivät vaarannu**

Vaikka tekoälyjärjestelmän käyttötilanne olisi lähtökohtaisesti suuririskinen, riskitasoa voidaan alentaa merkittävästi rajaamalla järjestelmän mahdollisuuksia vaarantaa perusoikeuksia. Riski pienenee riittävästi, jos tekoälyjärjestelmä ei ryhmittele eli profiloi luonnollisia henkilöitä ja sen tehtävä sopii johonkin seuraavista rajauksista:

- Suppea menettelyllinen tehtävä: järjestelmä suorittaa rajatun ja ennalta määritellyn tehtävän.
- Aiemman toiminnan tukeminen: tekoäly parantaa ihmisen aiemmin suorittaman toiminnan tulosta.

- Ei päätöksenteon korvaamista: järjestelmä ei korvaa ihmisen tekemää päätöstä eikä vaikuta siihen ilman ihmisen valvontaa.
- Valmistelutehtävä: tekoäly auttaa päätöksenteossa tuottamalla tietoa, mutta ei tee itse lopullisia päätöksiä.

Jos arvioit, että tekoälyjärjestelmän riskitaso alenee riittävästi sen rajatun tehtävän vuoksi, tämä arvio tulee dokumentoida huolellisesti. Lisäksi itse tekoälyjärjestelmä on rekisteröitävä viranomaiselle.

Lääkärin vastaanotolla on käytössä tekoäly, joka tiivistää potilaskäynnin keskustelun. Väärin toimiva tekoäly olisi riski potilaan terveydelle. Mikä seuraavista väittämistä on oikein?

- ☐ A) Tiivistelmä lääkärin vastaanotosta ei ole koskaan suuririskistä.
- ☐ B) Jos tiivistelmän tarkistaa, korjaa ja hyväksyy vastaanotolla ollut lääkäri, ei sen tekeminen tekoälyllä ole suuririskistä.
- ☐ C) Jos tiivistelmän tarkistaa, korjaa ja hyväksyy jokin muu lääkäri, ei sen tekeminen tekoälyllä ole suuririskistä.
- ☐ D) Tekoälyn tuottama tiivistelmä lääkärin vastaanotosta on aina suuririskistä.

SUBMIT

## Muut, matalan riskin tekoälyratkaisut

Mikäli tekoälyjärjestelmän riskitaso ei ole kestävä tai suuri, sitä pidetään matalariskisenä ja sen sääntely on vähäistä. Tämä antaa kehittäjille enemmän joustavuutta palveluiden toteuttamiseen. Lisäksi on hyvä huomioda, että uutta EU-tason tekoälysääntelyä ei ole odotettavissa lähivuosina, mikä vahvistaa kehittämisen oikeusvarmuutta.

On kuitenkin tärkeää muistaa, että kaikki lait ja säädökset ovat voimassa samanaikaisesti. Vaikka tekoälyasetus ei kieltäisi tiettyä toimintaa, myös muut lait, kuten tuoteturvallisuus-, tietosuoja- ja kyber turvallisuuslainsäädäntö, on huomioitava.



## Missä me neekään suuren riskin raja?

*Siivousfirma Putsis Oy:n toimitusjohtaja Lumi Valkamo on tyytyväinen yhtiönsä hyvin toimivaan TAP-järjestelmään. Käytyään tekoälyasetusta käsittelevässä koulutustilaisuudessa hän alkaa pohtia, miten tämä lainsäädäntö mahtaa vaikuttaa siihen tai sen käyttöön tulevaisuudessa. Erityisen epäselvää Lumille on, mikä järjestelmässä on tekoälyjärjestelmä tai yleiskäyttöinen tekoälymalli, joita sääntely vaikuttaa koskevan.*

*Asetuksesta Lumi löysi viittauksen "perustietojenkäsittelyyn", joka ei näytä kuuluvan asetuksen soveltamisalaan lainkaan. Tästä Lumi pääättelee, ettei järjestelmässä toimiva Excel-taulukko, johon työvuorot lopulta algoritmiavusteisen sovelluksen ehdotusten pohjalta merkitään, olisi lainkaan tekoälyjärjestelmä tai -malli.*

### PUTSIS OY

"Juuri näin", toteaa Atte Torney, jota Lumi kuitenkin päätti konsultoida.

"Entä se navigointi- ja liikennesovellus, joka ehdotukset tekee – onkohan se suuririskistä tekoälyä?" kysyy Lumi.

"Itsessään sellainen toiminto, joka ehdottaa ihmispäätäjälle työvuorojen järkevää jakamista päättämienne asiallisten muuttujien perusteella ei näyttäisi suuririskiseltä tekoälyjärjestelmältä. Pidättehan vaan tietosuojasta huolta. Siinäkin epätodennäköisessä tapauksessa, että se katsottaisiin suuririskiseksi, voisi siihen hyvin soveltua 6(3) artiklan "tukiälypoikkeus", eli tekoälyasetuksen vaatimukset eivät siihen ulottuisi", sanoo Atte.

"Sitten tämä mainio saavutettava chatbottimme. Niitähan nyt on jokaisella nettisivulla. Eihän tämä ole mikään tekoälyjärjestelmä?" kysyy Lumi.

Atte vastaa: "No juu, TAP-järjestelmää tuntematta ja tekniikkaa auttavasti ymmärtävänä juristina uskoisin sen olevan tavallinen suuren kielimalliin pohjautuva yleiskäyttöinen tekoälymalli eli järjestelmään integroituna yleiskäyttöinen tekoälyjärjestelmä. Ei erityisen riskikäs, mutta laskentakykyinen sellainen. Siksi tekoälyasetus tuskin edellyttää muuta kuin 50 artiklan avoimuutta sen suhteen, ettei asiakas keskustele ihmisen vaan botin kanssa. Bottiuskin lienee selvää jo asiayhteydestä, ja avoimuusvaatimus soveltunee mallinne joskus 2027 alkaen."

"Mitenkäs tämä työssä suoriutumisen tarkkailu sitten, kun järjestelmän tietokonenäkö poimii asiakasyritysten kameravalvontavirrasta kappale määrätiedon työpaidan perusteella tunnistettujen putsislaisten iloisista tervehdyksistä asiakkaille? Tämä taitaa olla sitä työsuhteessa olevien henkilöiden suorituksen ja käyttäytymisen seurantaa ja arviointia, joka luokitellaan suuririskiseksi", pääättelee Lumi.

Atte: "Juu, suorituksen ja käyttäytymisen seuranta työsuhteessa tekee tekoälyjärjestelmästä suuririskisen. Ja sehän tarkoittaa vain, että järjestelmään soveltuvat suuririskisiä koskevat tekoälyasetuksen vaatimukset. Mutta ..."

"Mitä mutta? Eikö ollut niin että tässä on pitkä siirtymäaika, jona voin vielä käyttää suuririskistä järjestelmää huolehti?" ihmettelee Lumi.

"Ihan tarkalleen, seuraatteko te vain tervehtimistä, vai nimenomaan sitä onko tervehdys iloinen?" kysyy Atte.

Lumi vastaa: "Iloisuutta toki, tervehdyksen lisäksi – se on iso osa meidän brändiämme!"

"Tämä on nyt ensinnäkin ongelmallista siksi, että tekoälyasetuksen 5(1)f artiklan mukaan tunteiden päättelyminen työpaikalla on kielletty tekoälyn liittyvä käytäntö", miettii Atte.

"Mitä? Onko koko TAP-järjestelmän käyttö nyt kielletty?" kauhistuu Lumi.

"Järjestelmän määritelmä on kyllä vähän epäselvä asetuksen pohjalta, mutta eiköhän siihenkin jotain suuntaviivoja piakkoin saada. Vaikea on tarkasti sanoa muodostaisiko TAP-järjestelmä kokonaisuutena tekoälyasetuksen tarkoittaman tekoälyjärjestelmän vai koostuuko se useammasta tällaisesta järjestelmästä", ajattelee Atte ääneen ja jatkaa pohdintaa: "Nyt joka tapauksessa olisi mietittävä onko mahdollista siirtyä seuraamaan tunteiden sijaan ainakin vain tervehtimisiä. Uskoisin, että nykyisellään kyse on suuririskisen tekoälyjärjestelmän sijaan kielletystä käytännöstä, jota ei alkuvuodesta 2025 enää saa tekoälyjärjestelmässä olla. Siitä voi seurata sanktioitakin."

Lumi: "Oho – tuota en olisi arvannut. Voiko tätä mitenkään kiertää? Työntekijän suostumuksella vaikka?"

"Ei voi, kyllä nyt on paras tehdä pikimmiten ainakin tämä muutos järjestelmään. Minun pitää miettiä vielä olisiko käytäntönne kielletty myös sosiaalisena pisteytyksenä vaikka lähtökohtanne on käsittääkseni vain sen pohjalta palkita työntekijöitä – mutta suuririskinen se nyt ainakin tavalla jos toisella tulevaisuudessa olisi. Siirtymäajan kulussa ehditään vielä miettiä, onko koko TAP-järjestelmä suuririskinen vai onko kyse useammasta tekoälyjärjestelmästä ja -mallista, joista osaa tekoälyasetuksen vaatimukset eivät juurikaan koske", vastaa Atte.

Lumi huolestuu: "Voi hyvä tavaton. Mitä luulet, miten tekoälyasetus suhtautuu meidän tekoälymoppimme kehitysprojektiin? Siinähan kanssa moppaajasta keätään terveystietoja..."

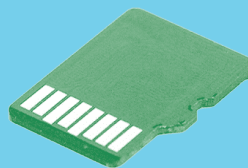
Atte miettii hetken: "Onhan siinä mukana kaikenlaisen tiedon keräämistä ja käyttöä, liekö biometristäkin? Mutta kyllä se oikein suunniteltuna voisi minun mielestäni olla suuririskisen tekoälyjärjestelmä, eikä kielletty käyttötarkoitus. Mutta kaikesta se on lääkinnällinen laite, jolloin sen tulee täyttää myös sitä tuoterihmää koskevat EU:n yhtenäistetyt tuotesäätelyn vaatimukset."



**Atte Torney**



**Lumi Valkamo**



## Muista ainakin nämä

1

Suuririskinen tekoäly ei ole kiellettyä, mutta vaatii riskien minimointia.

a. Suuririskisyys voi johtua joko tuoteturvallisuussääntelystä tai käyttötilanteen aiheuttamista riskeistä perusoikeuksille.

b. Näitä järjestelmiä tulee kehittää huolellisesti, ja niiden vaatimusten mukaisuus on dokumentoitava ja osoitettava CE-merkinnällä.

2

Kestämättömän riskin käyttötavat ovat kiellettyjä.

3

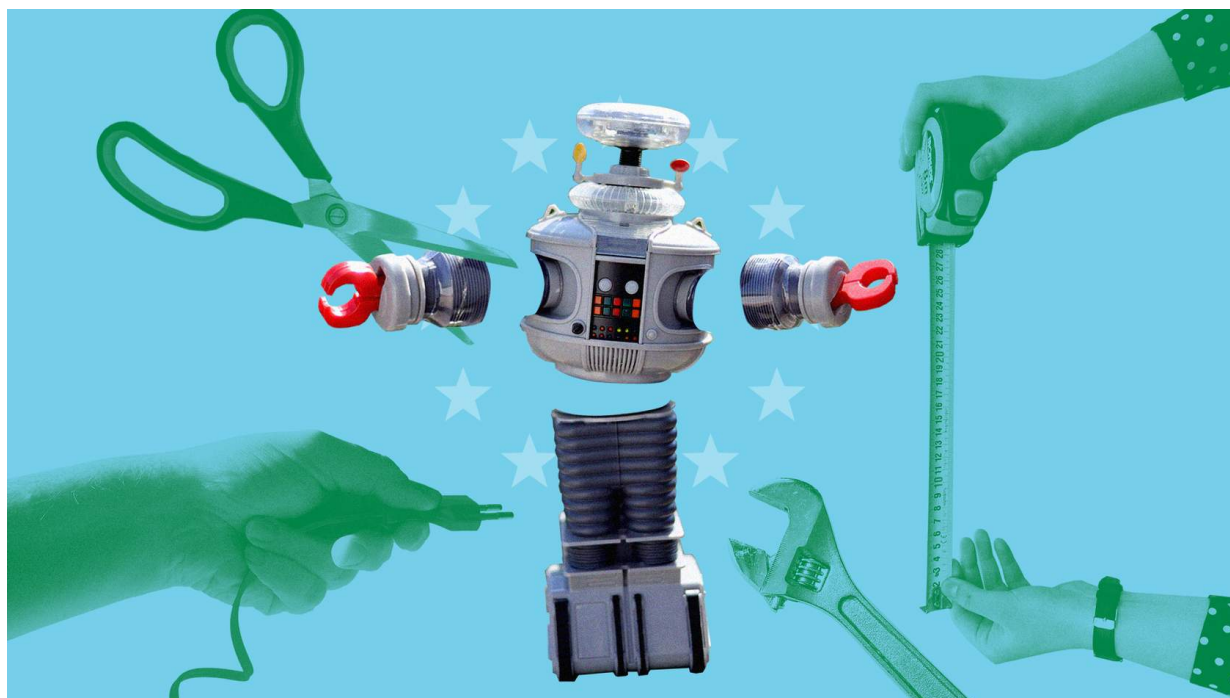
Matalan riskin käyttötapoja ei juurikaan säännellä.

**Jatka seuraavaan osioon**



# Näin kehität suuririskistä tekoälyä

---



---

**Jos tekoälyn aiheuttaman haitan riski on suuri,  
sen kehittämisessä ja dokumentoinnissa on  
noudatettava erityistä huolellisuutta.**

Oikein käytettynä suuririskinen tekoäly tarjoaa monia mahdollisuuksia. Jotta nämä hyödyt saavutetaan ja riskit pysyvät hallinnassa, suuririskinen tekoäly on kehitettävä huolellisesti ja mahdolliset haitat on

minimoitava kaikissa kehitysvaiheissa tekoälyasetuksen vaatimusten ja Euroopan komission antamien ohjeiden mukaisesti.

## Hyvät käytännöt ja dokumentointi

Tekoälyjärjestelmien kehittämisessä kannattaa panostaa huolellisuuteen, kuten kaikissa tietojärjestelmissä, joita on tarkoitus käyttää pitkäjänteisesti. Suuririskisen tekoälyjärjestelmän käyttöönotto on mahdollista vasta, kun riskit on minimoitu tekoälyasetuksen vaatimusten mukaisesti.

Vaadittavaa CE-merkintää ei saa käyttää, elleivät kaikki asetuksessa määritellyt vaatimukset täyty. Näitä vaatimuksia kannattaa pitää hyvänä ohjenuorana myös matalariskisissä tekoälyjärjestelmissä ja soveltaa niitä tapauskohtaisesti.

### Ota käyttöön riskienhallintajärjestelmä

Riskienhallintajärjestelmä on jatkuva ja kehittyvä prosessi, joka kattaa tekoälyjärjestelmän koko elinkaaren ja vaatii säännöllisiä päivityksiä. Tämä sisältää seuraavat vaiheet:

1. Tunnista ja analysoi kaikki ennakoitavat riskit, joita järjestelmä voi aiheuttaa terveydelle, turvallisuudelle tai perusoikeuksille.
2. Huomioi riskit sekä suunnitellussa käytössä että asetuksen mukaisesti "kohtuullisesti ennakoitavissa väärinkäyttöolosuhteissa".
3. Jatka riskianalyysiä seuraamalla järjestelmän toimintaa, kun se on markkinoilla.

Toteuta riskienhallintatoimenpiteet:

- Ota huomioon kaikkien vaatimusten yhteisvaikutukset ja minimoi riskit tasapainottamalla eri toimenpiteitä.
- Minimoi riskejä teknisin keinoin mahdollisimman pitkälle.
- Varmista, että jäljelle jäävä riski on hyväksyttävissä.
- Ohjaa lieventämis- ja valvontatoimenpiteet käsittelemään riskejä, joita ei voida poistaa.
- Tarjoa käyttäjille tarvittavat tiedot ja koulutus.

## Käytä laadukasta koulutus- ja testidataa

Varmista, että data täyttää seuraavat vaatimukset:

- **Relevanssi:** Tietoaineistot tulee valita niin, että ne ovat olennaisia järjestelmän aiottuun käyttötarkoitukseen.
- **Edustavuus:** Tietoaineistojen tulee olla riittävän edustavia ajatellen järjestelmän käyttökohteita ja kohderyhmiä.
- **Virheettömyys:** Datan tulee olla mahdollisimman tarkkaa ja virheetöntä.
- **Puolueettomuus:** Tietoaineistoissa ei saa olla vinoumia, jotka voisivat vaikuttaa haitallisesti terveyteen, turvallisuuteen, perusoikeuksiin tai johtaa syrjintään. On tärkeää kiinnittää huomiota puolueellisuuksiin, jotka voivat vaikuttaa järjestelmän tuleviin toimintoihin.
- **Tilastollinen pätevyys:** Tietoaineistojen tulee täyttää asianmukaiset tilastolliset vaatimukset.
- **Kohdentaminen käyttötilanteeseen:** Tietoaineistoissa tulee huomioida maantieteellinen alue, toimiala ja muut sen käyttöönottoon liittyvät erityispiirteet.

Vaatimukset koskevat testidataa, sekä tekoälymallia koulutettaessa myös koulutus- ja arviointidataa.

## Laadi tekninen dokumentaatio ennen käyttöönottoa

Ennen kuin viet suuririskisen tekoälyjärjestelmän markkinoille tai otat sen käyttöön, sinun on valmisteltava tekninen dokumentaatio, joka osoittaa järjestelmän täyttävän asetuksen vaatimukset. Tämä dokumentaatio on pidettävä ajan tasalla koko tekoälyjärjestelmän elinkaaren ajan. Teknisen dokumentaation on oltava selkeää ja kattavaa, jotta viranomaiset saavat kaikki tarvittavat tiedot vaatimustenmukaisuuden varmistamiseksi.

Tekoälyasetuksen liite IV sisältää tarkat vaatimukset. Komissio voi päivittää liitettä ja lisäksi julkaista tarkempia ohjeita ja dokumenttimalleja. Pk-yrityksille tarjotaan yksinkertaistettuja dokumenttipohjia. Teknisen dokumentaation keskeiset sisällöt ovat seuraavat:

- **Tekoälyjärjestelmän yleiskuvaus:** rooli, tavoite, tarjoaja, versio, yhteentoimivuus muiden järjestelmien kanssa, käytötavat, laitteistovaatimukset ja käyttöohjeet.
- **Kehityksen ja toiminnan kuvaus:** kehitysmenetelmät, muiden ratkaisujen käyttö, algoritmit, rakenne, arkkitehtuuri, datalähteet ja koulutusmenetelmät sekä järjestelmän valvonta.

- **Toiminnan seuranta ja riskienhallinta:** järjestelmän seuranta, arviointi, varotoimet, poikkeustilannesuunnitelmat, standardit ja sertifikaatit.

## Ota lokitiedot talteen koko elinkaaren ajalta

Kaikki tapahtumat on tallennettava lokiin. Näitä lokitietoja tulisi säilyttää asianmukainen ajanjakso, vähintään 6 kuukautta, ellei muu lainsäädäntö toisin määrää. Jäljitettävyyden vuoksi lokiin on tallennettava tapahtumat ja tiedot, jotka mahdollistavat seuraavat tavoitteet:

- Tunnistetaan tilanteet, joissa muodostuu suuri riski perusoikeuksille.
- Tunnistetaan tilanteet, joissa järjestelmän toimintaa muutetaan merkittävästi.
- Mahdollistetaan toiminnan tehokas valvonta ja seuranta.
- Käyttöönottajat voivat havaita suuririskiset tilanteet sekä raportoida niistä tarjoajalle ja valvontaviranomaiselle.

Muista, että sekä tarjoajien että käyttöönottajien on säilytettävä hallinnassaan olevia lokeja.

## Tee järjestelmästä riittävän läpinäkyvä

Käyttäjien tulisi pystyä ymmärtämään tekoälyjärjestelmän toiminta, arvioimaan sen toimintaa ja tunnistamaan sen vahvuudet ja heikkoudet.

## Laadi selkeät käyttöohjeet, joita käyttöönottajat seuraavat

Kaiken dokumentaation on oltava kattavaa ja helposti ymmärrettävää, ja se on kirjoitettava kohdeyleisön kielellä. Havainnollista järjestelmän ominaisuuksia esimerkeillä parantaaksesi ohjeiden ymmärrettävyyttä. Ohjeiden tulisi olla helposti saatavilla digitaalisessa muodossa ja tarjota

- ytimekkäitä ja selkeitä ohjeita, jotka ovat käyttäjille helposti ymmärrettäviä
- tietoa järjestelmän tarjoajasta ja tarvittaessa valtuutetusta edustajasta

- selityksiä järjestelmän suorituskyvystä, ominaisuuksista ja rajoituksista, kuten
  - käyttötarkoitus ja odotettu tarkkuus
  - millaisia syötteitä järjestelmä voi käsitellä
  - mahdollisia riskejä ja inhimillisen valvonnan tapoja
  - asennus-, konfigurointi- ja käyttöohjeet
  - tarvittava laitteisto- ja ohjelmistoympäristö
  - järjestelmän arvioitu käyttöikä ja huoltotarpeet
- tietoa turvaratkaisuista riskien vähentämiseksi.

## **Varmista, että ihmiset voivat valvoa tekoälyjärjestelmää**

Ihmisten tulee voida

- valvoa järjestelmän toimintaa
- puuttua toimintaan tarvittaessa tai pysäyttää se turvalliseen tilaan pysäytyspainikkeella
- varmistaa, että järjestelmää käytetään tarkoitulla tavalla
- ottaa huomioon kaikki järjestelmän negatiiviset vaikutukset sen elinkaaren aikana.

Sinun on annettava käyttäjille selkeät ohjeet tekoälyjärjestelmän valvontatoimenpiteistä. Ohjeisiin tulisi sisältyä

- valvojan tehtävät ja vastuut
- valvojan tarvitsema pätevyys, koulutus ja valtuudet
- ohjeet väliintuloon ja ongelmatilanteen laajenemisen estämiseen
- teknisiä työkaluja, kuten kojelautoja tai valvontajärjestelmiä, jotka auttavat ymmärtämään tekoälyjärjestelmän päätöksiä.

Valvontatoimenpiteiden tulisi vastata järjestelmän riskitasoa, autonomiaa ja käyttöyhteyttä. Suurempi riski tai autonomia vaatii yleensä tehokkaampaa valvontaa. Valvonta voidaan toteuttaa kahdella tavalla:

1. Ihmisen osallistumista edellyttävät järjestelmät (engl. human-in-the-loop): Näissä järjestelmissä vaaditaan ihmisen väliintulo tietyissä tilanteissa, kuten ennen päätösten tekemistä tai toiminnan aloittamista. Tämä

voi tarkoittaa, että henkilö tarkistaa tekoälyn tulokset ennen niiden toteuttamista tai valvoo aktiivisesti järjestelmän suoritusta ja puuttuu siihen tarvittaessa.

2. Ihmisen osallistumisen mahdollistava järjestelmät (engl. human-on-the-loop): Nämä järjestelmät toimivat itsenäisemmin, mutta ihmiset voivat silti valvoa ja puuttua toimintaan tarvittaessa. Näissä järjestelmissä ihmiset saavat reaaliaikaisen tiedon järjestelmän toiminnasta, voivat säätää parametreja tai sammuttaa järjestelmän, jos se ei toimi oikein.

Korkean riskin tekoälyjärjestelmiin tulisi sisällyttää ominaisuuksia, jotka helpottavat ihmisten valvontaa:

1. Sisäänrakennetut suojausmekanismit, jotka estävät järjestelmää ylittämästä tiettyjä rajoja tai tekemästä päätöksiä väärissä tilanteissa. Järjestelmä ei voi ohittaa näitä rajoja itse.
2. Järjestelmän tulee totella valtuutettujen henkilöiden komentoja ja antaa heidän hallita sen toimintaa tarvittaessa.
3. Ohjausmekanismit, kuten hälytykset tai selitykset, auttavat ihmisiä ymmärtämään järjestelmän toimintaa ja tekemään päätöksiä puuttumisesta.

## **Varmista, että tekoäly toimii tarkasti, vakaasti ja kyberturvallisesti**

Tekoälyjärjestelmän on täytettävä kaikki yleisten tietojärjestelmien kyberturvallisuusvaatimukset ja käyttötilanteen kriittisyydestä riippuvat lisävaatimukset.

Tekoälyn osalta on erikseen kiinnitettävä huomiota koulutusaineistojen myrkyttämiseen, mallien tai kirjastojen myrkyttämiseen, hyökkäviin käyttötapoihin, luottamuksellisuushyökkäyksiin tai malleista löytyneiden vikojen väärinkäyttöön. Käytön aikana oppivien tekoälyjärjestelmien on minimoitava vinoutuneen käytön mahdollisuudet vaikuttaa järjestelmän tulevaan toimintaan.

Virheiden ja epäjohtonmukaisen toiminnan mahdollisuudet on tehtävä mahdollisimman vähäisiksi sekä teknisillä että organisatorisilla keinoilla. Komissio tuottaa ja ylläpitää tarkempia mittareita tekoälyjärjestelmien tarkkuuden ja vakauden arviointiin.

## **Maahantuoja on varmistettava vaatimustenmukaisuus**

Maahantuoja, joka tuo tekoälyjärjestelmiä EU:n ulkopuolelta, tulee varmistaa suuririskisen tekoälyjärjestelmän osalta, että

- se on vaatimusten mukainen ja se on hyväksytty
- sen tekninen dokumentaatio on kunnossa
- siinä on CE-merkintä ja EU:n vaatimustenmukaisuusvakuutus
- sillä on valtuutettu edustaja.

Maahantuojan omien tietojen on oltava tekoälyjärjestelmän ohessa.

### **Ulkomaisen toimittajan edustaja vastaa raportoinnista ja yhteistyöstä viranomaisten kanssa**

EU:n ulkopuolella toimivan tekoälytoimittajan on nimettävä EU:ssa sijaitseva edustaja. Edustajalla on oltava kirjallinen valtuutus toimittajalta jollakin EU:n virallisella kielellä. Edustaja varmistaa, että tarjoaja on antanut järjestelmästä vaatimustenmukaisuusvakuutuksen dokumentaatioineen. Lisäksi edustajan tulee tarvittaessa toimittaa viranomaiselle todistusaineistot ja tehdä yhteistyötä viranomaisten kanssa riskien minimoimiseksi. Edustaja voi hakea hyväksynnän tekoälyjärjestelmälle tai vakuuttaa toimittajan tiedot oikeiksi tämän hakiessa hyväksyntää.

### **Ulkomaisen toimittajan jakelija seuraa vaatimustenmukaisuutta**

Jakelija tuo tekoälyjärjestelmän markkinoille, mutta ei toimi maahantuojana tai edustajana.

Jakelijat on varmistettava suuririskisen tekoälyjärjestelmän osalta, että

- järjestelmässä on CE-merkintä ja EU:n vaatimustenmukaisuusvakuutus
- sen tarjoaja ja maahantuoja on mainittu asianmukaisesti järjestelmän yhteydessä
- järjestelmä pysyy vaatimustenmukaisena.

Mikäli tekoälyjärjestelmä lakkaa olemasta vaatimusten mukainen, on jakelijan tehtävä korjaavat toimenpiteet tai poistettava järjestelmä markkinoilta. Sen on tehtävä yhteistyötä viranomaisten kanssa

ja ilmoitettava tilanteesta viranomaisille sekä tarjoajalle tai maahantuojalle.

### *Testaa tietosi*

Mitä suuririskisten tekoälyjärjestelmien kehittäjien tulee varmistaa?

- ☐ A) Riskienhallintajärjestelmä kattaa tekoälyjärjestelmän koko elinkaaren
- ☐ B) Tekoälyjärjestelmät edellyttävät CE-merkinnän ennen markkinoille viemistä
- ☐ C) Koulutus- ja testidatan tulee olla edustavaa, virheetöntä ja puolueetonta
- ☐ D) Lokitietoja on säilytettävä vähintään 6 kuukautta
- ☐ E) Käyttöönottajan työntekijät eivät tarvitse koulutusta järjestelmän käytöstä
- ☐ F) Käyttäjillä tulee olla mahdollisuus valvoa tekoälyjärjestelmän toimintaa ja puuttua siihen tarvittaessa
- ☐ G) Tekoälyjärjestelmien on oltava kyberturvallisia ja vakaasti toimivia



SUBMIT



**Putsis Oy**

### *Yritystarina*

#### **Näin dokumentoidaan riskialtis tekoälymoppi**

*Yksi Putsis Oy:n suurista asiakkaista on sairaala. Yhdessä asiakkaansa kanssa yritys on ideoinut maailmanvalloitukseen tähtäävää tuotekehitystä vähentääkseen siivouksesta – siivoojien levittämistä hengitystietulehduksista – aiheutuvia riskejä sairaalan tehohoito-osastolla. Ns. älymoppikehitysprojekti yhdistää siivoojan elintoimintojen tarkkailun, alkavan sairauden päättelyn niiden perusteella sekä tehokkaan ja hygieenisen lattianpuhdistusmopin, johon on sisäänrakennettu sensori-, mikrofoni- ja kamerateknologia, joka tarkkailee, että jokainen lattian neliösentti siivotaan puhtaaksi.*

*Tekoälymoppi luokitellaan suuririskiseksi tekoälyjärjestelmäksi. Siksi tuotekehitysryhmä on jo kehitysvaiheessa pysähtynyt pohtimaan, miten vaatimustenmukaisuusvakuutuksen lisäksi toteuttaa tekoälyasetuksen 11 artiklan teknistä dokumentointia koskevat vaatimukset. Asetuksen liite IV, jossa vaatimukset listataan, vaikuttaa pitkälti kuin nälkävuosi – yhdeksän kohtaa, joissa pisimmillään kahdeksan alakohtaa – joten Lumi päättää kysyä Atelta, voisiko sitä jotenkin kiertää.*

## PUTSIS OY

Atte: "No, liitehän on oikeastaan muistilista tiedoista, jotka suuririskisten tekoälyjärjestelmien tarjoajien on 18 artiklan mukaisesti 10 vuotta järjestelmän markkinoille saattamisesta tai käyttöönottamisesta pidettävä kansallisten viranomaisten saatavilla. Muistakaa myös 18 artiklassa listatut tiedot sekä mitä 19 artikla edellyttää lokitiedoista."

"Mutta ei meillä ole resursseja kaikkien näiden liitteen IV tietojen listaamiseen ja vähän tuntuu vaikealta edes päättää, mistä aloittaa", Lumi valittaa.

"Onneksi komissio tietää, että yrityksistä suurin osa on pk-kokoisia ja aloittavia yrityksiä (start-up) . Niitä varten komissio laatii yksinkertaistetun lomakkeen teknistä dokumentaatiota varten. Odottakaa sitä", lohduttaa Atte.



Videolla kuulet Cloud1:n datainsinööri Jane Seppälän näkökulman tekoälyasetukseen.



## **Tekoälyn sääntelyn testiympäristöt**

Ennen kuin tekoälyä asetetaan markkinoille, tarjoajalla on mahdollisuus testata sen toimintaa tekoälyn sääntelyn testiympäristössä (engl. AI regulatory sandbox). Tekoälyasetuksen myötä jokaisessa jäsenvaltiossa tulee olla vähintään yksi kansallisesti tarjottu testiympäristö elokuuhun 2026 mennessä, minne ensisijainen pääsy on kohdennettu pk-yrityksille. Lisäksi viranomaiset tarjoavat ohjeistusta ja materiaalia selventääkseen sääntely-ympäristön mahdollisia epäselvyyksiä, jotka liittyvät tekoälyn kehitykseen ja käyttöönottoon. Suuririskisten järjestelmien testaaminen todellisessa ympäristössä on myös mahdollista, kun se tehdään tarkkojen turvasäännösten mukaisesti.



### *Yritystarina*

#### **Olisiko hiekkalaatikolla harjoittelusta apua?**

*Tekoälymopin kehitys etenee, mutta siitä nousee yhä uusia kysymyksiä. Toimitusjohtaja Lumi alkaa epäillä, riittääkö pelkän tekoälyasetuksen noudattaminen ja täyttääkö visioitu tuote edes sen vaatimukset. Entä lääketieteellisiä laitteita koskeva sääntely? Mitä muuta lainsäädäntöä tulee noudattaa – erityisesti, jos tähdätään Yhdysvaltojen markkinoille?*

*Työryhmä ehdottaa hankkeen viemistä "hiekkalaatikkoon" eli tekoälyn sääntelyn testiympäristöön. Tästä Lumi ei tiedä mitään, joten hän soittaa Atelle.*

"Voiko hiekkalaatikko auttaa tekoälymopin lainmukaisuuden varmistamisessa?"

Atte vastaa: "Tarkoitat siis EU-maiden viranomaisten tarjoamia tekoälyn sääntelyn testausympäristöjä? Kyllä, pk-yritys voi hyvinkin hakea ja päästä hiekkalaatikkoon, ja tekoälyasetuksen mukaan tieto tästä pitää saada kolmen kuukauden kuluessa hakemuksesta. Hiekkalaatikossa viranomaiset ohjaavat yritystä täyttämään lain vaatimukset tekoälyyn liittyen. Loppujen lopuksi yritys vastaa siitä, että tuote täyttää lain vaatimukset. Testausympäristöissä voi olla neuvonnan lisäksi erilaisia teknisiä ratkaisuja, jotka voivat vaihdella jäsenmaittain. Voitte periaatteessa hakea minkä tahansa EU-valtion testausympäristöön."



**Lumi Valkamo**



**Atte Torney**

Seuraavalla videolla lakimies Anne Kaartinen Liikenne- ja viestintävirasto Traficomista valottaa viranomaisen roolia tekoälyn kehittämisen ja käyttöönoton tukemisessa.



## **Videolla mainitaan joitain tekoälyasetusta valvovia viranomaisia. Täydellinen luettelo viranomaisista**

- Liikenne- ja viestintävirasto Traficom
- Turvallisuus- ja kemikaalivirasto Tukes
- Lääkealan turvallisuus- ja kehittämiskeskus Fimea
- Finanssivalvonta
- Tietosuojavaltuutettu
- Yhdenvertaisuusvaltuutettu
- Tasa-arvovaltuutettu
- Yhdenvertaisuus- ja tasa-arvolautakunta
- Valtioneuvoston oikeuskansleri
- Eduskunnan oikeusasiamies
- Työsuojeluviranomainen (aluehallintovirastot)
- Kuluttaja-asiamies



## Tekoälyjärjestelmän tarjoajan ja kehittäjän tarkistuslista

- 1 Selvitä tekoälyjärjestelmän riskiluokitus. Tähän voit tarvita asiakasta, joka tuntee käyttötapauksen ja käyttötavat, joihin he aikovat uuden tekoälyn sijoittaa.
- 2 Jos asiakkaasi on julkisella sektorilla, asiakkaan on selvitettävä järjestelmän vaikutukset perusoikeuksiin. Järjestelmän kehittäjä voi auttaa tässä prosessissa ja osaltaan minimoida riskejä.
- 3 Epäselvissä tilanteissa ole yhteydessä vastuuviranomaiseen.

## Suuririskisen tekoälyjärjestelmän tarjoajan ja kehittäjän tarkistuslista

- 1 Varmista, että tekoälyjärjestelmä seuraa kaikkia tässä osiossa mainittuja vaatimuksia.
- 2 Lisää yrityksesi nimi, tavaramerkki ja yhteystiedot järjestelmään, sen ohjeisiin tai pakkaukseen.
- 3 Ylläpidä laadunvalvontajärjestelmää.

4

Ylläpidä dokumentaatiota.

5

Ylläpidä ja säilö automaattisesti tuotettuja lokeri- ja lainmukaisesti, kuitenkin ainakin 6 kuukautta.

6

Varmista, että järjestelmä saa viranomaisen hyväksynnän ennen sen käyttöön viemistä.

7

Laadi EU:n vaatimusten mukaisuusvakuutus.

8

Liitä CE-merkintä tekoälyjärjestelmään, sen ohjeisiin tai pakkaukseen.

9

Rekisteröi tekoälyjärjestelmä EU:n tietokantaan.

10

Tee tarvittavat korjaukset ja tiedota viranomaisia, mikäli järjestelmä lakkaa ole masta vaatimusten mukainen.

11

Valvovan viranomaisen pyynnöstä osoita tekoälyjärjestelmän vaatimusten mukaisuus.

12

Varmista tekoälyjärjestelmän saavutettavuus.

**Jatka seuraavaan osioon**



## Näin hankit ja otat käyttöön tekoälyä

---



---

**Tekoälyä käyttöön ottavan tahon on  
varmistettava, että sen omat käytännöt eivät  
kasvata riskejä.**

Tekoälyn hankkijalla eli käyttöönottajalla on myös velvoitteita tekoälyasetuksessa. Kaikkea vastuuta ei voi ulkoistaa tekoälyn tarjoajalle. Käyttöönottajalla on arvioitava oman käyttönsä riskitaso, ja mikäli se todetaan suuririskiseksi, on käyttöönottajalla seurattava kaikkia siitä seuraavia velvoitteita.

## **Henkilöstön osaaminen kuntoon**

Henkilöstön koulutus on ollut kaikille organisaatioille pakollista 2.2.2025 lähtien. Käytännössä työntekijöiden, jotka käyttävät tekoälyjärjestelmiä työssään, on ymmärrettävä, mitä tietoja niihin saa syöttää ja mitä ei, minkälaisia tuloksia järjestelmän voi odottaa tuottavan ja miten virhetilanteet havaitaan ja raportoidaan.

Vastaava osaamisvelvoite on kaikille tuttu jo yleisestä tietosuojasetuksesta (engl. General Data Protection Regulation, GDPR). Kaikkien työntekijöiden, jotka käsittelevät työssään henkilötietoja, on ymmärrettävä lain velvoitteet, eli millä perusteella tietoja käsitellään ja missä järjestelmissä, mitä tiedoilla ei saa tehdä ja miten tietojen säilyttäminen ja poistaminen hoidetaan asianmukaisesti.

Asianmukainen koulutus ei ole vain lain vaatimus, vaan myös keino minimoida riskejä ja varmistaa organisaation vastuullisuus tekoälyn ja henkilötietojen käytössä.



## Yritystarina

### Tekoälylukutaito, mitä ihmettä?

*Putsis Oy on hankkinut uuden toiminnon TAP-järjestelmäänsä. Se käyttää keräämiensä asiakastietojen analysointiin tekoälyä parantaakseen asiakaskokemusta, suosittelakseen uusia siivouspalveluita olemassa oleville asiakkaille sekä tunnistaakseen uusia asiakkaita ja markkinoidakseen Putsis Oy:n palveluita heille.*

## PUTSIS OY

Toimitusjohtaja Lumi huokaisee ääneen helpotuksesta start-up-perustajien kerhon kuukausittaisella avantouintivuorolla: "Onneksi aiemman asiakasrekisterimme korvaa järjestelmämme uusi tekoälytoiminto. Se on kyllä hieno, käyttää suositusten tekemiseen asiakkaille samoja algoritmeja kuin Amazon. Tietosuojavastavamme siirtyi juuri uusiin tehtäviin toiselle työnantajalle, ja tehtävään sopivia henkilöitä on ollut vaikea löytää. Nyt kaikki datamme kerätään tekoälyjärjestelmään, johon sovelletaan tekoälyasetusta – voimme vihdoinkin unohtaa GDPR:n."

Ylva Sarjayrittäjä kääntyy Lumin puoleen: "Kuule, ei GDPR mihinkään katoa – ei sakkomahdollisuus eikä mikään. Kumpikin asetus soveltuu kun tekoälyjärjestelmässä käsitellään henkilötietoja. Minä lähetin tietosuojavastaavani hyvissä ajoin tekoälyasetusta käsittelevälle kurssille. Siellä selvisi, että GDPR:ää pitää edelleen noudattaa aina kun on henkilötiedoista kyse, oli mukana tekoälyä tai ei. Mutta onneksi tekoälyasetus ei muuta GDPR-velvoitteita. Seuraavaksi pitää huolehtia henkilöstön tekoälylukutaidosta."

"Tekoälylukutaidosta?" kysyy Lumi.

"Niin, nyt tietosuojavastaavani huolehtii siitä, että kaikilla työntekijöillämme, jotka vastaavat tekoälyjärjestelmiemme toiminnasta ja käyttävät niitä, on riittävä tekoälylukutaito. Lisäksi hän valvoo, että myös meille palveluna ostetun järjestelmätuen toimittajan henkilökunnalla on riittävä tekoälylukutaito. Ja kaikesta tästä hän on luvannut raportoida minulle. Kätevää, eikö?"

"Mutta mitä on tekoälylukutaito?" hämmästelee Lumi.

"No, se vähän vaihtelee asiayhteyden mukaan", toteaa Ylva. "Mutta ymmärtääkseni taitojen tulee olla riittävät annettujen työtehtävien hoitamiseen sellaisella tavalla, joka noudattaa tekoälyasetuksen vaatimuksia. Älä huolestu, komissio muistaakseni linjaa jollain käytännesäännöillä tarkemmin, mitä se tarkoittaa. Muttei huonosta tekoälylukutaidosta voi käsittääkseni sakkoja seurata."



**Jos riskit ovat pienet, käyttöönotto on vaivatonta**

Mikäli tekoälyjärjestelmä ei ole suuririskinen, sen hankinta tai käyttöönotto on suhteellisen yksinkertaista. Käyttöönottaja voi luottaa tarjoajan tuottamiin ohjeisiin ja dokumentteihin, mutta on silti vastuussa omasta toiminnastaan.

### *Esimerkiksi*

Auton valmistaja vastaa siitä, että auto täyttää kaikki turvallisuusvaatimukset. Kuitenkin ajajan vastuulla on omata ajokortti, ajaa nollapromilleilla ja noudattaa liikennesääntöjä.

Samoin tekoälyn käyttöönottajan on huolehdittava omasta datanhallinnastaan, henkilöstön koulutuksesta, tekoälyn hyödyntämisprosesseista ja yleensä lainmukaisesta toiminnasta.

## **Kerro palvelun käyttäjälle, että tämä on tekoälyn kanssa tekemisissä**

Kun henkilö jollain tavalla on tekoälyn kanssa tekemisissä, tulee tämän tietää siitä. Jos tekoälyn rooli on ilmeinen tietyssä asiayhteydessä, ei tästä tarvitse erikseen mainita. Muissa tilanteissa tekoälyn rooli on tuotava asiallisesti esiin.

Mikäli rajoittuneen riskin tekoälyjärjestelmä toimii taustalla eikä suoraan näy ihmisille, ei tällaisesta toiminnasta tarvitse kertoa.

## **Merkitse synteettiset tekoälyn tuotokset asianmukaisesti**

Mikäli tekoälyjärjestelmä tuottaa keinotekoista sisältöä (kuten syväväärennöksiä), jonka yleisö voisi erehtyä luulemaan aidoksi, on nämä merkittävä asianmukaisesti tekoälyn tuottamiksi. Tällainen sisältö voi olla valokuvia, ääntä tai videota. Myös yleisiä etuja koskevista asioista tiedottaminen synteettisellä tekstillä on merkittävä tekoälyn tuottamaksi.

Tähän vaikuttaa myös käyttötilanne. Mikäli tekoäly tuottaa elokuvaan erikoiseffektejä, sitä ei erikseen tarvitse mainita. Mutta jos uutislähetyksessä olisi tekoälyn tuottama synteettinen “taiteilijan näkemys” uutistapahtumasta, tällaisen ilmoittaminen on tietenkin varsin tarpeellista.

### *Testaa tietosi*

Mitä tulee ottaa huomioon matalariskisiä tekoälyjärjestelmiä hankittaessa ja käytettäessä?

---

☐

A) Käyttäjien tulee olla tietoisia, että he ovat vuorovaikutuksessa tekoälyn kanssa

☐

B) Tekoälyn synteettisesti tuottama sisältö on merkittävä asianmukaisesti

☐

C) Käyttöönnottajan ei tarvitse huolehtia omasta datanhallinnastaan tai henkilöstön koulutuksesta

☐

D) Jos tekoäly toimii täysin taustalla eikä ole suoraan vuorovaikutuksessa ihmisten kanssa, siitä ei tarvitse erikseen kertoa

☐

E) Synteettisen sisällön merkintä on aina välttämätöntä, riippumatta käyttötilanteesta

SUBMIT

# Julkinen sektori asiakkaana: perusoikeudet kuntoon

Julkisen sektorin toimijoiden on tehtävä perusoikeusarviointi ennen suuririskisen tekoälyjärjestelmän käyttöönottoa. Arviointi sisältää seuraavat vaiheet:

- 1 kuvaus prosesseista, joissa tekoälyä käytetään
- 2 kuvaus käyttöajasta ja -taajuudesta
- 3 vaikutusentilaisten henkilöiden ja ryhmien luokat
- 4 erityisen haitan riskit, käyttöohjeiden tiedot huomioiden
- 5 kuvaus ihmisvalvonnasta käyttöohjeiden mukaisesti
- 6 toimenpiteet tilanteissa, joissa riskit toteutuvat.

Tekoälyjärjestelmän tarjoaja voi tukea julkisen sektorin toimijaa tämän arvioinnin tekemisessä.





### *Yritystarina*

#### **Perusoikeusarviointi on julkisen toimijan vastuulla**

*Hyvinvointialue tahtoo jatkaa Putsis Oy:n käyttöä sosiaalihuoltolain mukaisen siivoustukipalvelun toteuttajana. Tukipalveluiden hallintojohtaja Sari Hyvärinen on pohtinut tekoälyasetuksen noudattamista ja päätynyt siihen, että Putsis Oy:n TAP-järjestelmä on jo joka tapauksessa suuririskinen tekoälyjärjestelmä. Siksi hallintojohtaja Sari olettaa, että sitä voisi hyvin käyttää jatkossakin julkisen avun etuuksien (siivouksen) tarpeen arviointiin asiakkaan kevyen profiloinnin pohjalta.*

#### **PUTSIS OY**

Nyt hallintojohtaja Sari kysyy toimitusjohtaja Lumilta: "Toimittaako Putsis Oy:n TAP-järjestelmän tarjoaja tekoälyasetuksen edellyttämän vaatimusten mukaisuusvakuutuksen ja järjestelmän perusoikeusvaikutusten arvioinnin?"



"Juttelin juuri Aten kanssa ja ymmärsin, ettei vaatimusten mukaisuusvakuutusta lainkaan tarvita, kunhan TAP-tekoälyjärjestelmä säilyy sellaisena kuin se nyt jo on. Tämä on onnekasta, koska sitä olisi vaikeaa saada tarjoajalta, joka järjestelmän meille toimittaneen Tukiälypalvelut Oy:n mukaan on tehnyt konkurssin jo aikaa sitten", kertoo Lumi.

"Pätisiköhän sama perusoikeusvaikutusten arvioon? Ehkä kysynkin asiaa suoraan Atelta", sanoo Sari.

Atte vastaa: "Juu, periaatteessa tarjoajan on toimitettava suuririskisen järjestelmän vaatimusten mukaisuusvakuutus. Tästä on kuitenkin asetuksessa ajallinen poikkeus ennen 2026 käytössä olleille järjestelmille. Mutta 27 artiklan mukaan käyttöönottajien – ei tarjoajan tai muun – on tehtävä arviointi tällaisen järjestelmän käytön mahdollisista perusoikeusvaikutuksista. Eli tässä tapauksessa kai hyvinvointialueen."

Sari: "Mitä? Emmehän me ole koodareita! Emme me voi tietää, miten järjestelmä toimii."

Atte: "Perusoikeusvaikutusten arviointi on käyttöönottajien oma arvio tietyistä 27 artiklassa luetelluista asioista – prosessikuvaukset, ajanjakso, ryhmät, joihin vaikuttaa, riskit, ihmisvalvonta, varautuminen riskien toteutumiseen, sen sellaista. Asetus ei tätä sanamuodon pohjalta ihan tarkalleen ottaen vaadi, mutta jospa tunnistatte ensin perusoikeudet, joihin järjestelmä voisi vaikuttaa, siitä se lähtee – vaikka yksityisyys, yhdenmukainen kohtelu, oikeus sosiaaliturvaan, hyvä hallinto? Arvion tueksi komission tekoälytoimisto laatii mallikaavakkeen. En ole ihan varma, miten 111 artikla soveltuu tilanteeseen, mutta arvelisin, että sen ajallinen poikkeus tarkoittaa sitä, että teidän viranomaisten käytössä olevat suuririskiset tekoälyjärjestelmät ja niiden ylläpito on saatettava tekoälyasetuksen vaatimusten mukaiseksi elokuun alkuun 2030 mennessä. Sitä teillä on hetki aikaa selvittää."



**Sari Hyvärinen**



**Lumi Valkamo**



**Atte Torney**

**Jos räätälöit tekoälyä, olet vastuussa siitä**

Tekoälyjärjestelmää käyttöönotettaessa yrityksellä on usein mahdollisuus räätälöidä tuotetta omiin tarpeisiinsa sopivaksi, esimerkiksi jatkokouluttamalla järjestelmää omilla tietoineistoilla. On kuitenkin oleennaista ymmärtää, että käyttöönottaja on täysin vastuussa tekemästään räätälöinnistä ja sen vaikutuksista järjestelmän toimintaan.

Suuririskisten tekoälyjärjestelmien osalta vastuut siirtyvät räätälöijälle mikäli tämä tekee merkittäviä muutoksia. Näitä ovat seuraavat:

- Oma nimen tai tavaramerkin liittäminen suuririskiseen tekoälyjärjestelmään.
- Merkittävän muutoksen tekeminen, joka kuitenkin pitää järjestelmän edelleen suuririskisenä.
- Järjestelmän tai mallin muuttaminen suuririskiseksi.

Näissä tilanteissa alkuperäinen tarjoaja ei enää ole vastuussa järjestelmän vaatimusten mukaisuudesta. Käyttöönottajalla on vastuu noudattaa suuririskisille järjestelmille asetettuja vaatimuksia, esimerkiksi hankkia CE-merkintä sekä dokumentoida ja minimoida riskit.

Alkuperäisen tarjoajan on tehtävä yhteistyötä ja tarjottava kohtuudella se tuki, jota räätälöijä tarvitsee. Yhteistyötä ei vaadita, mikäli tarjoaja on julkaissut tuotteensa avoimella lisenssillä.



### *Yritystarina*

#### **Liukuminen tarjoajaksi räätälöinnin kautta**

*Nyt kun hyvinvointialueen hallintojohtaja Sari Hyvärisellä on syytä epäillä, että TAP-järjestelmän käyttö viranomaistarkoituksiin tulee tulevaisuudessa vaatimaan toimenpiteitä, joihin sen konkurssissa oleva tarjoaja ei tule ryhtymään, alkaa hän miettiä vaihtoehtoja.*

#### **PUTSIS OY**

Sari kysyy Atelta: "Jos järjestelmän jatkokäyttö tulevaisuudessa vaatii lisätyötä, voisiko järjestelmää kehittää toimimaan vielä paremmin hyvinvointialueen tarpeisiin? Jos, niin miten silloin tulisi menetellä, jotta järjestelmää voi varmuudella käyttää vielä 2030 jälkeenkin?"

Atte: "Kyllä järjestelmän jatkokehittäminen tekoälyasetuksen näkökulmasta on mahdollista. Siinä tapauksessa, että hyvinvointialue tekee tekoälyjärjestelmään merkittävän muutoksen, tulee alueesta järjestelmän tarjoaja. Tämä tarkoittaa sitä, että tarjoajan velvoitteet – kuten vaatimusten mukaisuuden arviointi ja dokumentointi – siirtyvät hyvinvointialueelle. Teidän on siis arvioitava järjestelmä ja dokumentoitava sen täyttävän tekoälyasetuksen vaatimukset ennen kuin järjestelmän voi saattaa markkinoille tai ottaa käyttöön."

Sari: "Eli meistä tulisi tarjoaja ja velvollisuuksiemme olisi varmistaa järjestelmän ikään kuin "uutena" täyttävän tekoälyasetuksen velvoitteet, jos tekisimme siihen merkittävän muutoksen?"

"Juuri näin", sanoo Atte.

"Mitähän merkittävä muutos tarkoittaisi käytännössä?" pohtii Sari.

"Jaa, se onkin vähän vaikeampi kysymys. Kuten tuotesääntelyssä yleensä, termi liittyy riskin kasvamiseen. Mutta siitä on tulossa komissioltta suuntaviivat."



**Sari Hyvärinen**



**Atte Torney**

Videolla Terveystalon Milla Keller kertoo tekoälyn hyödyntäjän näkökulman tekoälyasetuksesta.



## Suuririskisen tekoälyn hankinta on tehtävä huolellisesti

Käyttöönottajana on ensin arvioitava järjestelmän riskitaso oma toimintatapansa huomioiden. Riskitaso voi nousta tai laskea siitä, mihin tekoälyn tarjoaja on sen arvioinut.

Jos tekoälyjärjestelmä on käytössä suuririskinen, on sen käyttöönotto tehtävä huolellisesti. Muissakin tapauksissa on tietenkin hyvä seurata samoja käytäntöjä omaan toimintaan soveltaen.

### Tarkista CE-merkintä

Mikäli tekoälyjärjestelmä on suuririskinen, on siinä oltava CE-merkintä tarjoajan osoituksena siitä, että se on tekoälyasetuksen vaatimusten mukainen. CE-merkintä voi olla pakkauksessa, ohjeissa sekä digitaalisessa käyttöliittymässä ihmisluettavassa ja koneluettavassa muodossa.

## Seuraa ohjeita ja etsi hätäjarru

Suuririskisen tekoälyjärjestelmän mukana tulevat säädösten mukaiset tekniset dokumentaatiot ja käyttöohjeet. Näiden seuraaminen on pakollista.

Järjestelmä on voitava myös sammuttaa väliaikaisesti tai pysyvästi, jos sen havaitaan tuottavan vääriä tuloksia. Toimintaa valvovien henkilöiden on siis tiedettävä, missä hätäjarru on.

## Tekoälyn valvontaan nimetyillä henkilöillä on oltava riittävä koulutus, valtuudet ja tuki

Tekoälyn valvontaan on nimitettävä vastuuhenkilöt, joilla on oltava riittävä pätevyys, koulutus ja valtuudet. Heidän työlleen on annettava tarvittava tuki.

## Varmista tekoälyn syöttötietojen edustavuus

Valvottujen syöttötietojen on oltava riittävän edustavia ja merkityksellisiä.

## Ilmoita poikkeamista ja vaaratilanteista

Vaikka tarjoaja on ensisijaisesti vastuussa suuririskisen tekoälyjärjestelmän toiminnasta, käyttöönottajien velvollisuus on valvoa niiden toimintaa. Kaikki ongelmatilanteet on raportoitava tarjoajalle. Vaaratilanteesta on lisäksi ilmoitettava maahantuoajalle tai jakelijalle sekä viranomaisille. Kansallisen vaaratilanteen tapauksessa on lisäksi viipymättä ke skeyttävä järjestelmän käyttö.

## Säilytä lokitiedot asianmukaisesti

Lokitietoja on säilytettävä vähintään 6 kuukauden ajan tai asianmukainen ajanjakso, elleivät muut lait muuta sano.

## Informoi työntekijöitä ennentekoälyjärjestelmän käyttöönottoa

Mikäli suuririskisen tekoälyjärjestelmän toiminta kohdistuu yrityksen työntekijöihin, on työnantajan informoitava työntekijöitä ennen järjestelmän käyttöönottoa.

### Testaa tietosi

Mitä kaikkia vaatimuksia tulee noudattaa suuririskisen tekoälyjärjestelmän käyttöönotossa?

☐

A) Tarkista, että järjestelmässä on CE-merkintä

☐

B) Seuraa järjestelmän mukana tulevia käyttöohjeita ja teknistä dokumentaatiota

☐

C) Valvontaan nimetyt henkilöt eivät tarvitse erityistä koulutusta valvontatehtäviin

☐

D) Syöttötietojen on oltava edustavia ja merkityksellisiä

☐

E) Poikkeamat ja vaaratilanteet on raportoitava tarjoajalle ja tarvittaessa viranomaisille

☐

F) Lokitietoja on säilytettävä vähintään 6 kuukautta tai lain edellyttämän ajan

☐

G) Työnantajan on informoitava työntekijöitä ennen järjestelmän käyttöönottoa, jos järjestelmä vaikuttaa heidän työskentelyynsä

SUBMIT



## **Tekoälyjärjestelmän käyttöönottajan tarkistuslista**



1

Arvioi tekoälyjärjestelmän riskitaso huomioiden tarjoajan antamat tiedot ja omat käyttötapauksesi.

2

Mikäli riskitaso on suuri, on sinun minimoitava riskit oman toimintasi osalta tekoälyasetuksen vaatimusten mukaan.

3

Mikäli nostat matalariskisen järjestelmän riskitason suureksi omalla toiminnallasi, on sinun itse täytettävä kaikki tekoälyasetuksen vaatimukset.

**Jatka palautteeseen ja itsearviointiin**

# Palaute ja itsearviointi

Onnittelut, olet nyt käynyt läpi koko koulutuksen! Seuraavaksi voit antaa meille palautetta koulutuksen sisällöstä ja toteutuksesta. Samalla reflektoit ja arvioit omaa oppimistasi.

Palauteesi auttaa paitsi **sinua** viemään oppimasi asiat käytäntöön myös **meitä** tekemään entistä vaikuttavampia koulutuksia.

## Palaute ja itsearviointi

**Arvioi omaa oppimistasi ja koulutuksen toteutusta ja sisältöjä vastamalla lyhyeen kyselyyn.**

**ANNA PALAUTETTA**

## Jaa oppimaasi ja jatka oppimista

Saatuasi pian todistuksen koulutus on lopussa, mutta toisenlainen oppimismatka alussa! Nyt pääset viemään koulutuksen opit käytäntöön ja voit motivoida muitakin oppimaan.

- **Innosta** omalla esimerkilläsi.
- **Keskustele** oppimastasi avoimesti.

- **Haasta** kollegat koulutuksen pariin.
- **Jaa somessa** ajatuksiasi koulutuksesta tai vaikkapa todistukseksi
- #eoppiva #jottajokainenvoisioppia #HAUSfi
- **Tilaa  [uutiskirje](#)**, jotta saat tiedon eOppivan uusista koulutuksista.
- Opiskele lisää [eOppivan](#) laajasta koulutusvalikoimasta ja tutustu myös [HAUSin](#) koulutustarjontaan.

## TODISTUS JA SUORITUKSEN KIRJAAMINEN

# Todistus ja suorituksen kirjaaminen

## Onneksi olkoon!

Olet nyt suorittanut koulutuksen ja voit tilata suorituksestasi todistuksen! Tilaa todistus heti, jotta suorituksesi varmasti tallentuu.

Valitse alta oikea vaihtoehto sen mukaan, oletko töissä valtiolla.

(Jos et ole varma vastauksesta, tarkista täältä: [eOppivan käyttäjäorganisaatiot](#).)

### Olet töissä valtiolla (kirjaa suoritus ja lataa todistus)

Valtionhallinnon organisaation työntekijänä saat suorituksen kirjattua ja todistuksen ladattua näin:

- Kirjaudu alla olevasta linkistä eOppivan Moodleen (tarvitset toimivan Virta-tunnuksen tai työ sähköpostilla tehdyn käyttäjätunnuksen).
- Anna kurssiavain, joka on **Riski**
- Merkitse koulutus suorituksi. Halutessasi voit myös ladata Moodlesta todistuksen.

[EOPPIVAN MOODLEEN](#)

### En ole töissä valtiolla (tilaa todistus)

Saat todistuksen sähköpostiisi näin:

- Tilaa todistus heti, jotta suorituksesi ei katoa!
- Klikkaa alla olevaa "Tilaa todistus" -linkkiä ja täytä lomakkeelle yhteystietosi.
- Saat sähköpostiisi todistuksen koulutuksen suorittamisesta.

[TILAA TODISTUS](#)

## Kiitos osallistumisesta!

**Työryhmä:**

Tarmo Toikkanen, johtava asiantuntija, Sitra

Meeri Toivanen, asiantuntija, Sitra

**Tuotanto:** eOppiva 2025

Koulutuksen tekijänoikeudet kuuluvat työryhmälle. Ethän käytä koulutuksen materiaaleja ilman lupaa.

**Jotta jokainen voisi oppia.**