VALTIOKONTTORIN JULKAISUJA | TEKOÄLY 3/2025

Tekoälyn hallinta

Esimerkkinä Valtiokonttorin tekoälyn hallintamalli

Hotti Virpi, Mäki Riku

Valtiokonttori
Statskontoret
State Treasury

Kuvailulehti

Julkaisija: Valtiokonttori	Julkaisupäivämäärä: 27.6.2025
Tekijät: Hotti Virpi, Mäki Riku	Julkaisun teema: tekoäly
Julkaisun nimi: Tekoälyn hallinta Esimerkkinä Valtiokonttorin tekoälyn hallintamalli	ISSN/ISBN: 2489-4761/978-951-53-3903-4

Tiivistelmä:

Julkaisun tavoitteena on tarkastella tekoälyn hallintaan vaikuttavaa normatiivista ohjausta. Lisäksi siinä analysoidaan tekoälysäädöksen riskiluokitusten ja toimijaroolien merkitystä tekoälyjärjestelmien käyttöönottoon ja kehittämiseen. Julkaisussa käsitellään myös, miten nämä tekijät vaikuttavat järjestelmien käytönaikaiseen valvontaan ja vaatimustenmukaisuuden arviointiin.

Julkaisun sisällön muotoutumiseen on vaikuttanut työskentely Valtorin asiakasneuvottelukunnan alaisessa pilviyhteistyöryhmässä sekä virastojen (kuten ORK, Palkeet, PRH, THL, Traficom, Valtori, Vero) ja toimittajien (kuten CapGemini, IBM, Microsoft, Saidot, Sofigate) kanssa käydyt keskustelut ja työpajat.

Tekoälyn hallinta – esimerkkinä Valtiokonttorin tekoälyn hallintamalli -julkaisu tukee Tekoäly hyötykäyttöön valtionhallinnossa -oppaan Kohti tekoäly hallintaa -lukua (Hotti et al., 2026).

Asiasanat:	tekoäly, hallintamalli		
Kieli:	suomi	Sivumäärä:	30
Julkaisujen myynti/ jakelu:	https://www.valtiokonttori.fi/valtiokonttorin-julkaisut-ja-uutiskirjeet/valtiokonttorin-julkaisut/		

Beskrivningsblad

<table>
<tr><td colspan="2">Publicerare: Statskontoret</td><td colspan="2">Publiceringsdatum: 27.6.2025</td></tr>
<tr><td colspan="2">Utfärdare:
Hotti Virpi, Mäki Riku</td><td colspan="2">Publikationens tema:
artificiell intelligens</td></tr>
<tr><td colspan="2">Publikationens namn:
Styrning av AI
Exempel på Statskontorets styrmodell för AI</td><td colspan="2">ISSN/ISBN:
2489-4761/978-951-53-3903-4</td></tr>
<tr><td colspan="4">Sammandrag:

Syftet med publikationen är att granska den normativa styrningen som påverkar styrningen av artificiell intelligens (AI). Dessutom analyseras betydelsen av AI-förordningens risktaxonomi och operatörsroller för ibruktagandet och utvecklingen av AI-system. I publikationen behandlas också hur dessa faktorer påverkar övervakningen då systemen är i användning och bedömningen av överensstämmelsen med kraven.

Utformningen av publikationens innehåll har påverkats av arbetet i samarbetsgruppen för molntjänster som fungerar under Valtoris kunddelegation och genom diskussioner och workshoppar med ämbetsverk (såsom RRC, Palkeet, PRS, THL, Traficom, Valtori, Skatteförvaltningen) och leverantörer (såsom CapGemini, IBM, Microsoft, Saidot, Sofigate).

Styrning av AI – exempel på Statskontorets styrmodell för AI -publikationen stöder Styrning av AI -kapitlet i Effektiv användning av AI inom statsförvaltningen -guiden (Hotti et al., 2026).</td></tr>
<tr><td>Ämnesord:</td><td colspan="3">artificiell intelligens, styrmodell</td></tr>
<tr><td>Språk:</td><td>finska</td><td>Sidantal:</td><td>31</td></tr>
<tr><td>Publikationernas försäljning/utdelning:</td><td colspan="3">https://www.valtiokonttori.fi/valtiokonttorin-julkaisut-ja-uutiskirjeet/valtiokonttorin-julkaisut/</td></tr>
</table>

Description sheet

Published by: State Treasury	Publication date: 27/6/2025
Authors: Hotti Virpi, Mäki Riku	Theme of publication: artificial intelligence
Title of publication: AI Governance Example: The State Treasury AI governance model	ISSN/ISBN: 2489-4761/978-951-53-3903-4

Abstract:

The purpose of the publication is to examine regulatory guidance affecting the governance of artificial intelligence (AI). It also analyses the significance of the AI Act's risk classifications and operator roles for the deployment and development of AI systems. The publication also discusses how these factors affect the in-service monitoring and conformity assessment of systems.

The formulation of the content of the publication has been influenced by the work done in the cloud cooperation group under the Government ICT Centre Valtori's Customer Advisory Board as well as discussions and workshops with agencies (e.g. the Legal Register Centre, the Finnish Government Shared Services Centre for Finance and HR (Palkeet), the Finnish Patent and Registration Office, the Finnish Institute for Health and Welfare, Traficom, Valtori, the Finnish Tax Administration) and suppliers (e.g. CapGemini, IBM, Microsoft, Saidot, Sofigate).

The publication 'AI governance – Example: The State Treasury AI governance model' supports the chapter 'Towards AI governance' in the guide 'Making the most of AI in Finnish central government' (Hotti et al., 2026).

Keywords:	artificial intelligence, governance model		
Language:	Finnish	Pages:	31
Publication sales/distribution:	https://www.valtiokonttori.fi/valtiokonttorin-julkaisut-ja-uutiskirjeet/valtiokonttorin-julkaisut/		

Sisällys

1. Johdanto 6

2. Tekoälyn hallinta osana tiedonhallintaa 8

3. Valtiokonttorin tekoälyn hallintamalli 10

Periaatteet 10

Normatiivinen ohjaus 10

Tekoälyjärjestelmien käyttöönotto sekä kehittäminen tai kehityttäminen 13

4. Käyttötapausten arviointityökalujen käyttöesimerkki 15

5. Kohti kontrolloitua käyttöä 20

Hallintamalli yhteistyön ja jatkuvan kehittämisen tukena 21

Lähteet 22

Liite I 23

Liite II 25

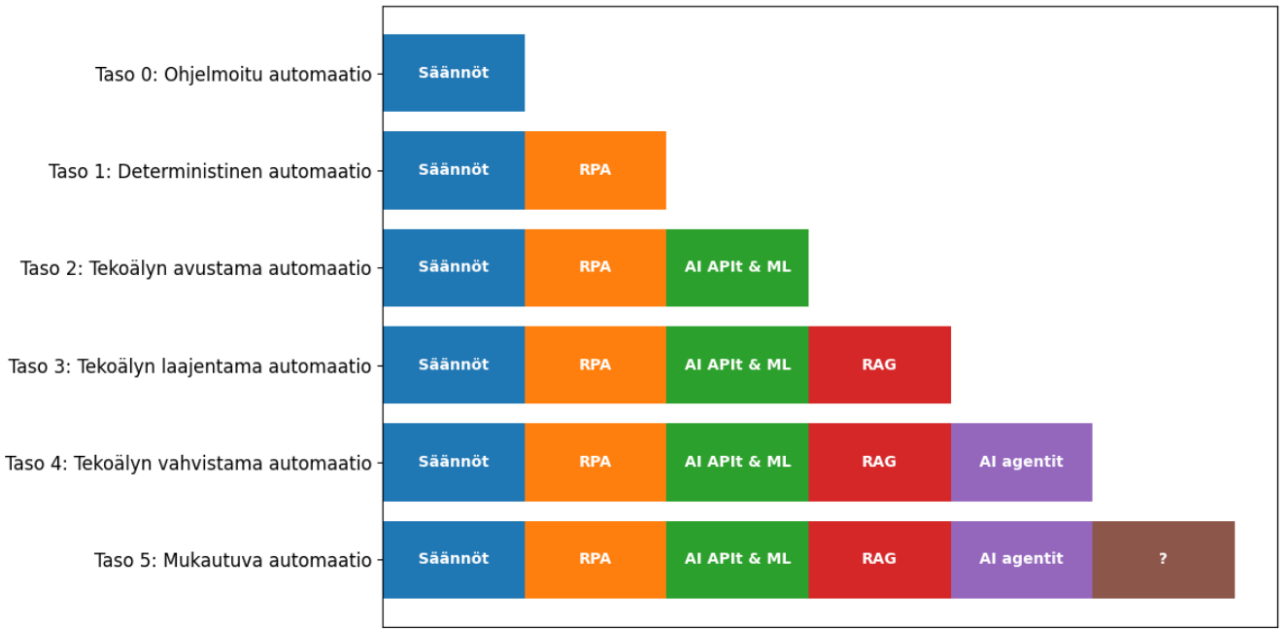
1. Johdanto

Suomessa on yli 5300[1] julkisomisteista tai julkisen hallinnon organisaatiota. Valtion budjettitalouteen kuuluu 66 kirjanpitoyksikköä. Neljä kirjanpitoyksikköä tarjoaa valtion yhteisiä palveluja ja valtiovarainministeriö ohjaa niitä auttamaan ”virastoja ja laitoksia [tulosohjattuja virastoja] tuottavuusohjelman mukaisten säästöjen aikaansaamisessa sekä painottamaan toiminnassaan kokonaisprosessin tehokkuutta ja tuottavuuden aikaansaamista erityisesti automatisaation ja tekoälyn keinoin”[2]:

- DVV: Digi- ja väestötietovirasto. Edistää sähköisiä asiointipalveluita ja luotettavaa sähköistä tunnistautumista (esim. Suomi.fi-palvelut), jotka ovat perusedellytyksiä monien prosessien automatisoinnille ja asiakaskokemuksen parantamiselle.
- Palkeet: Valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeet. Hyödyntää laajasti automaatiota ja tekoälyä omissa talous- ja henkilöstöhallinnon prosesseissaan (esim. laskujen käsittely, palkanlaskenta, matkalaskut). Lisäksi erityisosaamiskeskus (Center of Excellence, CoE) tekee virastoille ohjelmistorobotteja ja tarjoaa palveluna tekoälyagenttiratkaisuja.
- Valtiokonttori: Vastaa valtion lainanotosta, kassavarojen sijoittamisesta ja velan riskienhallinnasta. Se hoitaa tapaturma-, sotilasvamma- ja rikosvahinkokorvauksia sekä hallinnoi valtion lainoja, korkotukia ja takauksia. Valtiokonttori johtaa valtion konsernilaskentaa, taloushallintoa ja maksuliikennettä. Se kerää ja julkaisee kuntien ja hyvinvointialueiden taloustietoja sekä edistää tiedolla johtamista ja taloushallinnon digitalisaatiota. Valtiokonttori hyödyntää laajasti automaatiota ja ohjelmistorobotiikkaa varsinkin korvauspalveluissa. Valtiokonttori on vahvasti mukana edistämässä valtiohallinnon tekoälyn käyttöönottoa osallistumalla yhteisiin kehittämishankkeisiin ja linjausten määrittelyihin.
- Valtori: Valtion tieto- ja viestintätekniikkakeskus Valtori. Kehittää ja tarjoaa valtionhallinnon yhteisiä ICT-ympäristöjä ja -palveluja sekä hallinnoi teknologia-alustoja kuten Azure. Lisäksi Valtorille on perustettu tekoälyosaamiskeskus.

Uudet teknologiset kyvykkyydet (Kuva 1) mahdollistavat toiminnan kehittämisen ja uudelleen suunnittelun. Nopea teknologinen kehitys haastaa normatiivisen ohjauksen, sillä erityisesti julkisessa hallinnossa sitovan säätelyn puuttuminen tarkoittaa käytännössä sitä, että automatisointia mahdollistavaa teknologiaa käytetään vielä vähän. Esimerkiksi automaattinen ratkaisumenettely[3], joka pohjautuu käsittelysääntöihin, tuli vuonna 2023 osaksi tiedonhallintalakia ja säätelyn myötä automaattisia ratkaisumenettelyjä on sovellettu useissa tiedonhallintayksiköissä. Automaattiseen ratkaisumenettelyyn on olemassa tiedonhallintalautakunnan suositus, jota voidaan pitää pohjana tekoälyn hallintamallille, sillä siinä kuvattu tehtävänjako[4] sopii suoraan tai mukaillen myös tekoälyn hallintamallin vastuiden määrittelyyn.

[1] https://www.tutkihallintoa.fi/julkisen-hallinnon-organisaatiot/ (viitattu 22.6.2025)
[2] Konsernipolitiikkalinjaukset 2024-2027 (vm.fi)
[3] https://www.finlex.fi/fi/lainsaadanto/2019/906, luku 6a
[4] https://julkaisut.valtioneuvosto.fi/handle/10024/165446, luku 3.1



Kuva 1. Esimerkkejä automaation ja tekoälyn teknologisista kyvykkyyksistä[5]

Hallintamallit ovat hallintojärjestelmän/-tavan[6] (governance) kuvauksia, joiden avulla jäsennetään hallittavaan kohdealueeseen – kuten tekoälyn – kuuluvia asioita. Niissä kuvataan muun muassa normatiivisen ohjauksen tietopohja, vaatimukset ja velvoitteet sekä todenteet, jotka tukevat päätöksentekoa ja vastuullista toimintaa. Hallintamallien keskeinen tehtävä on varmistaa, että eri sidosryhmät toimivat yhteisten käytänteiden mukaisesti ja että ohjaus on läpinäkyvää ja ennakoitavaa.

Tämä dokumentti on tarkoitettu tekoälyn hallintamallin luomiseen ja kehittämiseen osana tiedonhallintaa (Luku 2). Valtiokonttorin tekoälyn hallintamalli on kalvosarja, jonka osakokonaisuudet (Luku 3) kiteyttävät normatiivisen ohjauksen, käyttötapausten käsittelyn ja periaatteet. Käyttötapausten arviointityökaluja esitellään rajoitetun riskin käyttötapauksiin (Luku 4) ja lopuksi käydään läpi käytön aikaista valvontaa ja sen valmistelua (Luku 5).

[5] RPA = Robotic Process Automation eli ohjelmistorobotti tekee työkulun mukaisia tehtäviä; AI APIt viittaavat rajapintojen kautta käytettäviin malleihin, kuten kielimallit, ja kognitiivisiin palveluihin kuten puhe tekstiksi: ML = Machine Learning eli koneoppimisen avulla ennakoidaan entiteettien käyttäytymistä; RAG = Retrieval Augmented Generation eli kielimalleille annetaan kehotteiden lisäksi ennalta koottujen tietoaineistojen sisältöjä

[6] governance | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)

2. Tekoälyn hallinta osana tiedonhallintaa

European AI Alliance on Euroopan komission vuonna 2018 perustama avoin ja monitoimijainen foorumi, jonka tarkoituksena on edistää laajaa ja osallistavaa keskustelua tekoälyn kehityksestä, sääntelystä ja vaikutuksista yhteiskuntaan ja talouteen. Foorumin julkaisuista löytyy muun muassa tekoälyn hallinnan konkretisointia kehyksistä käytäntöihin: ”Tekoälyn hallinnan keskeinen tehtävä on varmistaa eettinen ja vastuullinen tekoälyn kehittäminen ja käyttö. Tekoälyn hallinta on sääntöjen, prosessien, kehysrakenteiden ja teknisten työkalujen järjestelmä, joita organisaatio käyttää varmistaakseen, että tekoälyä käytetään yhteensopivasti organisaation periaatteiden, lakisääteisten vaatimusten sekä sosiaalisten ja eettisten normien kanssa”[7]; tekoälyn hallinta on osa muuta hallintaa kuten "osa organisaation hallintaympäristöä ja yhdistyy tietotekniikan hallintoon, tietohallintoon ja yleiseen hallintoon"[8].

Hallintamallien päätarkoitus on kuvata, kuinka varmistetaan, että hallintakohdealueen tunnistetut sidosryhmät käyttäytyvät halutulla tavalla. Haluttu tapa on määritelty hallintamallissa ja erityisesti julkisen hallinnon kontekstissa hallintamalli ottaa huomioon useista lähteistä tulevat vaatimukset ja velvoitteet:

- Euroopan unionista (EU) tulevat vaatimukset ja velvoitteet kuten tekoälysäädöksen vaatimukset ja velvoitteet.
- Suomen kansalliset vaatimukset ja velvoitteet kuten tiedonhallintalain vaatimukset ja velvoitteet.
- Hallinnonalan erityisvaatimukset, jotka voivat liittyä esimerkiksi tiettyihin sektoreihin, kuten terveydenhuoltoon, koulutukseen tai ympäristönsuojeluun.
- Organisaation sisäiset periaatteet ja tavoitteet sekä toimintatavat.

Kun kohdealueiden hallintamallit ovat olemassa, niin ne auttavat johtamisessa, jolla tarkoitetaan ”toimintatapoja ja menettelyjä, joilla organisaation johto pyrkii saamaan aikaan asetetut tavoitteet”[9]. Suomen julkisessa hallinnossa organisaatioiden hallinnon ohjaus[10] näkyy esimerkiksi tiedonhallintalain päivitysten ja lakia tukevien suositusten myötä esimerkiksi tiedonhallintamalleissa. Organisaatioissa tarvitaan myös teknologia-alustakohtaisia ja jopa teknologiakohtaisia hallintamalleja kuten tekoälyn hallintamallia.

Tekoälyn hallintamallin rakennetta suunniteltaessa kävimme läpi muun muassa European AI Alliance -foorumin suosittelemat kehykset, Gartnerin aineistoja ja tieteellisiä tietokantoja. Businessteknologiamallissa[11] ja Gartnerin hallintamallikonstruktioissa[12] käytetään kuusikulmaisia hunajakennoelementtejä kuvaamaan asioita, jotka liittyvät toisiinsa.

---

[7] suomennettu https://futurium.ec.europa.eu/en/european-ai-alliance/best-practices/implementing-ai-governance-framework-practice

[8] suomennettu https://futurium.ec.europa.eu/en/european-ai-alliance/best-practices/implementing-ai-governance-framework-practice

[9] Hallinnon ohjaus - Valtiovarainministeriö (vm.fi)

[10] Hallinnon ohjaus - Valtiovarainministeriö (vm.fi) – ”Hallinnon ohjauksella tarkoitetaan johtamista tukevien menettelyjen, järjestelmien, toimintatapojen ja niihin liittyvien asiakirjojen kokonaisuutta”

[11] https://www.btmalli.fi/

[12] kuten Gartner (8 January 2025 - ID G00821275) "Executive AI Governance Playbook"

Erilaisia hallintamalleja tarkasteltaessa nousi esiin kolme keskeistä osakokonaisuutta: operatiivisen ohjauksen malli, politiikat ja kontrollit sekä valvontajärjestelmät.

Jotta organisaation normatiivisen ohjauksen tietopohja voidaan muodostaa, tulee hallintamalleissa huomioida sitova ja ei-sitova säätely sekä toimeenpanoa tukevat työkalut. Sitova säätely (hard law) viittaa ensisijaisesti oikeudellisesti säädöksiin, joilla on täytäntöönpanomekanismit, kuten kansalliset lait. Ei-sitova säätely (soft law) käsittää esimerkiksi periaatteet ja suositukset, jotka voivat ohjata toimintaa ja edistää yhteistyötä, mutta joilla ei ole suoraa oikeudellista täytäntöönpanokelpoisuutta.

Euroopan unionin tekoälysäädös (EU AI Act) 2024/1689[13] määrittelee riskikategorioita ja toimijarooleja (kuten käyttöönottaja ja tarjoaja). Tekoälysäädöksen vaatimuksista ja velvoitteista suurin osa kohdistuu suuririskisiin tekoälyjärjestelmiin ja niiden tarjoajiin, jotka kehittävät tai kehityttävät tekoälyjärjestelmiä. Suurriskisyyden arvioinnissa tulee huomioida tekoälysäädöksen liite III ja 6 artiklan 3 kohta, joka määrittelee tekoälyjärjestelmän käyttötavan. Esimerkiksi ”tekoälyjärjestelmän käyttäminen ihmistyön tukena tekstin laadinnassa ei ole suuririskistä, käyttötapauksesta riippumatta” (Tammes-Peters, 2025, s. 13). Kun organisaatio tarkastelee olemassa olevia tekoälyjärjestelmiä tai suunniteltuja, niin suositellaan mahdollisuuksien mukaan suurriskisten tekoälyjärjestelmien poissulkemista tekoälysäädöksen liitteen III ja artiklan 6 kohta 3 mukaan.

Valtionhallinnon tietoturvan vastuuhenkilöiden verkoston (VAHTI) tietosuojan kehittämisen (TIKE) työryhmä on muodostanut työkaluja (Excel- ja Word-dokumentteja) tekoälyjärjestelmien kartoittamiseen ja käyttötapausten arviointiin. Niitä kutsutaan jatkossa käyttötapausten arviointityökaluiksi ja niiden avulla todennetaan vaatimustenmukaisuus. Käyttötapausten arviointityökalut ovat:

- 01 Organisaatioiden AI ratkaisujen kartoitus (Excel-tiedosto)
- 02 Käyttötapauksen kuvaus (Word-lomake)
- 03 Tekoälyjärjestelmän käyttötapauksen riskitason määritys (Excel-tiedosto)
- 04 Käyttöönottajaa koskevat vaatimukset (Excel-tiedosto)
- 05 FRIA perusoikeusvaikutustenarviointi (Excel-tiedosto)
- 06 Tekoälyn lisäkysymykset DPIAan[14] (Excel-tiedosto)
- 07 Hankinnan tekoälyvaatimukset ja tsekkilista (Excel-tiedosto)

[13] https://eur-lex.europa.eu/eli/reg/2024/1689
[14] Tietosuojan vaikutustenarviointi = Data Protection Impact Assessment, DPIA

3. Valtiokonttorin tekoälyn hallintamalli

Valtiokonttorin tekoälyn hallintamalli muotoutui erilaisten konstruktioiden jälkeen kalvosetiksi: organisaatiokohtaiset tekoälyn periaatteet (neljä kohtaa, yksi kalvo) ja strategiset tavoitteet (viisi tavoitetta, yksi kalvo) muodostavat oman osakokonaisuuden, normatiivinen ohjaus toisen osakokonaisuuden (seitsemän kohtaa ja kustakin yksi kalvo) ja käyttöönottajan ja tarjoajan toimet kolmannen osakokonaisuuden (kolme kohtaa ja kustakin yksi kalvo). Osa-alueita yhdistää normatiivisen ohjauksen tietopohjan vaatimukset ja velvoitteet, joihin haettiin vastinetta teknologia-alustakohtaisista kontrolleista ja politiikoista sekä valvontamekanismeista.

Periaatteet

1. Käytä ensisijaisesti Valtiokonttorin suosittelemia tekoälyjärjestelmiä ja yleiskäyttöisiä tekoälymalleja.
2. Syötä tekoälyjärjestelmään vain julkista tietoa ─ Valtiokonttori tekee erillisen päätöksen salassa pidettävän, turvallisuusluokitellun ja henkilötietoja sisältävän tiedon käsittelystä tekoälyjärjestelmässä.
3. Tarkista tekoälyjärjestelmän antamat tulokset ennen kuin jaat niitä eteenpäin tai käytät virallisessa päätöksenteossa ─ virkamies on aina viimekädessä vastuussa.
4. Käytä tekoälyn hallintamallia.
    - Jos kehität/kehitytät tai käyttöönotat tekoälyjärjestelmiä, niin noudata osiota: Tekoälyjärjestelmien käyttöönotto sekä kehittäminen tai kehityttäminen.
    - Jos tekoälyn hallintamalliin tarvitaan muutoksia, niin Mahdollistaja-yksikkö päivittää hallintamallia.

Normatiivinen ohjaus

1. Tekoälyn hallinta osana tiedonhallintaa. On tunnistettu, että tekoälyn hallinta on osa tiedonhallintaa ja sen normatiivisesta ohjauksesta vastaa IT-johtoryhmä.
2. Valtiokonttorin tekoälyn normatiivisen ohjauksen tietopohja. Organisaatiota velvoittaa erilaiset säädökset sekä määräykset, päätökset ja sopimukset. Organisaatio päättää, mitä muita ei-sitovaan säätelyyn kuuluvia normatiivisia asiakirjoja se noudattaa. Lisäksi organisaation kannattaa huomioida toimeenpanoa tukevat työkalut (Kuva 2).
3. Valtiokonttorin toimijaroolit ja velvoitteet. On tunnistettu, että Valtiokonttorilla ei ole tekoälysäädöksen riskiluokittelun mukaisesti suurriskisiä tekoälyjärjestelmiä ja

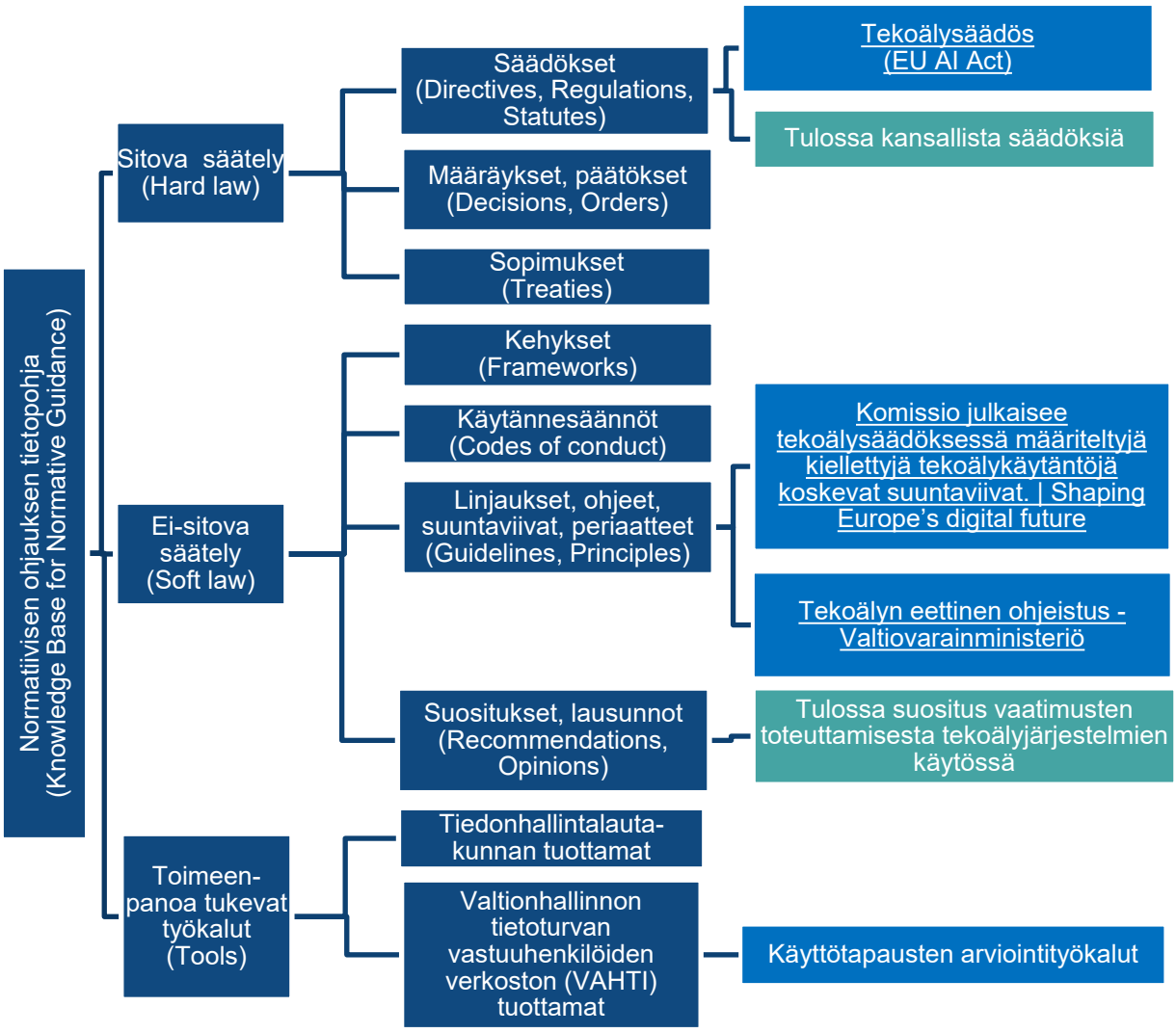
toimijarooleina on käyttöönottaja tai tarjoaja, jos kehitämme tai kehitytämme tekoälyjärjestelmiä.

4. Perustelut suurriskittömyydelle. Koska tekoälysäädös asettaa merkittäviä velvoitteita suurriskisten tekoälyjärjestelmien tarjoajille, on liitteen III ja artiklan 6 mukaisesti suljettu pois tällaisten järjestelmien olemassaolo.

5. Esimerkkejä päätösperusteluista. Työkalujen tekoälyominaisuudet sekä suunnitteilla olevat tekoälyjärjestelmät on käyty esimerkinomaisesti läpi, kuten seuraavassa esitetään: Valtiokonttorin asia- ja asiakirjahallinnan järjestelmän (Tasku) asiat ja asiakirjat muodostavat tietopohjan, jota käsitellään erilaisilla ohjelmistokirjastojen funktioilla (kuten Pythonin entiteettien tunnistaminen) ja valmiiksi koulutetuilla koneoppimismalleilla (kuten GPT4-o) → Kyseessä ei katsota olevan suurriskinen tekoälyjärjestelmä, sillä tekoälysäädöksen 6 artiklan mukaan tekoälyjärjestelmä on tarkoitettu suorittamaan valmistelutehtävää, joka koskee liitteessä III lueteltujen käyttötapausten kannalta merkityksellistä arviointia.

6. Kontrollit ja politiikat. Säädöksistä ja muista kehyksistä muodostetaan teknologia-alustoilla huomioitavia politiikkoja tai kontrolleja kuten Azuren alustapolitiikat ja Microsoft 365 säätelykontrollit.

7. Valtiokonttorin roolit ja vastuut. Muodostettu RACI-matriisi, jossa A = päätöksentekijä, R = tehtävän suorittaja, C = konsultoitu, I = informoitu (Taulukko 1).



Kuva 2. Valtiokonttorin tekoälyn hallinnan normatiivinen tietopohja

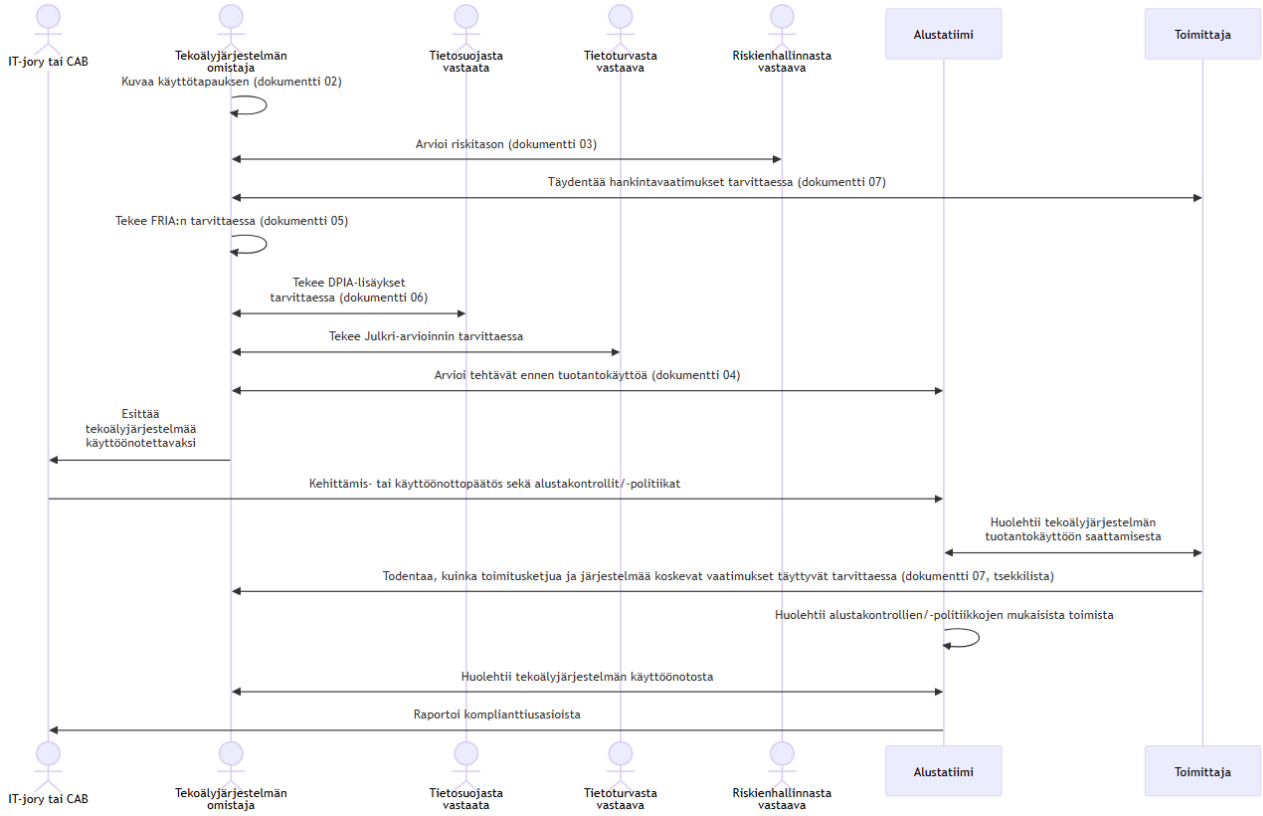
Taulukko 1. Valtiokonttorin tekoälyn hallinnan RACI-matriisi. CAB (Change Advisor Board) toimii IT-johtoryhmän valtuuttamana.

Vastuuosa-alue	**Työntekijät**	**Toimittajat**	**IT-johtoryhmä**	**Palvelu-/ tuoteomistaja**	**Tietoturvasta vastaava**	**Tietosuojasta vastaava**	**Riskienhallinnasta vas-taava**	**Alustatiimi**	**Mahdollistajat**
Normatiivinen ohjaus (ml. Periaatteet ja ta-voitteet)			A/**R**	I	C	C	C	C	C
Riskit ja niiden miti-gointikeinot			A	**R**	C	C	C (fasili-tointi)	C	C

Vastuuosa-alue	Työntekijät	Toimittajat	IT-johtoryhmä	Palvelu-/ tuoteomistaja	Tietoturvasta vastaava	Tietosuojasta vastaava	Riskienhallinnasta vastaava	Alustatiimi	Mahdollistajat
Kontrollit ja politiikat (kuten M365 ja Azure)			A	I	C	C	C	**R**	C
Käyttötapausten arviointi	I	I	A	**R**	C	C (DPIA:n tekemisessä mukana)	C	**I**	C
Tekoälyjärjestelmien käyttöönottolupa	I	I	A (CAB)	C	C	C	C	**R**	C
Vaatimustenmukaisuuden valvonta ja tilannekuvat			A	I	I	I	I	**R**	C

Tekoälyjärjestelmien käyttöönotto sekä kehittäminen tai kehityttäminen

1. Käyttötapausten arviointityökalut:
    - Käyttöönottaja täyttää lomakkeet (01–04) – jollei johonkin kysymykseen osaa vastata, niin voi tehdä 03-lomakkeen osalta Valtorille tiketin
    - Tarjoaja täyttää lomakkeen 07 yhdessä toimittajan kanssa
    - Kun lomakkeet on täytetty, tehdään tietosuoja-arviointi (huomioi lomakkeet 05-06) ja tietoturva-arviointi (kuten Julkri-arvio)
        - Tietoturva-arvioinnin yhteydessä käydään läpi tietojen turvaluokittelut ja salassapitomerkinnät
2. Käytön aikainen valvonta. Ennen kuin olemassa olevan työkalun tekoälyominaisuus tai kehitetty/kehitettävä tekoälyjärjestelmä otetaan käyttöön NIIN tuoteomistaja (tai palveluomistaja, jollei tuoteomistajaa ole olemassa) selvittää Hallinta alustatiimin kanssa, kuinka käytön aikana valvotaan tekoälyn käyttöä ja informoidaan käytön aikaisista havainnoista.
3. Sekvenssikaavio - käyttötapauksen kuvauksesta kontrolloituun käyttöön (Kuva 3)



Kuva 3. Sekvenssikaavio tekoälyn hallinnan rooleista ja tehtävistä sekä käyttötapausten arviointityökalujen hyödyntämisestä.

4. Käyttötapausten arviointityökalujen käyttöesimerkki

Valtiokonttori on ottanut käyttöön tai mukaillut Valtionhallinnon tietoturvan vastuuhenkilöiden verkoston (VAHTI) tietosuojan kehittämisen (TIKE) työryhmän muodostamia työkaluja. Tekoälyn hallintamallia tehtäessä käyttötapausten arviointityökalujen käytöstä tehtiin vain sekvenssikaavio (Kuva 3) eli työkalujen sisällöt ja käyttökelpoisuus täydentyy käyttötapausten arvioinnin myötä. Käyttötapausten arviointityökaluja varten tarvittava sisältö kootaan erillisissä tapaamisissa tekoälyn hallintamallin vastuutoimijoiden kanssa. Tekoälyjärjestelmien tiedot tulee tallentaa tiedonhallintamalliin ja CMDB:hen (Configuration Management Database) samaan tapaan kuin muidenkin tietojärjestelmien tiedot.

01 Organisaatioiden AI ratkaisujen kartoitus (Liite I). Valtiokonttori lisää tiedonhallintamalliinsa seuraavat tiedot:

- Tekoälyjärjestelmän/-ratkaisun nimi ja lyhyt kuvaus
- Tekoälysäädöksen riskiluokka: Rajoitettu riski, vähäinen riski
- Tekoälysäädöksen toimijarooli(t): Toimittaja, Käyttöönottaja
- Täydennetty DPIA – K/E
- Tiedot pysyvät EU Data Boundaryssä (TIA) – K/E
- Tietoturva-arviointi/-auditointi – K/E

02 Käyttötapauksen kuvaus. Valtiokonttori vastaa seuraaviin kysymyksiin.

- Kuka määrittää järjestelmän käyttötarkoituksen? [*kuvaa, määrittääkö käyttötarkoituksen järjestelmän valmistaja vai onko järjestelmällä useita mahdollisia käyttötarkoituksia, joista käyttöönottaja valitsee tarpeensa mukaisen käyttötarkoituksen*]
- Miksi käytätte tekoälyjärjestelmää? [*kuvaa, mihin tarpeeseen käytätte tekoälyä. Kuvatkaa myös ne lakisääteiset sekä hyvän hallinnon vaatimukset, josta tarpeenne muodostuu.*]
- Kuinka käytätte tekoälyjärjestelmää? [*kuvaa, kuinka tekoälyjärjestelmää käytetään edellä kuvatun tarpeen täyttämiseksi*]
- Mitä tekoälyjärjestelmä tekee [*kuvaa, mitä tekoälyjärjestelmä tekee käytännössä*]
- Mikä on ihmisen rooli tekoälyjärjestelmän käytössä? [*kuvaa, valvooko ihminen tekoälyjärjestelmän kouluttamista, käyttöä ja millä tavalla*]
- Mitä tekoäly ei tee käyttötapauksen yhteydessä? [*kuvaa tunnistetut osat käyttötapauksesta, johon tekoälyä voidaan käyttää, mutta sitä ei käytetä*]

03 Tekoälyjärjestelmän käyttötapauksen riskitason määritys. Valtiokonttori tekee riskitason määrityksen työkalun mukaisesti vastaamalla kyllä-/ei- kysymyksiin:

- Kielletyt käytännöt (Art. 5)
- Suuri riski (Liite I), turvallisuustuotteet ja komponentit
- Suuri riski (Liite III), profiloivat järjestelmät
- Rajoitettu riski (Art. 50), kommunikoivat järjestelmät (Taulukko 3)

- Vähäinen riski, jos järjestelmä ei kuulu muuhun riskiryhmään, se kuuluu tähän

Taulukko 2. 03 Tekoälyjärjestelmän käyttötapauksen riskitason määritys – rajoitetun riskin kysymykset

	Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	**Valitse kyllä tai ei, soveltuuko kohta järjestelmääsi**
1	Tekoälyjärjestelmä on tarkoitettu **luonnollisten henkilöiden kanssa suoraan vuorovaikutukseen**. Poikkeuksena, et voi valita ei-valintaa, jos seuraavat täyttyvät: tekoälyjärjestelmät, joita on lain mukaan sallittua käyttää rikosten paljastamiseen, estämiseen tai tutkimiseen ja rikoksiin liittyviin syytetoimiin, edellyttäen, että kolmansien osapuolten oikeudet ja vapaudet turvataan asianmukaisesti, paitsi jos kyseiset järjestelmät ovat julkisesti saatavilla rikosilmoitusten tekemistä varten.	
2	**Synteettistä ääni-, kuva-, video- tai tekstisisältöä** tuottavien tekoälyjärjestelmien, mukaan lukien yleiskäyttöiset tekoälyjärjestelmät. Poikkeuksena, et voi valita ei-valintaa, jos seuraavat täyttyvät: tekoälyjärjestelmät avustavat vakiomuokkaamista tai eivät olennaisesti muuta käyttöönottajan toimittamia syöttödataa tai sen semantiikkaa tai jos niitä on tekoälysäädöksen mukaan sallittua käyttää rikosten paljastamiseen, estämiseen ja tutkimiseen tai rikoksiin liittyviin syytetoimiin.	
3	Kyseessä on **tunteentunnistusjärjestelmän tai biometrisen luokitusjärjestelmä**. Poikkeuksena, et voi valita ei-valintaa, jos seuraavat täyttyvät: biometriseen luokitteluun ja tunteentunnistamiseen käytetty tekoälyjärjestelmä, jota on tekoälysäädöksen mukaan, luvallista käyttää rikosten paljastamiseen, estämiseen tai tutkimiseen, edellyttäen, että kolmansien osapuolten oikeudet ja vapaudet turvataan asianmukaisesti, ja että unionin oikeuden mukaisesti.	
4	Kyseessä on sellainen tekoälyjärjestelmä, joka **tuottaa tai manipuloi syväväärennöksen muodostavaa kuva-, ääni- tai videosisältöä.** Poikkeuksena, et voi valita ei-valintaa, jos seuraavat täyttyvät: jos käyttö on tekoälysäädöksen mukaan sallittu rikosten paljastamiseen, estämiseen ja tutkimiseen tai rikoksiin liittyviin syytetoimiin. Jos sisältö on osa selvästi taiteellista, luovaa, satiirista, fiktiivistä tai vastaavaa teosta tai ohjelmaa, tässä kohdassa säädetyt avoimuusvelvoitteet rajoittuvat siihen, että tällaisesta tuotetusta tai manipuloidusta sisällöstä ilmoitetaan asianmukaisesti tavalla, joka ei haittaa teoksen esittämistä tai sen käyttöä. Tekoälyjärjestelmän, joka **tuottaa tai manipuloi tekstiä, jonka julkaisemisen tarkoituksena on tiedottaa yleisölle yleistä etua koskevista asioista.** Poikkeuksena, et voi valita ei-valintaa, jos seuraavat täyttyvät: jos käyttö on tekoälysäädöksen mukaan sallittu rikosten paljastamiseen, estämiseen, tutkimiseen tai rikoksiin liittyviin syytetoimiin, tai jos tekoälyn tuottama sisältö on läpikäynyt ihmisen suorittaman arviointiprosessin tai toimituksellisen valvonnan ja jos luonnollisella henkilöllä tai oikeushenkilöllä on toimituksellinen vastuu sisällön julkaisemisesta.	

04 Käyttöönottajaa koskevat vaatimukset. Valtiokonttori käy läpi käyttöönottajaa koskevat vaatimukset riskitason mukaisesti, muttei vastaa suurriskisiä tekoälyjärjestelmiä koskeviin kysymyksiin (Taulukko 4).

Taulukko 3. 04 Käyttöönottajaa koskevat vaatimukset

X	Vastuu	Vastuu-henkilö	Noudattamisen aikataulu	Kuinka noudatetaan käytännössä ja muut huomiot. Voi myös olla linkki prosessikuvaukseen.
Rajoitetun riskin tekoälyjärjestelmät				
	Ilmoitus vuorovaikutuksesta			
	Ilmoitus keinotekoisesta tai manipuloidusta sisällöstä			
	Ilmoitus tunteentunnistuksesta tai biometrisestä luokituksesta			
	Ilmoitus syväväärennöksestä (deepfake)			
Suurriskiset tekoälyjärjestelmät				
	Tekniset ja organisatoriset toimenpiteet			
	Ihmisen suorittama valvonta			
	Järjestelmän suorituskykyyn liittyvät ilmoitukset			
	Riskiin ja vakavaan vaaratilanteeseen liittyvät ilmoitukset			
	Lokitietojen säilyttäminen			
	YT-menettely			
	Rekisteröintivelvoitteiden noudattaminen			
	Tietosuojan vaikutuksenarviointi DPIA			
	Järjestelmän käyttölupa erityistapauksissa			
	Ilmoittamisvelvollisuus päätöksen kohteelle			
	Viranomaisyhteistyö			
	Velvollisuus kuvata pyydettäessä liitteen III mukaisen järjestelmän rooli päätöksenteossa			
	Testaamista koskevat velvoitteet			
	Perusoikeusvaikutustenarvioinnin FRIA tekeminen			

05 FRIA perusoikeusvaikutustenarviointi. Valtiokonttori ei hyödynnä työkalua, koska Valtiokonttorilla ei toistaiseksi ole tekoälysäädöksen liitteen III mukaisia suurriskisiä tekoälyjärjestelmiä eikä Valtiokonttori tee artiklan 6 mukaista profilointia.

06 Tekoälyn lisäkysymykset DPIAan. Valtiokonttori arvioi tietosuojaa koskevaa vaikutustenarviointia ja siihen liittyviä lisäkysymyksiä käyttötapauskohtaisesti. Tietosuojan vaikutusten arvioinnin lisäkysymykset on jaettu kuuteen osakokonaisuuteen (Taulukko 7) ja ne (Liite II) käydään läpi yhteistyössä tietosuojavastaavan kanssa.

Taulukko 4. Tietosuojan vaikutusten arvioinnin lisäkysymysten osiot

Osaotsikko	Osakokonaisuus	Vastauksista vastuullinen
Osa 1: Kartoittavat kysymykset		Tilaaja vastaa, jos on ostanut valmiin tekoälyjärjestelmän tuotantokäyttöön.
Osa 2: Tekoälyn vaikutuksen ihmisiin ja vastuullisen tekoälyn periaatteet		Tilaaja vastaa, jos on ostanut valmiin tekoälyjärjestelmän tuotantokäyttöön.
Osa 3: Tekoälypalvelun kehittämisen elinkaari	Koulutusdatan laillinen käsittely, elinkaaren hallinta	Tilaaja vastaa, jos on ostanut tekoälyjärjestelmän kouluttamista
	Raakadatasta laadukkaaseen koulutustietojoukkoon (vahvistusoppiminen l. re-enforcing)	Tilaaja vastaa, jos on ostanut tekoälyjärjestelmän kouluttamista
	Vinoumien tunnistus ja tehokas korjaus (ohjattu oppiminen l. supervised learning)	Tilaaja vastaa, jos on ostanut tekoälyjärjestelmän kouluttamista
	Huolellisen testausprotokollan soveltaminen	Tilaaja vastaa, jos on ostanut tekoälyjärjestelmän kehittämistä
	Järjestelmän kehitysvaiheen aikainen laadun tarkkailu	Tilaaja vastaa, jos on ostanut tekoälyjärjestelmän kehittämistä
Osa 4: Vastuullinen tekoälyhallinto ja riskinhallinta		Tilaaja vastaa, jos on ostanut valmiin tekoälyjärjestelmän tuotantokäyttöön
Osa 5: AI projektien ja systeemien toteuttaminen		Tilaaja vastaa, jos on ostanut valmiin tekoälyjärjestelmän tuotantokäyttöön
Osa 6: Loppukysymys		Tilaaja vastaa, jos on ostanut valmiin tekoälyjärjestelmän tuotantokäyttöön

07 Hankinnan tekoälyvaatimukset ja tsekkilista. Valtiokonttori kehityttää tekoälyjärjestelmiä toimittajalla ja käy läpi hankinnan tekoälyvaatimukset (Taulukko 5) ja tarkistuslistan rajoitetun riskitason vaatimuksista (Taulukko 6) ennen käyttöönottoa. Hankinnan tekoälyvaatimuksiin on seuraava ohje tilaajalle: Tunnistakaa ensin Tilaajan käyttötapaus, eli mihin tarkoitukseen käytätte järjestelmää. Valitkaa käyttötapauksen perusteella riskitaso:
(1) suurriskinen tekoälyjärjestelmä, (2) rajoitetun riskin tekoälyjärjestelmä, tai (3) vähäisen riskin tekoälyjärjestelmä; yleiskäyttöinen tekoälymalli ei ole itsessään tekoälyjärjestelmä, eikä sen käyttöönottajalle ole velvoitteita.

Taulukko 5. 07 Hankinnan tekoälyvaatimukset.

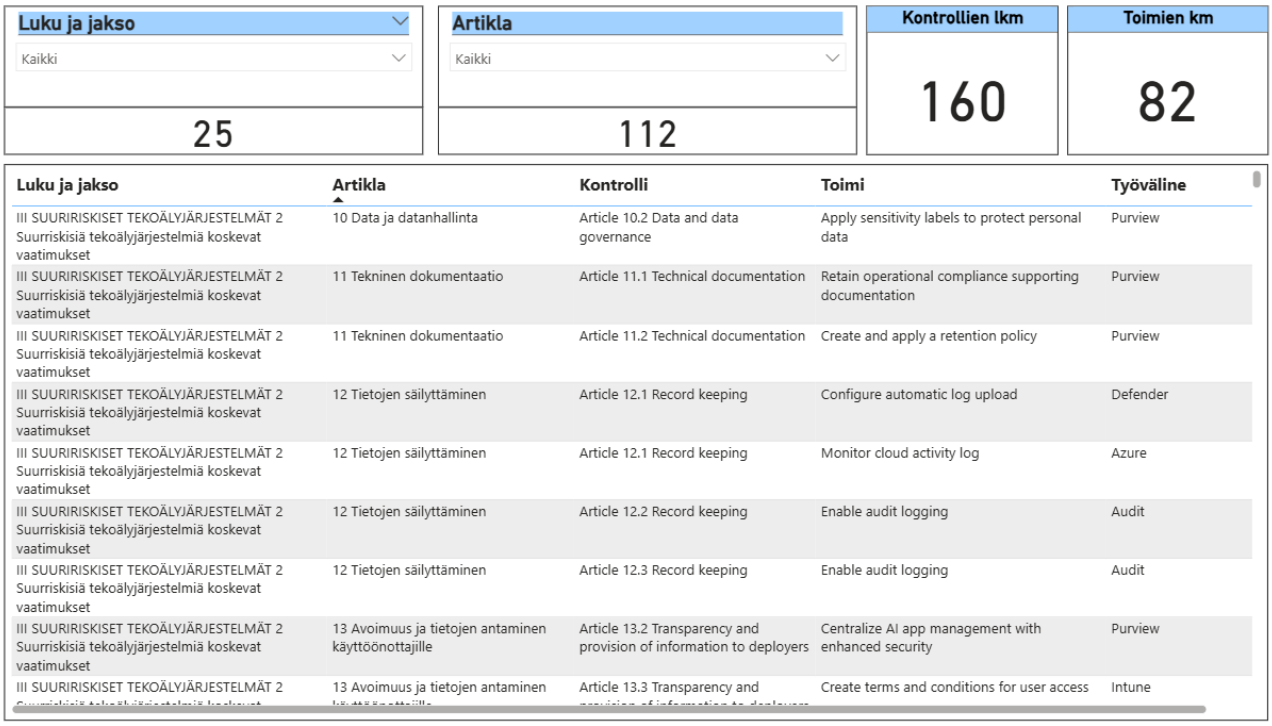
Vaatimuksen kohde	Vaatimus	Kyllä/ei -vastaus
Tekoälyjärjestelmä	Tekoälyjärjestelmä/tekoälykomponentti täyttää tilaajan käyttötapaukseen perustuvan riskitason mukaiset tekoälysäädöksen vaatimukset	
Toimitusketju	Toimittaja ja tekoälyjärjestelmän toimitusketju täyttää tilaajan käyttötapaukseen perustuvan riskitason mukaiset tekoälysäädöksen vaatimukset	
Toimittaja	Toimittaja ja sen koko toimitusketju avustavat käyttöönottajaa käyttötapaukseen perustuvan riskitason mukaisten tekoälysäädöksen vaatimusten toteuttamisessa	

Taulukko 6. 07 Hankinnan tarkistuslista – vaatimukset järjestelmälle, kun tekoälysäädöksen mukainen riskitaso on rajoitettu ja toimijarooli on käyttöönottaja tai tarjoaja. VAHTI-pohjassa on myös muita vaatimuksia ja niitä voidaan ottaa huomioon, kunhan niiden säädösperuste on selvillä.

Riskitaso	Vaatimus	Mistä vaatimus tulee
Rajoitettu	Tekoälyjärjestelmän, joka tuottaa tai manipuloi syvävääreennöksen muodostavaa kuva-, ääni- tai videosisältöä, käyttöönottajien on ilmoitettava altistuksen yhteydessä, että sisältö on keinotekoisesti tuotettu tai että sitä on manipuloitu (poikkeukset: rikosasiat).	Tekoälysäädös Art. 50
Rajoitettu	Luonnollisten henkilöiden kanssa suoraan vuorovaikutukseen tarkoitetut tekoälyjärjestelmä ilmoittaa käyttäjälle altistuksen yhteydessä, että hän on vuorovaikutuksessa tekoälyjärjestelmän kanssa.	Tekoälysäädös Art. 50
Rajoitettu	Synteettistä ääni-, kuva-, video- tai tekstisisältöä tuottavan tekoälyjärjestelmän (mukaan lukien yleiskäyttöisten tekoälyjärjestelmien) tuotoksesta näkyy, että se on keinotekoisesti tuotettu.	Tekoälysäädös Art. 50

5. Kohti kontrolloitua käyttöä

Tekoälyn hallintamalliin voi tulla muutoksia normatiiviseen ohjaukseen ja erityisesti käytön aikaiseen valvontaan sekä vaatimustenmukaisuuden arviointia tukeviin tilannekuviin. Organisaatiokohtaisesti on hyvä tunnistaa käytössä olevat teknologia-alustat ja miten ne tukevat vaatimustenmukaisuutta. Esimerkiksi Microsoft 365 -alustalla on joukko Microsoftin tekemiä kontrollointitoimia ja osasta vastaa alustaa käyttävä organisaatio (Kuva 4) – on hyvä huomata, että esimerkiksi tekoälysäädöksen artiklojen perusteella voidaan kohdentaa alustasensitiiviset kontrollit ja niihin kuuluvat toimet (actions) säädösvaatimuksiin ja velvoitteisiin.



Luku ja jakso	Artikla	Kontrolli	Toimi	Työväline
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	10 Data ja datanhallinta	Article 10.2 Data and data governance	Apply sensitivity labels to protect personal data	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	11 Tekninen dokumentaatio	Article 11.1 Technical documentation	Retain operational compliance supporting documentation	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	11 Tekninen dokumentaatio	Article 11.2 Technical documentation	Create and apply a retention policy	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.1 Record keeping	Configure automatic log upload	Defender
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.1 Record keeping	Monitor cloud activity log	Azure
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.2 Record keeping	Enable audit logging	Audit
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.3 Record keeping	Enable audit logging	Audit
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	13 Avoimuus ja tietojen antaminen käyttöönottajille	Article 13.2 Transparency and provision of information to deployers	Centralize AI app management with enhanced security	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2	13 Avoimuus ja tietojen antaminen	Article 13.3 Transparency and	Create terms and conditions for user access	Intune

Kuva 4. Microsoft 365 -alustan kontrollit ja toimet, jotka organisaatio hoitaa erilaisilla työvälineillä.

Tekoälysäädös ja siihen liittyvät alustakontrollit ja -politiikat eivät yksin riitä, vaan tarvitaan ymmärrystä esimerkiksi seuraavista kehityskontrollikoonneista[15]:

- Tietosuoja
    - EU GDPR eli General Data Protection Regulation, joka on tietosuoja-asetus
    - FI DP Act eli Finland - Data Protection Act
- Riskien hallinta
    - NIST AI RMF eli National Institute of Standards and Technology AI Risk Management Framework

[15] https://learn.microsoft.com/en-us/purview/compliance-manager-regulations-list

    - ISO/IEC 23894 eli International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 23894 IT— AI — Guidance on risk management
- Tietoturva
    - NIS2 eli Network and Information Security 2 direktiivi
    - DPB eli Microsoft Data Protection Baseline, joka sisältyy tilauksiin (subscriptions) ja se sisältää kontrolleja seuraavista: NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), FedRAMP (Federal Risk and Authorization Management Program) ja GDPR (General Data Protection Regulation of the European Union).
- Tiedonhallinta
    - ISO/IEC 42001 eli International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 42001 IT — AI — Management system

Hallintamalli yhteistyön ja jatkuvan kehittämisen tukena

Tekoälyn hallinta ei pääty käyttöönottoon. Valtiokonttori painottaa yhteistyötä, yhdessä oppimista ja rohkaisee kokeiluihin. Lisäksi korostamme tekoälyn käytön aikaista valvontaa ja tilannekuvien muodostamista. Teknologia-alustojen teknisten kontrollien ja politiikkojen sisällyttäminen hallintamalliin tukee tavoitteiden saavuttamista.

Valtiokonttorin malli toimii esimerkkinä muille julkishallinnon organisaatioille. Se osoittaa, että tekoälyn hallinta ei ole vain tekninen kysymys, vaan vaatii strategista otetta, yhteistyötä ja jatkuvaa kehittämistä.

Lähteet

Lähteet, joilla ei ole DOI- tai ISBN-tunnusta, on merkitty alaviitteisiin.

Hotti, V., Piela, R., Lähteenmäki, J., Vinblad, M., Tulonen, T., Hartikainen, E., Lahdelma, P., Kotala, M., Impiö, T., Mäki, R., Kynkäänniemi, P., Vuojärvi, J. & Backman, V. (2025). Tekoäly hyötykäyttöön valtionhallinnossa: Opas organisaation kehittäjille muutosmatkan alkutaipaleelle. Valtiovarainministeriön julkaisuja 2025:27. http://urn.fi/URN:ISBN:978-952-367-855-2

Tammes-Peters, H. (2025). Ohjeistus generatiivisen tekoälyn hyödyntämisestä työn tukena ja apuvälineenä julkisessa hallinnossa. Valtiovarainministeriön julkaisuja 2025:9. http://urn.fi/URN:ISBN:978-952-367-846-0

Liite I

01 Organisaation AI ratkaisuiden kartoitus

Inventoitava asia	*Inventointi tulos (esimerkki)*
Nimeä tekoälyjärjestelmä, tai järjestelmän tekoälykomponentti	*Tyrskylän kunnan liikuntapalveluiden verkkosivulla on saatavilla tietoa liikuntapalveluista. Taustalla on liikuntapalvelujen verkkosivut.*
Elinkaari: milloin AI komponentti on otettu käyttöön?	*Otettu käyttöön 1.8.2024*
Elinkaari: milloin AI komponentti poistetaan käytöstä?	*Pilotointiaika 1.8.2024-1.8.2025, jonka jälkeen tilaajalla on optiona ostaa palvelua kolme lisävuotta.*
Kuvaa AI Komponentti tai ratkaisu	*Verkkosivulla on Large Language Modelia käyttävä chatbot, joka vastaa kysymyksiin esimerkiksi latujen aurausaikataulusta.*
Nimeä järjestelmän/palvelun ja AI komponentin omistaja	*Tyrskylän kunnan liikuntapalvelujohtaja*
Kuvaa käyttäjäryhmät	*Kaikki liikuntapalveluiden asiakkaat, yhdistykset ja seurat ja kunnan liikuntapalveluiden henkilöstö.*
Määritä tekoälysäädöksen mukainen riskiluokka	*Kyseessä on "tietty järjestelmä", joka on vuorovaikutuksessa ihmisten kanssa. (Tekoälysäädöksen 50 artikla)*
Roolit: Tekoälysäädöksen mukainen organisaation rooli. Rooleja ovat: Käyttöönottaja, tarjoaja, jälleenmyyjä (eli toimittaja), maahantuoja ja nimetty edustaja EU:ssa.	*Tyrskylän kunta on palvelun käyttöönottaja.* *Toimittaja on palvelun tarjoaja, koska he kehittävät komponenttia itse.*
Roolit: GDPR mukaiset roolit Rooleja ovat rekisterinpitäjä ja käsittelijä.	*Tyrskylän kunta on rekisterinpitäjä verkkosivuillaan olevalle henkilötiedolle. Toimittajalla ei ole pääsyä henkilötietoihin.*
Kerro, mitä dataa tekoälykomponentti tai ratkaisu käsittelee	*GDPR: Chatbot ei käsittele kysyjän henkilötietoja, mutta käsittelee liikuntapalvelujen verkkosivulla olevia henkilötietoja. Yleisesti chatbot käsittelee liikuntapalvelujen verkkosivulla kalenterissa olevia tietoja. Chatbot käsittelee asiakkaiden kysymyksiä ja henkilöstön anonymisoimat kysymykset kouluttavat chatbottia.*
Kerro, kuka kehittää järjestelmää	*Toimittaja Oy kehittää tekoälykomponenttia.* *Liikuntapalvelut kehittää tekoälykomponentin vastauskykyä kysymys- ja vastausesimerkkien avulla.*

Inventoitava asia	*Inventointi tulos (esimerkki)*
Listaa tarvittavat ja tehdyt arvioinnit (DPIA, FRIA, turvallisuus) sekä sertifikaatit/auditoinnit + linkki	*Verkkosivulle on tehty tasapainotesti ja DPIA. [linkki aineistoihin]* *Tekoälysäädöksen mukaista FRIA:a ei tarvitse tehdä kommunikoivassa järjestelmässä.* *Ratkaisulla ei ole sertifikaattia.*
Toimenpiteet	*Chatbotin hankinnassa tulee noudattaa hankintalakia. Tekoälykomponentin tietoturvallisuus tulee arvioida hankinnassa.* *DPIA pitää päivittää uuden tekoälykomponentin osalta.* *Kommunikoinnista tekoälyn kanssa tulee ilmoittaa chatbotin käyttäjille.*
Muut huomiot	*Tämä on yksinkertainen esimerkki kartoitettavasta järjestelmästä. Organisaation tulee arvioida järjestelmän tai ratkaisun riskit ennen käyttöönottoa.*

Liite II

07 Tekoälyn lisäkysymykset DPIAan. Kysymysosia on kuusi ja ne on värikoodattu siten, että tuotantokäyttöön liittyvät osaotsikot ovat harmaita, kehittämiseen liittyvät otsikot ovat vaalean turkooseja ja tekoälyjärjestelmän kouluttamiseen liittyvät otsikot ovat limen vihreitä. Sarakeotsikko V = Vastaus ja K = Kommentti.

Kysymys	**V**	**K**	**Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.**
Osa 1: Kartoittavat kysymykset	Tekoälyjärjestelmää suunniteltaessa on tärkeää ottaa huomioon sen tavoite (tarkoitus) ja valittujen tekniikoiden oikeasuhteisuus: ovatko ne ehdottoman välttämättömiä tämän tavoitteen saavuttamiseksi? Seuraavat kysymykset voivat auttaa rekisterinpitäjää arvioimaan ehdotettuun järjestelmään liittyviä riskejä ja sen oikeasuhteisuutta ennen suunnitteluvaihetta.		
Toimiiko organisaatio tekoälypalvelun tarjoajana (ohjelmistovalmistaja) vai käyttöönottajana?			
Ovatko tekoälyjärjestelmän koulutus- ja tuotantovaiheet erillään? Oppiiko tekoälypalvelu tuotantovaiheessa?			
Minkä tyyppistä tekoälyjärjestelmää käytetään?			
Osa 2: Tekoälyn vaikutuksen ihmisiin ja vastuullisen tekoälyn periaatteet			
Käsittelyn vaikutusten suhteuttaminen yksilön perusoikeuksiin	Jotkut tekoälyjärjestelmiin liittyvät käsittelytoimet voivat olla erityisen häiritseviä tai niillä voi olla merkittäviä seurauksia yksilöille niiden laajuuden, rekisteröityjen ominaisuuksien tai muiden erityispiirteiden vuoksi. Tässä tilanteessa on entistä tärkeämpää säilyttää yksilöiden oikeudet ja vapaudet		
Onko tekoälyjärjestelmän kehittämisestä, käyttöönotosta ja valvonnasta vastaavat organisaatiot määritelty selkeästi?			
Ovatko tekoälypalvelu ylläpidosta, ongelmien korjaamisesta vastaavat ja sen toimintaan osallistuvat henkilöt selkeästi tunnistettu ja kaikkien tiedossa?			
Onko rekisteröityjen informointiin liittyvät lisävaatimukset huomioitu tekoälyjärjestelmää käytettäessä?			
Osa 3: Tekoälypalvelun kehittämisen elinkaari (jos organisaatio itse kehittää, vähemmän kysymyksiä, jos ostetaan toimittajan kehittämä valmis tekoälyjärjestelmä)			
Koulutusdatan laillinen käsittely, elinkaaren hallinta	Henkilötietoja sisältävää koulutustietokantaa (joko tekoälyjärjestelmän toimittajan luomia tai kolmannen osapuolen toimittamia) koottaessa on ryhdyttävä tiettyihin varotoimiin säännösten noudattamisen osoittamiseksi. Tarkastettavia asioita ovat erityisesti tietojen alkuperä, todelliset mahdollisuudet käyttää niitä uudelleen koulutustarkoituksiin tai väärinkäyttöriskin rajoittamiseksi toteutetut toimenpiteet. Seuraavat kysymykset voivat auttaa rekisterinpitäjää arvioimaan, täyttääkö se vaatimukset säännösten mukaisen koulutustietokannan laatimiselle.		

Kysymys	V	K	Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.
Käytetäänkö organisaation henkilötietoja sisältävää dataa tekoälyjärjestelmän opettamiseen?			
Jos tietokanta käytetään uudelleen, onko tietokanta koottu tietosuojasäädösten mukaisesti?			
Jos on käytetty julkisesti saatavilla olevaa tietokantaa, onko selvitetty, soveltuuko se käyttötarkoitukseensa?			
Mikä on koulutustietojen käsittelyn oikeusperuste?			
Arkaluonteisia tietoja (terveys, rikosrekisteri jne.) voidaan käsitellä vain, jos ne täyttävät jonkin GDPR:n artiklassa 9 mainituista poikkeuksista[16]. Mihin näistä poikkeuksista arkaluonteisten henkilötietojen käyttö koulutusdatana perustuu?			
Miten koulutustietojen käsittelyn vaatimustenmukaisuutta valvotaan (DPIA:n suorittaminen, uudelleentunnistuksen riskin analysointi, jne.)?			
Täyttääkö koulutukseen käytettävien tietojoukkojen tuottaminen minimointiperiaatteen			
Onko data anonymisoitu?			
Tarkennus: jos on anonymisoitu, miten se tapahtuu			
Onko data pseudonymisoitu?			
Tarkennus: Jos on pseudonymisoitu, miten se tapahtuu?			
Onko uudelleentunnistumisen riskit arvioitu?			
Raakadatasta laadukkaaseen koulutustietojoukkoon, re-enforcing	Algoritmin tuloksen laatu on kiinteästi sidoksissa koulutustietojoukon laatuun riippumatta siitä, mitä tietoluokkia käytetään. Tietyt kriteerit on tarkistettava, jotta voidaan rajoittaa virheriskiä algoritmia käytettäessä, varsinkin kun sillä on seurauksia yksilöille.		
Onko tietojen oikeellisuus tarkistettu?			
Onko tiedon luokittelussa käytetty asianmukaisia metatietoja?			Järjestelmän koulutusvaiheessa tehtävässä tiedon luokittelussa on käytetty asianmukaisia metatietoja.
Mitä menetelmiä on käytetty edustavuuden varmistamiseksi? (ettei tule syrjivä algoritmi)			
Mikä mekanismi on toteutettu jatkuvaa oppimista käyttävän tekoälyjärjestelmän tapauksessa jatkuvasti käytettävän datan laadun varmistamiseksi?			
Onko käytössä säännöllisiä mekanismeja laadun heikkenemisen tai tietojen jakelun muutosten arvioimiseksi?			
Vinoumien tunnistus ja tehokas korjaus, supervised learning	Vinoutuneisiin tietoihin opetetun algoritmin käyttöön liittyvät syrjinnän riskit tunnetaan nykyään laajalti. Näihin riskeihin vaikuttavia tekijöitä ei kuitenkaan tunnistettu ja keinot niiden korjaamiseksi ovat vielä kokeellisia. Harjoittelutietojoukko on siksi tarkastettava perusteellisesti mahdollisen vinoumien varalta.		

[16] L_2016119FI.01000101.xml

Kysymys	V	K	Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.
Onko koulutusdata keräämiseen käytetty menetelmä riittävän tunnettu? Kuvaa keräysmenetelmä.			
Onko mahdollista, että käytetystä menetelmästä tai erityisistä keräysolosuhteista aiheutuu vinouma?			Toimittajan käyttämästä menetelmästä tai tiedon keräysolosuhteista ei aiheudu vinoumaa.
Koulutetaanko järjestelmää yksilöiden erityispiirteisiin liittyvillä tiedoilla, kuten sukupuoli, ikä, fyysiset ominaisuudet, arkaluonteiset tiedot yms.			
Jos vinoumia on havaittu, mihin toimiin on ryhdytty niiden vähentämiseksi?			Jos toimittaja havaitsee tuotantokäytössä vinoumia, se kykenee korjaamaan ne kohtuullisessa ajassa.
Huolellisen testausprotokollan soveltaminen	Luomalla protokollan tekoälyjärjestelmän koulutukseen palveluntarjoaja voi haastaa algoritmin suorituskyvyn ja oikeudenmukaisuuden validointimenetelmien valinnan ja toteuttaa validointitestit kriittisimmissä vaiheissa. Koska ne tarjoavat ensimmäisen mahdollisuuden tarkkailla algoritmia, koulutus- ja validointimittarit on valittava huolellisesti. Esim. tarttuvan taudin seropositiivisuustestissä on tärkeämpää rajoittaa vääriä negatiivisia kuin vääriä positiivisia tuloksia.		
Onko tekoälyn testauksessa käytetty protokolla riittävän objektiivinen ja kattava? Millä toimilla ongelmia on vähennetty (esim. tekniset, tai hallinnolliset mittarit)?			
Onko tunnistettu ja ohjeistettu tilanteet ja käyttötapaukset, joissa järjestelmä ei tuota luotettavia tuloksia?			
Tarkennus: Lisätäänkö turvamekanismeja näiden tilanteiden käsittelemiseksi (esimerkiksi antamalla hallinta järjestelmällisesti ihmiskäyttäjälle)?			
Jatkuvan oppimisen skenaario: toteutetaanko toimenpiteitä suorituskyvyn heikkenemisen, mallien ajautumisen tai algoritmin tuloksiin vaikuttamiseen tähtäävien hyökkäysten välttämiseksi (esim. online-chatboteista tulee rasistisia)?			
Järjestelmän kehitysvaiheen aikainen laadun tarkkailu	Algoritmia ja koko järjestelmää koskevat testit on suoritettava olosuhteissa, jotka mahdollistavat käsittelyn kattavan validoinnin. Käyttäjien tarpeet ja heidän asiantuntemuksensa tulee ottaa tässä vaiheessa mahdollisimman paljon huomioon.		
Miten järjestelmän laatua varmistetaan kehitysvaiheessa?			
Ovatko tarvittavat sidosryhmät (esim. käyttäjät) mukana testauksessa?			
Osa 4: Vastuullinen tekoälyhallinto ja riskinhallinta			
Noudatatteko tekoälyn hallinnossa tekoälyjärjestelmien käyttöönottoa säätelevää organisaation sisäistä linjausta tai ohjetta? Esim. Tekoälypolitiikka, tai eettiset ohjeet.			

Kysymys	V	K	Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.
Hyökkäysmallien tunnistaminen ja niiltä suojautuminen	Monet viimeaikaiset tutkimukset osoittavat, että tekoälyjärjestelmiin voidaan hyökätä tai ne voidaan muuttaa tarkoituksestaan. Tekoälyjärjestelmän tarjoajan ja käyttäjän on tiedettävä nämä uudet hyökkäysmallit. Näiden hyökkäysten ennennäkemättömän luonteen vuoksi on ryhdyttävä varotoimiin aina kun mahdollista.		
Ottaako järjestelmälle tehty tietoturvan riskianalyysi huomioon tekoälyalgoritmien erityiset hyökkäysmallit? Mitä toimenpiteitä on tehty?			
Tarkennus: Jos tekoälyä on koulutettu käyttämällä henkilötietoja, onko mahdollista, että tekoäly antaa tuloksena henkilötietoja? Kuvaa, kuinka näitä riskejä rajoitetaan?			
Tarkennus: Onko koulutusaineisto suojattu asianmukaisesti ja riittävällä tavalla GDPR:n asettaman turvallisuusvelvoitteen kannalta?			
Lokitus valvonnan parantamiseksi	Ylläpitämällä lokia koko ketjun ajan tekoälyjärjestelmän käyttäjien on kyettävä tunnistamaan ja selittämään epänormaali toiminta.		
Mitä lokitetaan? Mistä näkökulmasta lokeja kerätään (esimerkiksi tekoälyjärjestelmän tuotosten perusteleminen, tekoälyjärjestelmän käyttäjien valvonta) miten lokeja hyödynnetään (esim. rekisteröityjen pyynnöt, laadunvarmistus jne.) ja kuinka se vaikuttaa lokien säilytysaikoihin.			
Pääsynhallinta	Käytettiinpä AI järjestelmää fyysisessä maailmassa tai ohjelmistossa, pääsyä muutosten tekemiseen tulee vähentää ja hallinnoida.		
Miten pääsynhallinta hoidetaan? Esim. peruskäyttäjätaso, ylläpitäjätaso ja kehittäjätaso.			
Käsittelyn kaikkien vaiheiden turvaaminen	Rajoittamatta käytetylle tekoälyjärjestelmälle ominaisia turvatoimia, on lisäksi otettava käyttöön tavanomaiset turvatoimenpiteet henkilötietojen käsittelyssä tai käsittelyssä, jolla on seurauksia yksilöille.		
Onko sisäinen tai ulkoinen arviointi (pakollinen), tai auditointi (tarvittaessa) tehty käsittelyn kaikkiin vaiheisiin? Kuvaa tarkemmin.			
Standardien, sertifikaattien ja käytännesääntöjen noudattaminen todisteena osoitusvelvollisuudessa	On julkaistu lukuisia standardeja ja sertifiointiprosesseja, joista osa perustuu itsearviointiin, jotta tekoälyn tarjoajat voivat todistaa, että heidän järjestelmänsä täyttää vähimmäisvaatimukset.		
Onko tekoälyjärjestelmä tiettyjen standardien mukainen (IEEE, ISO jne.)?			
Täsmennä minkä:			
Onko tekoälyjärjestelmä sertifioinut kolmannen osapuolen organisaatio, tai viranomainen?			
Täsmennä kuka:			

Kysymys	V	K	Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.
Onko tekoälyjärjestelmä tiettyjen käytännesääntöjen tai parhaiden käytäntöjen mukainen? (jos sellaisia on kyseiselle järjestelmälle olemassa)			
Täsmennä minkä:			
Dokumentointi luotettavuuden varmistamiseksi	Ajantasaisen dokumentaation avulla palveluntarjoaja, käyttäjä, henkilö ja valvontaviranomaiset voivat tunnistaa käsittelyyn liittyvät riskit ja siten auttaa hallitsemaan niitä.		
Onko dokumentaatiota siitä, miten koulutus- ja tuotantotiedot kerätään ja hallitaan, algoritmista, tulosten laadusta, käytetyistä työkaluista, kirjaamisesta ja turvatoimista?			Käytä tarvittaessa: Toimittaja toimittaa Tilaajalle tarvittaessa dokumentaatiota siitä, miten koulutus- ja tuotantotiedot kerätään ja hallitaan, algoritmista, tulosten laadusta, käytetyistä työkaluista, kirjaamisesta ja turvatoimista
Osa 5: AI projektien ja systeemien toteuttaminen			
Annetaan ihmiselle mahdollisuus säilyttää hallinta (AI as a socio-technical system)	Vaikka tekoälyjärjestelmät voivat automatisoida tehtäviä ja voivat joskus olla tehokkaampia kuin ihminen, ihminen on tarvittaessa kutsuttava väärinkäytön estämiseksi ja sen varmistamiseksi, että tietyt virheet eivät tule systemaattisiksi. Tämän saavuttamiseksi toteutettavien toimenpiteiden on oltava tunnistettuja, tehokkaita ja kestäviä. Seuraavat kysymykset voivat auttaa rekisterinpitäjää toteuttamaan puitteet, jotka mahdollistavat näiden ehtojen noudattamisen.		
Onko ihmisen suorittama valvonta suunniteltu?			
Voiko käyttäjä muokata tekoälyjärjestelmän tekemää päätöstä manuaalisesti (esim. muokata videonjakoalustan käyttäjälle annettua profiilia) tai lopettaa sen toiminnan (esim. katkaista pääsyn online-chatbottiin)?			
Onko tarvittavat henkilö- ja aineelliset resurssit ja henkilöiden roolit ja vastuut selvästi suunniteltu?			
Tarkennus: Ovatko he saaneet riittävästi koulutusta?			
Onko tunnistettu tilanteet, joissa ihmisen puuttuminen on tarpeen?			
Miten harhariski (käyttäjän taipumus luottaa liikaa tekoälyjärjestelmän tuotoksiin) on otettu huomioon?			
Läpinäkyvyys	Luottamuksen rakentamiseksi rekisteröityjen ja tekoälyjärjestelmän rekisterinpitäjän välille tulee noudattaa suurta avoimuutta sekä järjestelmän toiminnan selittämisessä että yksittäisten päätösten selittämisessä. Selittävä kirjaaminen ei kuitenkaan saisi tapahtua toimijoiden tai rekisteröityjen yksityisyyden kustannuksella.		
Kertooko tekoälyjärjestelmä, että tuotos on sen tuottamaa?			
Onko lokissa tietoja, joita voidaan käyttää selittämään takautuvasti tekoälyjärjestelmän tiettyä tuotosta?			Käytä tarvittaessa: Tilaaja pystyy tarvittaessa selittämään tekoälyjärjestelmän [minkä tuotoksen] jälkikäteen järjestelmän lokin avulla.

Kysymys	V	K	Hankintavaiheessa on hyvä olla seuraava vaatimus, jos tekoälyjärjestelmä ostetaan tuotantovalmiina.
Käsittelyn laadun varmistaminen	Käyttöön otettujen läpinäkyvyys- ja valvontatoimenpiteiden lisäksi teknisillä toimenpiteillä on varmistettava, että tekoälyjärjestelmän tuotoksen laatu säilyy koko sen käyttöiän ajan.		
Miten tekoälyjärjestelmän toiminnan luotettavuutta ja toimivuutta arvioidaan tuotantovaiheessa? Onko tekoälyn jatkuvan kehittämisen malli suunniteltu tuotantovaiheessa?			
Seurataanko tekoälyjärjestelmän tuotoksen laatua tekoälyjärjestelmän elinkaaren aikana?			
Jos tekoälyjärjestelmä louhii henkilötietoja isosta tietojoukosta, onko varmistettu, että kerätään vain tarvittavat henkilötiedot?			
Tarkistetaanko tietojen ajantasaisuus ja todenperäisyys ja julkisuusaste?			
Tarkistetaanko käyttäjän/järjestelmän käyttövaltuuksien laajuus?			
Osa 6: Loppukysymys			
Kannattaako järjestelmää ottaa käyttöön, eli ylittääkö saavutettu lisäarvo (esim. tehokkuus, kustannukset, yksityisyyden suoja, palvelun tavoitteet) rekisteröidyn oikeuksiin kohdistuneet heikennykset (ks. turvallisuusarviointi ja tämän DPIA:n tulokset)?			

VALTIOKONTTORIN JULKAISUJA | TEKOÄLY 3/2025

Tekoälyn hallinta

Esimerkkinä Valtiokonttorin tekoälyn hallintamalli

Valtiokonttori

Julkaisija: Valtiokonttori
ISSN/ISBN: 2489-4761/978-951-53-3903-4
Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. 0295 50 2000, Faksi 0295 50 3333, www.valtiokonttori.fi

Valtiokonttori
Statskontoret
State Treasury