Tekoälyn hyödyntäminen – huoneentaulut ja tarkistuslistat - tiivistelmä

VAHTI hyvät käytännöt -tukimateriaali
13.6.2024 ver. 2.5

DIGI- JA VÄESTÖTIETO-VIRASTO

Johdanto

- Tämä tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn ja toiminnan edistämiseksi.
- VAHTI hyvät käytännöt -tukimateriaalit pohjautuvat Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI, https://dvv.fi/vahti) asiantuntijaryhmien kokoamiin suosituksiin
- Näitä ohjeita päivitetään. Otamme mielellämme vastaan parannus- ja korjausehdotuksia ja julkaisemme päivitetyn version, kun niitä on kertynyt riittävästi. Palautetta: digiturva@dvv.fi (otsikkoon: ”VHK tekoäly huoneentaulut”).
- Vaikka VAHTI hyvät käytännöt -tukimateriaalit ovat ensisijaisesti suunnattu julkisen hallinnon organisaatioille ja ne ovat vapaasti minkä tahansa organisaation hyödynnettävissä.
- Tämän dokumentin ensimmäinen versio muodostettiin hyödyntämällä muun muassa tekoälyä ja se julkaistiin 15.6.2023. Ensimmäinen asiantuntijoiden jatkokehittämä versio (1.0) julkaisiin 12.9.2023. Version 2.0 kehittämiseen osallistui 17.11.2023 työpajassa 100 asiantuntijaa VAHTI-työryhmistä ja DVV:ltä, ja se julkaistiin 12.12.2023. Versio 2.5. julkaistiin 13.6.2024 VAHTI-kesäseminaarissa.
  - VAHTI hyvät käytännöt tukimateriaalien tuottamisessa hyödynnämme apunamme tekoälytyökaluja, kuten on tehty tämän dokumentin aiemmissa versioissa.
  - Kaikki sisällöt käyvät läpi tarkistus- ja kommentointiprosessin.
- Julkaisun jakelu: https://dvv.fi/digiturvajulkaisut

Taustatehtävät

- **Organisaatiot voivat vapaasti hyödyntää, sovittaa ja muokata huoneentaulujen listoja**, jotka on kohdistettu eri toimijaryhmille suunnattuun viestintään ja ohjaukseen.
  - Organisaatioiden tulee ohjeistaa tarkemmin käyttöön hyväksytyistä tekoälypalveluista ja niiden turvallisesta käytöstä.
  - Jokainen organisaatio ja asiantuntija **vastaa siitä, että tämän tukimateriaalin sisältö sovitetaan vastaamaan organisaation omaa toimialaa ja sitä koskevaa lainsäädäntöä**.
  - **Materiaalia ei saa ottaa käyttöön sellaisenaan** ilman läpikäyntiä, muokkaamista omaan tarkoitukseen sekä siihen liittyvää asianmukaista viestintää organisaatiossa ja tarvittaessa sen sidosryhmille.
- Tässä materiaalissa tekoälyllä tarkoitetaan
  - laajasti järjestelmiä, prosesseja ja palveluita, joissa hyödynnetään tekoälyä sekä
  - joissain tapauksissa myös sellaisia kehittyneitä järjestelmiä, joiden algoritmit tai rakenne ovat siinä määrin kompleksisia, että ne ovat verrannollisia tekoälyyn tai voivat näyttäytyä sellaisina käyttäjälle.
- Tällä tavallista laajemmalla rajauksella halutaan sisällyttää eri määritelmiä kattavasti sekä kiinnittää huomiota siihen, että tekoälyyn liittyvä teknologiat kehittyvät nopeasti, niiden vaikutukset ulottuvat kauan ja eri tasoille.
  - Tekoälyä voidaan määritellä ja luokitella muun muassa hallinnollisesta, juridisesta, käyttäjäkokemuksellisesta, evolutionaarisesta ja teknisestä näkökulmasta, jotka kaikki vastaavat eri tarpeisiin
  - **Ei siis ole olemassa vain yhtä ”keskiarvoista” tekoälyä.** Eri käyttötapauksiin voidaan nähdä liittyvän erilaisia toiminnallisuuksia, uhkia, hallintorakenteita, sääntelyä ja odotuksia – muun muassa.

Suunnitelmallinen perusta

1. Organisaation **tekoälynkäytön tulisi olla suunnitelmallista, ohjattua ja johdonmukaista**.
   - Täten ohjaavana pohjana organisaatioilla tulisi olla suunnitelma tekoälyä varten, riippumatta siitä, onko organisaatio itse eturintamassa sen käyttöönotossa vai vasta viimeisten joukossa.

2. Tekoäly on jollain aikavälillä **tulossa osaksi organisaatioiden normaalia toimintaa**, mikä edellyttää muutoksia ja niiden toteuttamisen johtamista. Tähän perustuen, organisaation ohjauksen tukemiseksi
   - Tekoälyn johtamista ja hallintaa varten on muodostettava suunnitelma. On suositeltavaa, mutta organisaation päätettävissä, tehdä se strategian ja politiikan tasoisina
   - Tekoälystrategia ja -politiikka tulisi muodostaa sillä tavoitteella, että ne aikanaan (linjausten, teknologian ja osaamisen maturiteetin kehityttyä), voidaan tuoda osaksi normaalia johtamista ja toimintaa.
   - Tulisi tunnistaa tekoälyn mahdolliset **vaikutukset sisäiseen ja ulkoiseen toimintaan sekä toimintaympäristöön**, jotta näitä voidaan ennakoida.
   - **Tekoälystrategiaan** tulisi sisältyä muun muassa:
     - mitä tekoäly sille on,
     - mitä organisaatio tavoittelee tekoälyn käytöllä,
     - miten tekoäly auttaa saavuttamaan organisaation tavoitteita sekä
     - miten edetään erillisestä tekoälyn ohjauksesta sisäistettyyn normaaliin toimintaan
   - **Tekoälypolitiikkaan** tulisi sisältyä muun muassa:
     - miten strategian tavoitteisiin päästään,
     - mihin tekoälyä voidaan käyttää ja mihin ei,
     - miten tekoälytoimia hallitaan,
     - miten organisaatiossa käytetään tekoälyä,
     - miten tekoälyn vaikutukset käsitellään sekä
     - miten varaudutaan toimimaan ilman tekoälyä.

3. Organisaation tekoälytoiminnan **strategiaa ja politiikkaa tulee pitää yllä ja uudistaa** teknologian ja järjestelmien kyvykkyyksien muuttuessa, lainsäädännön ja muun regulaation kehittymisen mukaan sekä tekoälyn käytöstä tunnistettujen hyötyjen ja haittojen perusteella.
   - Strategian ja politiikan välinen ero ei aina ole selkeä ja organisaatioilla voi olla erilaisia hallintokulttuureita näiden sisältöjen määrittelyssä, minkä vuoksi käytettyä jakoa voi pitää lähinnä ohjeellisena.

Johdolle

1. **Hanki tietoa:** Kouluttaudu ja tutustu tekoälyn perusteisiin eri näkökulmista ja ota se agendalle
   - Valmistele visio, suunnitelma, tiekartta, strategia ja/tai politiikka organisaation toiminnan tueksi, osallistaen mahdollisimman paljon eri tahoja
2. **Luo hallintarakenteet ja resurssit:** Tekoälyyn liittyvien roolien, vastuiden ja resurssien määrittely sekä budjetointi
   - Nimeä tekoälyjen hallinnointiin vastaava johdon edustaja ja asiantuntija(t) sekä varmista, että organisaation riskienhallinnasta, toiminnan jatkuvuudesta, tietoturvasta ja tietosuojasta vastaavat henkilöt tuntevat organisaation kehittämiin tai hyödyntämiin tekoälypalveluihin liittyvät linjaukset ja kehittämishankkeet.
   - Varmista, että organisaatiolla on joko omaa tai erikseen hankittavaa erityisasiantuntemusta lainsäädännöllisiin sekä muihin tekoälyn ympärillä tapahtuviin uudenlaisiin tilanteisiin ja ilmiöihin. Osoita riittävä varaus tekoälykoulutukseen vastuullisille asiantuntijoille sekä käyttäjille.
3. **Varmista riskienhallinta:** Varmista, että tekoälyn hyödyntämisessä ja palveluiden kehittämisessä sovelletaan organisaation käyttämää riskienhallintamallia sekä tunnistetut riskit käsitellään ja otetaan hallintaan.
   - Pysy tietoisina riskien kehityksestä nopeasti kehittyvällä kentällä ja tarkastele niitä laajasti, mukaan lukien koko palvelu- tai prosessiketju, johon tekoäly sisältyy.
   - Huolehdi yhteistyöstä sidosryhmien kanssa ja pyri yhteisiin linjauksiin
   - Vastuuta sopimusten tekoälyyn liittyvä vastuiden hallinta
   - Varmista, että organisaatiossa on mahdollisuus tutkia ja kokeilla tekoälyä eri muodoissaan turvallisesti, jotta hyötypotentiaali on mahdollista tunnistaa. Varaudu myös mahdollisesti toteutuvien riskien hallintaan.
4. **Viesti ja johda:** Suunnittele ja toteuta muutosjohtaminen ja -viestintä, kun tekoälyyn liittyviä tai sisältäviä kokonaisuuksia toteutetaan käyttöön (mm. vaikutukset työntekoon, asiakkaiden palveluihin, sidosryhmiin)
   - Varmista, että organisaation henkilöstö tietää ajantasaisen strategian ja politiikan sekä tuntee henkilöstön ohjeistuksen.

Huoneentaulu tekoälyn käyttöä, tietoturvallisuutta, tietosuojaa ja muita tukitoimia ohjaaville asiantuntijoille

1. **Ohjeista** mitä sovelluksia, järjestelmiä ja palveluita saa tai ei saa käyttää ja miksi sekä missä rajoissa käyttö on sallittua

2. Varmista, että **tekoälyn käyttö ja kehittäminen, ohjeistukset sekä sopimus- ja lisenssiehdot vastaavat organisaation strategiaa ja politiikkaa sekä lakia**
   - Varmista, miten tekoäly tukee lakisääteisiä tehtäviä ja toimii sallituissa rajoissa
     - Huomioi palveluiden laajennusten, uusien moduulien tai versioiden mukana tulevat käyttöehtojen muutokset.
   - Huomioi tekoälyn käytön yhteydessä mahdolliset tekijänoikeuskysymykset (syötetty data, oppimisdatan jäänteet tuotoksissa)

3. **Arvioi riskiperustaisesti, voiko jotain asiaa tai materiaalia käsitellä** tekoälyä hyödyntäen tai tekoälyä hyödyntävässä järjestelmässä.
   - Huomioi tietosuoja ja tiedon luokittelu. Ohjeista henkilöstöä sallittujen ja kiellettyjen aineistojen käytöstä. Luokitteluiden ja metatietojen tulee soveltua tekoälyllä hyödynnettäviksi
   - Huomioi varautuminen tekoälyn käytön rajoituksiin, estymiseen sekä myös omatoimiseen alasajon tarpeeseen.

4. **Varmista ja sovi kirjallisesti** missä määrin ja millä edellytyksillä tekoälypalveluita voidaan mahdollisesti hyödyntää **hankkiessa alihankintana** sovelluskehitystä tai muita palveluita.
   - Varmista, ettei sovelluskehityksen yhteydessä vuodeta organisaation toiminnan kannalta kriittistä tietoa.
   - Mikäli tekoälyä hyödynnetään, sovi miten tarkistus, testaus, laadunvarmistus ja kehityksen seuranta tapahtuvat.
   - Varmista tekijänoikeudellisten riskien vastuut sopimuksissa

5. **Ohjeista ja kouluta henkilöstöä** tekoälyyn liittyvistä periaatteista, muun muassa: avoin ja läpinäkyvä käyttö; oikeudenmukaisuus, syrjimättömyys ja vinoumat; tietosuoja ja yksityisyys; turvallisuus ja luotettavuus; ihmiskeskeisyys; eettinen suunnittelu ja käyttö; jatkuva käyttöpalautteen ja virhetietojen käsittely sekä poikkeamatilanteet; tekoälyn käytöstä viestiminen; osallistuminen ja yhteistyö

6. Huomioi tekoälyn hyödyntämiseen liittyvien eettisten ohjeiden ja riskienhallinnan kehittyminen sekä **päivitä organisaation ohjeistuksia ja prosesseja** vastaavasti.

7. **Verkostoidu** muiden organisaatioiden ja sidosryhmien kanssa kokemuksista, linjauksista ja muusta vertaistuesta

8. **Viesti säännöllisesti** tekoälyn ajankohtaisista asioista selkeästi ja osallistavasti.

9. **Ohjeista, miten tuotosten vastaanottajille tulee kertoa tekoälyn hyödyntämistä** materiaalin tuottamisessa (tekstit, kuvat, videot).

10. Tekoälyn käytön alkuvaiheessa arvioi tilannetta tapauskohtaisesti. Yleisesti pätevät ohjeet muokkautuvat kokemuksen karttuessa. **Oleellista on kerätä tietoa.**
    - Luo järjestelmä, jolla voidaan kerätä tietoa kaikista tekoälyyn liittyvistä poikkeamista. Kukin tekoälyjärjestelmä voi olla erilainen ja niissä voi olla seurattavan erityisiä ominaisuuksia, mutta huolehdi kokonaisnäkymän muodostumisesta.
    - Huomioi järjestelmän yhteys ja yhdenmukaisuus tietoturvapoikkeamailmoituksiin, riskitietoihin, laadunhallintaan, asiakaspalatteisiin ja ohjelmistokehitykseen siten kuin ne ovat tehokkainta järjestää.

Henkilöstölle

1. **Noudata organisaation käyttöperiaatteita** (politiikkaa, ohjeistuksia, roolituksia, prosesseja) tekoälyn kokeiluissa, käyttöönotossa ja käytössä.
   - Käytä tekoälysovelluksia vain organisaation hyväksymään tarkoitukseen.
2. **Käytä vain organisaation hyväksymiä tekoälysovellutuksia** tietojen käsittelyyn.
   - Mikäli käyttämäsi ohjelmisto tai verkkopalvelu ilmoittaa ottaneensa käyttöön tekoälyyn perustuvia ominaisuuksia, ilmoita tästä ohjelmistojen hyväksymisistä vastaavalle taholle.
   - Tarkista, onko käyttämäsi palvelu kaikille avoin, yleinen tekoälypalvelu vai oman organisaatiosi tarjoama palvelu ja noudata niiden käytöstä annettuja ohjeita.
3. **Älä oleta, että tekoäly on aina oikeassa**. Tekoäly ei ole erehtymätön, ja sen päätökset voivat olla vääriä. Älä luota sokeasti sen päätöksiin tai tuottamaan tietoon.
   - Älä käytä tekoälyn tuottamaa aineistoa (esim. koodia, dataa, käännöksiä), jos et ymmärrä mitä se tekee, sisältää ja tarkoittaa
   - Tarkasta tekoälyn tuottamat tiedot muuta kautta, jos et voi itse niitä varmistaa.
4. **Mikäli tekoäly tuottaa huonolaatuista, virheellistä, vaarallista tai muuten epäilyttävää ja sopimatonta materiaalia, lopeta sen käyttö.** Dokumentoi kopioimalla tekstit, ottamalla kuvakaappauksia tai tallentamalla mahdolliset virhe- ja lokitiedot analysointia varten.
   - **Ilmoita sovitulla tavalla tekoälyn tekemistä erityyppisistä virheistä**. Pienetkin virheet voivat kertautua huomattavaksi ongelmaksi. Organisaatiosi ohjeistaa miten ja mistä ilmoitetaan.
5. Varmista aina tekoälysovellutusta käyttäessäsi, **ettet syötä sovellutukselle organisaation rajoittamaa materiaalia**.
   - Esimerkkejä kielletyistä voivat olla henkilötiedot, salassa pidettävät tiedot, turvaluokitellut tiedot, tekijänoikeudelliset tiedot jne.
6. **Jos olet epävarma, kysy organisaation tekoälyvastaavalta**, tietoturva-asiantuntijalta, tietosuojavastaavalta tai muulta asiantuntijalta.
   - Anna palautetta tekoälyvastaavalle ja tietoturva-asiantuntijoille, jos huomaat ohjeissa ”porsaanreiän” tai muun epäkohdan.
7. **Pidä itseäsi ajan tasalla**, osallistu koulutuksiin ja muihin tilaisuuksiin.
8. **Noudata hyvän, avoimen hallinnon periaatteita ja muista virkavastuu** – vastuuta ei voi siirtää tekoälylle.
   - Tekoälyn tuottamasta sisällöstä on pääsääntöisesti ilmoitettava organisaation ohjeen mukaisesti
9. Näe tekoäly positiivisena, uudenlaisena, osaamistasi laajentavana tukipalveluna

Tuoteomistajille, ylläpitäjille ja kehittäjille

TEE NÄIN (1/3):

1. Käytä tekoälypalveluita ja -resursseja annettujen ohjeiden mukaisesti työn tekemiseen ja suunniteltujen projektien toteuttamiseen.
   - Kokeiluiden tekemistä tulisi tukea. Niiden on kuitenkin oltava riittävän rajattuja, riskit tulee arvioida ja riskien toteutumiseen tulee etukäteen varautua.
2. Kehitystoimien ja tekoälyn hyödyntämisen tulee noudattaa organisaation strategiaa ja politikkaa. Mahdolliset poikkeamat linjauksista ja kokeilut tulee käsitellä etukäteen.
3. Noudata lakeja ja määräyksiä. Varmista, että tekoälyn käyttö järjestelmän toiminnan apuna noudattaa kaikkia sovellettavia lakeja ja määräyksiä, mukaan lukien tietosuoja- ja syrjimättömyyslait. Päivitä tietämystäsi aika-ajoin niiden tulkinnasta ja pyri huomioimaan kehitteillä olevan EU:n tekoälysäädöksen (AIA) pääkohdat ennakoivasti järjestelmäsi ominaisuuksissa.
4. Sovi ulkopuolisten konsulttien kanssa miten ja missä rajoissa tekoälyä voidaan hyödyntää kehittämisessä. Sovi kirjallisesti laadunhallinnasta ja vastuista.
5. Ota turvallisuus huomioon jo tekoälyjärjestelmän suunnitteluvaiheessa, ei vasta käyttöönoton yhteydessä.
   - Käytä luotettavia ja testattuja järjestelmiä. Tekoälyjärjestelmät voivat olla monimutkaisia, joten on tärkeää käyttää hyvin suunniteltuja ja testattuja järjestelmiä.
   - Käy läpi järjestelmän toiminta ja asetukset turvallisuuden ja tietosuoja osalta. Rajaa kehitys- ja testausympäristöt vaatimusten mukaisesti
   - Tee ilmoitus kaikista palveluiden käyttöön liittyvistä ongelmista, tunnistamistasi uhkista ja havaitsemistasi riskeistä organisaatiosi ohjeiden mukaisesti.
   - Varaudu mahdollisiin ongelmiin. Vaikka tekoälyjärjestelmät ovat usein luotettavia, on tärkeää valmistautua mahdollisiin ongelmiin tai vikoihin.
   - Huomioi myös palvelun päättyvä ylläpito ja äkillinen loppuminen. Tämä voi tarkoittaa esimerkiksi varasuunnitelmien tekemistä vaihtoehtoisille tavoille päästä käsiksi ja käsitellä dataa sekä nopeaa viestintää.
   - Huolehdi tekoälypalveluita käyttäessäsi kaikista normaaleista palveluiden käyttöön liittyvistä tietoturvakontrolleista (mm. salasanojen laatu, MFA)
6. Arvioi ja varmista tekoälyjärjestelmien turvallisuus ennen käyttöönottoa muun muassa huolellisella testauksella.

Tuoteomistajille, ylläpitäjille ja kehittäjille

TEE NÄIN (2/3):

7. Ymmärrä tekoälyn rajoitukset. Jokainen tekoälyjärjestelmä on suunniteltu tiettyyn tarkoitukseen ja sillä on omat rajoitteensa. Hahmota käyttämäsi tekoälyn tuottamien vastausten vinoumat. Ymmärrä nämä rajoitukset ja sovella sitä ne huomioiden.
8. Suunnittele tekoälyjärjestelmän käyttäjäkokemus ihmiskeskeisesti. Siten, että se on helppokäyttöinen ja palvelee käyttäjiensä tarpeita. Tekoälyjärjestelmän tulisi aina palvella ihmisen tarpeita, ei päinvastoin.
9. Varmista, että palvelun tuottamat ratkaisut ovat mahdollisimman eettisesti hyväksyttäviä, syrjimättömiä ja noudattavat yksityisyydensuojaa. Pyri hyödyntämään netistä löytyviä resursseja, tarkistuslistoja, standardeja, ulkopuolisia tarkastuksia sekä käyttäjien ja sidosryhmien kommentointimahdollisuuksia.
10. Ota huomioon tekoälyn vaikutus työntekijöihin. Tekoäly voi muuttaa työpaikan dynamiikkaa ja työntekijöiden rooleja. Tunnista nämä vaikutukset ja suunnittele muutokset huolellisesti.
11. Arvioi, millainen riski syntyy, jos kaikkea tekoälypalveluun syötettyä organisaation opetusdataa aletaan yhdistelemään, syntyykö tällaisen kasautumisvaikutuksen kautta salassa pidettävää tai muuten sellaista tietoa, joka voi vahingoittaa organisaatiota?
12. Kouluta henkilöstöä, jotta kaikilla työntekijöillä on turvalliseen käyttöön tarvittava tieto ja ymmärrys kehitetyn tekoälyjärjestelmän kyvyistä ja rajoista.
13. Kerro käyttäjälle selkeästi, mikäli järjestelmää toteutettaessa on hyödynnetty tai sen käyttää materiaalien tuottamiseen tai tietojen käsittelyssä tekoälyä (mihin, miten, miksi, mitä palvelua, missä laajuudessa jne.).
14. Ylläpidä avointa viestintää. Olipa kyseessä sisäinen tiimi tai ulkoiset sidosryhmät, avoin ja jatkuva viestintä on avain tekoälyn turvalliseen ja tehokkaaseen hyödyntämiseen.

Tuoteomistajille, ylläpitäjille ja kehittäjille

ÄLÄ TEE NÄIN (3/3):

15. Älä käytä tekoälyä ilman tarkoitusta. Se on vain työkalu, jonka käytön pitäisi aina palvella selkeää tarkoitusta. Älä käytä tekoälyä vain sen takia, että se on uusi ja kiinnostava teknologia.

16. Älä oleta, että tekoäly ratkaisee kaikki ongelmasi. Tekoäly voi auttaa monissa asioissa, mutta se ei ole ratkaisu kaikkeen. Älä oleta, että tekoäly voi korvata kaikki muut työkalut ja prosessit.

17. Älä unohda ihmistä tekoälyn takana. Tekoälyjärjestelmät ovat ihmisten suunnittelemia ja toteuttamia, joten huomioi tästä aiheutuvat vinoumat. Huomioi myös ihminen tekoälyjärjestelmän edessä, joka tulkitsee järjestelmän toimintaa ja tuotoksia – järjestelmän taustalla olevien näkökulmien ja tavoitteiden esiintuonti auttaa tässä tulkinnassa.

18. Älä syötä palveluun mitään salassa pidettäviä tai turvallisuusluokiteltuja tietoja, mikäli et tiedä onko järjestelmä hyväksytty niitä käsittelemään. Tekoälyjärjestelmissä on huomioitava tietojen ”muistaminen” sekä mahdollinen käyttö järjestelmän kehittämiseen, jolloin tiedot voivat tulla esiin muussa yhteydessä.
    - Älä syötä julkiseen palveluun sellaista tietoa, johon sinulla tai organisaatiolla ei ole tekijänoikeutta.
    - Älä unohda tietosuojaa. Tekoälyjärjestelmät käyttävät usein suuria määriä dataa, jota on erittäin tärkeää suojata ja käsitellä oikein.

19. Älä unohda jatkuvaa seurantaa. Tekoälyn turvallisuus ei ole kertaluonteinen tapahtuma, vaan jatkuva prosessi, joka vaatii säännöllistä seurantaa ja päivitystä.

20. Älä sivuuta käyttäjien palautetta. Käyttäjien palaute on arvokas resurssi tekoälyn turvallisuuden ja tehokkuuden parantamisessa. Älä jätä huomiotta heidän kokemuksiaan ja ehdotuksiaan.

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi