

Vastutav osakond: Strateegia- ja finantsosakond	Kinnitatud: kantsleri 09.09.2026 käskkirjaga nr 43
Protsessi koordinaator: Strateegia- ja finantsosakonna teabehalduse ja -tehnoloogia nõunik	Versioon: 01

Tehisintellekti kasutamise põhimõtted

Rahandusministeeriumis

Andmed dokumendi muutmise kohta

Versiooni nr	Käskkirja kpv ja nr	Jõustumise kuupäev	Muudatuse kirjeldus
Ver 01	09.09.2026 43	09.09.2026	Algse täisversiooni loomine.

Sisukord

1.	Eesmärk ja üldsätted.....	1
2.	Mõisted.....	1
3.	Tehisintellekti rakendused.....	2
4.	Kasutaja isiklik vastutus.....	2
5.	Peamine kasutusala	3
6.	Eetilised põhimõtted.....	3
7.	Lubatud ja keelatud tegevused tehisintellekti rakendustes	4
8.	Kontaktid ja intsidentidest teavitamine	5

1. Eesmärk ja üldsätted

- 1.1. Tehisintellekti kasutamise põhimõtted määravad Rahandusministeeriumis (edaspidi RAM) tehisintellekti kasutamise üldised nõuded ja vastutustundliku kasutamise. Põhimõtete eesmärk on aidata töötajatel kasutada tehisintellekti oma tööülesannetes nii, et oleksid maandatud andmekaitse, infoturbe, õiguslikud ja usaldusväärusega seotud riskid.
- 1.2. Põhimõtted kohalduvad kõigil juhtudel, kui töös kasutatakse tehisintellekti. See hõlmab nii vestlusrobotite kasutamist kui ka tehisintellekti sisaldavaid rakendusi, agente ja tööülesandeid automatiseerivaid lahendusi. Põhimõtete koostamisel on lähtutud Euroopa Liidu tehisintellektimäärusest ning RAM-is kehtivate infoturbe-, andmekaitse- ja IKT kasutamise nõuetest.
- 1.3. Tehisintellekti kasutades tuleb olla tähelepanelik, et kaitstud oleksid isikuandmed, ametkondlikuks kasutamiseks mõeldud teave ja juurdepääsupiiranguga andmed. Sisemine tehisintellekti rakendus (Microsoft 365 Copilot) võib vastuseid koostades arvestada kogu teabega, millele töötajal on Microsoft 365 keskkonnas juurdepääs. Seetõttu võib vastusesse sattuda ka teavet, mis on piiratud juurdepääsuga või mitteasjakohane.
- 1.4. Tehisintellekti kasutamisel tuleb enne teabe sisestamist hinnata, kas teave sobib valitud rakenduses kasutamiseks, ning järgida kehtivaid andmekaitse-, infoturbe- ja konfidentsiaalsusnõudeid.
- 1.5. Tehisintellekti väljundid võivad olla ebatäpsed, iganenud või ebausaldusväärsed. Väljundeid tuleb käsitleda abistava sisendina, mitte lõpliku või ametliku seisukohana.

2. Mõisted

- 2.1. Tehisintellekt - tehnoloogia, mis võimaldab arvutisüsteemidel täita ülesandeid, mis eeldavad tavapäraselt inimese mõtlemist näiteks teksti mõistmine ja loomine, andmete

Vastutav osakond: Strateegia- ja finantsosakond	Kinnitatud: kantsleri 09.09.2026 käskkirjaga nr 43
Protsessi koordinaator: Strateegia- ja finantsosakonna teabehalduse ja -tehnoloogia nõunik	Versioon: 01

analüüs, kokkuvõtete tegemine, ideede pakkumine või otsuste ettevalmistamise toetamine.

- 2.2. Töötaja - Rahandusministeeriumi ametnik, töötaja või muu isik, kes täidab Rahandusministeeriumi ülesandeid või kasutab tööülesannete täitmiseks Rahandusministeeriumi töövahendeid, infosüsteeme, andmeid või Microsoft 365 keskkonda.
- 2.3. Sisemine tehisintellekti rakendus (Microsoft 365 Copilot) - RAM Microsoft 365 keskkonda integreeritud lahendus, mis järgib kehtivaid andmekaitse- ja infoturbenõudeid ning on RAM-i ja Riigi IT Keskuse (edaspidi RIT) poolt heaks kiidetud.
- 2.4. Väline tehisintellekti rakendus - väljaspool Microsoft 365 turvalist keskkonda pakutavad rakendused, näiteks ChatGPT, Gemini jt, mille andmetötluse, andmekaitse ja infoturbe tingimusi ei ole RIT ja RAM heaks kiitnud.

3. Tehisintellekti rakendused

- 3.1. RAM-is kasutatakse nii sisemisi kui ka väliseid tehisintellekti rakendusi. Kasutamisele kohalduvad erinevad andmekaitse-, infoturbe- ja kasutuspiirangud.
 - 3.1.1. **Copilot Chat** on RAM kontoga ilma litsentsita kasutatav vestluspõhine tehisintellekti rakendus, mida saab kasutada üldiste küsimuste, ideekorje, mustandite koostamise, keeleabi ja avalikul teabel põhinevate päringute jaoks. Copilot Chat ei pääse ligi ega saa kasutada RAM sisest Microsofti keskkonna infot.
 - 3.1.2. **Microsoft 365 Copilot** on Microsoft 365 rakendustesse integreeritud tehisintellekti rakendus, mis on kasutatav litsentsiga ning mille abil saab koostada kokkuvõtteid, analüüsida dokumente, e-kirju, koosolekute sisu ning muud tööalast teavet, millele kasutajal on Microsoft 365 keskkonnas juurdepääs. Microsoft ei kasuta nimetatud infot mudelite arendamiseks. Microsoft 365 Copilot ei anna kasutajale täiendavaid juurdepääsuõigusi ega muuda olemasolevaid õigusi. Kuna Microsoft 365 Copiloti litsents on tööandja jaoks kulu, jälgitakse selle kasutusaktiivsust kord kvartalis väljavõttega kasutaja lõikes, et teha otsuseid organisatsiooni kuluefektiivsuse lähtekohast. Vajaduse korral võidakse vähese kasutusaktiivsusega litsents suunata kasutamiseks teisele töötajale. Microsoft 365 Copiloti kasutamisel logitakse kasutusandmeid, sealhulgas teave kasutamise aja, kasutajakonto ja kasutaja esitatud päringute ehk viipade arvu. Kasutaja sisestatud päringute sisu ja Copiloti koostatud vastuste sisu ei logita.
 - 3.1.3. **Välised tehisintellekti rakendused** asuvad väljaspool Microsoft 365 keskkonda ning nende kasutamisel võib töödelda üksnes avalikku või anonüümseks muudetud teavet.

4. Kasutaja isiklik vastutus

- 4.1. Töötaja on kohustatud tutvuma ja järgima RAM-is kehtivaid tehisintellekti kasutamise põhimõtteid ning lähtuma neist oma tööülesannete täitmisel.
- 4.2. Enne tehisintellekti kasutamist hindab töötaja, kas kasutatav teave on sellesse rakendusse sisestamiseks lubatud. Töötaja kasutab tehisintellekti minimaalsuse põhimõttel, sisestades ainult sellise teabe, mis on konkreetse tööülesande täitmiseks vajalik.
- 4.3. Töötaja vastutab tehisintellekti väljundi edasise kasutamise eest oma töös. Enne väljundi kasutamist ja edastamist ametlikus dokumendis tuleb kontrollida selle täpsust, ajakohasust ja sobivust konkreetse olukorraga. Tehisintellekti väljund ei ole ametlik allikas, tõendusmaterjal ega õiguslik alus ning otsuste tegemisel, seisukohtade

Vastutav osakond: Strateegia- ja finantsosakond	Kinnitatud: kantsleri 09.09.2026 käskkirjaga nr 43
Protsessi koordinaator: Strateegia- ja finantsosakonna teabehalduse ja -tehnoloogia nõunik	Versioon: 01

kujundamisel ja dokumentide koostamisel tuleb tugineda kontrollitud allikatele, ametlikele registritele, kehtivatele õigusaktidele ja kinnitatud dokumentidele.

- 4.4. Töötaja vastutab selle eest, et tehisintellekti abil loodud teave või dokument sisaldaks ainult vajalikku teavet ning oleks esitatud säästlikult, eesmärgipäraselt ja lugeja vajadusi arvestades.
- 4.5. Töötaja peab enne tehisintellekti kasutamist tutvuma asjakohaste juhiste ja koolitusmaterjalidega. Töötaja täiendab oma teadmisi vastavalt kasutatava rakenduse võimalustele, riskidele ja kasutuskontekstile.

5. Peamine kasutusala

- 5.1. Tehisintellekti on soovituslik kasutada eelkõige järgmistes tegevustes:
 - 5.1.1. loomingulise mõtlemise toetamisel ja ideede genereerimisel;
 - 5.1.2. rutiinsete tegevuste lihtsustamisel;
 - 5.1.3. tekstide esmasel koostamisel, ümber sõnastamisel, lühendamisel ja keelelisel toimetamisel;
 - 5.1.4. tekstide kokkuvõtete tegemisel;
 - 5.1.5. koosolekute, arutelude või märkmete põhjal kokkuvõtete koostamisel;
 - 5.1.6. tekstide tõlkimisel ja toimetamisel;
 - 5.1.7. dokumentide ja info otsimisel SharePointist, Outlookist (Microsoft 365 Copilot);
 - 5.1.8. tööprotsesside ja teenuste arendamisel ning automatiseerimisel, sealhulgas tehisintellektil põhinevate lahenduste loomisel ja kasutuselevõtul;
 - 5.1.9. õppimisel ja enesearendamisel.

6. Eetilised põhimõtted

- 6.1. Tehisintellekti ei tohi kasutada inimeste kohta otsuste tegemiseks ega soovitude, hinnangute või järjestuste koostamiseks, mis võivad mõjutada inimese õigusi. Tehisintellekt võib toetada värbamisprotsessi või teisi inimeste üle otsustamist sisaldavaid protsesse tehnilistes ja administratiivsetes tegevustes. Inimese õigusi või kohustusi mõjutavad otsused, sealhulgas värbamis- ja hindamisotsused, peavad põhinema inimese enda sõltumatul hinnangul.
- 6.2. Töötaja vastutab, et tehisintellekti väljundi kasutamisel ei kasutata kolmandate isikute autoriõigusega kaitstud materjali ilma nõuetekohase viiteta või kontrollimata, kas selle kasutamine on lubatud.
- 6.3. Tehisintellekti vastused võivad peegeldada või võimendada andmetes sisalduvaid eelarvamusi. Seetõttu tuleb kontrollida, kas vastus on tasakaalustatud, neutraalne ja põhjendatud. Vajaduse korral tuleb küsida eri vaatenurki, sealhulgas poolt- ja vastuargumente.

Vastutav osakond: Strateegia- ja finantsosakond	Kinnitatud: kantsleri 09.09.2026 käskkirjaga nr 43
Protsessi koordinaator: Strateegia- ja finantsosakonna teabehalduse ja -tehnoloogia nõunik	Versioon: 01

7. Lubatud ja keelatud tegevused tehisintellekti rakendustes

7.1. Järgnevalt on toodud, millist teavet võib erinevates tehisintellekti rakendustes kasutada andmekategooriate lõikes:

Andmekategooria selgitustega	Copilot Chat, RAM kontoga ilma litsentsita sisemine vestlusrobot	Microsoft 365 Copilot, litsentsiga sisemine tehisintellekti rakendus	ChatGPT, Gemini ja teised välised tehisintellekti rakendused
Avalik info Info, mis põhineb avalikel dokumentidel, juhenditel, protsessidel või muul avalikul infol. Näited: teenuse kirjeldus, avalik dokument, avalik andmebaas, juhendi mustand.	LUBATUD	LUBATUD	LUBATUD
Anonüümitud andmed Andmed, millest ei ole võimalik tuvastada konkreetset isikut/asutust ei otseselt ega kaudsete tunnuste abil. Näited: koondatud statistika, anonüümitud tekst, üldistatud juhtumikirjeldus.	LUBATUD	LUBATUD	LUBATUD
Isikuandmed Isikuandmed, mille põhjal saab inimese ära tunda või mille avaldamine võib kahjustada eraelu puutumatust. Näited: nimi ja juhtumi kirjeldus, isikukood, kontaktandmed koos kontekstiga.	KEELATUD	LUBATUD	KEELATUD
Eriliigilised isikuandmed Kõik tundlikud andmed, nagu tervise-, biomeetrilised, geneetilised, poliitilised või usulised andmed.	KEELATUD	KEELATUD	KEELATUD
AK-märkega või sisult AK teave Asutusesiseseks kasutamiseks märgitud teave või oma sisult piiratud juurdepääsuga teave, ka juhul kui sellele ei ole lisatud AK-märget, välja arvatud eriliigilised isikuandmed. Näited: AK-dokument, asutusesisene memo.	KEELATUD	LUBATUD	KEELATUD
Euroopa Liidu CONFIDENTIAL tasemega dokumendid	KEELATUD	KEELATUD	KEELATUD
Sisselogimisandmed ja muud juurdepääsuandmed Paroolid, PIN-koodid ja muud andmed, mille abil saab süsteemidele, rakendustele või andmetele juurde pääseda.	KEELATUD	KEELATUD	KEELATUD

Vastutav osakond: Strateegia- ja finantsosakond	Kinnitatud: kantsleri 09.09.2026 käskkirjaga nr 43
Protsessi koordinaator: Strateegia- ja finantsosakonna teabehalduse ja -tehnoloogia nõunik	Versioon: 01

8. Kontaktid ja intsidentidest teavitamine

- 8.1. Tehisintellekti kasutamisel tekkinud intsidendi või selle kahtluse korral tuleb kasutajal teavitada viivitamata. Teavitada tuleb ka juhul, kui rikkumise tegelik ulatus ei ole veel selge, kuid esineb kahtlus, et tehisintellekti rakendusse on sisestatud lubamatu teave, väljundis on avaldunud piiratud juurdepääsuga teave või kasutajal on tekkinud ootamatu juurdepääs teabele, millele tal ei peaks olema ligipääsu.
- 8.2. Tehisintellekti kasutamisel tekkinud intsidendi või selle kahtluse korral, sealhulgas lubamatu teabe sisestamisel, piiratud juurdepääsuga teabe avaldumisel või andmelekkedega seotud kahtlusel ilmnemisel, tuleb lähtuda RAM IKT teenuste kasutamise korra peatükkides 8 ja 9 sätestatud teavitamise korrast ning pöörduda RIT IT-abi poole, kontakteerudes läbi RITi iseteenindusportaali <https://itabi.rit.ee>, helistades telefoninumbril 663 6464 või kasutades e-posti aadressi itabi@rit.ee.
- 8.3. Intsidendi või selle kahtluse korral tuleb peatada tehisintellekti kasutamine asjakohases tööloigis ning vältida juhtumiga seotud väljundi edasist kasutamist või jagamist kuni asjaolude selgitamiseni.
- 8.4. Juhtumi sisust sõltuvalt tuleb kaasata ka järgmised vastutajad:
 - 8.4.1 infoturbe nõunik - infoturbeintsidendid, andmelekked või nende kahtlused;
 - 8.4.2 andmekaitse spetsialist - isikuandmete ja eriliigiliste isikuandmete töötlemise, avaldamise, edastamise või võimaliku rikkumisega seotud juhtumid;
 - 8.4.3 teabehalduse ja -tehnoloogia nõunik - tehisintellekti kasutamise põhimõtete rakendamine ning lubatud ja keelatud kasutusjuhtude tõlgendamine.
- 8.5. Teavituses tuleb võimaluse korral kirjeldada kasutatud tehisintellekti rakendust, sisestatud või avaldunud teabe liiki, juhtumi aega, võimalikku mõju ning kasutaja tehtud esmaseid toiminguid.
- 8.6. Tehisintellekti kasutamise põhimõtteid vaadatakse üle vähemalt kord aastas või varem, kui muutuvad tehisintellekti rakendused, andmetöötluse tingimused, õiguslikud nõuded või RAM-i infoturbepoliitika ja IKT kasutamise kord.