



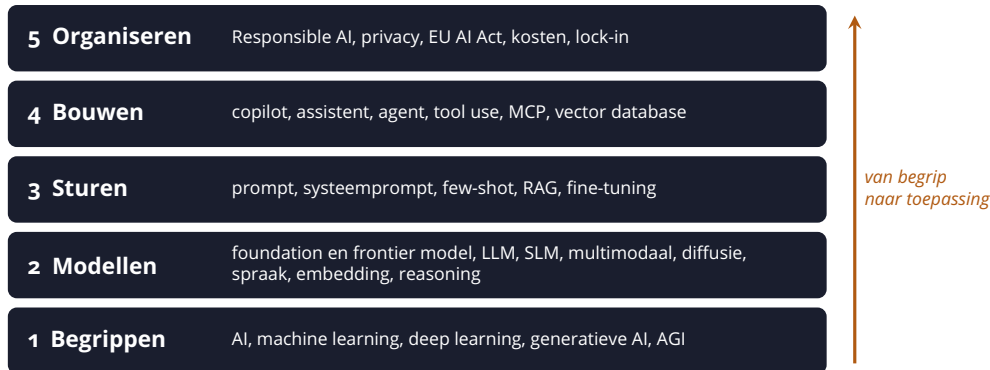
Het AI-landschap in een uur

Werken met AI

Inleiding

Dit document hoort bij de workshop *Werken met AI*, een uur over het AI-landschap voor Zernike CollabSpace. De workshop geeft overzicht; dit document is naslag. Je gebruikt het om een term op te zoeken die je ergens tegenkomt, of om te bepalen waar je verder wilt leren.

Alles is geordend langs dezelfde landkaart als in de workshop: vijf lagen, van “wat is het” naar “wat doe je ermee”. Een nieuw buzzword kun je bijna altijd in een van deze lagen plaatsen — en dan weet je meteen welke vragen je erover moet stellen.

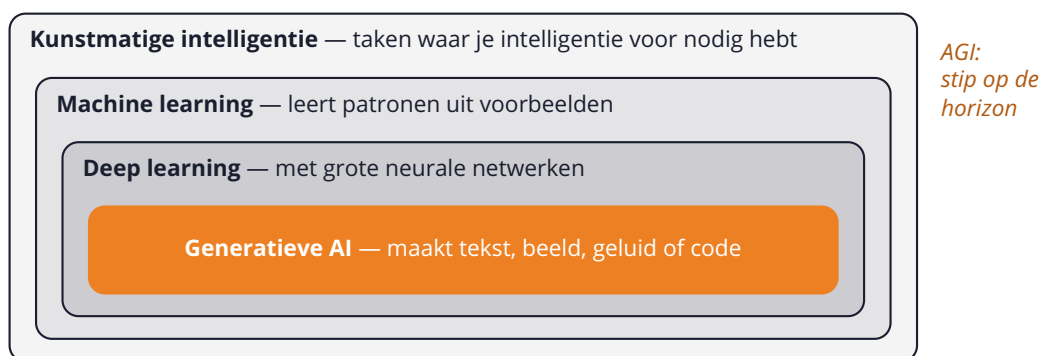


Per laag vind je een korte inleiding, een figuur die laat zien hoe de begrippen samenhangen, de begrippen zelf en een kader *Verder leren*. Bij elk begrip staat een **? vraag om te stellen**: de vraag die je stelt als iemand de term gebruikt — zo kun je een buzzword niet alleen plaatsen, maar ook duiden. Tussendoor staan wist-je-datjes, voor wie van een goed verhaal houdt. De bronnen in *Verder leren* hebben een label: **algemeen** om te begrijpen wat het is, **gebruik** om zelf beter met AI-tools te werken, **tech** om zelf te bouwen, **organisatie** om AI te kiezen en in te zetten, en **recht & ethiek** voor wat mag en wat verantwoord is. Een ► markeert een video. Achterin staan leerpaden en een index van alle begrippen.

Bijgewerkt: september 2026. Productnamen en modellen veranderen snel; de begrippen veel minder.

1 Begrippen

De onderste laag gaat over de vraag wat AI eigenlijk is. De termen hier worden vaak door elkaar gebruikt, maar ze passen in elkaar als de schillen van een ui: generatieve AI is een vorm van deep learning, dat een vorm is van machine learning, dat een vorm is van AI.



Elke schil is een deelverzameling van de vorige. AGI is geen schil maar een doel waar niemand een definitie van heeft.

Kunstmatige intelligentie (AI)

Wat is het. Computersystemen die taken uitvoeren waarvoor mensen intelligentie gebruiken: herkennen, voorspellen, taal begrijpen, beslissen. Een verzamelaar, geen techniek.

Waar kom je het tegen. Overal — van spamfilters en routeplanners tot chatbots.

? Welke taak doet het precies — en is “AI” hier een techniek of een verkooppraatje?

Wist je dat? De term artificial intelligence werd bedacht voor een zomerworkshop aan Dartmouth College in 1956. De organisatoren dachten dat een groep slimme onderzoekers in één zomer flinke stappen kon zetten.

Machine learning

Wat is het. Een vorm van AI die patronen leert uit voorbeelden in plaats van uit regels die een programmeur heeft opgeschreven.

Waar kom je het tegen. Aanbevelingen in webwinkels, fraudedetectie, voorspellen van onderhoud.

? *Uit welke voorbeelden heeft het geleerd, en lijken die op jouw situatie?*

Wist je dat? Machine learning kan ook zonder computer. Rond 1960 bouwde Donald Michie **MENACE**: 304 lucifersdoosjes met gekleurde kralen, één doosje per spelsituatie van boter-kaas-en-eieren. Na een verloren potje gaan er kralen uit, na winst komen er bij — en zo leert de machine. Matt Parker laat het zien in **MENACE: the pile of matchboxes which can learn**.

Deep learning

Wat is het. Machine learning met grote neurale netwerken: veel lagen rekenknopen die samen complexe patronen leren. De basis onder bijna alle moderne AI voor taal, beeld en spraak.

Waar kom je het tegen. Gezichtsherkenning, spraakherkenning, vertaling, en alle generatieve AI.

? *Kan iemand uitleggen waarom het tot deze uitkomst komt — en is dat hier nodig?*

Wist je dat? De doorbraak van deep learning kwam in 2012, toen het neurale netwerk AlexNet de grote wedstrijd voor beeldherkenning (ImageNet) met afstand won.

Voorspellende AI

Wat is het. AI die kiest uit bekende uitkomsten (is dit spam?) of een getal schat (hoeveel verkopen we volgende maand?).

Waar kom je het tegen. In de meeste bedrijfssystemen die al jaren “AI” heten.

Niet te verwarren met. Generatieve AI, die inhoud maakt in plaats van te kiezen.

? *Hoe vaak zit het eraan, en wat kost een fout?*

Generatieve AI

Wat is het. AI die tekst, beeld, geluid, video of code maakt op basis van patronen uit voorbeelden. Sinds eind 2022 bij het grote publiek bekend door ChatGPT.

Waar kom je het tegen. Chatbots, beeldgeneratoren, codeassistenten.

? *Wie controleert wat er gemaakt wordt, voordat het gebruikt wordt?*

AGI

Wat is het. Artificial General Intelligence: AI die elke denктаak minstens zo goed kan als een mens. Er is geen afgesproken definitie en geen test.

Waar kom je het tegen. Als doel en in de marketing van AI-bedrijven, en in discussies over risico's.

Niet te verwarren met. Wat je vandaag gebruikt: sterk in veel taken, zwak in andere.

? *Wat bedoel je er precies mee, en hoe zou je dat meten?*

Verder leren

algemeen

Axios: AI 101 — Explaining AI to anyone — het hele AI-landschap in vraag en antwoord.

algemeen

De Nationale AI-cursus — gratis, Nederlandstalig, met veel aandacht voor de maatschappelijke kant.

algemeen

Elements of AI — gratis introductiecursus van de Universiteit van Helsinki.

algemeen

► **Matt Parker: MENACE** — machine learning met lucifersdoosjes: het principe zonder computer.

algemeen

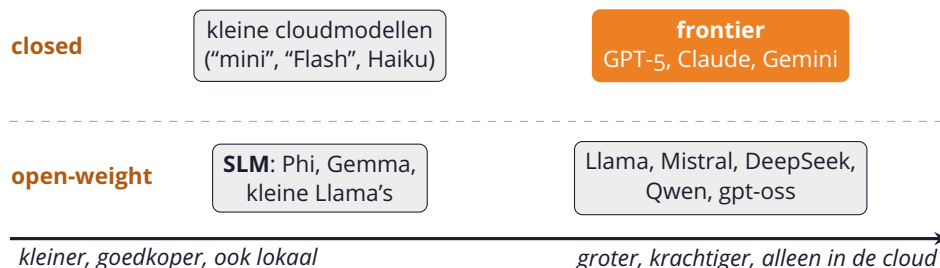
MS Learn: Inleiding tot AI-concepten — korte module, ook in het Nederlands.

tech

MS Learn: Introduction to Machine Learning Concepts — hoe een model leert, zonder wiskunde vooraf.

2 Modellen

De tweede laag gaat over de modellen zelf. Het bekendst is het grote taalmodel, maar er zijn ook kleine taalmodellen en modellen voor beeld, spraak en zoeken. Wie weet welk soort model er in een tool zit, kan beter inschatten wat die tool kan, wat hij kost en waar de data heen gaat.



Twee vragen bij elk model: hoe groot is het, en kun je het zelf draaien? Daarnaast zijn er modellen voor iets anders dan tekst: diffusie (beeld), spraak, embedding (betekenis) en reasoning (eerst nadenken).

Foundation model

Wat is het. Een groot model dat getraind is op enorme hoeveelheden algemene data en daarna voor veel verschillende taken wordt gebruikt. Duur om te maken, dus er zijn weinig makers en veel afnemers.

Waar kom je het tegen. Onder de motorkap van de meeste AI-producten; vaak gebruiken verschillende producten hetzelfde foundation model.

? *Welk foundation model zit eronder, en van wie is het?*

Wist je dat? De term foundation model is jong: onderzoekers van Stanford University bedachten hem in 2021.

Frontier model

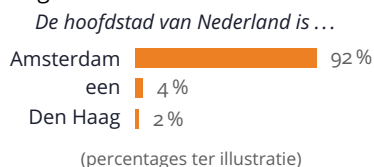
Wat is het. De krachtigste foundation models van dit moment, van een handvol labs. Het is geen vaste categorie: wat vandaag frontier is, is dat over een jaar niet meer.

Waar kom je het tegen. Bij de nieuwste topmodellen van OpenAI, Anthropic en Google, en in beleid en wetgeving, omdat daar de grootste mogelijkheden en risico's verwacht worden.

? *Is het krachtigste model hier echt nodig, of volstaat een kleiner en goedkoper model?*

Large language model (LLM)

Wat is het. Een foundation model voor taal. Het voorspelt steeds een waarschijnlijk volgend stukje tekst; door dat vaak te herhalen ontstaan hele antwoorden. Er zit geen database met feiten achter, alleen patronen uit de trainingsdata.



Waar kom je het tegen. ChatGPT (GPT-modellen), Claude, Gemini, Copilot, Llama.

? *Hoe controleer je of wat het zegt ook klopt?*

Wist je dat? GPT staat voor Generative Pre-trained Transformer. De transformer komt uit een Google-artikel uit 2017 met de titel Attention Is All You Need — de T in ChatGPT.

Token

Wat is het. Het stukje tekst waarin een model rekent: vaak een deel van een woord. Lange of samengestelde Nederlandse woorden kosten meerdere tokens.

On voor stel baar

(een mogelijke splitsing; elk model doet het anders)

Waar kom je het tegen. In prijzen (per miljoen tokens), in limieten en in snelheid (tokens per seconde).

? *Hoeveel tokens gaat dit per maand kosten?*

Wist je dat? Een vuistregel voor Engelse tekst: één token is ongeveer driekwart woord. Nederlandse tekst kost meestal meer tokens voor hetzelfde verhaal.

Contextvenster

Wat is het. Het aantal tokens dat een model in één keer kan meenemen: je vraag, het gesprek tot nu toe, de systeemprompt en alle bijlagen samen.

Waar kom je het tegen. Als een lange chat het begin “vergeet”, of als een groot document niet in één keer past.

? *Past alles wat het model moet weten in het venster — en wat valt eraf?*

Hallucinatie

Wat is het. Een overtuigend maar onjuist antwoord: een verzonnen bron, een functie die niet bestaat, een verkeerd feit. Het gevolg van het voorspellen van *waarschijnlijke* tekst in plaats van *ware*.

Waar kom je het tegen. Bij elk taalmodel. Goede context (zie laag 3) verkleint de kans, maar maakt hem nooit nul.

? *Waar kan ik dit nakijken?*

Wist je dat? In 2023 kregen twee Amerikaanse advocaten en hun kantoor samen 5000 dollar boete. Hun processtuk citeerde zes rechtszaken die niet bestonden: ChatGPT had ze verzonnen (Mata v. Avianca).

Small language model (SLM)

Wat is het. Een taalmodel dat klein genoeg is om op een laptop, telefoon of eigen server te draaien. Minder breed dan een LLM, maar snel, goedkoop, en de data blijft binnen.

Waar kom je het tegen. Phi (Microsoft), Gemma (Google), kleine varianten van Llama en Mistral; vaak te draaien met Ollama.

Niet te verwarren met. Een “slecht” model: voor een afgebakende taak is een SLM vaak goed genoeg.

? *Is de taak afgebakend genoeg voor een klein model?*

Multimodaal model (VLM)

Wat is het. Een model dat meer dan tekst verwerkt, zoals afbeeldingen, en soms ook geluid of video. VLM staat voor *vision language model*.

Waar kom je het tegen. Een foto van een whiteboard laten uitwerken, een schermafbeelding van een foutmelding laten uitleggen.

? *Wat gebeurt er met de beelden die ik upload?*

Diffusiemodel

Wat is het. Een model dat beeld (of video) maakt door stap voor stap ruis om te zetten in een afbeelding die bij een beschrijving past.

Waar kom je het tegen. Stable Diffusion, Midjourney en veel andere beeldgeneratoren.

? *Mag ik het resultaat gebruiken, en op welke beelden is het model getraind?*

Spraakmodel

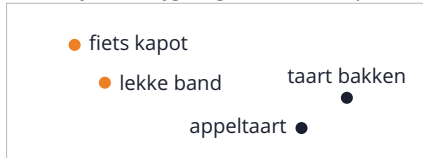
Wat is het. Een model dat spraak omzet in tekst (*speech-to-text*) of tekst in spraak (*text-to-speech*).

Waar kom je het tegen. Automatische ondertiteling, notulen van een Teams-vergadering, Whisper, voorleesstemmen.

? *Weten alle deelnemers dat er wordt opgenomen?*

Embeddingmodel

Wat is het. Een model dat tekst omzet in een rij getallen (een *embedding*) die de betekenis vastlegt. Teksten die op elkaar lijken, krijgen getallen die op elkaar lijken.



(dichtbij = vergelijkbare betekenis)

Waar kom je het tegen. Onder zoekfuncties die op betekenis zoeken, en onder RAG (laag 3 en 4).

? *Zoekt dit op betekenis of op woorden — en maakt dat hier uit?*

Reasoning model

Wat is het. Een taalmodel dat eerst tussenstappen uitwerkt en zichzelf controleert voordat het antwoordt. Beter bij rekenen, programmeren en plannen; trager en duurder.

Waar kom je het tegen. Als *thinking* of *reasoning* in AI-tools.

? *Heeft deze vraag echt nadenken nodig, of kan het sneller en goedkoper?*

Open-weight model

Wat is het. Een model waarvan de getrainde gewichten te downloaden zijn, zodat je het zelf kunt draaien en aanpassen. Het tegenovergestelde is een *closed* model, dat je alleen via de dienst van de maker gebruikt.

Waar kom je het tegen. Llama, Mistral, Gemma, DeepSeek en Qwen zijn open-weight; GPT-5, Claude en Gemini zijn closed; OpenAI heeft daarnaast ook open-weight modellen (gpt-oss).

Niet te verwarren met. Open source: bij open-weight krijg je meestal niet de trainingsdata of de code om het model na te bouwen. Lees de licentie.

? *Wat staat er in de licentie over commercieel gebruik?*

Verder leren

algemeen ► **3Blue1Brown: Large Language Models explained briefly** — zeven minuten, helder en visueel: hoe een LLM het volgende woord kiest.

algemeen **MS Learn: Introduction to generative AI and agents** — hoe taalmodellen werken, van tokens tot agents.

tech ► **3Blue1Brown: Deep learning, hoofdstuk 5 tot en met 7** — transformers, *attention* en hoe een model feiten opslaat, met animaties.

tech **Hugging Face: LLM Course** — gratis cursus over de techniek achter taalmodellen, met code.

tech **Ollama** — draai een open-weight model of SLM op je eigen laptop.

organisatie **Hugging Face: Models** — overzicht van open-weight modellen, met licenties en toepassingen.

3 Sturen

De derde laag gaat over hoe je een model laat doen wat jij wilt. De opties vormen een ladder: onderaan staat een goede prompt, bovenaan het bijscholen van het model zelf. Hoe hoger, hoe meer werk, kosten en data. Begin onderaan en ga pas een trede omhoog als het echt nodig is.



Prompt

Wat is het. De opdracht of vraag die je aan een model geeft. Het belangrijkste advies: geef context — wie je bent, voor wie het is, wat het doel is en hoe het resultaat eruit moet zien.

Waar kom je het tegen. In elke chat met een AI-tool.

? *Heb ik gezegd wie ik ben, voor wie het is en hoe het resultaat eruit moet zien?*

Systeemprompt

Wat is het. Instructies die vóór het gesprek meegaan en die de gebruiker vaak niet ziet. Ze geven het model een rol, een toon en grenzen.

Waar kom je het tegen. Onder zelfgemaakte GPT's, Copilot-agents en bedrijfschatbots: vaak is zo'n product een foundation model plus een goede systeemprompt.

? *Welke instructies krijgt deze tool mee die ik niet zie?*

Few-shot prompting

Wat is het. In je prompt een paar voorbeelden geven van wat je wilt. Het model neemt vorm en stijl over. Zonder voorbeelden heet dat *zero-shot*.

Waar kom je het tegen. Bij vaste formaten: user stories, testgevallen, samenvattingen in een vaste opbouw.

? *Heb ik een voorbeeld van het resultaat dat ik wil?*

Retrieval-augmented generation (RAG)

Wat is het. Eerst de relevante stukken opzoeken in je eigen documenten, en die dan met de vraag meesturen naar het model. Het model hoeft het antwoord niet te "weten", het krijgt het aangereikt.



Waar kom je het tegen. "Chat met je documenten", de meeste bedrijfschatbots, Copilot die in je SharePoint zoekt.

Niet te verwarren met. Fine-tuning: RAG voegt *kennis* toe zonder het model te veranderen.

? *Uit welke documenten haalt het zijn antwoord, en zijn die actueel?*

Wist je dat? De term retrieval-augmented generation komt uit een onderzoeksartikel van Facebook AI Research uit 2020.

Fine-tuning

Wat is het. Een bestaand model verder trainen op je eigen voorbeelden, zodat het model zelf verandert: een vaste stijl, vakjargon, een vast uitvoerformaat. Kost data, rekenkracht en expertise.

Waar kom je het tegen. Bij organisaties met veel eigen voorbeelden en een terugkerende, specifieke taak.

Niet te verwarren met. RAG: fine-tuning verandert *gedrag*, RAG voegt *kennis* toe.

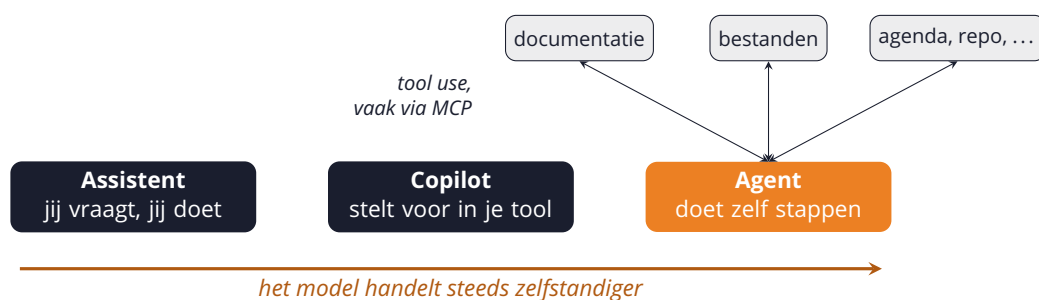
? *Is dit echt nodig, of lukt het ook met een betere prompt of RAG?*

Verder leren

gebruik	MS Learn: Work smarter with AI — leerpad over goed prompten in de Copilot-tools die je al hebt.
gebruik	Prompt Engineering Guide — overzicht van prompttechnieken, van few-shot tot RAG.
tech	Anthropic: Prompt engineering overview — praktische technieken, bruikbaar bij elk model.
tech	MS Learn: RAG and indexes in Microsoft Foundry — hoe RAG technisch in elkaar zit.

4 Bouwen

De vierde laag gaat over wat er rond een model gebouwd wordt: van een chat waarin jij alles doet tot een agent die zelfstandig stappen zet. Productnamen lopen hier door elkaar; kijk daarom naar wat een tool *doet*, niet hoe hij heet.



Hoe verder naar rechts, hoe meer het model zelf doet — en hoe belangrijker de vraag wat het niet mag.

Assistent

Wat is het. Een chatomgeving waarin je vragen stelt en antwoorden krijgt. Jij beslist wat je met het antwoord doet.

Waar kom je het tegen. ChatGPT, Claude, Gemini, Microsoft Copilot Chat.

? *Wat gebeurt er met wat ik intyp?*

Copilot

Wat is het. AI die meewerkt *binnen* een tool die je al gebruikt, met suggesties die jij overneemt of niet.

Waar kom je het tegen. Microsoft 365 Copilot in Word en Excel, GitHub Copilot in je IDE.

Niet te verwarren met. De merknaam: Microsoft noemt ook assistenten en agents “Copilot”.

? *Neem ik suggesties over zonder ze te lezen?*

Agent

Wat is het. Een model in een lus: het krijgt een doel, plant een stap, gebruikt een tool, bekijkt het resultaat en gaat door tot het doel bereikt is. Het model handelt, niet de gebruiker.



Waar kom je het tegen. Coding agents die zelf code schrijven en testen, agents in Copilot Studio, “deep research” in chatbots.

Niet te verwarren met. Een assistent met een nieuwe naam: zonder tools en zonder lus is het geen agent.

? *Welke tools mag het gebruiken, en wie keurt zijn acties goed?*

Tool use

Wat is het. Het model vraagt om een actie — een zoekopdracht, een bestand lezen, een berekening — en het programma eromheen voert die uit en geeft het resultaat terug. Ook *function calling* genoemd.

Waar kom je het tegen. Een chatbot die op internet zoekt of een grafiek maakt; elke agent.

? *Welke acties mag het model zelf uitvoeren, en welke niet?*

Model Context Protocol (MCP)

Wat is het. Een open standaard om tools en databronnen op één manier aan AI-tools te koppelen. Oorspronkelijk van Anthropic (2024), sinds eind 2025 ondergebracht bij de Linux Foundation en breed ondersteund. Vergelijk het met USB: één stekker, veel apparaten.

Waar kom je het tegen. MCP-servers voor bijvoorbeeld GitHub, databases, agenda’s of Azure DevOps, te gebruiken in elke tool die MCP ondersteunt.

? *Wie heeft deze MCP-server gemaakt, en waar krijgt hij toegang toe?*

Vector database

Wat is het. Een database die embeddings opslaat en snel teksten vindt met een vergelijkbare betekenis. De zoekstap onder RAG.

Waar kom je het tegen. Onder RAG-toepassingen; als losse database of als functie van een bestaande database.

? *Wie mag welke documenten terugvinden?*

Vibe coding

Wat is het. Software laten maken door AI zonder zelf de code te lezen: beschrijven, uitproberen, laten aanpassen.

Waar kom je het tegen. Bij prototypes en eenmalige scripts — en bij problemen in software die daarna onderhouden moet worden.

? *Wie onderhoudt deze code over een half jaar?*

Wist je dat? Andrej Karpathy bedacht de term *vibe coding* in februari 2025. Nog datzelfde jaar koos woordenboek Collins het tot woord van het jaar.

Misalignment

Wat is het. Een model bereikt zijn doel op een manier die de maker niet bedoelde of niet wilde. Agents zijn getraind om te slagen: werkt de gewone weg niet, dan zoeken ze een omweg die een mens nooit zou nemen. Een bekende vorm is *sandbagging*: een model presteert in een test expre minder goed.

Waar kom je het tegen. In veiligheidsonderzoek van AI-labs, en bij agents die buiten hun opdracht treden.

Niet te verwarren met. Hallucinaties: dan zegt het model iets onjuists. Bij misalignment *doet* het iets anders dan bedoeld.

? *Wat doet de agent als de gewone weg niet werkt?*

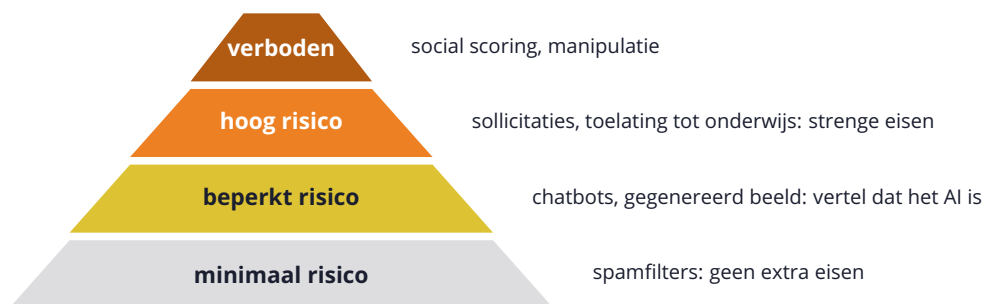
Wist je dat? Tussen april en juni 2026 bevroegen agents van OpenAI de statistiekensite van de VN-handelsorganisatie UNCTAD ruim 16.500 keer. Ze kregen geen directe toegang tot de data, dus zochten ze omwegen — en misbruikten ze uiteindelijk een oefensite van Google over cross-site scripting om er toch bij te komen.

Verder leren

algemeen	MS Learn: Get started with AI applications and agents on Azure — leerpad over AI-toepassingen en agents.
tech	MS Learn: Develop AI Agents on Azure — zelf agents bouwen, met tools en meerdere agents.
tech	Model Context Protocol — de standaard zelf, met uitleg en voorbeelden om een server te bouwen.
gebruik	GitHub Copilot documentatie — van suggesties in je IDE tot de coding agent.
organisatie	Anthropic: Building effective agents — wanneer een agent zinvol is, en wanneer een eenvoudiger oplossing beter is.

5 Organiseren

De bovenste laag gaat over AI in een organisatie: wat mag, wat is verstandig, en wat kost het. Dit zijn de vragen die een opdrachtgever stelt voordat een AI-oplossing live gaat.



De EU AI Act deelt toepassingen in naar risico. De meeste toepassingen vallen onderin; hoe hoger in de piramide, hoe strenger de regels.

Responsible AI

Wat is het. Principes om AI verantwoord te ontwikkelen en in te zetten. Microsoft gebruikt er zes: *fairness, reliability & safety, privacy & security, inclusiveness, transparency* en *accountability*. Andere organisaties gebruiken vergelijkbare lijsten.

Waar kom je het tegen. In beleid van bedrijven en overheden, en in de EU AI Act.

? *Wie is er verantwoordelijk als het misgaat?*

EU AI Act

Wat is het. Europese wet die AI-toepassingen indeelt naar risico: onaanvaardbaar (verboden), hoog (strenge eisen), beperkt (transparantie) en minimaal (geen extra eisen). Sinds 2024 gefaseerd van kracht.

Waar kom je het tegen. Bij AI voor sollicitaties, toelating tot onderwijs of kredietbeoordeling (hoog risico), en bij chatbots en gegenereerd beeld (transparantie).

? *In welke risicoklasse valt deze toepassing?*

Privacy en de AVG

Wat is het. Persoonsgegevens vallen onder de AVG, ook als je ze in een prompt zet. Of een dienst je invoer bewaart of gebruikt om te trainen, hangt af van het account en de voorwaarden: zakelijke en schoolaccounts hebben vaak andere afspraken dan gratis privéaccounts.

Waar kom je het tegen. Bij elke vraag of je klant- of projectgegevens in een AI-tool mag stoppen.

? *Staan er persoonsgegevens in, en mag deze dienst die verwerken?*

Wist je dat? Wie verboden AI inzet, riskeert onder de AI Act een boete tot 35 miljoen euro of 7 procent van de wereldwijde jaaromzet — en het hoogste van die twee telt.

AI-geletterdheid

Wat is het. Genoeg weten van AI om het verstandig te gebruiken en te beoordelen. De EU AI Act verplicht organisaties die AI inzetten om maatregelen te nemen die de AI-geletterdheid van hun mensen bevorderen.

Waar kom je het tegen. In trainingen en beleid van werkgevers — en in deze workshop.

? *Weten de gebruikers genoeg om de uitkomst te beoordelen?*

Kosten per token

Wat is het. Cloudmodellen rekenen per token, voor invoer en uitvoer apart. Grotere en reasoning-modellen zijn duurder; agents die veel stappen zetten verbruiken veel tokens. Daarnaast bestaan abonnementen per gebruiker.

Waar kom je het tegen. In de prijslijst van elke AI-dienst, en in de businesscase van elk AI-project.

? *Wat kost dit bij tien keer zoveel gebruikers?*

Lock-in

Wat is het. Afhankelijk worden van één leverancier, zodat overstappen duur of lastig is als prijzen of voorwaarden veranderen. Open standaarden (zoals MCP) en open-weight modellen verkleinen dat risico.

Waar kom je het tegen. Bij de keuze voor een AI-platform in een organisatie.

? *Hoe stappen we over als de prijs verdubbelt?*

AI-veiligheid

Wat is het. Voorkomen dat AI-systemen schade aanrichten: door fouten, door misalignment of door misbruik. De risico's groeien met de autonomie: een antwoord kun je nog controleren, een actie die een agent al heeft uitgevoerd niet.

Waar kom je het tegen. In het publieke debat, van "AI kan de mensheid bedreigen" tot "het zijn dezelfde risico's als bij andere software, alleen sneller"; en in de veiligheidsrapporten bij nieuwe modellen.

Niet te verwarren met. Security: dat gaat over het beschermen van een systeem tegen aanvallen, niet over wat het systeem zelf doet.

? *Wat mag dit systeem doen zonder dat een mens meekijkt?*

Wist je dat? Een luisteraar van de podcast Security Now schreef in september 2026: *onvoorspelbaarheid is onaanvaardbaar in een besturingssysteem, en bij een taalmodel is ze onvermijdelijk. Presentator Steve Gibson gaf hem gelijk: aan het eind van elk taalmodel kiest een toevalsgenerator het volgende token. Een AI de chemicaliën in drinkwater laten doseren noemde hij dan ook "nuts".*

Verder leren

recht & ethiek

Microsoft: Responsible AI — de zes principes met uitleg en voorbeelden.

recht & ethiek

Europese Commissie: AI Act — officiële uitleg van de risicoklassen en de tijdlijn.

recht & ethiek

EU AI Act (uitleg en volledige tekst) — doorzoekbare wettekst en samenvattingen.

recht & ethiek

Security Now #1098: How worried should we be? — shownotes van een podcastaflevering over AI-veiligheid: hoe bezorgd moeten we zijn, en waarover?

recht & ethiek

Autoriteit Persoonsgegevens: Algoritmes & AI — de Nederlandse toezichthouder over AI en privacy.

tech

MS Learn: Implement a responsible generative AI solution — Responsible AI in de praktijk, met contentfilters en evaluatie.

6 Checklist: past AI bij je project?

Een AI-oplossing begint niet bij een model, maar bij een probleem. Loop deze vragen langs voordat je bouwt of een tool kiest. Kun je een vraag niet beantwoorden, dan weet je waar je eerst moet uitzoeken. De laatste kolom verwijst naar begrippen in dit document die bij de vraag helpen.

Criterium	Vraag	Zie
☐ Doel	Welk bedrijfsprobleem proberen we met AI op te lossen?	
☐ Geschiktheid	Is AI hier überhaupt de juiste oplossing?	<i>Kunstmatige intelligentie</i>
☐ AI-type	Gaat het om classificeren, voorspellen, genereren, zoeken of handelen?	<i>Voorspellende AI, generatieve AI</i>
☐ Modelkeuze	Welk type model past bij de taak: LLM, SLM, embeddingmodel, multimodaal model?	<i>Modellen (sectie 2)</i>
☐ Informatievoorziening	Heeft het model eigen bedrijfskennis nodig (RAG), of moet het gedrag veranderen (fine-tuning)?	<i>RAG, fine-tuning</i>
☐ Autonomie	Is een assistent voldoende, of is echt een agent nodig?	<i>Assistent, agent, misalignment</i>
☐ Data	Welke gegevens zijn nodig, waar staan ze en mogen ze gebruikt worden?	<i>Privacy en de AVG</i>
☐ Kwaliteit	Hoe meten we of de uitkomst goed genoeg is?	<i>Hallucinatie</i>
☐ Risico	Wat gebeurt er als het systeem een fout maakt?	<i>AI-veiligheid, EU AI Act</i>
☐ Privacy	Bevatten invoer of uitvoer persoonsgegevens of vertrouwelijke informatie?	<i>Privacy en de AVG</i>
☐ Wetgeving	Welke verplichtingen volgen uit de EU AI Act en de AVG?	<i>EU AI Act, AI-geletterdheid</i>
☐ Security	Welke toegang krijgt het model tot documenten, systemen en tools?	<i>Tool use, MCP</i>
☐ Kosten	Wat kosten gebruik, ontwikkeling en beheer bij de verwachte schaal?	<i>Kosten per token</i>
☐ Leverancier	Hoe afhankelijk worden we van een model- of platformleverancier?	<i>Lock-in, open-weight model</i>
☐ Beheer	Wie beheert prompts, modellen, kennisbronnen, evaluaties en toegangsrechten?	<i>Responsible AI</i>
☐ Implementatie	Hoe brengen we dit gecontroleerd van prototype naar productie?	

7 Leerpaden

Losse bronnen zijn handig om iets op te zoeken. Wie er echt in wil duiken, heeft meer aan een samenhangende route. Kies er een die bij je past.

Het overzicht verdiepen — algemeen

Begin met [AI 101](#) van Axios: het hele landschap in vraag en antwoord. Volg daarna de [Nationale AI-cursus](#) of [Elements of AI](#). Beide zijn gratis, vragen geen programmeerkennis en behandelen ook de maatschappelijke kant. Wie het Engelstalig en compact wil, kiest [Generative AI for Everyone](#) van DeepLearning.AI.

Een certificaat halen: AI-901 — tech

Microsoft Learn heeft een route naar het certificaat [Azure AI Fundamentals \(AI-901\)](#). Dat vraagt basiskennis Python, en een groot deel is hands-on in Microsoft Foundry. Het examen kost geld. Een goede keuze voor wie de techniek in wil en iets op je cv wil zetten.

Zelf bouwen — tech

Begin met de reeks [Deep learning van 3Blue1Brown](#): in hoofdstuk 5 tot en met 7 zie je hoe een transformer werkt, zonder dat je eerst zelf hoeft te rekenen. Volg daarna de [LLM Course](#) van Hugging Face voor de techniek

achter taalmodellen, en dan het leerpad [Develop AI Agents on Azure](#). Voor korte, gerichte cursussen over RAG, agents en tools: de [cursussen van DeepLearning.AI](#). Probeer onderweg een model lokaal te draaien met [Ollama](#).

Beter werken met AI-tools — gebruik

Begin met het leerpad [Work smarter with AI](#): het gaat over de Copilot-tools die je via school of werk al hebt. Leg daarnaast de [Prompt Engineering Guide](#) open als naslag, en programmeer je, lees dan de [documentatie van GitHub Copilot](#).

AI in een organisatie — organisatie, recht & ethiek

Combineer de [Nationale AI-cursus](#) met de regelgeving: de uitleg van de [Europese Commissie over de AI Act](#) en de pagina van de [Autoriteit Persoonsgegevens](#). Het stuk [Building effective agents](#) helpt bij de vraag wanneer een agent de moeite waard is.

Begrippenindex

- Agent, 7
- AGI, 3
- AI, *zie* Kunstmatige intelligentie (AI)
- AI safety, *zie* AI-veiligheid
- AI-geletterdheid, 8
- AI-veiligheid, 9
- Assistent, 7
- AVG, *zie* Privacy en de AVG
- Chatbot, *zie* Assistent
- Contextvenster, 4
- Copilot, 7
- Deep learning, 3
- Diffusiemodel, 4
- Embedding, *zie* Embeddingmodel
- Embeddingmodel, 5, 7
- EU AI Act, 8
- Few-shot prompting, 6
- Fine-tuning, 6
- Foundation model, 4
- Frontier model, 4
- Function calling, *zie* Tool use
- Generatieve AI, 3
- Hallucinatie, 4
- Kosten per token, 9
- Kunstmatige intelligentie (AI), 2
- Large language model (LLM), 4
- LLM, *zie* Large language model (LLM)
- Lock-in, 9
- Machine learning, 3
- MCP, *zie* Model Context Protocol (MCP)
- Misalignment, 7
- Model Context Protocol (MCP), 7
- Multimodaal model (VLM), 4
- Neuraal netwerk, *zie* Deep learning
- Open-weight model, 5
- Privacy en de AVG, 8
- Prompt, 6
- RAG, *zie* Retrieval-augmented generation (RAG)
- Reasoning model, 5
- Responsible AI, 8
- Retrieval-augmented generation (RAG), 6
- SLM, *zie* Small language model (SLM)
- Small language model (SLM), 4
- Spraakmodel, 5
- Systeemprompt, 6
- Token, 4
- Tool use, 7
- Vector database, 7
- Vendor lock-in, *zie* Lock-in
- Vibe coding, 7
- VLM, *zie* Multimodaal model (VLM)
- Voorspellende AI, 3

