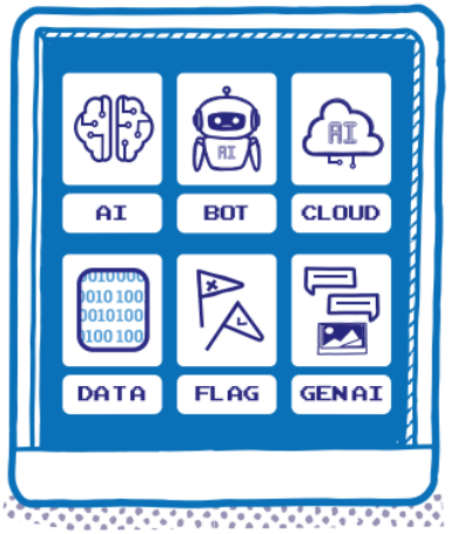
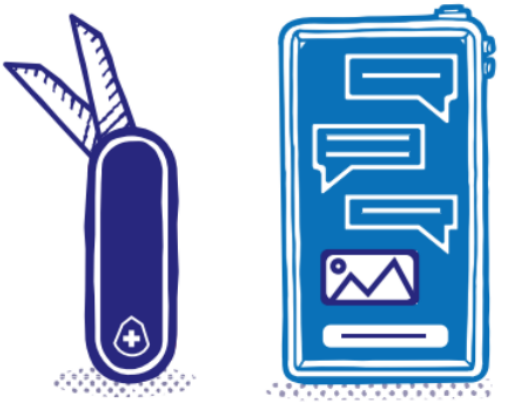
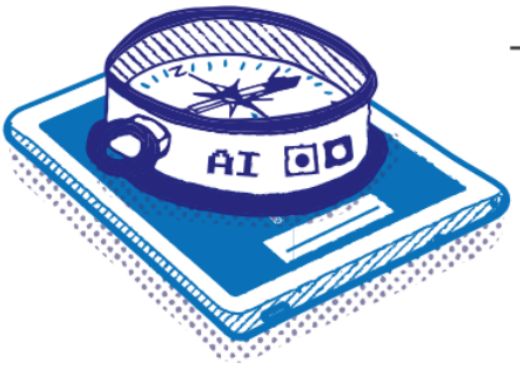
Grip op de

AI Act





De gids over de AI Act
met tips, adviezen en
stappenplannen



Geschreven door:
Joris Hutter, Sander van der Smissen,
Lenna Essink en Alfonso Okué

Wolters Kluwer

Grip op de AI Act

Joris Hutter
Sander van der Smissen
Lenna Essink
Alfonso Okué

Illustraties:
Anouk Paap
Immie Ooijevaar

Wolters Kluwer
Deventer – 2025

Inhoud

1 Inleiding

De wijze waarop artificiële intelligentie (AI) onze manier van leven beïnvloedt, wordt steeds duidelijker zichtbaar. Ook voor organisaties heeft het grote impact op hoe zij diensten aanbieden en taken uitvoeren. Het schept nieuwe mogelijkheden om activiteiten sneller, effectiever en persoonlijker uit te voeren. Tegelijkertijd zien we dat de technologie en het gebruik daarvan ook negatieve impact kan hebben in de vorm van leed en schade bij personen, groepen, organisaties, samenleving en omgeving.

De AI Act heeft als eerst tot doel om mensgerichte en betrouwbare artificiële intelligentie (AI) te bevorderen. Daarbij moet een hoog niveau van bescherming van de gezondheid en de veiligheid bestaan. Er moeten voldoende waarborgen zijn om de schadelijke gevolgen van AI-systemen tegen te gaan. De officiële Nederlandse naam is Verordening Artificiële Intelligentie, maar in dit boek gebruiken wij de naam AI Act. Deze AI Act is vanaf augustus 2024 van toepassing en wordt stapsgewijs tot augustus 2026 in werking gesteld. Begin 2025 dienen de 'verboden toepassingen' gestopt te zijn. In de loop van dat jaar nemen de plichten toe en is er bijvoorbeeld een vorm van managementsturing op AI vereist.

Veel organisaties gebruiken AI (bewust of onbewust) in hun huidige dienstverlening. Daarnaast bestaan er op veel plekken wensen om meer AI in te zetten om de bedrijfsprocessen te verbeteren. Maar hoe verhoudt deze nieuwe wetgeving (de AI Act) zich dan tot zulke organisaties? De complexiteit van AI als technologie en de nieuwe wetgeving kan organisaties het gevoel geven dat zij de grip hierop verliezen. Dit boek reikt praktische handvaten aan voor het omgaan met AI en de AI Act. Hiermee kan op korte termijn al een (vliegende) start gemaakt worden om aan de slag te gaan met verantwoorde inzet van AI.

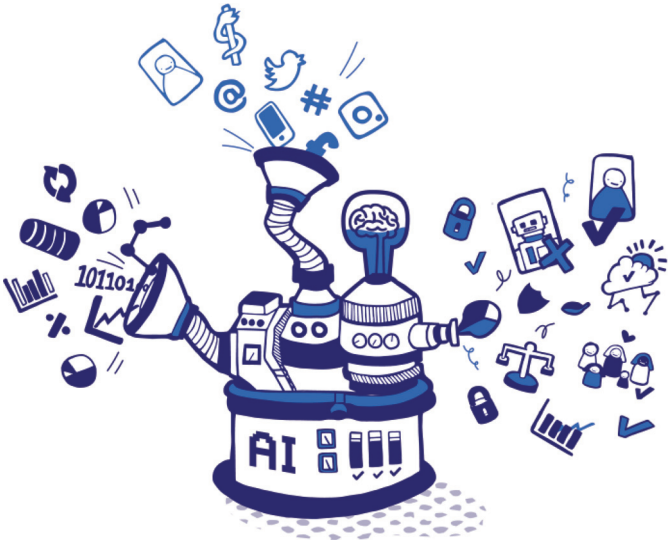
Om de AI Act goed te begrijpen wordt er in het boek eerst aandacht besteed aan artificiële intelligentie als technologie. Wat is het nou eigenlijk en voor welke toepassingen wordt het ingezet? Vervolgens plaatsen we dit in de context van de verschillende Europese digitaliseringswetten, want AI wordt door meer wetten gereguleerd dan enkel de AI Act. Daarna wordt de stap gemaakt richting de AI Act en vervolgens wordt er uitgebreid stilgestaan bij de definitie, de reikwijdte, de relevante rollen, de waardeketen en de risicocategorieën. Deze onderdelen zijn essentieel om uiteindelijk de vertaling te maken naar *compliance*. Nadat *compliance* is uitgelegd, wordt in het laatste hoofdstuk tijd voor de praktische aanpak genomen. Hierin wordt een voorstel gedaan voor een aanpak om in een korte

tijd aan de slag te gaan met de inrichting van AI governance. Vanaf dat moment kan er bestuurlijk op AI-ontwikkelingen in de organisatie worden gestuurd en verantwoording worden afgelegd.

Dit boek is vooral geschreven voor lezers die AI in hun organisatie gaan gebruiken en daarvoor een AI-systeem implementeren. In de AI Act wordt die rol 'gebruiksverantwoordelijke' genoemd. De maker van het AI-systeem wordt 'aanbieder' genoemd en deze aanbieder heeft juist weer andere verplichtingen. Met dit boek willen wij een praktisch hulpmiddel aanbieden om de AI Act te begrijpen en volgens de geest toe te passen. We geven de algemene lijn aan vanuit de AI Act en zijn niet altijd 100% compleet op specifieke situaties en uitzonderingen. Raadpleeg daarom rechtstreeks de AI Act als je vermoedt dat in jouw organisatie zo'n uitzondering van toepassing is. Op plaatsen waar dat nodig is, verwijzen we naar artikelen of overwegingen van de AI Act. We baseren ons op de AI Act van augustus 2024. In de loop van 2025 zullen er aanvullende richtlijnen verschijnen vanuit het Europese adviesorgaan en ook vanuit de markt zullen ongetwijfeld verdere richtlijnen ontstaan.

De begripsopbouw van de AI Act en wat daarbij de verplichtingen zijn wordt in de hoofdstukken 2 tot en met 6 gedaan. Hoofdstuk 7 'Aan de slag', geeft handvatten en aandachtspunten om hier vorm aan te geven. Dat hoofdstuk start met een samenvatting van de eerdere hoofdstukken met een verwijzing naar paragrafen waar meer uitleg te vinden is.

Ofschoon de auteurs dat kort hadden overwogen is het boek niet door AI gegenereerd, maar nog op een klassieke wijze samengesteld en geschreven.



2 Technologie

Om de AI Act goed te begrijpen is het belangrijk om te weten wat er wordt bedoeld met artificiële intelligentie. Het is namelijk een verzamelnaam waar verschillende onderdelen onder vallen. In dit hoofdstuk wordt uitgelegd wat AI is en wat herkenbare toepassingen zijn.

2.1 Wat is artificiële intelligentie (AI)?

AI is een breed begrip en bevat toepassingen die taken kunnen uitvoeren waarvoor voorheen menselijke intelligentie vereist was. Het vertoont mensachtige vaardigheden zoals redeneren, leren, plannen en vormen van creativiteit. Met AI worden verbanden gelegd tussen veel data, gestructureerd en ongestructureerd. Hieruit worden uitkomsten tot stand gebracht die bruikbaar zijn om inzichten te genereren of problemen uit het dagelijks leven op te lossen. Ook kunnen sommige AI-systemen taal verwerken en daar betekenis uit halen of beelden en stemmen herkennen en deze ook weer genereren. Het kan lijken dat een AI-systeem iets begrijpt, maar dat is een misvatting en valkuil. Een AI-systeem legt goede of minder geslaagde verbanden tussen data maar 'begrijpt' of 'voelt' niets.

Om AI verder uit te leggen worden weleens de volgende definities gebruikt:

- Het gebruik van slimme algoritmes. Een algoritme is een soort wiskundige formule die je kan vergelijken met een instructie of stappenplan.
- De nabootsing van menselijke intellectuele vermogens of van complexe menselijke vaardigheden door computers of machines.
- Technologie die op een voorspellende manier met de omgeving kan omgaan.
- Systemen die intelligent gedrag vertonen door hun omgeving te analyseren en met enige graad van autonomie actie ondernemen om specifieke doelen te bereiken.

AI heeft in ieder geval te maken met een hoge mate van rekenkracht, data en uitkomsten die van toepassing zijn op de omgeving. Dit kan de fysieke omgeving zijn zoals een robot die in een optimale route artikelen uit een magazijn oppakt, of het kan een virtuele omgeving zijn zoals bijvoorbeeld een gepersonaliseerde aanbeveling. Denk hierbij aan een streamingdienst die aanbevelingen doet voor andere films of series die waarschijnlijk passen bij de kijker.

Een deel van de AI-systemen is in staat om de uitkomsten in bepaalde mate aan te passen en te verbeteren. Hierbij 'leren' zij vanuit de uitgevoerde actie. Op deze categorie van AI-systemen is de AI Act van toepassing. De AI Act benoemt een AI-systeem als volgt: 'een op een **machine** gebaseerd systeem dat is ontworpen om met verschillende niveaus van **autonomie** te werken en dat na het inzetten ervan **aanpassingsvermogen** kan vertonen, en dat, voor expliciete of impliciete **doelstellingen**, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die **van invloed** kunnen zijn **op fysieke of virtuele omgevingen**'.

AI en filebestrijding

Verkeersmanagement stimuleert een optimale verkeersdoorstroming. Actuele files worden bestreden, maar ook toekomstige verstoringen worden voorspeld en beheerd. Dat is belangrijk voor de leefbaarheid, de veiligheid, economie en het milieu. Dit wordt gedaan op basis van veel *realtime* verkeersgegevens en voorspellende filemodellen. Die verkeersgegevens komen vanuit de verkeersinfrastructuur, maar ook vanuit voertuigen. De output bestaat uit verkeersinformatie opdat weggebruikers hun route en gedrag kunnen aanpassen, maar ook via verkeerslichten en andere geleidingssystemen voor een betere doorstroming. In de Verenigde Staten zijn al proeven uitgevoerd waar AI-aangedreven voertuigen met cruisecontrol-algoritmen de snelheid optimaliseren op basis van de verkeersomstandigheden en daarmee ook het gedrag van andere weggebruikers beïnvloeden.

2.2 Regelgebaseerde AI, *machinelearning* en *deep learning*

De betekenis van AI kan abstract en lastig te begrijpen zijn, maar ondertussen wordt het gebruikt in veel toepassingen in het dagelijks leven. Zo kan het onderdeel zijn van softwareapplicaties zoals vertaalprogramma's, klantenservice of toepassingen om de logistiek te optimaliseren. Maar AI kan ook ingebouwd zijn in fysieke producten zoals zelfrijdende auto's, robots of apparaten in huis zoals *smart speakers*. Deze toepassingen zijn bekend, maar hoe komen deze systemen tot nuttige antwoorden? Om dit uit te leggen bespreken we drie verschillende vormen van AI: regelgebaseerde AI, *machinelearning* en *deep learning*.

In de jaren tachtig van de twintigste eeuw kwamen de eerste regelgebaseerde AI-systemen op. Deze vorm van AI is in de afgelopen twintig jaar sterk gegroeid. Regelgebaseerde AI bestaat uit vastgelegde regels en formules die worden toegepast op de inputdata. Dus als X en Y ieder een bepaalde waarde heeft dan wordt Z de uitkomstwaarde. Dit kunnen complexe beslisbomen, lineaire toepassingen of

statistische toepassingen zijn. Ook robots functioneren bijna altijd op basis van vastgelegde regels. Het gaat dan om geprogrammeerde systemen die geen aanpassingsvermogen hebben. Via de code is verklaarbaar hoe zij tot een uitkomst of actie komen en zij zijn daarmee ook goed uitlegbaar. Een voorkomende toepassing is een expertsysteem. Deze bestaat uit een kennisbasis in een specifiek domein zoals gezondheidszorg, financiële dienstverlening of engineering. Op basis van een vraag of input van de gebruiker komt het expertsysteem op basis van regelgebaseerde logica met een gepast antwoord.

In de jaren die volgden zijn er verschillende veranderingen geweest die ervoor hebben gezorgd dat AI nog meer succes heeft behaald. Ten eerste heeft de regelgebaseerde AI plaatsgemaakt voor statistische modellen. Daarnaast is de rekenkracht enorm toegenomen en is er meer data beschikbaar dan ooit. Hierdoor is er ruimte ontstaan voor wat we *machinelearning* noemen. Dit zijn algoritmes en statistische modellen die verwerkte data kunnen gebruiken om vervolgens nog beter te presteren. Dit is wat er wordt bedoeld met AI die in staat is om te leren. Patronen in heel grote datasets worden gevonden en gebruikt om vervolgens nog gerichter output te leveren, zoals bijvoorbeeld voorspellingen. Een voorwaarde is wel dat er gestructureerde data beschikbaar is.

AI en kankeronderzoek

AI helpt bij het vroegtijdig herkennen van kanker. Via beeldherkenning en achterliggende modellen wordt een nauwkeuriger en consistenter beeld op mogelijke kankercellen opgebouwd, dan wat met een geoefend oog mogelijk is. Vanuit dit beeld kan de arts verdere acties uitvoeren.

Ook kan AI worden toegepast bij het opstellen van behandelplannen. Op basis van beeldkenmerken, genetische data en klinische data van de patiënt kan het AI-model voorspellen wat voor die patiënt de meest effectieve behandeling en de te verwachten levenswinst is.

Deep learning is een onderdeel van *machinelearning* maar bestaat uit vele niveaus van algoritmes die samen een 'neuraal netwerk' vormen. Dit wordt zo genoemd omdat het gelijkenissen heeft met het menselijk brein. *Deep learning* werkt met miljoenen datapunten en het ontwikkelen van een *deep learning*-model is daarmee veel kostbaarder dan bij *machinelearning*. *Deep learning* werkt zowel met gestructureerde gegevens, numerieke waarden maar ook met beelden, vormen, tekst, taal en geluid. De resultaten van *deep learning* zijn vaak moeilijk uitlegbaar omdat er veel verschillende berekeningen plaatsvinden om tot een output te komen.

AI en klantenservice

De chatbox en ook de *voice response* bij customerservice zijn volop in ontwikkeling. Deze gebruiken taalmodellen om de geschreven of de ingesproken tekst te verwerken en interpreteren. Daarbij wordt ook onderzocht wat de emotie is van de klant, om daar gerichter mee om te gaan, bijvoorbeeld door het gesprek te leiden naar een *call agent*.

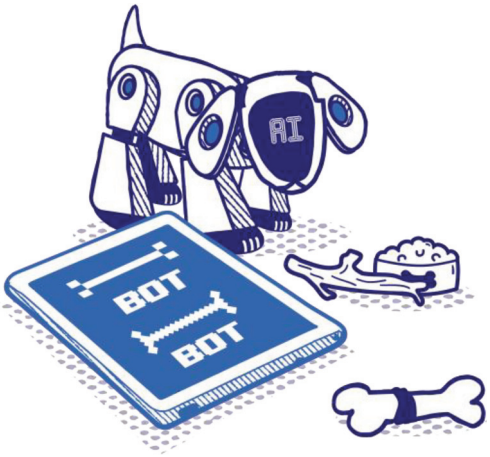
Veel standaardvragen en benodigde acties kunnen via deze *interface* worden beantwoord en uitgevoerd. Dit gebeurt met behulp van modellen en organisatiedata die op die vragen zijn ingericht en zich daarop ook kunnen verbeteren. Bij een goede inrichting en uitvoering leidt dit voor de eindklant tot een snelle en effectieve beantwoording die altijd beschikbaar is. Voor de organisatie leidt dit tot lagere kosten.

Ook is het mogelijk om de interactie met de klant steeds persoonlijker te maken op basis van de gegevens van de klant die bij de organisatie bekend zijn.

Een belangrijk onderdeel van AI is dus het zelflerende vermogen. Dit zelflerende vermogen wordt opgebouwd door een model te trainen met data. In de praktijk kun je de manieren waarop AI leert onderverdelen in vier verschillende categorieën:

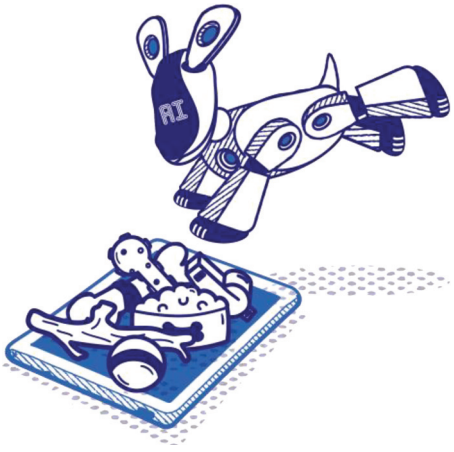
1. Supervised learning

Bij *supervised learning* is het belangrijk dat de data die zijn gebruikt om te trainen worden gelabeld. Bijvoorbeeld in het geval dat de trainingsdata uit afbeeldingen van honden bestaat met steeds het label hond, dan zal een goed getraind model bij een nieuwe afbeelding 'geleerd' hebben hoe een hond te classificeren is. Deze modellen worden gebruikt om inputdata te classificeren, bijvoorbeeld het herkennen van verkeersborden bij zelfrijdende auto's. Een belangrijke vereiste voor *supervised learning* is dat er veel data beschikbaar zijn en daarnaast moeten deze data dus ook al over een label beschikken. Dit is niet altijd aanwezig en het is kostbaar om dit samen te stellen.



2. *Unsupervised learning*

In tegenstelling tot *supervised learning* wordt er bij *unsupervised learning* data gebruikt die niet gelabeld zijn. In een bak met allemaal data gaat het model zoeken naar statistische overeenkomsten, verschillen of relaties. Het model geeft dan in de output een clustering van data die op bepaalde kenmerken veel op elkaar lijken. Als data in bepaalde relaties tot elkaar kunnen staan, kan het model die relaties ontdekken. Dit soort systemen worden bijvoorbeeld gebruikt voor het herkennen van klantsegmenten op basis van eigenschappen en gedrag van die klanten. Een andere toepassing is het signaleren van afwijkingen en onregelmatigheden bij fraudedetectie.



3. Reinforcement learning

Bij *reinforcement learning* staat *trial-and-error* centraal als methode om te trainen. Het model geeft een bepaalde uitkomst waarna iemand aangeeft of dat een juiste of onjuiste uitkomst is. Op deze manier 'leert' het model steeds beter wat goed of fout is.

4. Semi-supervised learning

Bij *semi-supervised learning* is sprake van een combinatie van gestructureerde en ongestructureerde data. Het (kleine) deel dat gestructureerd en gelabeld is helpt bij het classificeren van de rest van de data waarbij geen label aanwezig is door verbanden te leggen tussen de data.

Uitbesteden AI-labeling naar Global South

Data labeling is de activiteit om gegevens te identificeren en te taggen om daarmee *machinelearning* modellen te trainen. Dit gaat om beelden, teksten, audio of video waaraan een of meerdere relevante labels worden verbonden om context te bieden. Dit is vanzelfsprekend een heel arbeidsintensief karwei. Als het om een beperkte webshop of catalogus gaat, dan is de organisatie vaak zelf nog wel in staat om die data te labelen.

Veelal wordt echter dat labelen uitbesteed naar lagelonenlanden. De verdiensten zijn daar laag, ook in verhouding tot het loonniveau in die landen. Ook al geven opdrachtgevers aan dat hiermee werkgelegenheid wordt geboden, wordt daar niet echt geprofiteerd van de AI-technologie.

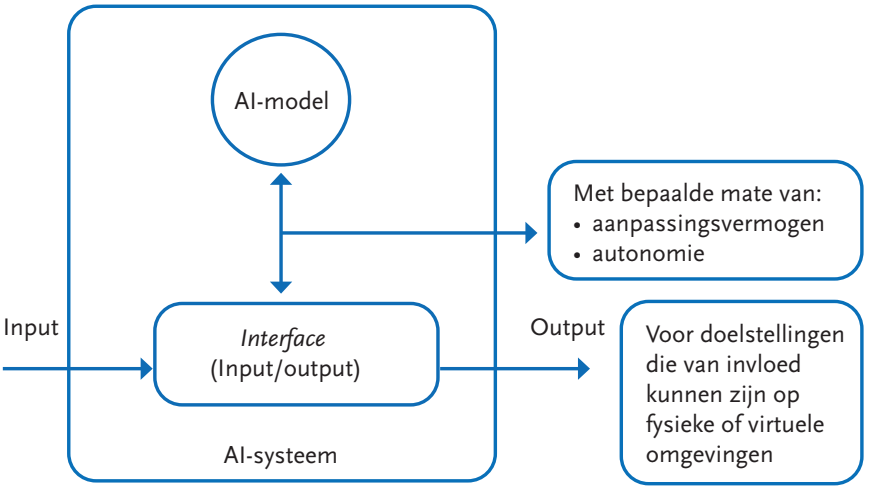
2.3 AI toepassen om problemen op te lossen

Zodra een model 'getraind' is kan het gebruikt worden in verschillende systemen. Dit kunnen simpele of meer complexe toepassingen zijn. Over het algemeen is AI in staat om specifieke en concrete problemen op te lossen. Dit wordt ook wel gecategoriseerd als '**smalle AI**'. Dit kan iets alledaags zijn als een handschrift herkennen of een aanbeveling voor een volgende serie op Netflix. Complexere toepassingen zijn het detecteren van kankercellen in medische beelden, maar ook in die gevallen is de taak die AI heeft gekregen concreet en 'simpel'.

Daarnaast heb je AI voor algemene doeleinden. Dit wordt ook wel *General Purpose AI* (GPAI) genoemd en soms ook een *foundation model*. Dit is technologie die geen specifiek doel heeft, maar kan worden ingezet voor uiteenlopende toepassingen. De modellen vormen de fundering (*foundation*) voor diverse uiteindelijke toepassingen. Zo kan het basis zijn voor systemen in zowel de financiële wereld als het onderwijs, of het wordt gebruikt door tolken/vertalers én voor *content creation* en marketing. Een voorbeeld is het Large Language Model GPT-4 van OpenAI. Een dergelijk model is getraind met zeer veel data.

Tegelijkertijd gaan er veel discussies rond over of AI slimmer zou zijn dan mensen. Bij '**brede AI**' zou AI in staat zijn om verschillende taken autonoom uit te voeren en dan ook nog eens beter dan een mens. Hoewel toepassingen als ChatGPT ons laten zien dat er veel mogelijk is, is het niet zo dat AI daadwerkelijk de menselijke intelligentie kan evenaren.

AI bestaat uit verschillende (technische) onderdelen die er samen voor zorgen dat het een bruikbare toepassing wordt die een specifiek probleem kan oplossen. Deze onderdelen lichten we hieronder verder toe.



Onderdelen van een AI-systeem

AI-model

Een AI-model bestaat uit algoritmen die zijn getraind op bepaalde data. De eerdergenoemde manieren van leren (zoals *supervised learning*) zorgen ervoor dat er uiteindelijk een model ontstaat dat nieuwe inputdata kan beoordelen en op basis daarvan output kan genereren. Kenmerkend voor een AI-model is ook dat nieuwe output hergebruikt kan worden om het model verder mee te trainen. De verbanden die zijn gelegd door het AI-systeem worden dan in een volgende analyse weer meegenomen. Dit wordt ook wel de *feedbackloop* genoemd. Het AI-systeem kan daarmee steeds betere output leveren. Maar als er een vertekening zit in de data of de manier hoe het AI-systeem conclusies trekt uit die data, dan wordt die vertekening geleidelijk steeds groter.

Een AI-model bestaat vaak uit verschillende soorten algoritmen en modellen die specifieke taken uitvoeren. Een AI-model met *machinelearning* en aanpassingsvermogen kan voor diverse taken regelgebaseerde AI gebruiken.

Van grote AI-modellen zijn er online zogenoemde *model cards* te vinden. Dit zijn documenten waarin bepaalde informatie over het AI-model wordt opgenomen. Bijvoorbeeld welke data voor de input zijn gebruikt, wat de output is, wat de output is, wat de toepassingen zijn en welke beperkingen het model kent.

AI-systeem

Het model wordt uiteindelijk gebruikt in een specifiek systeem met een input en een output. De input kan van een gebruiker komen of van een ander systeem. En

Grip op de AI Act

Artificiële intelligentie ontwikkelt zich razendsnel en opent een wereld aan mogelijkheden. Tegelijkertijd zijn er ook risico's die we onder controle moeten houden. De AI Act is in werking getreden en vanaf 2026 moeten alle organisaties die AI inzetten aan deze wetgeving voldoen.

Maar wat is AI eigenlijk en welke verplichtingen volgen er uit de AI Act? Dit boek is voor iedereen die verantwoordelijkheid draagt voor de implementatie van AI binnen de organisatie. Grip op de AI Act vertaalt complexe wetgeving naar heldere taal en biedt handvatten om direct aan de slag te gaan. Door nu al te starten met een duidelijke visie en een doordacht plan van aanpak, zorg je stap voor stap voor meer grip op het gebruik van AI.

"Dit boek over AI is een onmisbare gids voor iedereen die de toekomst wil omarmen. Een inspirerend werk dat je helpt om met vertrouwen de AI-revolutie tegemoet te treden."
Marlon Domingus - Functionaris Gegevensbescherming
Erasmus Universiteit Rotterdam

"De titel overdrijft niet. Dit boek doet precies wat de titel suggereert: op een no nonsens manier de AI Act uitleggen én praktische handvatten geven. Grip op de AI Act, een aanrader."
Jan Pronk - Manager BI&AI Haga Ziekenhuis

"Het boek Grip op de AI Act combineert juridische inzichten met concrete stappen, biedt meer verdieping dan gebruikelijk en reikt praktische handvatten voor organisaties en verschillende professionals aan om verantwoord met AI aan de slag te gaan."
Martijn Groenewegen - CIO Gemeente Eindhoven

www.wolterskluwer.nl

9 789013 180107

Wolters Kluwer