

**VERDONCK
KLOOSTER &
ASSOCIATES**
A HIGHBERG COMPANY

 **JPR**
advocaten

ChatGPT: Impact & Implementatie

Luuk Wassink (JPR), Yaşar Bayram (JPR), Sabine Steenwinkel-
den Daas (VKA) & Sebastiaan Bouthoorn (VKA)



Camera uit



Microfoon uit



Vragen stellen in de chat



De meeting wordt opgenomen



Na afloop ontvangt u de slides
en een Q&A

Even kennismaken



Yaşar Bayram
Advocaat
IE, ICT & Privacy
bayram@jpr.nl
06 - 82091996



Luuk Wassink
Juridisch medewerker
IE, ICT & Privacy
wassink@jpr.nl
06 - 45378511



Sebastiaan Bouthoorn
Adviseur Data & AI
sebastiaan.Bouthoorn@vka.nl
06 - 51580537



**Sabine Steenwinkel-den
Daas**
Adviseur Data & AI
sabine.dendaas@vka.nl
06 - 86813931

VERDONCK
KLOOSTER &
ASSOCIATES

A HIGHBERG COMPANY

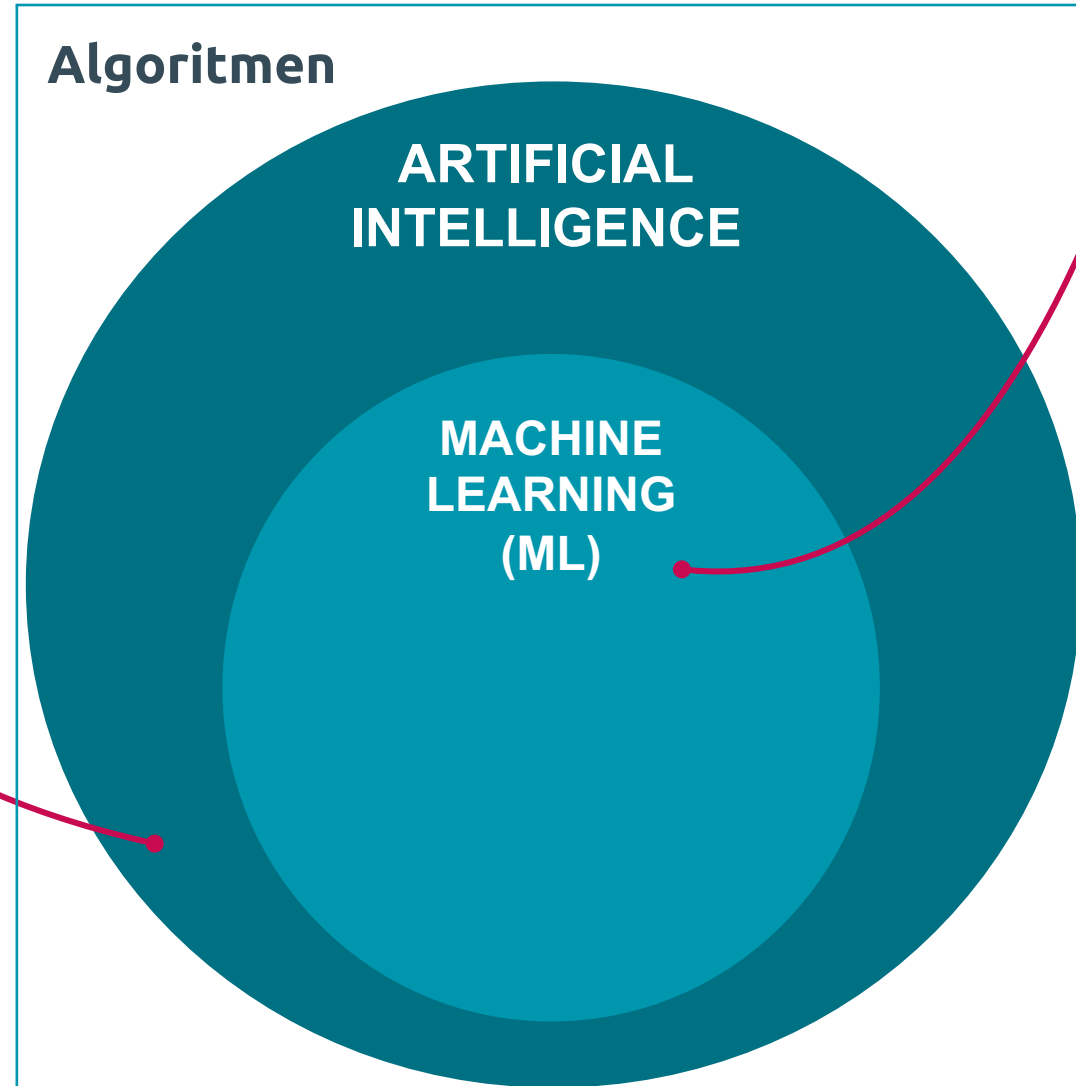


JPR
advocaten

General Purpose AI

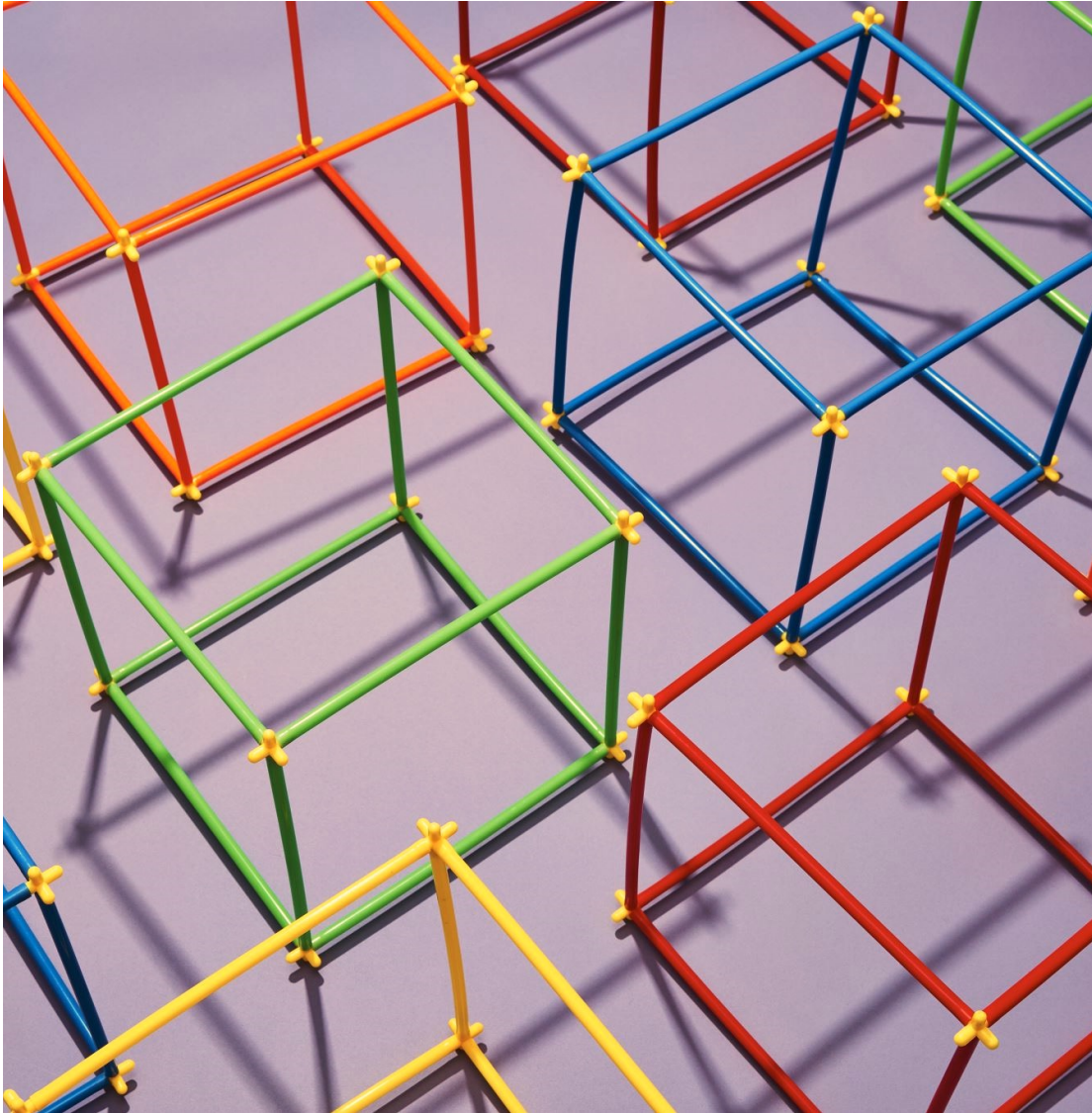
Algoritmen, Artificiële Intelligentie (AI) versus Machine Learning (ML)

Artificiële Intelligentie (AI)
Elke technologie / techniek waarmee computers intelligentie kunnen nabootsen



Machine Learning (ML)
Deelverzameling van AI-technieken die statistische methoden gebruiken om machines in staat te stellen om een resultaat te verbeteren op basis van data

General Purpose AI



In staat zijn om verschillende taken en problemen op te lossen, in tegenstelling tot gespecialiseerde AI-systemen die zijn ontworpen voor specifieke taken. Beide zijn zelflerend en kennen een 'mensachtig' denkvermogen

General Purpose AI is

- Breder toepasbaar
- Meer flexibel en aanpasbaar
- Meer contextonafhankelijk
- Meer mogelijkheden voor abstract redeneren

Generatieve AI

Creatie van nieuwe content

- Beeld
- Geluid
- Tekst
- Many-to-many



Large Language Models



- Grote hoeveelheden data om patronen van te leren zoals in welke volgorde woorden vaak worden gebruikt, wat alternatieven zijn en zelfs grammatica.
- Pre-training: algemene taalkennis; fine-tuning per taal en specifieke taken

ChatGPT: “*Het belangrijkste onderscheidende kenmerk is dat ChatGPT specifiek is afgestemd op het voeren van conversaties en daardoor goed presteert in situaties waar interactie en dialoog met gebruikers een cruciale rol spelen.*”

Voorbeelden toepassingen van ChatGPT



Beantwoorden veelgestelde vragen



Content generatie



Uitleggen



Samenvatten



Vertalen

VERDONCK
KLOOSTER &
ASSOCIATES
A HIGHBERG COMPANY

 **JPR**
advocaten

Juridische kaders

Risico's, voorzorgsmaatregelen en de voorgestelde AI-verordening

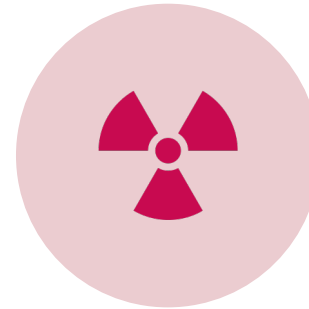
Inhoud



PRIVACY



AUTEURSRECHT



MAATSCHAPPELIJ
KE RISICO'S



AI-ACT

Risico's – privacy

NOS Nieuws • Vrijdag 31 maart 2023, 15:08



Italië trekt voorlopig stekker uit chatbot ChatGPT

Italië legt voorlopig het gebruik van de populaire chatbot ChatGPT aan banden. Het bedrijf daarachter, het Amerikaanse OpenAI, biedt te weinig duidelijkheid over welke persoonsgegevens met de chatbot worden verzameld. Daarmee houdt het techbedrijf zich niet aan de Europese privacywet, zegt de Italiaanse toezichthouder. ChatGPT komt in het land pas weer beschikbaar als duidelijk is dat aan de Europese regels wordt voldaan.

'Overheid Nederland wil ambtenaren verbieden ChatGPT en Midjourney te gebruiken'

De Nederlandse demissionaire staatssecretaris voor Digitalisering Alexandra van Huffelen werkt aan een voorstel om ambtenaren te verbieden toepassingen voor generatieve AI te gebruiken. Daarbij gaat het onder meer om ChatGPT en Midjourney.

Bron: Tweakers.net – 16 november 2023

Risico's – privacy

Risico's van een AI-systeem zelf:


- Geen AVG-grondslag
- Geen grip op persoonsgegevens

Risico's bij het gebruiken van een AI-systeem:

- Discriminerende output
- Geen AVG-grondslag gebruiker
- Beïnvloeding van de keuzevrijheid
- Geen grip op input

Samsung reportedly leaked its own secrets through ChatGPT

Well that didn't take long, now did it?

 [Laura Dobberstein](#)

Thu 6 Apr 2023 // 05:27 UTC

Less than three weeks after Samsung lifted a ban on employees using ChatGPT, the chaebol has reportedly leaked its own secrets into the AI service at least three times – including sensitive in-development semiconductor information.

The ban was intended to protect company data, though was lifted on March 11 to enhance productivity and keep staff engaged with the world's latest cool tech tools.

According to a Korean media [report](#), staff at Samsung subsequently dumped into ChatGPT corporate secrets, including equipment measurement and yield data from the conglomerate's device solution and semiconductor business unit.

One employee told journalists they copied all the problematic source code of a semiconductor database download program, entered it into ChatGPT, and inquired about a solution.

Tips ter vermindering van privacyrisico's

Pas op met het invoeren van persoonsgegevens in AI-systemen

Let op met het gebruiken van output

Zorg voor bewustwording bij jezelf en binnen jouw organisatie over persoonsgegevens, AI en bijbehorende risico's

Waak voor verliezen van gevoelige informatie

THE SHIFT

An A.I.-Generated Picture Won an Art Prize. Artists Aren't Happy.

"I won, and I didn't break any rules," the artwork's creator says.

Share full article



1.5K



Risico's – auteursrecht

- Het recht van de maker om een 'werk' te gebruiken
- Origineel + resultaat van creatieve keuzes van de (menselijke) maker + objectiveerbaar
- Output niet auteursrechtelijk beschermd, tenzij...
- Geen registratie vereist en ©-teken benodigd
- Als output ChatGPT te veel lijkt op de input, dan kan sprake zijn van inbreuk



- Voor scrapen geldt: artikel 15o Aw / 4 DSM

Amerikaanse schrijvers, onder wie John Grisham, klagen maker van ChatGPT aan

'New York Times' considers legal action against OpenAI as copyright tensions swirl

Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement

AI companies ask U.S. court to dismiss artists' copyright lawsuit

Google hit with class-action lawsuit over AI data scraping

- Openbaarmaking en/of verveelvoudiging werk= inbreuk

Tips ter vermindering van auteursrechttrisiko's

Ga ervan uit dat output inbreuk kan maken

Let op dat de output vaak geen bescherming oplevert

Toevoegingen van AI kunnen auteursrecht op output wegnemen

Risico's – maatschappelijk

- (On)bewust genereren en verspreiden van onjuistheden
- Cybercriminaliteit
 - Identiteitsfraude
 - Genereren spam & phishing
- Manipulatie van kwetsbaren – minderjarigen
- Gevolgen voor onderwijs
- Gevolgen voor de wetenschap

Fake Pentagon explosion photo caused a real dip in the stock market

Authorities confirm the suspected AI image is fake.

Bron: mashable.com – 22 mei 2023

Tips ter vermindering van maatschappelijke risico's

Wees je bewust van mogelijke onwaarheden

Benadruk het belang van cyberveiligheid

Blijf de menselijke creativiteit waarderen

De risico's op een rij

Privacy

- Geen AVG-grondslag voor maker en gebruiker van AI-systeem
- Geen grip op input en output persoonsgegevens
- Onjuiste en discriminerende output
- Mogelijk sturende intenties van AI-systemen
- Verliezen controle over gevoelige informatie

Auteursrecht

- Resultaat van AI is potentieel inbreukmakend
- Output vaak niet auteursrechtelijk beschermd
- Toevoegingen AI kunnen oorspronkelijke auteursrechten wegnemen

Maatschappelijk

- Onbewust delen van bedrijfsgeheimen
- Verspreiden onwaarheden/hallucinaties
- Cybercriminaliteit
- Manipulatie van kwetsbare mensen, zoals kinderen
- Gevolgen voor onderwijs en de wetenschap

De AI-verordening

Deze verordening is van toepassing op:

- (b) **gebruikers van AI-systemen die zich in de Unie bevinden;**

“gebruiker”: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem **onder eigen verantwoordelijkheid gebruikt**, tenzij het AI-systeem wordt gebruikt in het kader van een **persoonlijke niet-beroepsactiviteit**;

Hoog risico AI-systemen zijn bijvoorbeeld:

- Systemen die worden gebruikt voor **biometrische identificatie** op afstand van natuurlijke personen in real time en achteraf
- Systemen die de **toegang** van natuurlijke personen tot een **onderwijs- en beroepsinstelling** bepalen
- Systemen die natuurlijke personen selecteren in het kader van **sollicitaties**
- Systemen die door of namens overheidsinstanties beoordelen of natuurlijke personen in aanmerking komen voor **overheidsuitkeringen en -diensten**.

EC-voorstel

De AI-verordening – verplichtingen

Uitgangspunt hoog risico AI-systemen:

Altijd rekening houden met het **beoogde doel** van het AI-systeem en het **systeem voor risicobeheer**

Gebruikersverplichtingen bij hoog risico AI-systemen:

1. Volgen gebruiksaanwijzingen van het systeem
2. Zorgen dat inputdata relevant is voor het beoogde doel
3. Monitoren van de werking van het AI-systeem
4. Bewaren automatisch gegenereerde logs
5. Transparant naar natuurlijke personen over interactie met AI-systeem

Extra verplichtingen amendement:

1. Verplichte beoordeling grondrechten
2. Verplicht raadplegen werknemersvertegenwoordigers en informeren werknemers
3. Registratieverplichting overheidsinstanties
4. Informatieplicht bij AI-systeem dat beslissingen neemt
5. Recht op toelichting natuurlijke personen

EC en Parlement voorstel



VERDONCK
KLOOSTER &
ASSOCIATES

A HIGHBERG COMPANY



JPR
advocaten

In de praktijk

CASUS beleid schrijven (1/4)

Er is je gevraagd om beleid te schrijven waarvoor je LLM wel en niet kan gebruiken voor je dagelijks werk. Hoe kan ChatGPT je daarbij ondersteunen?

- **Beantwoorden veelgestelde vragen:** over zichzelf!
- **Content generatie:** voorbeelden van wat wel en niet werkt
- **Uitleggen:** tastbaar maken aan iedereen
- **Samenvatten:** essentie naar voren laten komen
- **Vertalen:** ook in andere talen beschikbaar maken

CASUS beleid schrijven (2/4)

Namens ChatGPT:

Natuurlijk kan ik je helpen bij het schrijven van beleid! Beleidsdocumenten variëren sterk afhankelijk van het onderwerp, de context en het doel. Om je zo goed mogelijk te kunnen assisteren, is het handig als je wat meer informatie deelt, zoals:

1. **Onderwerp:** Wat is het specifieke onderwerp van het beleid waar je aan wilt werken?
2. **Doel:** Wat is het doel van dit beleidsdocument? Gaat het om het vaststellen van richtlijnen, het oplossen van problemen, het reguleren van een bepaalde activiteit, of iets anders?
3. **Doelgroep:** Voor wie is dit beleid bedoeld? Zijn het medewerkers, klanten, overheidsinstanties, of een andere groep?
4. **Juridische of regelgevende vereisten:** Moet het beleid voldoen aan specifieke wetten, regels of voorschriften?
5. **Lengte en diepgang:** Moet het beleidsdocument kort en beknopt zijn, of moet het in detail treden en uitgebreid uitleggen?
6. **Bestaande informatie:** Heb je al bestaand materiaal dat als basis kan dienen voor dit beleidsdocument?

Bron: ChatGPT account JPR Luuk

CASUS beleid schrijven (3/4)





Vijf vragen die je minimaal moet stellen bij gebruik:

1. Wat heb ik nodig van ChatGPT?
2. Hoe ga ik het antwoord inzetten en wat is mijn bijdrage?
3. Welke informatie geeft mijn vraag prijs?
4. Hoe zorg ik dat ik antwoord krijg op mijn vraag?
5. Hoe zorg ik dat het antwoord juist is en bruikbaar?



© DALL-E

CASUS beleid schrijven (4/4)

	Voorbeeld prompt	Nodige Fact check	Mate van voorzichtigheid	Creativiteit vanuit ChatGPT
Informatie verzamelen	<ul style="list-style-type: none"> • Leg in maximaal 5 punten uit wat LLM is. • Noem drie voordelen en drie nadelen van gebruik van LLM in de praktijk. • Waarvoor kan ik LLM niet gebruiken? 	✓✓✓	✗	
Voorbeelden genereren	Geef me drie voorbeelden van toepassing van LLM in [sector]	✓✓	✗	
Samenvatten	Vat "[tekst]" samen in maximaal 1000 tekens/350 woorden/ 2 alinea's	✓	✗✗✗	
Uitlegbaar maken	Beschrijf dit/[tekst] zodat een kind van 6 het begrijpt	✓	✗✗	
Vertalen	Geef antwoord in [taal]/ vertaal "[tekst]" naar [taal]	✓	✗✗	

Nog 3 tips namens ChatGPT:

Natuurlijk, hier zijn drie gouden tips voor het schrijven van prompts voor ChatGPT:

1. Wees specifiek en duidelijk:

- Formuleer uw prompt zo duidelijk en specifiek mogelijk. Geef de AI voldoende context om de gewenste informatie of actie te begrijpen.
- Vermijd vage of dubbelzinnige instructies. Hoe duidelijker uw vraag of verzoek, hoe beter ChatGPT u kan helpen.

2. Experimenteer met meerdere instructies:

- Soms kan het nuttig zijn om meerdere instructies of vragen in uw prompt op te nemen, vooral als u complexe informatie nodig hebt.
- Probeer verschillende formuleringen en instructies om te zien welke de beste resultaten oplevert.

3. Stel beperkingen en duidelijke verwachtingen:

- Als u wilt dat de AI bepaalde stappen volgt of specifieke informatie verstrekt, maak dat dan expliciet in uw prompt.
- U kunt beperkingen of duidelijke verwachtingen toevoegen, zoals: "Beantwoord de vraag in maximaal 100 woorden" of "Geef drie voorbeelden."

Het is belangrijk om uw prompts te testen en aan te passen op basis van de reacties van ChatGPT. Dit proces van iteratie kan u helpen om de gewenste resultaten te bereiken en optimaal gebruik te maken van de AI.

**VERDONCK
KLOOSTER &
ASSOCIATES**
A HIGHBERG COMPANY

 **JPR**
advocaten

ChatGPT: Impact & Implementatie

Luuk Wassink (JPR), Yaşar Bayram (JPR), Sabine Steenwinkel-
den Daas (VKA) & Sebastiaan Bouthoorn (VKA)

[Download het Whitepaper 'Omgaan met AI op de werkvloer checklist' van JPR](#)