Ministerie van Justitie en Veiligheid

Directie Informatievoorziening en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
Henrique Barnard

T 070 370 79 11

Datum
22 mei 2023

Projectnaam
AI

Ons kenmerk
4673194

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLM Microsoft, Google Cloud en Amazon Web Services, geinteresseerden

memo

AI ontwikkelingen Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (AWS).

Inleiding

Binnen de overheid is, onder meer met de beschikbaarheid van ChatGPT / (OpenAI), in toenemende mate interesse in het gebruik van Artificial Intelligence (AI).[1] Leveranciers investeren in (mogelijke) AI-integratie in hun diensten en bieden in het geval van Microsoft zelfs al concreet 'AI-diensten' aan.

Het doel van dit memo is om deze ontwikkelingen in de context van SLM kort te beschrijven. Daarnaast wordt beknopt aangegeven welke kaders in ontwikkeling zijn om op verantwoorde wijze gebruik te maken van de AI die deze leveranciers leveren of gaan leveren. Tot slot volgt een aantal aandachtspunten voor organisaties die zich oriënteren op de eventuele inzet van dergelijke toepassingen van één van de door SLM beheerde leveranciers. Daarbij wordt aangetekend dat de kaders nog volop in ontwikkeling zijn en dit memo in een later stadium wordt opgevolgd met nadere adviezen.

1. Ontwikkelingen bij Microsoft

Microsoft biedt diverse producten aan die gebruik maken van AI en meer specifiek taalmodellen (´large language models´) zoals GPT-4, bekend van ChatGPT. Zo is Microsoft 365 Copilot momenteel in private preview[2] en wordt AI aangeboden binnen het toekomstige Microsoft teams premium.[3] Ook is Azure OpenAI al beschikbaar. Binnen Azure OpenAI kunnen gebruikers gebruik maken van meerdere ´large language models´.[4] Bij deze laatste toepassing blijven de verwerkingen en de datasets binnen de klantomgeving. Voorgaande zijn voorbeelden van Enterprise-diensten. Dit ter onderscheid van consumentendiensten als Bing[5], waarin ook AI-functies beschikbaar zijn. Van belang is dat Microsoft AI, waaronder GPT-4, toepast in onderdelen binnen haar

[1] Ook zijn er ontwikkelingen op dit vlak in de European Data Protection Board (EDPB). Zo is er een ´dedicated task force´ opgericht n.a.v. een handhavingsactie van de Italiaanse toezichthouder naar Chat GPT. Het doel hiervan is om samenwerking te bevorderen en informatie uit te wisselen over mogelijke handhavingsacties. Zie ook: EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT | European Data Protection Board (europa.eu).

[2] Introducing Microsoft 365 Copilot – your copilot for work - The Official Microsoft Blog.

[3] Microsoft Teams Premium: Cut costs and add AI-powered productivity | Microsoft 365 Blog.

[4] What is Azure OpenAI Service? - Azure Cognitive Services | Microsoft Learn.

[5] The new Bing - Our approach to Responsible AI (microsoft.com).

diensten. Dit betekent overigens niet dat de applicatie ChatGPT ook geïntegreerd is binnen de dienstverlening van Microsoft.

Er moet per geval goed gekeken worden naar de dienst en de daarin gebruikte AI-component, waarbij Enterprisediensten en consumentendiensten van elkaar onderscheiden moeten worden. Voor Enterprisediensten zijn de door SLM afgesloten contracten met Microsoft van toepassing.

SLM heeft in samenwerking met Microsoft twee talkshows georganiseerd. Hierbij wordt ingegaan op hoe Microsoft AI gebruikt binnen haar dienstverlening. Deze vinden plaats op 15 en 29 juni 2023 en zijn online te volgen. Inchrijven kan via de volgende link: https://minjenv.webinargeek.com/watch/wedJSbJL62uVF_FVJemRMdNxcBb2F1mKaO5j3ti-Nv4/.

2. Wettelijk kader

SLM onderstreept dat het gebruik van AI niet zonder risico is. Het is van essentieel belang is dat publieke waarden en mensenrechten, zoals het verbod op discriminatie, privacy en autonomie voorop staan bij de inzet van AI.[6]
Om verantwoorde inzet van AI te bewerkstelligen is het in ieder geval van belang dat alle relevante bestaande wet- en regelgeving wordt nageleefd. Bij het gebruik van AI-systemen moeten bedrijven en overheden onder meer rekening houden met de Algemene Verordening Gegevensbescherming. Deze verordening gaat over de persoonsgegevensbescherming van betrokkenen. Het uitvoeren van een Data Protection Impact Assessment[7] (DPIA) waarbij (ook) goed gekeken wordt naar de inzet van AI kan dan ook noodzakelijk zijn.

Ook zal de AI Act (AI-verordening), die nu nog in concept is, medebepalend worden voor het rechtmatig inzetten van AI-systemen. De Europese Commissie heeft in 2021 het voorstel voor de AI Act gedaan. Deze verordening bevindt zich tijdens het schrijven van dit document nog in concept en is nog aan verandering onderhevig. Het doel van de verordening is het harmoniseren van regels voor de ontwikkeling en gebruik van AI op de EU markt, waarbij grondrechten van individuen en veiligheid geëerbiedigd worden.[8] Naar verwachting komt het kabinet ook met een visie over generatieve AI en wordt er ook gewerkt aan een implementatiekader voor AI.[9]

De AI Act is vooral relevant voor AI systemen met een hoog risico zoals genoemd in de bijlagen van de (concept) AI Act. Van belang is om per casus te onderzoeken in welke mate er sprake is van een hoog risico-AI toepassing. Daarvan kan ook sprake zijn als een door een leverancier op de markt gebracht

[6] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/artificiele-intelligentie-ai/.

[7] Onder de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) kunnen organisaties verplicht zijn een DPIA uit te voeren. Dat is een instrument om vooraf de risico's omtrent privacy en gegevensbescherming van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

[8] Zie voor meer informatie: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022D45419&did=2022D45419 en https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022D49419&did=2022D49419.

[9] https://open.overheid.nl/documenten/ronlff6212cbf76de34f7572e5e13dca9c2617d6c547/pdf.

AI-systeem door de afnemer wordt gebruikt voor één van de hoog risico-scenario's uit de concept AI-act, in afwijking van de functie waarvoor dit systeem op de markt is gebracht door de leverancier.

Onderscheid moet worden gemaakt tussen het zelf ontwikkelen van een AI-toepassing als organisatie en het afnemen van een 'klant en klare' AI-toepassing die door een leverancier wordt aangeboden. Van groot belang voor de inschatting van de risico's en de bijkomende verplichtingen, in alle mogelijke scenario's, is voor welk doel de inzet van de AI door de rijksorganisatie beoogd is.

3. Relevante punten voor Rijksoverheidsorganisaties in dit stadium

- Het inzetten van AI is niet zonder risico. Net als bij andere technieken kunnen AI-systemen fouten bevatten die, afhankelijk van het systeem, gevolgen kunnen hebben zoals discriminatie, beïnvloeding, onjuiste informatie en inbreuk op privacy. Ook kan de transparante van de output problematisch zijn. Los van het wettelijk kader is het daarom belangrijk om goed na te denken voordat AI-systemen worden ingezet.
- Mocht de toepassing van een AI-systeem binnen de reikwijdte van de AI Act vallen en kwalificeren als een hoog risico AI, dan kan een zogeheten 'conformity assessment'[10] verplicht zijn. Eveneens kan het uitvoeren van een Impact Assessment voor Mensenrechten (IAMA) of een AI Impact Assessment (AIIA) dienen als hulpmiddel voor de afweging van het inzetten van AI. Ook kunnen de toolkits verantwoord datagebruik en ethisch verantwoorde innovatie hieraan bijdragen.[11]
- In de context van het gebruik van AI-systemen door rijksorganisaties is het aannemelijk dat de gebruiker van een AI systeem wordt aangemerkt als een ´verwerkingsverantwoordelijke´ in de zin van de AVG indien met het AI-systeem persoonsgegevens worden verwerkt. Indien een DPIA verplicht is, is het aan te bevelen om ook in de DPIA voldoende aandacht te besteden aan de (werking van de) AI component.
- Verder is het van belang om bij de voorgenomen aanschaf van een AI-systeem in een vroegtijdig stadium na te denken over specifieke contractuele aspecten die anticiperen op o.a. de AI Act. Bijvoorbeeld transparantie, auditrechten en informatieplichten. Een voorbeeld van contractuele voorwaarden die aan AI-aanbieders gesteld kunnen worden kunt u bij uw jurist opvragen. Vanzelfsprekend moeten ook aanbestedingsrechtelijke vraagstukken in acht worden genomen.

Mocht u vragen hebben over het inzetten van AI-diensten (of AI-functies in diensten) van Microsoft, Google Cloud of Amazon Web Services, neem dan contact met ons op.

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services

[10] Zie art. 3 onder 20 van de concept AI Act 21-4-2021. Het doel van deze beoordeling is dat er vooraf goed wordt gekeken naar de kwaliteit en de toepassing van het systeem.

[11] https://realisatieibds.pleio.nl/cms/view/628d59dd-0755-4c20-8217d3f26d9d8a5c/toolbox-voor-verantwoord-datagebruik.