Ministerie van Justitie en Veiligheid

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLM Microsoft, Google Cloud en AWS Rijk, geïnteresseerden

Hoofddirectie Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

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

Contactpersoon
SLM Microsoft, Google Cloud en AWS Rijk

SLMMicrosoft@minjenv.nl

Datum
18 december 2024

Onze referentie
x

memo M365 Copilot DPIA en FRAIA

Inleiding

SLM heeft een Data Protection Impact Assessment (DPIA) uitgevoerd op Microsoft Copilot voor Microsoft 365 (hierna: M365 Copilot). M365 Copilot is een general purpose AI system die medewerkers ondersteunt bij onder andere het maken van samenvattingen, teksten en gesprekken binnen applicaties van Microsoft, zoals Word, Excel, PowerPoint, Outlook en Teams. Microsoft biedt onder de naam Copilot verschillende general purpose AI systems aan. De scope van de DPIA is echter M365 Copilot.

Dit memo deelt de belangrijkste bevindingen van de DPIA een gaat in op het vervolgtraject. Daarnaast worden de resultaten en het proces besproken van de Fundamental Rights Impact Assessment (FRAIA), die is beëindigd voordat deze volledig kon worden afgerond

DPIA

Uit de DPIA volgt dat er in dit stadium vier hoge risico's gepaard gaan met het gebruik van M365 Copilot. In hoofdzaak zijn dit risico's die veroorzaakt worden door onvoldoende transparantie van Microsoft over verwerkingen van persoonsgegevens. Het gevolg van deze intransparantie is onder meer dat personen onvoldoende hun recht op inzage kunnen uitoefenen, er door organisaties onvoldoende gewaarborgd kan worden dat persoonsgegevens accuraat worden verwerkt en dat organisaties onvoldoende zicht en controle hebben over de verwerking van persoonsgegevens die Microsoft nodig zegt te hebben voor het leveren van m365 Copilot.

SLM heeft herhaaldelijk contact gehad met Microsoft en haar de gelegenheid gegeven om maatregelen voor te stellen die deze hoge risico's mitigeren. Ook zijn er door SLM suggesties gedaan hoe Microsoft dit concreet zou kunnen invullen. Microsoft heeft nog geen concrete toezeggingen gedaan waardoor er momenteel geen effectieve maatregelen zijn voor het mitigeren van de hoge risico's.

Microsoft heeft bevestigd zich te committeren aan overleggen met SLM met het doel om nadere maatregelen te bespreken die de risico's mitigeren. Deze overleggen worden vanaf januari gevoerd. Zodra er overeenstemming is bereikt over maatregelen die voldoende waarborgen bieden, zal SLM deze maatregelen evalueren en een herbeoordeling uitvoeren.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Datum
18 december 2024

Onze referentie
x

Niet alleen Microsoft, maar ook overheidsorganisaties die M365 Copilot willen inzetten, moeten maatregelen nemen om aan de AVG te kunnen voldoen. Dit is een combinatie van technische (instellingen) en organisatorische maatregelen, waarbij de laatste het meeste zullen vergen van een overheidsorganisatie.
Een belangrijk onderdeel van deze organisatorische maatregelen is het trainen van medewerkers die met M365 Copilot werken, zodat zij de tool verantwoord kunnen gebruiken en alert zijn op onjuiste of onnauwkeurige output. Daarnaast is een goed ingericht identiteits- en toegangsbeheer (IAM) en zorgvuldige data governance essentieel bij de implementatie van M365 Copilot. Dit omdat M365 Copilot gebruikmaakt van bestaande machtigingen en beleidsregels om (relevante) informatie te leveren uit de interne bestanden van de overheidsorganisatie. Dit betekent dat gevoelige informatie binnen de organisatie goed beheerd en gecontroleerd moet worden om ongeautoriseerde toegang of onjuiste verwerking te voorkomen.

FRAIA
SLM heeft naast de DPIA ook een Fundamental Rights and Algorithms Impact Assessment (FRAIA) uitgevoerd op M365 Copilot. Een FRAIA beoordeelt de impact van M365 Copilot ook op andere fundamentele rechten dan privacy. Hoewel een FRAIA op deze dienst niet verplicht is onder de AI Act, zijn we hier mee wel gestart om ervaring op te doen met deze methodologie, vanwege het belang van zorgvuldigheid bij het inzetten van AI in een overheidscontext. Tijdens het onderzoek bleek dat het huidige FRAIA-model minder geschikt is om een general purpose AI system zoals M365 Copilot te beoordelen. De specifieke aard en complexiteit van dit type AI vraagt om aanvullende evaluatiemethodieken. Derhalve is dit onderzoek tijdelijk gestopt en zal SLM eerst op zoek gaan naar aanvullende methodieken en *guidance* door onder meer de EU Commissie (AI office) en de nationale toezichthouder.

Advies
Op basis van de huidige bevindingen uit de DPIA is M365 Copilot nog niet compliant te gebruiken. Dit kan veranderen als gesprekken over maatregelen tussen SLM en Microsoft, die starten in januari 2025, positief verlopen. Verdere berichtgeving van SLM over voortgang volgt zodra er ontwikkelingen te melden zijn.

Organisaties kunnen echter nu al stappen ondernemen om zich voor te bereiden op de inzet van M365 CoPilot of andere general purpose AI systems. Daarbij adviseert SLM om aandacht te besteden aan het versterken van de data governance, zodat deze past op de eisen en risico's van dergelijke technologieën. Ook is het van belang om nu al na te denken over mogelijke use cases of domeinen waarin deze AI kan worden ingezet en om beleidskaders te ontwikkelen die deze inzet ondersteunen.

Begin 2025 verwacht SLM nog een aanvulling op deze organisatorische maatregelen te kunnen publiceren.

Bovenstaande hoeft niet te verhinderen dat lopende pilots/sandboxes voor M365 Copilot met een beheersbare omvang en toepassing gecontinueerd worden. Beheersbaar kan betekenen dat er geen volledige inproductiename is, geen

verboden of hoog risico-toepassingen (zoals gedefinieerd in de AI act) worden ingezet, er voldoende intern toezicht is georganiseerd, er geen use case wordt toegepast die gericht is op de verwerking van persoonsgegevens etc. Deze afweging moet zorgvuldig door de organisatie gemaakt worden.

Voor vragen over dit memo kun je contact opnemen met SLM via je bestaande contacten met SLM-teamleden of via de SLM-mailbox.

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services Rijk

Hoofddirectie Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Datum
18 december 2024

Onze referentie
x