



SLM Microsoft, Google Cloud & AWS

De rol van SLM bij inkoop van AI

Rob Herkemij en Šeila Akagić

18 juni 2024



SLM scope

- › Rijksoverheid
- › Microsoft, Google en AWS
- › Compliant en doelmatig gebruik mogelijk maken
- › Framework agreements
 - Compliance met wet- en regelgeving
- › Contractbeheer (onderzoeken, impact wetgeving etc)
- › Eventuele Europese alternatieven



SLM en de leveranciers

- › Relatief is de Nederlandse (Rijks)overheid klein voor hyperscalers
- › Echter:
 - We worden geholpen door EU-wetgeving
 - We publiceren onze rapporten (ook bij slecht nieuws)
 - We hebben een netwerk in de EU
 - We hebben toegang tot beslissers bij de leveranciers
 - We zoeken naar oplossingen
 - De toezichthouder verwijst naar ons werk



SLM en inkoop

- › SLM koopt niets
- › SLM schept de juridische voorwaarden waaronder hyperscalers aan gecontracteerde partijen aanbieden
- › Als een organisatie software/diensten (functioneel) uitvraagt via de aanbestede Rijksmantels



Hoe helpen we de organisaties?

- › We leggen de voordelen van de FWA uit
- › We lichten het portfolio van de leveranciers toe
 - De verschillende cloudopties
 - Advies over user controls
 - Pricing
 - Support, consultancy-opties etc
- › We adviseren IT'ers, beleidsmakers, FG's en Privacy Officers, CTO's, CIO's, buitenlandse collega's en nog veel meer...
- › We hebben overleg met andere publieke organisaties in NL



SLM en AI

- › SLM kan het gebruik van AI-tools voor organisaties mogelijk maken
- › Organisaties willen weten of ze AI binnen wettelijke kaders en beleidskaders in kunnen zetten
- › SLM's onderzoek als input voor afweging organisaties
- › Niet acceptabele risico's worden gemitigeerd of advies om AI niet in te zetten in bepaalde scenario's
- › Veel ervaring met DPIA's, specifiek AI-onderzoek is nieuw
- › Afbakening op leveranciers, diensten en scenario's



Te bereiken resultaten

- › Helder advies over welke tools in welke scenario's compliant te gebruiken zijn
- › Welke user controls zijn er
- › Goede (contractuele) waarborgen bij leverancier



FRAIA/DPIA Copilot for Microsoft 365

- Waarom dit onderzoek?
- Over welke Copilot gaat het?
- Aanpak/ Planning
- Wat te verwachten
- Vragen?



Waarom dit onderzoek?

- Veel vragen over AI component hyperscalers
- Contractueel valt **Copilot for Microsoft 365** onder het SLM contract, echter...
- De AI-component zorgt voor aanvullende compliance normen
- Transparantievragen over LLM en het Microsoft-filter (RAI)
- Organisaties zijn bezig deze dienst te verkennen



Waarom Fraia (IAMA)?

- Assessment model FRAIA/IAMA gecreëerd door Data School van Universiteit Utrecht, NL
- › Op verzoek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ontwikkelden Mirko Tobias Schäfer, Arthur Vankan en Iris Muis van Utrecht Data School en hoogleraar fundamentele rechten Janneke Gerards, het [Impact Assessment Mensenrechten en Algoritmes](#) (IAMA)
- › Nog niet verplicht wel aanbevolen.

Microsoft 365 Copilot basic architecture



Microsoft 365 Copilot

Microsoft 365 Apps



Microsoft 365 Service Boundary

Response + app commands

User prompt

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation models

Large Language Model

Azure OpenAI instance is maintained by Microsoft, OpenAI has no access to the data or the model.

Azure OpenAI

RAI

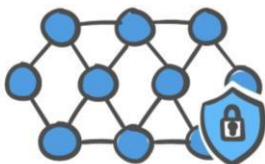
RAI is performed on input prompt and output results

Modified prompt
LLM response

Pre-processing

Grounding

Microsoft Graph



Semantic Index

Your context and content
emails, files, meetings, chats,
calendars, and contacts

Post-processing

Grounding

Customer Microsoft 365 Tenant

Data flow (🔒 = all requests are encrypted via HTTPS and wss://)

- 1
- 2 Copilot accesses Graph and Semantic Index for pre processing
- 3 Copilot sends modified prompt to Large Language Model
- 4 Copilot receives LLM response
- 5 Copilot accesses Graph and Semantic Index for post processing
- 6 Copilot sends the response, and app command back to Microsoft 365 Apps



Aanpak

- Aandacht gevraagd bij de hoogste Microsoft-leiding in VS/Corp.
- Uitvoering DPIA en FRAIA (Privacy Company)
- Utrecht University Data School begeleidt de FRAIA
- 15 uses cases
- DPIA-rapport en FRAIA-rapport
- Mitigeren van risico's en of geschiktheid voor gebruik
- Publicatie beide eindrapporten
- Overall coördinatie SLM Rijk.



Wat te verwachten?

- › Is Copilot bruikbaar in een aantal 'veilige' gebruiksscenario's?
- › Informatiebeheer aan gebruikerskant (garbage in = garbage out)
- › Het gebruik van Microsoft clouddiensten is onvermijdelijk bij Copilot
- › De menselijke controle blijft van belang
- › Afronding en publicatie van de rapporten- na de zomer
- › 'SLM Connects Compliance' event -> d.d. 24 september.



Vragen? Contact

SLM Rijk Microsoft, Google en AWS

www.slmmicrosoftrijk.nl

E-mail: SLMMicrosoft@minjenv.nl

