



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
R.B. Herkemij
*Strategisch
leveranciersmanager*

M 0652815630
r.b.herkemij@minjenv.nl

memo

Stand van zaken lopende onderzoeken SLM

SLM Microsoft, Google Cloud en AWS (SLM) is continu bezig om te anticiperen op de bruikbaarheid van diensten van Microsoft, Google Cloud en AWS. Hierbij is het van belang dat bij het eventueel gebruik van deze diensten er voldaan kan worden aan geldende wet- en regelgeving. Omdat er in snel tempo meer (Europese) wetgeving wordt ontwikkeld neemt SLM, daar waar relevant, deze nieuwe wet- en regelgeving ook mee in zijn beoordeling van diensten en/of zorgt dat de Rijksbrede contracten tijdig worden aangepast.

Met onderstaand overzicht informeert SLM je over lopende en recent afgeronde compliance-onderzoeken.

Datum
3 juli 2024

Onze referentie
03072024

Microsoft

Privacy-audit

Op 27 maart 2024 heeft SLM een memo gepubliceerd over de resultaten van de door EY in opdracht van SLM uitgevoerde audit op Microsoft's verwerkingen van persoonsgegevens voor eigen bedrijfsdoeleinden (Legitimate Business Operations). De conclusie van de audit is dat Microsoft passende technische en organisatorische maatregelen heeft getroffen om te waarborgen dat deze verwerkingen alleen plaatsvinden voor zover dat noodzakelijk en proportioneel is.

BIO Compliance

Op 20 oktober 2023 heeft SLM het auditrapport van EY gepubliceerd inzake BIO-compliance. Centraal stond de opdracht van SLM om de mate van compliance van Microsoftdiensten in relatie tot de Baseline Informatiebeveiling Overheid (BIO) te onderzoeken. Er is onderzocht of de diensten Microsoft Teams en Microsoft Azure Active Directory BIO-compliant gebruikt kunnen worden. De (gedetailleerde) afbakening, aanpak en resultaten zijn in het rapport te lezen.

Microsoft 365 Copilot

SLM is momenteel bezig met het uitvoeren van een DPIA en een Fundamental Rights and Algorithm Impact Assessment (FRAIA). SLM hecht veel belang aan het goed in beeld te krijgen welke risico's er bestaan bij het gebruik van (generatieve) AI binnen Microsoft365. Ook wordt ingegaan op de mitigerende maatregelen die getroffen kunnen worden bij het gebruik van Copilot in Microsoft 365.

Het onderzoek wordt in opdracht van SLM uitgevoerd door Privacy Company in samenwerking met Utrecht Data School (de ontwikkelaars van het Rijksmodel IAMA).

SLM is van plan voor het einde van dit jaar zijn onderzoeksrapporten te publiceren.

Edge for Business

Oorspronkelijk is dit onderzoek begonnen als een DPIA op Edge (de webbrowser van Microsoft). In de loop van de tijd heeft Microsoft zijn aanbod gewijzigd en een Edge for Business-variant in de markt gezet. Omdat deze laatste variant het meest passend lijkt voor zakelijke gebruikers, zijn we over deze dienst in gesprek met Microsoft.

Het gebruik van Edge (for Business) valt niet onder de Rijksbrede contractafspraken van SLM met Microsoft. SLM vindt dit niet wenselijk en heeft hierover gesprekken gevoerd met Microsoft. Microsoft heeft aan SLM verklaard dat zij niet voornemens is om voor Edge een 'processor-versie' aan te bieden. Het gevolg hiervan is dat Microsoft alleen onder consumentenvoorwaarden een webbrowser aanbiedt en zichzelf hiervoor als zelfstandig verwerkingsverantwoordelijke ziet. Omdat deze dienst niet onder de Rijksbrede afspraken met Microsoft valt en Microsoft haar reguliere privacy-statement van toepassing verklaart, betekent dit ook dat Microsoft persoonsgegevens kan verwerken voor onder meer commerciële doeleinden.

Microsoft heeft wel een lijst met privacy-vriendelijke instellingen aan SLM gestuurd waarmee de verwerkingen van Microsoft beperkt kunnen worden. SLM is nog in afwachting van een aanvullend document van Microsoft met nadere instellingen. Na ontvangst van de complete documentatie laat SLM deze testen en haar achterban hierover informeren.

Om eventuele alternatieven in kaart te brengen is SLM gestart met een kort onderzoek naar Mozilla Firefox (welke bekend staat als een privacy-vriendelijke browser).

SLM verwacht nog enkele maanden nodig te hebben voordat de resultaten hiervan gepubliceerd kunnen worden.

Windows processor-versie

In lijn met eerdere toezeggingen van Microsoft aan SLM heeft Microsoft een gedeeltelijke processor-versie ontwikkeld van onder meer Windows 10 en Windows 11 Enterprise. Gedeeltelijk in de zin dat Microsoft alleen voor (bij het gebruik van deze besturingssystemen gegenereerde) telemetrie-data een contractueel commitment aanbiedt. De juridische en technische consequenties hiervan worden momenteel verder onderzocht en zullen onderwerp zijn voor verdere discussie met Microsoft. Zodra hier meer nieuws over te melden is, zal SLM dit naar buiten brengen.

In de tussentijd verwijst SLM naar de aanbevolen privacy-instellingen in Windows zoals gepubliceerd op de SLM-website.¹

Planner, Calender, Project, Forms, ToDo, Bookings

Uit dit onderzoek is een aantal issues gekomen die momenteel onderwerp van gesprek zijn met Microsoft. Zo is SLM onder meer van mening dat er meer transparantie nodig is over de verwerkingen om tot een goede risicobeoordeling te kunnen komen. De door Microsoft aangeleverde informatie wordt beoordeeld en hieruit zal blijken of het gebruik van deze apps op een verantwoorde wijze kan plaatsvinden.

Het streven is om de resultaten van dit onderzoek binnen enkele maanden te publiceren.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening
en Inkoop
Strategische Inkoop

Datum
3 juli 2024

Onze referentie
03072024

¹ Handleiding-privacyvriendelijke-instellingen-Microsoft-365-V2-20231114.pdf (slmmicrosoftrijk.nl) (p. 15-18).

Azure

Een DPIA op de basisfunctionaliteiten van Azure, te weten compute, storage en database, wordt momenteel voorbereid. Dit met het doel om een vergelijkbaar onderzoek te hebben voor basis-cloudfunctionaliteiten bij AWS, Microsoft en Google cloud. De AWS DPIA is in 2023 door SLM gepubliceerd, zie hiervoor de SLM-website.

SLM verwacht nog enkele maanden nodig te hebben voordat de uitkomsten kunnen worden gepubliceerd.

BIO-template

Microsoft heeft een template ontwikkeld waarmee het organisaties in staat stelt om klantconfiguraties binnen het Microsoft Azure IaaS/PaaS platform te detecteren die in strijd zijn met de BIO. Dit template is openbaar beschikbaar en kan worden geïmplementeerd binnen Azure. SLM is een onderzoek gestart naar deze BIO-template om de toepasbaarheid en randvoorwaarden in kaart te brengen. De planning is dat de resultaten in Q4 2024 worden gepubliceerd.

Google

Workspace

De DPIA en de DTIA in verband met Google Workspace zijn inmiddels afgerond. De privacy-risico's die met het gebruik van Workspace samenhangen zijn gemitigeerd door doeltreffende maatregelen met Google overeen te komen.

De Tweede Kamer is op 25 juli jl. geïnformeerd over dit resultaat door de minister van JenV. De onderzoeksrapporten zijn beschikbaar op de SLM-website.

Google Cloud platform

Zie de toelichting bij Azure. In deze dienst zitten de basis cloud-functionaliteiten van Google en deze selectie uit het dienstenaanbod onder Cloud platform wordt onderzocht in een met AWS en Azure vergelijkbare scope in een DPIA.

AWS

Privacy audit

In deze audit wordt dezelfde scope onderzocht als in de eerdergenoemde privacy audit bij Microsoft ten aanzien van de Legitimate Business Operations.

De audit is inmiddels gestart en de planning is dat de resultaten beschikbaar zijn vanaf einde 2024.

Tot slot

Bij vragen over deze onderzoeken kunt u contact opnemen met SLM via de algemene mailbox slmmicrosoft@minjenv.nl of direct bij één van de SLM-teamleden.

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS

Hoofddirectie

Bedrijfsvoering

Directie Informatievoorziening
en Inkoop
Strategische Inkoop

Datum

3 juli 2024

Onze referentie

03072024