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
Bas Dekker
T 070 370 79 11

Datum
27 maart 2024

memo

Audit Legitimate Business Operations Microsoft

Aanleiding memo

Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (SLM) heeft onderzoek laten doen naar het proces gerelateerd aan verwerkingen van persoonsgegevens door Microsoft voor eigen bedrijfsdoeleinden. Dit betreft de zogeheten 'Legitimate Business Operations'. Dit onderzoek heeft geresulteerd in een assurancerapportage. Aan de inhoud van zo'n rapportage zijn strenge regels verbonden en dat kan het rapport minder toegankelijk maken voor lezers die niet bekend zijn met deze regels. Daarom is met dit memo beoogd om duiding bij de assurancerapportage te geven.

Allereerst wordt ingegaan op de vraag wat Legitimate Business Operations zijn en hoe dit in de situatie van Microsoft is vormgegeven. Daarna volgt een samenvatting van de interpretatie van de resultaten.

Legitimate Business Operations (LBO's)

SLM heeft met Microsoft een verwerkersovereenkomst gesloten. Daarin staat onder meer opgenomen voor welke gelimiteerde doeleinden Microsoft, in haar hoedanigheid als verwerker, persoonsgegevens mag verwerken. Een voorbeeld hiervan is het kunnen leveren van diensten. Ook staat helder omschreven voor welke verwerkingen Microsoft expliciet geen goedkeuring heeft gekregen zoals verwerking voor profiling of commerciële doeleinden.

Voor bepaalde en specifiek omschreven doeleinden is overeengekomen dat Microsoft persoonsgegevens wel mag verwerken als (zelfstandig) verwerkingsverantwoordelijke. Dit betekent dat Microsoft voor bepaalde doeleinden toestemming heeft gekregen om als verwerkingsverantwoordelijke persoonsgegevens te verwerken, nadat zij deze gegevens aanvankelijk als verwerker heeft verkregen/verwerkt. Dit is nodig om Microsoft in staat te stellen om bijvoorbeeld te kunnen te kunnen voldoen aan financiële rapportageverplichtingen of om cyberaanvallen tegen te gaan. Dit is alleen toegestaan in verband met de levering van gecontracteerde diensten. Microsoft kan en mag dus geen persoonsgegevens verwerken ten behoeve van LBO´s als er geen

diensten worden afgenomen. Vanuit privacy- en securityoverwegingen is het essentieel dat een verwerking in het kader van LBO´s niet verder gaat dan strikt noodzakelijk is en er adequate maatregelen zijn getroffen om dit te bereiken.

De hoofdvraag die ten grondslag ligt aan deze audit is dan ook: *'Heeft Microsoft passende technische en organisatorische maatregelen getroffen om te waarborgen dat persoonsgegevens in het kader van LBO's alleen worden verwerkt (door Microsoft) voor zover dat noodzakelijk en proportioneel is?'* Daarbij is gekeken naar het proces waarvoor voor de volgende LBO's, persoonsgegevens worden ontsloten:

(A) Compensation
(B) Customer billing and account management
(C) Financial reporting
(D) Legal Obligations

Bij (D)´Legal Obligations´ is separaat gekeken naar het verwerken van persoonsgegevens ten behoeve van wettelijke verplichtingen waaraan Microsoft moet voldoen. Specifiek gaat het dan om de vraag welke maatregelen Microsoft heeft getroffen om ervoor te zorgen dat als Microsoft wettelijk verplicht zou zijn om persoonsgegevens te verstrekken aan een autoriteit of bevoegde instantie, dit uitsluitend wordt gedaan voor zover dit strikt noodzakelijk en proportioneel is. In het licht van de (opnieuw) actuele discussie over de risico's van dit vraagstuk, is het relevant om dit in deze audit (nader) te onderzoeken. Omdat ten aanzien van de LBO 'Legal Obligations' aparte 'Controls' en 'Control Objectives'[1] door Microsoft zijn aangedragen moet deze LBO apart worden bezien.

De LBO's zijn onderzocht voor verwerkingen bij gebruik van de dienst Microsoft Teams inclusief Microsoft Azure AD (nu Entra ID).

Samenvatting van de bevindingen

De resultaten van deze audit laten een positief beeld zien van hoe Microsoft haar processen heeft ingericht. Ten aanzien van alle controls zijn *opzet en bestaan* aangetoond. Zo volgt bijvoorbeeld uit deze audit dat Microsoft adequate controls heeft om data te pseudonimiseren, te aggregeren of ongeoorloofde toegang te voorkomen. Uit het assurance rapport volgt dat Microsoft zelf verantwoordelijk is voor de omschrijving van de controls en de control objectives. EY heeft als onafhankelijke auditer uiteraard wel gekeken of de controls en de control objectives voldoende zijn om de bestaande risico's te mitigeren.

Betreffende *de werking* zijn er slechts twee relevante opmerkingen te maken die beide uitsluitend verband houden met de LBO 'Legal Obligations'.

1. Werking niet aangetoond als gevolg van 'non-occurrence'

[1] 'Controls' zijn de procedures of beleidsmaatregelen die Microsoft heeft ontworpen om haar doelstellingen (de Control Objectives) te bereiken.

Ten aanzien van enkele controls (zie CO-BO 11.1 e.v.) is *werking* niet aangetoond vanwege een zogenaamde non-occurrence. Concreet houdt dit in dat Microsoft in de onderzochte periode geen enkele 'legal orders' of 'legal requests' heeft ontvangen die gerelateerd waren aan deelnemers van de SLM framework agreement. Feitelijk heeft Microsoft deze dus ook niet kunnen overleggen. Dit is in lijn met het beeld dat toegang door derde landen zoals Amerika in de praktijk zeer klein is.[2]

2. Werking niet aangetoond als gevolg van 'sensitivity of the policies'.

Voor bepaalde controls (CBO 12.3, 12.4 en 12.5) is werking niet aangetoond als gevolg van de gevoeligheid van de procedures die Microsoft hanteert. Om de werking aan te kunnen tonen zou toegang zijn vereist tot zeer gevoelige gegevens. Zoals Microsoft aangeeft (in Appendix 2) is het haar (contractueel) niet toegestaan hier een auditor toegang toe te verschaffen. Dat neemt niet weg dat er wel diepgaand is gekeken naar 'opzet en bestaan' van deze controls. Zoals aangegeven, zijn deze dan ook vastgesteld.

Conclusie:

SLM constateert dat de bevindingen van deze audit aantonen dat Microsoft passende technische en organisatorische maatregelen heeft getroffen om te waarborgen dat persoonsgegevens in het kader van LBO's alleen worden verwerkt (door Microsoft) voor zover dat noodzakelijk en proportioneel is. SLM blijft gebruik maken van haar bedongen auditrecht om te kijken of Microsoft in lijn met alle relevante wet- en regelgeving blijft handelen.

Met vriendelijke groet,
Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

[2] Zie ook: 20240304-Memo-SLM-reactie-NOS-artikel.pdf (slmmicrosoftrijk.nl). In Appendix 2 in het Assurance report geeft Microsoft aan, overheden nimmer direct toegang te geven tot 'customers' data of hen te faciliteren in het doorbreken van encryptie.