Ministerie van Justitie en Veiligheid

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

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
21 februari 2022

Projectnaam
Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

Ons kenmerk
3867538

memo

DPIA Microsoft Teams, OneDrive en SharePoint online

Uitkomsten DPIA: zes lage risico's

SLM Rijk heeft een gegevensbeschermingseffectbeoordeling (DPIA) laten uitvoeren op de gegevensverwerking via Microsoft Teams, OneDrive en SharePoint Online. SLM Rijk stelt vast dat er geen hoge risico's optreden bij het gebruik van deze diensten.

Er is nog ruimte voor verbetering in de transparantie van telemetriegegevens. Microsoft heeft toegezegd het inzageproces (via de systeembeheerders) te verbeteren, en betere uitleg te geven waarom veel verzamelde gegevens óf geen persoonsgegevens zijn, óf onmiddellijk geanonimiseerd en dus niet meer terug te koppelen aan een individuele inzageverzoeker.

Hoog risico

Als organisaties Microsoft Teams, SharePoint of OneDrive Online gebruiken voor de verwerking van bijzondere persoonsgegevens ontstaat een hoog risico. Organisaties kunnen dit hoge risico voor bijzondere persoonsgegevens in bestanden op OneDrive en SharePoint beperken door hun eigen encryptiesleutels te gebruiken, met Microsoft Double Key Encryption. Microsoft biedt nog geen end-to-end encryptie voor de streaming communicatie met meerdere deelnemers in Teams, alleen voor ongeplande één-op-één videogesprekken. Microsoft heeft bevestigd dat ze E2EE mogelijk maakt in Teams-groepsvergaderingen en voor de chats maar noemt nog geen termijn.

Risico's van doorgifte van persoonsgegevens naar de VS

De belangrijkste risico's hangen samen met het feit dat Microsoft een Amerikaans bedrijf is. Daardoor bestaat de mogelijkheid dat Amerikaanse opsporings- en inlichtingendiensten toegang eisen tot persoonsgegevens van gebruikers van de diensten. Dat betekent dat er bij gebruik van de Microsoft-diensten formeel sprake is van doorgifte naar een land buiten de EU zonder adequaat beschermingsniveau van de persoonsgegevens.

Aanvullend op bovenstaande is het relevant te melden dat het EDPB (European Data Protection Board) heeft aangekondigd dat ze eind dit jaar het onderzoek hoopt af te ronden naar het gebruik van clouddiensten door overheidsinstellingen.

De kans dat opsporings- en inlichtingendiensten toegang vorderen lijkt vooral theoretisch. Microsoft heeft verklaard dat ze nog nooit gegevens van werknemers van publieke sectorinstellingen heeft verstrekt aan enige overheid. Dus ook niet

Directie Informatievoorziening en Inkoop

Datum
21 februari 2022

Ons kenmerk
3867538

aan de Amerikaanse overheid. Bovendien verwerkt en bewaart Microsoft bijna alle persoonsgegevens van werknemers van de Nederlandse overheid inmiddels al exclusief in Europese datacentra, niet in de VS. Alleen de pseudonieme telemetriegegevens worden nu nog systematisch naar de VS verzonden. Eind 2022 verwerkt Microsoft ook die persoonsgegevens automatisch uitsluitend in de EU.

Om de risico's van de toegang tot de persoonsgegevens op basis van toepasselijk Amerikaans recht in kaart te brengen heeft SLM Rijk advies gevraagd aan het internationale advocatenkantoor Greenberg Traurig LLP over toepasselijk Amerikaans recht. Deze kennis is vertaald in een Q&A die later openbaar wordt gemaakt.

Data Transfer Impact Assessment (DTIA)
Per soort persoonsgegevens die Microsoft verwerkt via de drie diensten zijn de risico's op oneigenlijke verdere verwerking in kaart gebracht in een Data Transfer Impact Assessment (DTIA). Er zijn zeven soorten persoonsgegevens bepaald waarop een berekening van de kansen dat de gegevens op grond van toepasselijke wetgeving worden ingezien of opgevraagd door de Amerikaanse opsporings- en inlichtingendiensten is uitgevoerd:

1. Live inhoudelijke gegevens (Teams)
2. Opgeslagen inhoudelijke gegevens (Teams, OneDrive, SharePoint)
3. Diagnostische gegevens (telemetrie) (Teams, OneDrive, SharePoint)
4. Diagnostische gegevens (servicelogs) (Teams, OneDrive, SharePoint)
5. Supportgegevens (Teams, OneDrive, SharePoint)
6. Securitygegevens (VS) (Teams, OneDrive, SharePoint)
7. Accountgegevens (Azure AD)

De DTIA is gebaseerd op een openbaar model van de Zwitserse advocaat David Rosenthal, en aangepast door Privacy Company. Deze Excel wordt binnenkort openbaar gemaakt, zodat andere organisaties de DTIA kunnen hergebruiken.

Met vriendelijke groet,

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