Ministerie van Justitie en Veiligheid

ONGERUBRICEERD

CIO Rijk, CIO Beraad, CIO Raad, CTO Raad, CTO Overleg, deelnemers SLM Microsoft Rijk en geïnteresseerden

Directie
Informatievoorziening en Inkoop

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

Contactpersoon
P.J.G. van den Berg

M 06 500 576 06
p.j.van.den.berg@minjenv.nl

Datum
18 augustus 2020

Projectnaam
SLM Microsoft Rijk

memo

Stand van Zaken Microsoft augustus 2020

Er is in de afgelopen 12 maanden weer een flink aantal ontwikkelingen geweest in het Microsoft-dossier. Nu we veel meer moeten werken op afstand en beeldbellen en -vergaderen een grote vlucht heeft genomen zijn veel van de bij SLM Microsoft Rijk (SLM) aangesloten onderdelen druk in de weer met het innoveren van de werkplek.

Mobile Apps, Office for the Web en Intune

In onze update[1] van 17 juli 2019 gaven wij een aantal implementatiebeperkingen aan en als belangrijkste adviseerden we als volgt:

“Maak geen gebruik van Office Online en de mobiele Office apps die onderdeel zijn van de Office 365 licentie tot de vijf hoge risico’s zijn gemitigeerd.”

Na afronding van de DPIA zijn SLM en Microsoft maatregelen overeengekomen om de hoge risico's te beperken. Nadat Microsoft deze maatregelen heeft doorgevoerd, en mits overheidsorganisaties de aanbevelingen voor overheidsorganisaties in de DPIA volgen, zijn alle in de DPIA geïdentificeerde hoge risico’s gemitigeerd.
De maatregelen die Microsoft per 1 augustus 2020 toegezegd had zijn uitgevoerd en door SLM gecontroleerd. De nog te nemen maatregelen worden volgens planning vanaf september tot aan het einde van dit jaar uitgevoerd.

Wij verwachten vanuit AVG-perspectief geen problemen voor het gebruik van deze producten.

Gedetailleerde documentatie over de inhoud van de maatregelen en afspraken is te vinden op Rijksoverheid.nl[2]

Wij zijn voornemens begin 2021 een update te publiceren over de voortgang van de implementatie van de maatregelen.

[1] Link naar rijksoverheid.nl
[2] Link naar vindplaats Mobile Apps Office for the Web afspraken

Professional Services

SLM is bezig alle Professional Services van Microsoft onder het regime van de instructies voor verwerking van persoonsgegevens te brengen zoals dit al geldt voor online diensten. Dat betekent dat op korte termijn het support, inclusief premier en unified support, en consultancydiensten van Microsoft onder hetzelfde beschermingsniveau vallen als de online-diensten.

Doorgifte van persoonsgegevens naar de Verenigde Staten

Op 16 juli 2020 heeft het Europese Hof van Justitie (het Hof) een belangrijke uitspraak[3] gedaan met betrekking tot de doorgifte van persoonsgegevens naar landen buiten de Europese Unie, in het bijzonder de Verenigde Staten van Amerika.

De uitspraak heeft ook gevolgen voor Nederlandse overheidsorganisaties die diensten afnemen of producten gebruiken van Microsoft, voor zover gegevens worden doorgegeven aan partijen in de Verenigde Staten.
Daarvan is in elk geval sprake bij Microsoftproducten en -diensten met een online component die vallen onder de 'Microsoft Voorwaarden voor Online Diensten'.

Als gevolg van de uitspraak kan, met onmiddellijke ingang, de doorgifte van persoonsgegevens vanuit de Europese Unie naar de Verenigde Staten niet langer worden gebaseerd op het zogenaamde Privacy Shield. De door de Europese Commissie opgestelde modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers (de Modelcontractbepalingen of SCC) blijven onder voorwaarden wel geldig. SLM onderzoekt of aan deze voorwaarden wordt voldaan.

Deze Modelcontractbepalingen zijn al opgenomen in de door SLM met Microsoft getekende contracten, als geamendeerd en in combinatie met de ingevulde 'checkbox-instructies' die onderdeel uitmaken van het amendement.
Microsoft heeft desgevraagd direct na de uitspraak van het Hof schriftelijk aan SLM bevestigd dat alle doorgiftes aan Microsoft in de Verenigde Staten in het kader van Online Diensten waarvoor Microsoft verwerker is, onder de bestaande Modelcontractbepalingen worden doorgegeven, en dus niet langer (deels) onder het Privacy Shield.
We hebben een uitvoerige analyse van de uitspraak van het Hof in een nota uitgewerkt en gedeeld met de gebruikelijke gremia.[4]

Hiermee heeft SLM de zaak voor wat betreft de Online Diensten voor dit moment onder controle voor Nederlandse overheidsorganisaties.

Als Nederlandse overheidsorganisaties zijn aangesloten bij het Rijksbrede Microsoft Business and Services Agreement (MBSA) die in beheer is bij SLM en de aanbevelingen van SLM voor AVG-compliant gebruik van de Online Diensten

[3] HvJ, zaak C-311/18, 16 juli 2020 (Data Protection Commissioner tegen Facebook Ireland Ltd en Maximilian Schrems).
[4] Nota - impact uitspraak Europese Hof mbt Privacy Shield op gebruik Microsoftproducten - 20200722.docx

volgen, is er op dit moment geen aanleiding om het gebruik van Microsoft Online Diensten op te schorten of te beëindigen.

Beperkingen

Voor alle duidelijkheid, terwijl de door SLM met Microsoft overeengekomen technische productwijzigingen wereldwijd voor alle zogenaamde Enterprise-klanten beschikbaar zijn gekomen, geldt dit niet voor de aanvullende afspraken waarin de verplichtingen van verwerkingsverantwoordelijke en verwerker geregeld zijn. De reikwijdte van SLM strekt niet verder dan de Rijksdiensten en de daarbij behorende ZBO's en Agentschappen. Deze aanvullende afspraken zijn daarom uitsluitend van toepassing op díé Rijksonderdelen inclusief ZBO's die aangesloten zijn bij de Rijksbrede MBSA. Andere organisaties zoals gemeenten en de onderwijssector hebben eigen afspraken via hun koepel die grotendeels het model van het Rijk volgen.

Audit

Er is overeengekomen dat SLM de naleving van de gemaakte afspraken kan controleren door middel van audits door een door de SLM aangestelde onafhankelijke derde. Microsoft heeft zich verbonden mee te werken aan dergelijke audits door de systemen waarmee zij gegevens verwerkt, faciliteiten en ondersteunende documentatie die relevant zijn voor het verwerken van gegevens en persoonsgegevens van de bij SLM aangesloten organisaties beschikbaar te stellen en de auditors toegang te geven. Begin dit jaar is EY gestart met een audit met als thema gebruikersprofielen. Deze heeft door de situatie rond COVID-19 en de reisbeperkingen naar de VS vertraging opgelopen. De auditprocedure is nu aangepast en de resultaten worden in november verwacht.

Hoe verder met de DPIA's ?

Een gegevensbeschermingseffectbeoordeling (data protection impact assessment - DPIA) moet worden uitgevoerd als er waarschijnlijke sprake is van hoge risico's voor de gegevensbescherming van betrokkenen. Voorafgaand aan het gebruik van een gegevensverwerkend systeem, moeten de effecten van de voorgenomen verwerkingsactiviteiten op de gegevensbescherming van betrokkenen worden beoordeeld.

Op dit moment dienen alle gegevensverantwoordelijken van de Staat (lees in dit geval de Diensten) ieder een eigen een DPIA uit te voeren, omdat zij persoonsgegevens verwerken voor uiteenlopende doelen, als gevolg van de wettelijke taken die zij uitvoeren. De beschermingsmaatregelen en contractuele afspraken die SLM Microsoft Rijk met Microsoft is overeengekomen, zijn een belangrijk onderdeel van deze DPIA's.
Om te voorkomen dat de verwerkingsverantwoordelijken ieder hun eigen beoordeling van de afspraken met Microsoft zullen maken heeft SLM Microsoft Rijk een aangepaste DPIA voor Windows 10 Enterprise en Microsoft Office ProPlus (inclusief Office for the Web, Intune en de mobiele Office apps) laten maken op grond van de met Microsoft gemaakte afspraken. Deze DPIA geldt dan als een 'technische model DPIA' die ziet op de rol van Microsoft als gegevensverwerker en de overeenkomst met Microsoft. Alle Diensten kunnen bij het uitvoeren van hun

DPIA refereren aan deze technische model DPIA. De verwerkingsverantwoordelijken hoeven dan in aanvulling op de technische model DPIA alleen hun eigen gebruik van de Microsoftdiensten te beoordelen (lees: de risico's die zijn verbonden aan de verwerkingen van de specifieke persoonsgegevens die zij verwerken met inzet van de Online Services van Microsoft). Dit komt de uniformiteit in de risicobeoordeling ten goede en scheelt tijd en geld. Ook is met Microsoft afgesproken dat alle in de Online Service Terms beschreven producten en diensten onder de verbeterde voorwaarden van het Rijk vallen. Daarom is het niet nodig om telkens vooraf een DPIA te maken van elke nieuwe versie van een product of een nieuwe functionaliteit. In de eerder genoemde audits wordt de naleving van Microsoft op de in de OST aangeboden producten en diensten en de overige on-premise producten die onder de afspraken die SLM met Microsoft gemaakt heeft of nog gaan vallen gecontroleerd.

Advies van SLM

Samenvattend is het advies voor onderdelen van de Rijksoverheid als volgt:

1. Sluit aan bij SLM Microsoft Rijk om toegang te krijgen tot de benodigde contractuele voorwaarden,
   a. Om volledig te voldoen aan de AVG en het gebruik van de Standard Contractual Clauses is het noodzakelijk het daarvoor opgestelde “Checkbox” amendement in te vullen en (via SLM) naar Microsoft te sturen.
2. Gebruik Windows 10 Enterprise vanaf versie 1903 (mei 2019) of later met Timeline Sync uit en stel de telemetrie in op het laagste niveau Beveiliging (of het telemetrieverkeer geblokkeerd).
3. Wat betreft Microsoft Office 365 producten en diensten het volgende:
   a. Verbied het gebruik van Controller Connected Experiences door deze centraal uit te zetten.
   b. Gebruik versie 1905 of hoger van Office 365 ProPlus en zet het telemetrie level naar ‘Neither’.
   c. Zet het sturen van data voor het Customer Experience Improvement Program uit.
   d. Zet de Linked-In integration met Microsoft employee work accounts uit.
   e. Er is geen DPIA gedaan voor Workplace Analytics and Activity Reports in het Microsoft 365 admin center. De reden hiervoor is dat deze functies een werknemervolgsysteemachtige werking hebben wat bij voorbaat onwenselijk is in meeste organisaties. Ons advies is dan ook deze functies niet te gebruiken. Als organisaties deze tools willen gebruiken, dienen ze een DPIA uit te voeren. Hiervoor kan een organisatie contact opnemen met SLM.
4. Afhankelijk van de specifieke situatie in iedere organisatie is het gebruik van Customer Lockbox en Customer Key te overwegen om de inhoud van bestanden nog beter te beschermen.
5. Om gebruik te kunnen maken van de Rijksvoorwaarden dient een organisatie een zogenaamd enrollment af te sluiten met de daar bij behorende enrollment amendementen. Dit enrollment moet dan verwijzen naar de Rijksbrede MBSA en EA met de daar weer bij behorende amendementen. Dit is complex en wij helpen organisaties graag bij het op de juiste manier contracteren. Maak zonder overleg met SLM geen

gebruik van andere contractvormen zoals MPSA of CSP. Deze contractvormen bieden niet dezelfde bescherming als de Rijksvoorwaarden en in het algemeen is AVG-compliant gebruik dan niet mogelijk.

Tenslotte

Het team van SLM helpt u graag met het krijgen van antwoorden op allerlei vragen over de aanschaf van Microsoftproducten en –diensten, licenties, voorwaarden etc. U kunt contact opnemen via slmmicrosoft@minjenv.nl