Ministerie van Justitie en Veiligheid

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
Paul van den Berg

M 06 524 704 25
p.j.van.den.berg@minvenj.nl

Datum
17 juli 2019

memo

Stand van zaken Microsoft

Op 7 november 2018 publiceerde het Ministerie van Justitie (via het onderdeel Strategisch Leveranciersmanagement Microsoft Rijk (SLM Microsoft Rijk, het centrale aanspreekpunt voor Microsoft binnen de Rijksoverheid), een uitvoerig rapport over de wijze waarop Microsoft door middel van haar producten Office 2016 en Office 365 ProPlus, kort gezegd persoonsgegevens en andere data verzamelt en verwerkt. Dit rapport is bekend als de 'DPIA diagnostic data in Microsoft Office ProPlus' (DPIA).

Uit de DPIA blijkt dat Office niet aan alle eisen van de AVG voldoet en dat Microsoft en de Rijksoverheid een aantal maatregelen zouden moeten treffen om het verzamelen en gebruik van persoonsgegevens in lijn te brengen met de eisen van de AVG.

SLM Microsoft Rijk heeft voorafgaand aan de publicatie van de DPIA overeenstemming bereikt met Microsoft over een verbeterplan. Microsoft verplichtte zich in dit plan om haar producten zodanig te wijzigen dat het gebruik daarvan mogelijk was voor de Nederlandse overheid conform de AVG. De meest urgente wijzigingen heeft Microsoft inmiddels conform het verbeterplan aangebracht. Deze zijn door SLM Microsoft Rijk in juni 2019 getest en in orde bevonden.

SLM Microsoft Rijk wenste op onderdelen het verzamelen en gebruik van persoonsgegevens en andere data verder te beperken om verdere verregaande bewerkingen (door derden) op persoonsgegevens te voorkomen.

In april en mei 2019 zijn met Microsoft onderhandelingen gevoerd om de benodigde maatregelen bindend vast te leggen, de juiste juridische basis te geven en afdoende controlemiddelen en controlerechten te verkrijgen.

Kamerbrieven
Na aanleiding van vragen uit de Tweede Kamer zijn er door de ministers Grapperhaus en Ollongren twee Kamerbrieven geschreven. De eerste

brief van 20 december 2018 informeerde over het verbeterplan en de daarbij behorende planning. De tweede brief van 1 juli 2019 rapporteert over de resultaten van het verbeterplan met als conclusie:

> *"Gezien de behaalde resultaten zoals hierboven beschreven ziet SLM Microsoft Rijk, vanuit AVG-perspectief geen bezwaren voor bij SLM Microsoft aangesloten organisaties Microsoft Office ProPlus, Windows 10 Enterprise en Azure te gebruiken. Het blijft altijd de eigen afweging van een organisatie als verwerkingsverantwoordelijke om te besluiten of en welk product of dienst geschikt is voor een specifieke toepassing. Hierbij dienen ook andere factoren zoals informatiebeveiligingsaspecten en specifieke wet- en regelgeving voor de organisatie gewogen te worden."*

Conclusies
SLM Microsoft Rijk heeft de risico's weggenomen die zijn geïdentificeerd in de DPIA, of deze afdoende gemitigeerd. Daarnaast heeft SLM Microsoft Rijk vergelijkbare risico's met betrekking tot andere producten en diensten van Microsoft weggenomen of afdoende gemitigeerd (dit geldt voor alle diensten die onder de Microsoft Online Service Terms vallen) danwel is er voldoende zicht op het wegnemen of mitigeren van dergelijke risico's (dit geldt voor de overige producten en diensten, waaronder Windows 10 Enterprise). Tenslotte heeft SLM Microsoft Rijk afdoende auditrechten bedongen en zijn alle afspraken bindend vastgelegd.

Het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's) door de Diensten kan nu veel uniformer en efficiënter verlopen. Dit leidt tot betere resultaten en zal tijd en kosten schelen.

Beperkingen
Voor alle duidelijkheid, terwijl de door SLM Microsoft Rijk 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 worden. De reikwijdte van SLM Microsoft 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 en ZBO's die aangesloten zijn bij het Rijksbrede Microsoft Business en Services Agreement (MBSA) onder beheer bij SLM Microsoft Rijk. Wij helpen natuurlijk graag met informatie en advies.

Verdere beperkingen: Mobile Apps en Office Online
Ter voorkoming van twijfel: Microsoft Office Online en de mobiele Microsoft Office apps, verkrijgbaar via de Apple Store voor iOS en via de Google store voor Android, zijn inmiddels onderzocht en voldoen nog niet aan de gestelde eisen. Dit wordt toegelicht in een tweede DPIA rapport

dat gelijktijdig met de DPIA's over Windows 10 en Office 365 ProPlus wordt gepubliceerd. SLM Microsoft Rijk is nog in gesprek met Microsoft om duidelijkheid te krijgen over de gebruiksvoorwaarden. Het gebruik van de mobiele Office apps wordt dus vooralsnog afgeraden. Voor Office Online geldt dat het op dit moment – in weerwil van de afspraken met Microsoft- nog niet mogelijk is om de Controller Connected Experiences uit te zetten. Daarom wordt het gebruik hiervan vooralsnog eveneens afgeraden.

Wat is bereikt?

Geautoriseerde gebruiksdoelen: doelbinding

De DPIA identificeerde acht risico's ten aanzien van Office. De onderhandelingen in april en mei zaten met name op risico 6 ('lack of purpose limitations' oftewel 'onvoldoende doelbinding/basis voor geautoriseerde doelen'). Dit risico is weggenomen door:

- zeer gedetailleerd overeen te komen voor welke doelen Microsoft gegevens van de Staat (zowel de inhoudelijke gegevens als alle gegevens over het gebruik van de diensten) die onder de reikwijdte van de overeenkomsten tussen de Staat en Microsoft vallen, mag gebruiken;
- gebruik en doorgifte van gegevens aan derden voor data analytics, profilering, adverteren, marktonderzoek te verbieden, tenzij dit is toegestaan op basis van schriftelijke instructies van de Staat;
- gedetailleerd overeen te komen hoe gegevens moeten worden geanonimiseerd, en daarbij aan te sluiten bij de WP29 Opinie 05/2014 over Anonimiseringstechnieken (WP216);
- een ruime reikwijdte aan de doelbindingsafspraken te geven, door zowel te refereren aan 'Gegevens van de Klant' (ook wel 'Customer Data') als aan persoonsgegevens die door Microsoft worden gegenereerd in verband met het gebruik door de Rijksoverheid van de Online Diensten; en
- voor de zogenaamde Controller Connected Services af te spreken dat deze door beheerders centraal kunnen worden uit- en aangezet.

Audit

Daarnaast is overeengekomen dat SLM Microsoft Rijk de naleving van de gemaakte afspraken kan controleren door middel van audits door een door de SLM Microsoft Rijk 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 Microsoft Rijk aangesloten organisaties beschikbaar te stellen en de auditors toegang te geven.

De andere zeven risico's

De onderhandelingen in april en mei 2019 zagen zoals gezegd met name op risico zes. Een deel van de andere risico's was al eerder afgedekt of

afdoende gemitigeerd. De resterende risico's zijn meegenomen in de onderhandelingen van april en mei jl. en toen weggenomen of afdoende gemitigeerd.

Vastlegging afspraken en toepasselijkheid op enrollments
Alle afspraken zijn vervat in een amendement op de overeenkomst met Microsoft die het hoogste in rang is (de MBSA). Dit amendement kan niet op een lager niveau worden gewijzigd.

Op alle enrollments die verwijzen naar de centrale MBSA van SLM Microsoft Rijk zijn per 1 mei jl. alle aanvullende afspraken, zoals toegelicht in dit memo, automatisch van toepassing. De Rijksonderdelen die gebruik maken van de centrale MBSA hoeven dus geen separate acties te ondernemen om de verbeterde afspraken van toepassing te laten zijn.

Voor de datatransfers van de EU naar de VS die met het gebruik van de OST-diensten gemoeid gaan, is er een appendix ontwikkeld die tegemoet komt aan het detailniveau dat door de AVG vereist wordt. Via deze appendix wordt inzichtelijk gemaakt welke typen data door Microsoft Corp., de importeur van deze data, worden verwerkt en waarvoor Microsoft Corp. zich aan alle benodigde waarborgen verbindt. Deze appendix dient per enrollment door het Rijkonderdeel ingevuld te worden.

SLM Microsoft Rijk benadert de reeds aangesloten Rijksonderdelen in de komende weken om deze appendix aan de enrollement toe te voegen.

Hoe verder met de DPIA's? - Efficiencyvoordeel
Een gegevensbeschermingseffectbeoordeling (data protection impact assessment - DPIA) moet worden uitgevoerd als er sprake is van hoge risico's voor de gegevensbescherming van betrokkenen. In een DPIA dienen de effecten van de beoogde verwerkingsactiviteiten op de gegevensbescherming van relevante betrokkenen te 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 online 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 dan 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 Microsoft diensten 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 veel tijd en kosten schelen.

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.
2. Gebruik Windows 10 Enterprise vanaf versie 1903 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. Er is ook geen DPIA gedaan voor gebruikerstoegang tot MyAnalytics and Delve. Indien organisaties deze tools willen gebruiken, dienen ze een DPIA uit te voeren. Hiervoor kan een organisatie contact opnemen met SLM Microsoft Rijk.
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. 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 die beschreven worden in het addendum van de DPIA, zijn gemitigeerd.

Documentatie

Er is een aanzienlijke hoeveel documentatie zoals de DPIA’s maar ook een implementatie handreiking gepubliceerd op deze link naar Rijksoverheid.nl

Paul van den Berg
Strategisch Leveranciers Manager Microsoft Rijk