26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 622 Brief van de ministers van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 juli 2019

Op 20 december 2018 berichtte ik u, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, over dataverzameling en -opslag door Microsoft.[1] Ik berichtte u ook over het overeengekomen verbeterplan met Microsoft en u medio 2019 per brief nader te informeren over de door Strategisch Leveranciers-management Microsoft Rijk (SLM Microsoft Rijk) uitgevoerde verificatie op de uitvoer van het verbeterplan met Microsoft.

De minister van BZK bevordert vanuit de verantwoordelijkheid voor het Rijksinkoopstelsel, een gecoördineerde benadering van strategische ICT-leveranciers van de rijksoverheid. De verantwoordelijkheid voor de uitvoering hiervan is, conform de governance van het Rijksinkoopstelsel, bij verschillende ministeries belegd. Het aanspreekpunt voor Microsoft is SLM Microsoft Rijk en wordt voor het Rijk uitgevoerd door het ministerie van Justitie en Veiligheid.

SLM Microsoft heeft in 2018 een Data Protection Impact Assessment (DPIA) laten uitvoeren op diagnostische dataverzamelingen (dat is data over het gebruik van de software) in nieuwe versies van Microsoft Office. Met de DPIA is vastgesteld dat er via het product 'Microsoft Office ProPlus' diagnostische gegevens van en over de gebruiker verzameld en opgeslagen werden in een database in de VS. Het verzamelen, opslaan en gebruik van deze gegevens is niet conform de Algemene Verordening Gegevensbescherming (AVG).

SLM Microsoft Rijk is met Microsoft in gesprek gegaan en heeft op 26 oktober 2018 overeenstemming bereikt over een verbeterplan. Microsoft verplichtte zich in dit plan om haar producten dusdanig te wijzigen dat het gebruik daarvan voor de bij SLM Microsoft Rijk aangesloten Rijksorganisaties conform de AVG mogelijk is.

De meest urgente wijzigingen, zoals een instellingsmogelijkheid voor beheerders om de verzamelde gegevens tot een minimum te beperken en een mogelijkheid de verzamelde gegevens te verifiëren, heeft Microsoft inmiddels conform het verbeterplan aangebracht. Microsoft heeft eind april een nieuwe versie van de software aangeboden ter verificatie. Deze nieuwe versie van de software is getest en in orde bevonden. Zowel in het product Office ProPlus als ook Windows 10 Enterprise heeft Microsoft wereldwijd de beloofde verbeteringen doorgevoerd.

[1] Kamerstukken 26 643 en 32 761, nr. 585.

Tevens zijn er, zoals afgesproken in het verbeterplan, in mei 2019 aanvullende afspraken gemaakt tussen de Nederlandse Staat en Microsoft waarmee de verplichtingen van de Rijksorganisaties als verwerkingsverantwoordelijke enerzijds en die van Microsoft als verwerker anderzijds nader geregeld worden. De aanvullende afspraken betreffen de verplichtingen die betrekking hebben op de door Microsoft aangeboden producten en diensten met online componenten[2], waaronder Office ProPlus, Windows 10 Enterprise en de maatregelen op de in de DPIA geïdentificeerde acht risico's ten aanzien van Office ProPlus. De aanvullende afspraken gaan met name over risico 6 ("onvoldoende doelbinding/basis voor geautoriseerde doelen"). Dit risico is weggenomen door in de aanvullende afspraken:

- zeer gedetailleerd overeen te komen voor welke doelen Microsoft gegevens van de verwerkingsverantwoordelijke (inclusief persoonsgegevens) 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 worden geanonimiseerd[3].

Hiermee zijn de in de DPIA genoemde risico's in voldoende mate geadresseerd zodat er geen AVG-overtredingen meer hoeven te zijn als een Rijksorganisatie - aangesloten bij SLM Microsoft Rijk- de Microsoftproducten en -diensten besluit te gebruiken en daarbij de implementatierichtlijnen aanhoudt.

Om naleving van Microsoft op de contractuele bepalingen en de AVG te kunnen controleren, een verantwoordelijkheid van de verwerkingsverantwoordelijke, heeft de Nederlandse Staat een procedure voor uitoefening van de verbeterde auditrechten bedongen. Deze audits vinden jaarlijks plaats, waarna een samenvatting van de bevindingen zal worden gepubliceerd op de website van SLM Microsoft.

Voor alle duidelijkheid, terwijl de door de Nederlandse Staat met Microsoft overeengekomen 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 die Rijksonderdelen en ZBO's die aangesloten

[2] Deze producten en diensten staan beschreven in de zogenaamde Online Service Terms
[3] WP29 Opinie 05/2014 over Anonimiseringstechnieken (WP216)

zijn bij het Rijks Microsoft Business en Services contract onder beheer bij SLM Microsoft Rijk.

Het is voor de bedrijfsvoering van de belang dat er gebruik wordt gemaakt van de courante versies van de software van een leverancier. Deze versies bieden de beste mogelijkheden om de ICT-omgevingen up-to-date en veilig te houden en de beveiliging tegen cyberaanvallen en zijn bovendien aangepast aan de meest recente wetgeving zoals de AVG.

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.

De minister van Justitie en Veiligheid,

F.B.J. Grapperhaus

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

K.H. Ollongren