# Samenvatting DPIA Office 365 ProPlus versie 1905

23 juli 2019

SLM Microsoft Rijk (Strategisch Leveranciersmanagement Microsoft Rijk) heeft in mei 2019 opdracht gegeven om een nieuwe gegevensbeschermings-effectbeoordeling (DPIA) uit te voeren op de verwerking van gegevens over het gebruik van de Microsoft Office 365 ProPlus software. Deze DPIA beoordeelt de voortgang van de toezeggingen die Microsoft heeft gedaan na publicatie van de eerste DPIA, in november 2018. Dit rapport bevat een technische analyse van de gegevens over het gebruik van de Office 365 ProPlus software in versie 1905 zoals die door Microsoft wordt aangeboden sinds 11 juni 2019. Gelijktijdig met dit rapport publiceert de Rijksoverheid een DPIA over het gebruik van Office Online en de mobiele Office apps.

## Resultaat: geen hoge privacyrisico's meer

Het resultaat van deze DPIA op Office 365 ProPlus is dat Microsoft en de Rijksoverheid erin zijn geslaagd, door een combinatie van technische, contractuele en organisatorische maatregelen, om de acht hoge privacyrisico's te mitigeren uit de eerste DPIA. Deze hoge risico's werden vooral veroorzaakt door een gebrek aan transparantie, een gebrek aan doelbinding en rechtsgrond, gebrek aan duidelijkheid over de rol van Microsoft als verwerker of als verantwoordelijke, en de doorgifte van gegevens over het gebruik, inclusief de inhoud van bestanden, naar de Verenigde Staten zonder dat er effectieve controlemogelijkheden bestonden. Als de systeembeheerders van Office 365 ProPlus bij de Rijksoverheidsinstellingen de adviezen opvolgen uit deze DPIA, onder andere om de telemetrie op het laagste niveau van 'Neither' te zetten en de Controller Connected Experiences uit te zetten, dan zijn er, dankzij de technische en contractuele maatregelen, geen bekende hoge privacyrisico's meer voor betrokkenen met betrekking tot de verzameling van gegevens over het gebruik van Microsoft Office 365 ProPlus.

## Gebruik door 300.000 ambtenaren

De Office software wordt op grote schaal gebruikt door verschillende overheidsorganisaties, zoals de ministeries, de rechtbanken, de politie en de belastingdienst. Naar schatting 300.000 ambtenaren werken dagelijks met de software, om e-mail te versturen en te lezen, om tekst en rekenbestanden te maken en om visuele presentaties te maken. In het algemeen slaan de organisaties de inhoudelijke bestanden die ze met de Office software maken op in eigen datacentra, on premise. Maar de Nederlandse overheid test ook het gebruik van de online opslagdiensten SharePoint Online en OneDrive for Business. Daarom is het gebruik van deze diensten inbegrepen in deze DPIA, net als het gebruik van de zogenaamde Connected Experiences. Dit zijn online microdiensten die heel nauw verweven zijn met de Office software, zoals de spelling checker (Editor) of de mogelijkheid om plaatjes in te voegen van internet.

## Naleving van de AVG en paraplu-DPIA

De inkoopafdeling van het Rijk die verantwoordelijk is voor de aanschaf van Microsoft producten en diensten, SLM Microsoft Rijk, heeft onderhandeld met Microsoft, maar de individuele overheidsorganisaties kopen de licenties en bepalen de instellingen en de omvang van de diagnostische gegevensverwerking door Microsoft Corporation in de Verenigde Staten. Deze paraplu-DPIA is bedoeld om de organisaties te ondersteunen bij het uitvoeren van eigen DPIA's, maar kan de specifieke risico-inschattingen niet vervangen die de organisaties zelf moeten maken. Die risico-inschattingen zijn namelijk afhankelijk van de specifieke manier waarop de instellingen de software aanbieden, de mate van vertrouwelijkheid van het werk, en de soorten persoonsgegevens die ze verwerken.

## Scope: diagnostische gegevens, geen inhoudelijke of functionele gegevens

Dit rapport behandelt de privacyrisico's van de opslag door Microsoft van gegevens over het gebruik van het individuele gebruik van de Office 365 ProPlus software, inclusief het gebruik van de Connected Experiences en de cloud opslagdiensten. Deze metadata (over het gebruik van de diensten en de software) worden in dit rapport diagnostische gegevens genoemd.

Microsoft verzamelt de diagnostische gegevens op meerdere technische manieren, via systeem-gegenereerde logboeken van gebeurtenissen op haar eigen servers en via de zogenaamde telemetrie-client in Office ProPlus. Net als in Windows 10 heeft Microsoft software ingebouwd in de geïnstalleerde versies van Office die systematisch diagnostische (telemetrie)berichten verzamelt op het apparaat van de gebruiker en regelmatig in *batches* verstuurt naar Microsoft's servers in de Verenigde Staten.

De DPIA gaat over de risico's voor betrokkenen van de verwerking van deze diagnostische gegevens en dus niet over de inhoudelijke gegevens die gebruikers door Microsoft laten verwerken, zoals tekst, foto's en video's. De diagnostische gegevens zijn ook anders dan de functionele gegevens die Microsoft (tijdelijk) moet verwerken om gebruikers in staat te stellen om gebruik te maken via internet van de online diensten van Microsoft.

## Getroffen maatregelen Microsoft Office 365 ProPlus

Microsoft heeft in de afgelopen zes maanden, na de publicatie van de eerste DPIA op Office 365 ProPlus, een groot aantal technische en organisatorische maatregelen doorgevoerd om de geconstateerde privacyrisico's voor Office 365 ProPlus wereldwijd te verlagen.

Sinds mei 2019 publiceert Microsoft uitgebreide documentatie over de diagnostische gegevens over het gebruik van Office ProPlus. Microsoft heeft haar bestaande Data Viewer Tool voor Windows 10 aangepast om ook de Office 365 ProPlus telemetrie gegevens te tonen. Hierdoor kunnen betrokkenen de Office ProPlus gegevens bekijken die Microsoft van hun apparaat verzamelt.

Microsoft biedt sinds mei 2019 een groot aantal veelgebruikte en onmisbare Connected Experiences zoals de spellingchecker, de vertaalmodule en de Office helpfunctie aan als verwerker, en niet meer als verantwoordelijke). Er zijn 14 Connected Experiences waarvoor Microsoft verantwoordelijke blijft, maar Microsoft stelt systeembeheerders van Office ProPlus in staat om het gebruik van deze Controller Connected Experiences centraal uit te zetten. Het centraal uitzetten van deze diensten voorkomt het risico dat werknemers een vraag krijgen van Microsoft om toestemming te geven voor deze diensten, terwijl toestemming geen geldige grondslag is voor deze gegevensverwerking.

**Microsoft optionele Controller Connected Experiences**

| | |
|---|---|
| 3D-kaarten | LinkedIn CV-assistent |
| Kaartgrafieken | Office Store |
| Onlineafbeeldingen invoegen | Online Video insluiten |
| Online-3D-modellen invoegen | Onderzoek |
| PowerPoint Snelstart | Weerbalk in Outlook |
| Onderzoeker | Feedback (behalve in Outlook) |
| Slim zoeken | Een functie voorstellen (in Outlook) |

Sinds Office 365 ProPlus versie 1904, zoals die door Microsoft ter beschikking wordt gesteld sinds 29 april 2019, heeft Microsoft ook een keuzemogelijkheid ingebouwd voor systeembeheerders om het telemetrieniveau te kunnen minimaliseren. Microsoft biedt drie mogelijkheden: Required (noodzakelijk), Optional (optioneel) en Neither (geen van beide).

Uit het technische onderzoek voor deze DPIA blijkt dat Microsoft een beperkt aantal telemetrieberichten verzamelt over het gebruik van de Office ProPlus software. Zowel op het niveau Required als het niveau Neither bevatten de gegevens geen inhoud uit bestanden, e-mails of conversaties, en geen direct identificerende gegevens zoals gebruikersnamen of e-mailadressen. De berichten die betrekking hebben op de Processor (verwerker) Connected Experiences zoals de spellingchecker en de vertaalmodule bevatten ook geen fragmenten van de inhoud.

Sommige berichten op het niveau Required bevatten wel gevoeligere informatie, zoals het exacte aantal pagina's, alinea's, regels, woorden, karakters, spaties, plaatjes en citaten in een Word bestand, of de exacte tijd in milliseconden dat een betrokkene actief bezig was met een bestand.

Er lijkt verder weinig verschil te bestaan tussen de twee telemetrieniveaus, ondanks de uitleg van Microsoft dat er bij keuze voor Neither géén diagnostische gegevens over het gebruik van de geïnstalleerde software naar Microsoft worden verstuurd.

Microsoft heeft naar aanleiding van deze bevindingen uitgelegd dat er nog twee soorten diagnostische gegevens zijn die altijd worden verzameld en niet worden beïnvloed door de telemetriekeuzeknop. Het gaat om 'Required service data' over het gebruik van de Connected Experiences, en gegevens over Essential Services, zoals authenticatie, telemetrie en controle van de licentie. De informatie over deze verwerkingen schiet tekort.

## Contractuele maatregelen om de risico's te verlagen

Microsoft heeft een aantal contractuele privacygaranties opgenomen in de mantelovereenkomst met de Nederlandse Rijksoverheid. Deze garanties gaan over doelbinding en de mogelijkheid voor de Nederlandse overheid om naleving van deze afspraken te kunnen controleren door effectieve auditrechten. Ook de gewijzigde rol van Microsoft als verwerker voor de meeste Connected Experiences is contractueel vastgelegd.

Microsoft erkent dat zij als verwerker voor de verwerking van gegevens over het gebruik van Office 365 ProPlus, de meeste Connected Experiences en de cloud opslagdiensten persoonsgegevens verwerkt via de metadata en dat ze deze gegevens maar voor drie toegestane doelen mag verwerken, en alleen als dat proportioneel is. Deze doelen zijn: (1) het technisch aanbieden en verbeteren van de dienst, (2) de dienst up to date houden en (3) beveiligd.

Deze strikte doelbinding geldt zowel voor de inhoudelijke gegevens (Customer Data) als voor alle soorten diagnostische gegevens, inclusief de systeem-gegeneerde logboeken van gebeurtenissen op de eigen servers van Microsoft. Microsoft heeft aanvullend gegarandeerd dat zij beide soorten gegevens nooit zal gebruiken voor profilering, data analytics, marktonderzoek of adverteren, tenzij de klant er expliciet om vraagt. Hierbij is specifiek een verbod opgenomen in de overeenkomst op het gebruik van diagnostische gegevens om 'aanbevelingen' te tonen over producten van Microsoft die de klant niet heeft gekocht of niet gebruikt.

De Rijksoverheid heeft effectieve auditrechten bedongen, en heeft zich er ook aan gecommitteerd om een onafhankelijke auditor een jaarlijkse audit uit te laten voeren om de naleving te controleren van deze maatregelen en afspraken. SLM Microsoft Rijk zal een samenvatting van de bevindingen publiceren.

## Overzicht van door Microsoft getroffen maatregelen om de hoge risico's te mitigeren

| Nr. | Hoog risico | Getroffen maatregelen door Microsoft |
|---|---|---|
| 1 | Gebrek aan transparantie | Publieke documentatie en data viewer tool |
| 2 | Geen controle over aard en hoeveelheid diagnostische gegevens | Sinds december 2018 tijdelijke instellingen om de verwerking te minimaliseren |
| | | Sinds release van versie 1904: instellingsmogelijkheid systeembeheerders telemetrieniveau |
| 3 | Onrechtmatige verzameling en opslag gevoelige soorten persoonsgegevens door de Connected Experiences en diagnostische gegevens over gebruik cloud servers met bv bestandsnamen | Contractuele doelbinding: verwerking alleen nog voor de 3 doelen waarvoor de overheidsinstellingen een grondslag hebben |
| | | Microsoft treedt op als verwerker voor de meeste Connected Experiences + centrale technische opt-out voor de Controller Connected Experiences |
| | | Contractuele uitsluiting van verwerking voor profilering, data analytics, marktonderzoek en adverteren. |
| 4 | Onterechte kwalificatie Microsoft als verwerker | Contractuele doelbinding |
| | | Microsoft treedt op als verwerker voor de meeste Connected Experiences + centrale technische opt-out voor de Controller Connected Experiences |
| 5 | Niet genoeg controle op subverwerkers en | Effectieve auditrechten voor de Rijksoverheid + |

| | | |
|---|---|---|
| | feitelijke verwerkingen | verbintenis om jaarlijkse audit te verrichten en samenvatting bevindingen te publiceren |
| 6 | Gebrek aan doelbinding ProPlus, Connected Experiences en cloud diensten | Contractuele doelbinding |
| 7 | Chilling effect van personeelsvolgsysteem | - |
| 8 | Lange bewaartermijn van diagnostische gegevens | Microsoft treedt op als verwerker voor de meeste Connected Experiences + centrale technische opt-out voor de Controller Connected Experiences |
| | | Contractuele doelbinding |
| | | Beperking van toekomstige gegevensverzameling door telemetriekeuzemogelijkheid |
| 9 | Doorgifte van (beperkte hoeveelheid) diagnostische gegevens naar de VS | Beperking van toekomstige gegevensverzameling door telemetriekeuzemogelijkheid + Effectieve auditrechten + Contractuele doelbinding . Zie de paragrafen 7 and 16.8.2 voor maatregelen die de EU wetgever moet treffen |

## Aanbevolen maatregelen overheidsorganisaties

Om de resterende privacyrisico's te mitigeren kunnen de overheidsorganisaties ook zelf een aantal maatregelen treffen.

De aanbevolen maatregelen zijn:

- Verbiedt centraal het gebruik van de Controller Connected Experiences;
- Upgrade naar versie 1905 of hoger van Office 365 ProPlus en zet de telemetrie op het niveau 'Neither'. Op het niveau Required verzamelt Microsoft iets meer gevoelige gegevens;
- Actualiseer het bestaande werknemers privacybeleid met specifieke informatie voor welke doelen en onder welke omstandigheden de organisatie de verschillende soorten diagnostische gegevens uit Microsofts verschillende diensten en producten mag bekijken;
- Zet het telemetrieniveau in Windows 10 Enterprise op Security (Beveiliging), of blokkeer het telemetrieverkeer en sta gebruikers niet toe om hun activiteiten te synchroniseren via de Tijdlijn functionaliteit. Windows telemetrie verzamelt op hogere niveaus ook informatie over het gebruik van de Office applicaties;
- Schakel het Customer Experience Improvement Programma (CEIP) uit;
- Zet LinkedIn integratie uit voor Microsoft werknemer accounts;
- Voer DPIA's uit voorafgaand aan het gebruik van Workplace Analytics and Activity Reports in het Microsoft 365 admin center en voordat werknemers gebruik kunnen maken van MyAnalytics and Delve;
- Overweeg gebruik van Customer Lockbox en Customer Key, afhankelijk van de gevoeligheid van de inhoudelijke gegevens;
- Stel beleid op om werknemers te waarschuwen dat zij de mobiele Office apps en de Controller Connected Experiences niet mogen gebruiken, totdat de vijf hoge risico's zijn gemitigeerd.

## Conclusies

Zoals beschreven in de brief van 1 juli 2019 aan de Kamer van de minister van Justitie en Veiligheid en de minister van Binnenlandse Zaken en Koninkrijksrelaties zijn Microsoft en de Rijksoverheid erin geslaagd door een combinatie van technische, contractuele en organisatorische maatregelen om de acht privacyrisico's uit de eerste DPIA te mitigeren. Als de systeembeheerders van de overheidsorganisaties de adviezen opvolgen uit deze DPIA, dan zijn er, dankzij de technische en contractuele maatregelen, geen bekende hoge dataprotectierisico's meer voor betrokkenen met betrekking tot de verzameling van gegevens over het gebruik van Microsoft Office 365 ProPlus.