Samenvatting DPIA Office Online en mobiele Office apps

23 juli 2019

De Microsoft Office 365 Enterprise licentie omvat het gebruik van drie verschillende versies van de software Microsoft Office kan op drie manieren worden gebruikt: geïnstalleerd op de computers en laptops van gebruikers (Office 365 ProPlus), geïnstalleerd op smartphones en tablets (mobiele Office apps voor iOS en Android) en in de vorm van online applicaties die in de browser draaien (Office Online). Deze gegevensbeschermingseffectbeoordeling (DPIA) gaat over het gebruik van de laatste twee versies van de software: Office Online en de mobiele Office apps. Gelijktijdig met dit rapport publiceert de Rijksoverheid een DPIA over het gebruik van versie 1905 van Office ProPlus, zoals die door Microsoft sinds 11 juni 2019 wordt aangeboden. Beide rapporten houden rekening met de resultaten van de onderhandelingen tussen Microsoft en het Rijk over de bereikte contractuele en technische verbeteringen van de Office software.

Resultaat: vijf hoge privacyrisico's

Het resultaat van deze DPIA is dat er vijf hoge restrisico's zijn voor betrokkenen en vier lage risico's, ondanks de technische, contractuele en organisatorische maatregelen die Microsoft heeft getroffen om de dataprotectierisico's te verlagen. De hoge risico's zijn het gevolg van de volgende drie omstandigheden:

1. Microsoft gedraagt zich als een verantwoordelijke voor de mobiele Office apps, en verwerkt de persoonsgegevens voor alle veertien doelen van haar (op consumenten gerichte) privacyverklaring. Eén van deze doelen is adverteren, en minstens drie van de apps op iOS sturen persoonsgegevens naar een marketingbedrijf uit de Verenigde Staten
2. Microsoft heeft nog geen technische opt-outmogelijkheid gemaakt om het gebruik van de Controller Connected Experiences te verbieden in Office Online en de mobiele Office apps
3. De systeembeheerders van de overheidsinstellingen kunnen het gebruik van de mobiele Office apps technisch niet voorkomen

De risico's worden beschreven in de twee tabellen onderaan deze samenvatting, met maatregelen die Microsoft en de overheidsorganisaties kunnen treffen om de risico's weg te nemen.

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 privacyisico's van de opslag door Microsoft van gegevens over het gebruik van de vijf meest gebruikte applicaties in Office Online en de mobiele Office apps: Word, PowerPoint, Outlook, Excel en Teams. Deze apps zijn onderzocht in combinatie met het gebruik van de Connected Experiences and de cloud opslag en email diensten van Microsoft. 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 de mobiele Office apps. Net als in Windows 10 heeft Microsoft software ingebouwd in de geïnstalleerde versies van de Office die systematisch diagnostische gegevens 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.

Technische analyse persoonsgegevens

Privacy Company heeft technisch onderzoek gedaan naar de gegevensverwerking via de mobiele Office apps en is erin geslaagd om een flink deel van de gegevens leesbaar te maken. De Data Viewer Tool die Microsoft ter beschikking stelt voor Windows 10 en Office 365 ProPlus is niet geschikt om de gegevens uit de mobiele Office apps te kunnen bekijken.

Om ook zicht te krijgen op de gegevens die Microsoft verwerkt op haar eigen servers over het gebruik van Office Online en de cloud opslag en e-maildiensten zijn er inzageverzoeken ingediend bij Microsoft, zoals bedoeld in artikel 15 van de AVG, nadat er testscenario's zijn uitgevoerd.
Uit de technische analyse van de gegevens uit de mobiele Office apps en de resultaten van de inzageverzoeken blijkt dat Microsoft direct identificerende persoonsgegevens verzamelt, zoals de gebruikersnaam en het e-mailadres en de tijdstippen waarop medewerkers activiteiten hebben verricht in de verschillende applicaties. Microsoft verzamelt niet veel diagnostische gegevens over het gebruik van de mobiele Office apps en Office Online, en geen inhoudelijke gegevens uit de inhoud van bestanden, e-mails of chats, net zomin als bestands- of padnamen. Maar als overheidsorganisaties gebruik maken van de cloud opslag en e-maildiensten SharePoint Online, OneDrive for Business en Exchange Online dan verzamelt Microsoft wél inhoudelijke gegevens uit de bestands- en padnamen en de onderwerpsregel van mails in haar systeem-gegenereerde logboeken van gebeurtenissen op haar servers.

Het opgevangen netwerkverkeer laat zien dat Microsoft vanuit tenminste drie van de Office apps op iOS (Word, PowerPoint en Excel) diagnostische gegevens verstuurt naar een marketingbedrijf uit de Verenigde Staten, Deze verwerking vindt plaats zonder dat de gebruiker dit weet, zonder enige informatie over de aanwezigheid of doelen van deze verwerking. Hoewel het gegeven op zich niet gevoelig is dat een unieke medewerker op een specifiek tijdstip met een specifieke applicatie heeft gewerkt, wordt deze overgedragen naar een bedrijf in de Verenigde Staten dat niet gebonden is aan de privacygaranties die Microsoft informatie wel geeft. Het bedrijf is gespecialiseerd in het opstellen van voorspellende profielen over individuen voor commerciële doelen, *predictive profiling*.

Veel risicomitigerende maatregelen Microsoft niet van toepassing op Office Online en de mobiele Office apps

Uit de DPIA over de dataprotectierisico's van de verwerking van diagnostische gegevens door Office 365 ProPlus blijkt dat er dankzij de onderhandelingen tussen SLM Microsoft Rijk en Microsoft geen bekende hoge risico's meer zijn voor Nederlandse overheidsorganisaties. Maar Microsoft heeft veel van de technische en organisatorische maatregelen niet toegepast op Office Online, terwijl de maatregelen in het geheel niet gelden voor de mobiele Office apps.

Microsoft kwalificeert zichzelf als een verantwoordelijke voor de mobiele Office apps. Dat betekent dat de contractuele verbeteringen die SLM Microsoft Rijk met Microsoft heeft onderhandeld, niet van toepassing zijn, ondanks Microsoft's garantie dat alle privacygaranties effectief van toepassing zijn op alle gegevens die zij verwerkt over gebruikers die zijn ingelogd met hun Azure Active Directory account.

Microsoft heeft nog geen technische opt-outmogelijkheid gemaakt om het gebruik van de Controller Connected Experiences te verbieden in Office Online en de mobiele Office apps. Sinds mei 2019 biedt Microsoft de meeste onmisbare Connected Experiences zoals de Editor (de spelling checker) aan vanuit een rol als verwerker (in plaats van als verantwoordelijke). Toch zijn er ook nog veertien Connected Experiences waarvoor Microsoft verantwoordelijke blijft.

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)

Als overheidsorganisaties toestaan dat medewerkers gebruik maken van de mobiele Office apps en de Controller Connected Experiences dan worden ze gezamenlijk verantwoordelijk met Microsoft voor de diagnostische gegevensverwerking. Dit heet tot gevolg dat de overheidsorganisaties aangesproken kunnen worden op de risico's die betrokkenen lopen met betrekking tot onrechtmatige verwerking van hun persoonsgegevens.

Microsoft heeft geen informatie gepubliceerd over de diagnostische gegevens uit de mobiele Office apps of Office Online, en biedt beheerders in deze softwareversies geen keuze om de gegevensstroom te minimaliseren.

Risico's en maatregelen

Op dit moment leidt de verwerking van diagnostische gegevens over het gebruik van Office Online en de mobiele Office apps in de grootzakelijke Enterprise omgeving, in combinatie met het gebruik van de Controller Connected Experiences, tot vijf hoge en vier lage dataprotectierisico's voor betrokkenen.

Nr.	Hoog risico	Maatregelen die Microsoft kan treffen
1	Gebrek aan transparantie	Publiceer informatie over de diagnostische gegevens mobiele Office apps en de Controller Connected Experiences
		Maak gebruik van Data Viewer Tool ook mogelijk voor de mobiele Office apps
		Stel betrokkenen in staat hun AVG-rechten uit te oefenen m.b.t. de Controller Connected Experiences en de mobiele apps
2	Geen technische opt-out Controller Connected Experiences en mobiele Office apps	Tijdelijke oplossing: Geef technische mogelijkheid om te verhinderen dat betrokkenen de mobiele Office apps gebruiken OF vraag niet om toestemming en staak de verwerking van de diagnostische gegevens buiten de Azure AD om.
		Permanente oplossing: word verwerker voor de mobiele apps
		Bouw een centrale technische opt-out voor verantwoordelijken om het gebruik te verhinderen van de Contr. Connected Experiences via Office Online en de mobiele apps
3	Onrechtmatige verzameling en opslag gevoelige soorten persoonsgegevens door de Controller Connected Experiences	Word verwerker voor de mobiele Office apps + bouw centrale technische opt-out voor de Contr. Connected Experiences + contractuele uitsluiting van verwerking voor de doelen van profilering, data analytics, marktonderzoek of adverteren.
4	Gebrek aan doelbinding mobiele apps en Contr. Connected Experiences	Word verwerker voor de mobiele Office apps
5	Niet genoeg controle op subverwerkers en feitelijke verwerkingen	Verzeker effectieve auditrechten voor de Nederlandse overheid met betrekking tot de mobiele Office apps en de Controller Connected Experiences

De overheidsorganisaties kunnen maar weinig effectieve maatregelen nemen om deze hoge risico's te mitigeren.

1. Stel beleid op om werknemers te waarschuwen dat zij de mobiele Office apps en de Controller Connected Experiences niet mogen gebruiken.
2. Informeer werknemers over hun recht op inzage van de diagnostische gegevens die Microsoft verzamelt via de DSR en de audit logbestanden.
3. Zet de Controller Connected Experiences uit zodra dat technisch mogelijk is.

Nr.	**Laag risico**	**Maatregelen die Microsoft kan treffen**
6	Geen controle over aard en hoeveelheid diagnostische gegevens	Bouw technische data minimalisatie keuzes voor de diagnostische gegevens in alle Office 365 diensten (niet alleen voor ProPlus)
7	Chilling effect van personeelsvolgsysteem	Dataminimalisatie, privacy by default instellingen
8	Lange bewaartermijn van diagnostische gegevens	Word verwerker voor de mobiele Office apps + centrale technische opt-out voor Contr. Connected Experiences
		Publiceer informatie over de verschillende bewaartermijnen van de diagnostische gegevens
9	Doorgifte van (beperkte hoeveelheid) diagnostische gegevens naar de VS	Dataminimalisatie + Word verwerker + effectieve auditrechten. Zie paragrafen 7 and 16.8.2 voor maatregelen die de EU wetgever moet treffen

De overheidsorganisaties kunnen zelf een paar technische en organisatorische maatregelen treffen om de resterende lage dataprotectierisico's te mitigeren.

1. 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;
1. 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;
2. Kies het laagste, minimumniveau voor de verzameling van diagnostische gegevens zodra dat technisch mogelijk is;
3. Ondersteun SLM Microsoft Rijk in het beoordelen van de geldigheid van doorgifte instrumenten na toekomstige jurisprudentie van het Europees Hof van Justitie. Het is aan het Europees Hof van Justitie om de risico's in te schatten van massa surveillance in de Verenigde Staten en aan de Europese wetgever om de resterende risico's te verlagen van doorgifte van diagnostische gegevens vanuit de EU naar de VS.

Conclusies

Op dit moment zorgt de verwerking van diagnostische gegevens over het gebruik van de mobiele Office apps en de Controller Connected Experiences voor vijf hoge dataprotectierisico's. Alleen Microsoft kan deze risico's effectief wegnemen. SLM Microsoft Rijk adviseert de overheidsorganisaties om beleid op te stellen voor werknemers om Office Online en de mobiele Office apps tijdelijk niet te gebruiken. SLM Microsoft Rijk zet haar onderhandelingen met Microsoft voort om ervoor te zorgen dat Microsoft de onderhandelde verbeteringen doorzet voor alle diensten die inbegrepen zijn bij de Office 365 licentie.