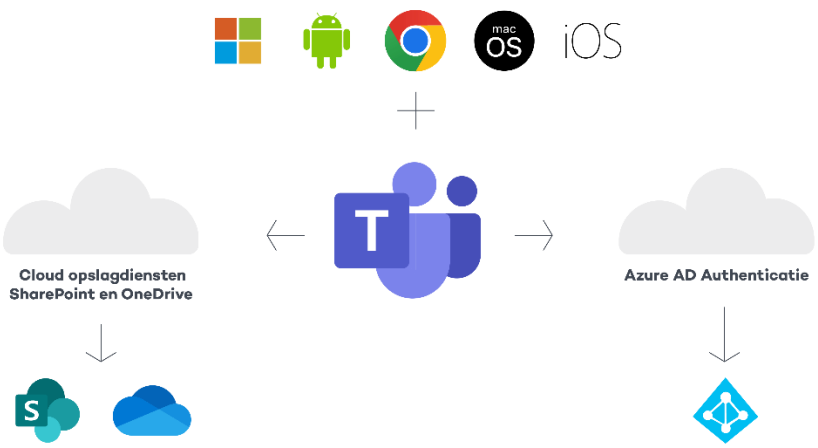
Samenvatting

Deze Data Protection Impact Assessment (DPIA) beoordeelt de gegevensbeschermingsrisico's van het (professionele) gebruik van Microsoft Teams in combinatie met OneDrive, SharePoint Online en de Azure Active Directory.

Teams is een online tool voor videobellen, chatten en het delen van bestanden. Als onderdeel van Office 365 levert Microsoft twee cloudopslagdiensten aan eindgebruikers: OneDrive en SharePoint Online. Deze diensten worden vaak gebruikt voor het openen en opslaan van bestanden die via Teams worden gedeeld. Om gebruik te kunnen maken van de online diensten van Microsoft moeten eindgebruikers en systeembeheerders, net als gastgebruikers, worden geauthenticeerd via de online clouddienst Azure Active Directory.

Reikwijdte van de DPIA

De gegevensverwerking via Teams en de drie clouddiensten is getest in de drie verschillende versies van de Office-software die inbegrepen zijn bij de Microsoft 365 Enterprise-licentie. Teams, SharePoint en OneDrive kunnen worden geïnstalleerd op de computers en laptops van werknemers (Office 365 ProPlus), geïnstalleerd op smartphones en tablets (mobiele Office-apps voor iOS en Android) en als online toepassingen die in een browser draaien (Office voor het Web, voorheen bekend als Office Online).



Deze DPIA is een herhaalde beoordeling van het gebruik van Teams, SharePoint en OneDrive op twee versies van de Office-software: Office voor het Web en de mobiele Office-apps. Deze DPIA bevat uitkomsten met betrekking tot de verwerking van diagnostische gegevens in Office voor het Web en de mobiele Office-apps per 31 mei 2020, zoals opnieuw getest in september 2021.

Deze DPIA is uitgevoerd in opdracht van SLM Rijk, de centrale onderhandelaar voor producten en diensten van Microsoft, Google en Amazon Web Services voor de rijksoverheid, en voor SURF, de centrale IT-inkooporganisatie voor Nederlandse hogescholen en universiteiten.

Uitkomst: zes lage privacyrisico's

De uitkomst van deze DPIA, na herhaald overleg met Microsoft, is dat er geen bekende hoge risico's meer zijn voor de verwerking van Diagnostische Gegevens. Wel is er een hoog risico als organisaties Microsoft Teams gebruiken om zeer gevoelige en bijzondere categorieën gegevens te verwerken, vanwege de mogelijke toegang door opsporings- en inlichtingendiensten in de VS.

Zes lage privacyrisico's bij de verwerking van Diagnostische Gegevens

De zes lage gegevensbeschermingsrisico's hangen samen met de volgende omstandigheden:

1. De huidige systematische **doorgifte van een beperkte hoeveelheid Diagnostische Gegevens en de incidentele doorgifte van beveiligingsgegevens naar de VS** leveren allebei gegevensbeschermingsrisico's op. Organisaties kunnen deze risico's aanvaarden, omdat deze risico's uiterlijk eind 2022 zullen zijn weggenomen, na voltooiing van de EU Data Boundary van Microsoft. Vanaf dat moment verwerkt Microsoft alle inhoudelijke, diagnostische, account- en support gegevens van Enterprise- en Education-klanten uit de EU uitsluitend in de EU-datacenters van Microsoft. Hoewel Microsoft nog steeds sommige persoonsgegevens naar de VS blijft doorgeven, om security risico's op te sporen en op te lossen, zullen deze doorlopende doorgiftes incidenteel zijn, niet structureel, en over het algemeen alleen pseudonieme en geaggregeerde gegevens bevatten.
2. Microsoft is **niet erg transparant over de browser-gebaseerde verzameling van telemetriegegevens** en de telemetrie-events over het gebruik van de zogenaamde *verbonden ervaringen* (Connected Experiences). Microsoft noemt deze diagnostische gegevens *Required Service Data*. Zelfs als een klant het verzamelen van Office-telemetriegegevens heeft geminimaliseerd, door 'geen/neither' te selecteren, heeft deze instelling geen invloed op het verzamelen van *Required Service Data*. Volgens Microsoft zijn deze gegevens te dynamisch of vertrouwelijk van aard om in detail te publiceren, maar Microsoft belooft deze gegevens alleen te verwerken voor de drie overeengekomen verwerkingsdoeleinden.
3. Microsoft heeft toegezegd haar inzage-tool voor Diagnostische Gegevens te verbeteren, om beheerders te helpen bij eventuele **inzageverzoeken** van individuele werknemers. Dit hulpmiddel is momenteel nog moeilijk te gebruiken.
4. Er is **één uitzondering** op de garantie van Microsoft dat de *Required Service Data* **geen direct identificeerbare (leesbare) gebruikersnamen/mailadressen of documentnamen bevatten**. Uit de technische analyse van het netwerkverkeer die voor deze DPIA is uitgevoerd blijkt dat Microsoft de gebruikersnaam en/of het e-mailadres van een werknemer kan verzamelen, samen met de naam van de klant (de *tenant*) en het bestandspad met de volledige naam van het document. Microsoft heeft uitgelegd waarom dit nodig kan zijn in OneDrive, bijvoorbeeld als meerdere gebruikers tegelijkertijd in hetzelfde document werken. Microsoft heeft ook uitgelegd dat de toegang tot deze diagnostische OneDrive-gegevens wordt gecontroleerd, beperkt is tot de *just-in-time* security groep, en beperkt is tot technici die een goedgekeurde zakelijke rechtvaardiging hebben. Bovendien worden deze specifieke telemetriegegevens nooit langer dan 30 dagen bewaard.
5. Microsoft biedt **twee verschillende analytische diensten voor Teams**: *Teams Analytics & reports* en *Viva Insights*. De eerste tool (*Teams Analytics & reports*) biedt gedetailleerd inzicht aan beheerders in individueel werkgedrag. Hoewel Microsoft de mogelijkheid biedt om de namen van de medewerkers te pseudonimiseren, is het niet duidelijk of dit enig effect heeft op de ruwe datalogs van Microsoft. Ervaren beheerders van universiteiten en overheidsorganisaties kunnen dit risico zelf beperken, door deze functionaliteit uit te schakelen. Microsoft is niet bereid om de standaardinstelling te wijzigen. De andere tool, *Viva Insights*, staat standaard uit. Deze tool omvat *MyAnalytics* en *Workplace Analytics*, tools die respectievelijk werknemers informatie bieden over hun productiviteit, en managers inzicht bieden in de werkpatronen van individuele werknemers. Als een beheerder de dienst bewust inschakelt, heeft de individuele gebruiker nog steeds de mogelijkheid om zich af te melden.
6. Microsoft is bezig om het **verkeer naar zijn zoekmachine Bing vanuit SharePoint structureel te verwijderen** wanneer een Enterprise- of Education-klant de verbonden ervaringen heeft uitgeschakeld waarvoor Microsoft de verantwoordelijke is (de zogenaamde *Aanvullende, optionele Verbonden Ervaringen*). Tijdens de eerste tests voor deze DPIA in mei 2021 verzond SharePoint beeld zoekopdrachten naar Bing vanuit de browser. Aangezien Microsoft verwerkingsverantwoordelijke is voor de gegevensverwerking van Bing, staat Microsoft zichzelf toe persoonsgegevens te verwerken voor alle 17 (commerciële) doelen uit haar (consumenten) privacyverklaring. Het verkeer naar Bing moet in juli 2022 definitief zijn verwijderd.

Hoog risico in verband met toegang tot onversleutelde bijzondere persoonsgegevens

Er is een hoog gegevensbeschermingsrisico in verband met de mogelijke toegang van opsporings- en inlichtingendiensten uit de VS tot zeer gevoelige en bijzondere persoonsgegevens. Dit risico doet zich voor ondanks het feit dat de inhoudelijke gegevens in Teams, OneDrive en SharePoint nu al uitsluitend in de Europese datacentra van Microsoft worden verwerkt en opgeslagen. Dit omdat er toegang tot deze gegevens kan worden gevorderd via Amerikaanse wetgeving zoals de US CLOUD Act. Organisaties kunnen dit hoge risico voor bijzondere persoonsgegevens in bestanden op OneDrive en SharePoint beperken door hun eigen encryptiesleutels te gebruiken, met Microsoft Double Key Encryption. Microsoft biedt nog geen end-to-end encryptie voor de streaming communicatie met meerdere deelnemers in Teams, alleen voor ongeplande één-op-één videogesprekken. Hoewel Microsoft in reactie op deze DPIA heeft bevestigd dat ze E2EE mogelijk zal maken in Teams-groepsvergaderingen en voor de chats, noemt ze nog geen termijn.

Voor "gewone" soorten persoonsgegevens worden de doorgifterisico's als zeer laag beoordeeld, ook al kunnen de mogelijke gevolgen voor de betrokkenen zeer groot zijn. De kans dat Microsoft wordt gedwongen persoonsgegevens van EU-klanten uit de publieke sector te verstrekken, is zeer klein. Microsoft mag niet bekendmaken of ze specifieke vorderingen heeft ontvangen die onder een geheimhoudingsplicht vallen, maar Microsoft verklaart publiekelijk: "Microsoft verstrekt geen persoonsgegevens van EU-klanten uit de publieke sector aan enige overheid, en heeft dat ook nooit gedaan." Dit historische feit, in combinatie met het gebruik van de versleuteling door Microsoft (met eigen sleutels), haar juridische garanties dat ze elk bevel zal aanvechten, haar bewezen staat van dienst en haar transparantieverslagen, volstaat om het risico van ongeoorloofde toegang tot de "gewone" persoonsgegevens in te schatten als een laag gegevensbeschermingsrisico. Organisaties mogen echter geen zeer gevoelige of bijzondere persoonsgegevens via Teams uitwisselen, tenzij de gegevens van nature openbaar zijn (zoals universitaire colleges of sommige rechtszaken), omdat zij niet zelf de encryptiesleutels beheren.

Scope: Inhoudelijke, Diagnostische en Account Gegevens

Deze DPIA gaat in de eerste plaats over de gegevensbeschermingsrisico's van het opslaan door Microsoft van gegevens over het individuele gebruik van Teams, OneDrive en SharePoint, in combinatie met het gebruik van de Azure AD, op alle platforms. Deze metagegevens (over het gebruik van de diensten en software) worden in de DPIA Diagnostische Gegevens genoemd.

Technisch gezien verzamelt Microsoft de Diagnostische Gegevens op verschillende manieren, via systeemgegenereerde event logs op haar eigen cloud servers en via de telemetrie clients in de verschillende applicaties en via de browser. Vergelijkbaar met de telemetrieclient in Windows 10 en in Office 365 ProPlus, heeft Microsoft de mobiele Office-apps en Office voor het Web geprogrammeerd om systematisch telemetriegegevens op het apparaat te verzamelen en deze regelmatig naar de servers van Microsoft in de VS te sturen. Daarnaast creëert Microsoft gedetailleerde analytische inzichten over het individuele gebruik van Teams.

De scope van deze DPIA omvat daarnaast ook de verwerking van de Inhoudelijke Gegevens en de Account Gegevens, met het oog op de risico's van doorgifte naar de VS.

Technische analyse persoonsgegevens

Het technische onderzoek naar de gegevensverwerking is uitgevoerd door een groot aantal uitgeschreven scenario's uit te voeren en het uitgaande netwerkverkeer te onderscheppen en te analyseren. Daarnaast zijn er inzageverzoeken ingediend via de inzagetool die Microsoft beschikbaar stelt aan beheerders, en zijn de auditlogbestanden bekeken over het individuele gebruik van Teams, SharePoint en OneDrive.

Inhoud telemetrieverkeer

Uit het onderzoek blijkt dat Microsoft beperkte gegevens verzamelt over het individuele gebruik van Teams, SharePoint en OneDrive via de telemetrie-events. Hoewel de telemetriegegevens unieke UserID's, apparaat-ID's en correlatie-ID's bevatten, is de inhoud onleesbaar gemaakt. Uit de technische analyse blijkt dat Microsoft zich niet houdt aan zijn belofte om nooit gebruikersnamen op te nemen op het (laagste) telemetrieniveau van 'geen/neither'. Sommige telemetrie-events bevatten de (leesbare) gebruikersnaam in Sharepoint URL's in de events gegenereerd door Teams, OneDrive en SharePoint voor het Web (benaderd via een browser) en in OneDrive op iOS. Volgens de reactie van Microsoft op deze DPIA is het verzamelen van deze Inhoudelijke (direct identificeerbare) Gegevens, in combinatie met de pseudonieme gebruikersidentificatie, strikt noodzakelijk voor een beperkte opsporing van fouten in de software.

Behalve deze direct identificeerbare gebruikersnamen en OneDrive-padnamen, heeft Privacy Company geen Inhoudelijke Gegevens waargenomen in de onderschepte telemetrie-events. De events bevatten ook geen informatie over bestandsnamen of andere door de gebruiker verstrekte gegevens, zoals apparaat- of profielnamen.

Inhoud service-gegenereerde service logs

Uit de auditlogbestanden en de resultaten van de inzageverzoeken voor de Diagnostische Gegevens blijkt dat Microsoft direct identificeerbare persoonsgegevens verwerkt in de Diagnostische Gegevens over het gebruik van Teams, OneDrive en SharePoint in combinatie met de Azure AD. Uit de logbestanden over de test-gebruikers blijkt dat een direct identificeerbare persoon op een specifiek tijdstip een handeling heeft verricht in een geteste app, met welke browser en vanuit welk besturingssysteem. Microsoft registreert ook of er een inlogfout was, wat de oorzaak was, en hoe de gebruiker werd geauthenticeerd. De gebruikers zijn direct te identificeren door de velden met de gebruikersnaam en het e-mailadres. Deze toegangsbestanden bevatten ook het gebruikte IP-adres.

Omdat elke logregel de combinatie van UserId en Organisation ID bevat, is elke logregel een persoonsgegeven. Daarnaast bevatten deze logbestanden informatie over acties op de servers, en Inhoudelijke Gegevens in de namen van paden en bestanden.

Doelen, rollen en grondslagen

In het door SLM Rijk en SURF onderhandelde privacy amendement is vastgelegd dat Microsoft de persoonsgegevens die zij verkrijgt van, via, of door het gebruik van de online diensten in beginsel alleen als verwerker mag verwerken, voor drie geautoriseerde doelen, maar alleen wanneer dat proportioneel is. Deze drie doelen zijn:

1. de dienst verlenen en verbeteren,
2. de dienst up-to-date te houden, en
3. de dienst beveiligen.

In overeenstemming met dit privacy-amendement verwerkt Microsoft de persoonsgegevens over het gebruik van Teams, OneDrive, SharePoint en de Azure AD inderdaad als een verwerker.

Privacyrisico's en mitigerende maatregelen

In de onderstaande tabel staan de ene hoge, en zes lage, privacyrisico's voor betrokkenen, en de mitigerende maatregelen die overheidsorganisaties, universiteiten en Microsoft kunnen nemen.

Nr.	Hoog risico	Maatregelen overheden en universiteiten	Maatregelen Microsoft
1.	Inhoudelijke Gegevens verwerkt in de EU zijn toegankelijk	Wissel geen gevoelige of bijzondere persoonsgegevens uit via Teams-gesprekken die niet end-to-end versleuteld zijn	Maak een duidelijke termijn bekend wanneer E2EE zal worden ondersteund voor groepsvergaderingen en chatten

Nr.	Hoog risico	Maatregelen overheden en universiteiten	Maatregelen Microsoft
	voor Microsoft, indien geen E2EE	Gebruik *Double Key Encryption* voor bestanden met gevoelige of bijzondere persoonsgegevens die zijn opgeslagen in SharePoint/OneDrive. Hieronder vallen ook opnamen van Teams-gesprekken. Gebruik Customer Lockbox om andere opgeslagen persoonsgegevens te beschermen	Voldoe aan de SCC-eis om klanten te informeren wanneer Microsoft niet langer kan voldoen aan de gegevensbeschermingsgaranties in de SCC
		Schakel E2EE standaard in voor 1-op-1 gesprekken in Teams, en instrueer eindgebruikers om ook E2EE in te schakelen	
		Maak een Teams en OneDrive privacybeleid voor interne en gastgebruikers, stel regels op voor het delen van bestanden en afbeeldingen. Laat medewerkers en gastgebruikers deze regels accepteren door middel van voorwaarden die door Azure AD worden opgelegd	
2.	Structurele *doorgifte* van telemetriegege-vens naar de VS (tot december 2022)	Accepteer het tijdelijke risico van de doorgifte van deze pseudoniem gegevens terwijl Microsoft bezig is met de ontwikkeling van de EU Data Boundary	Pas uiterlijk eind 2022 de EU Data Boundary op alle persoonsgegevens (met de bekende uitzonderingen)
	Mogelijke toegang vanuit de VS tot auditlogbestan-den en Account Gegevens in de Azure AD en telemetriegege-vens die nu al, of na 2022, in de EU worden verwerkt en opgeslagen	Accepteer het risico van toegang tot namen en e-mailadressen in de Azure AD of overweeg het gebruik van pseudoniemen in de Azure AD.	Informeer klanten over de actuele status per dienst/applicatie van de EU Data Boundary
		Gebruik geen SMS voor authenticatie om de doorgifte te voorkomen van niet-versleutelde mobiele telefoonnummers naar derde landen. Gebruik in plaats daarvan de Authenticator app of een hardware token	
		Gebruik pseudoniemen wanneer de Azure AD wordt gebruikt voor Single Sign On met externe leveranciers voor medewerkers waarvan de werkidentiteit vertrouwelijk moet blijven	
	Incidentele *doorgifte* van pseudonieme gegevens aan de VS voor security doelen	Stel bij het gebruik van OneDrive en SharePoint beleidsregels op om te voorkomen dat bestandsnamen en bestandspaden persoonlijke gegevens bevatten	
3.	Voortdurende incidentele *doorgifte* van gebruikersnamen/ e-mailadressen/ padnamen op OneDrive naar de VS	Overweeg het gebruik van pseudonieme accounts voor werknemers van wie de werkidentiteit vertrouwelijk moet blijven	
		Stel bij het gebruik van OneDrive en SharePoint beleidsregels op om te voorkomen dat bestandsnamen en bestandspaden persoonsgegevens bevatten	
4.	Gebrek aan transparantie Telemetriegege-vens	Maak regelmatig gebruik van de Data Viewer Tool, indien beschikbaar, en vergelijk de resultaten met de openbare documentatie van Microsoft	Biedt een functionele Data Viewer Tool aan voor de OneDrive telemetriegegevens op Windows en MacOS
		Gebruik Microsofts inzagetool voor beheerders om toegang te krijgen tot Diagnostische Gegevens, en vergelijk die met een incidentele analyse van het netwerkverkeer	Controleer de naleving van de doelbinding door specifieke auditvragen toe te voegen over de inhoud, de gebruiksdoelen en de bewaartermijnen van de *Required Service Data*.

Nr.	Hoog risico	Maatregelen overheden en universiteiten	Maatregelen Microsoft
		Informeer werknemers over hun toegangsmogelijkheden via het hulpprogramma Data Viewer, of door een DSAR in te dienen bij de admin van de organisatie	Verstrek meer informatie over de *Required Service Data*, waaronder de telemetriegegevens uit Office voor het Web
5.	Beperkingen aan het inzagerecht in de *Required Service Data*	Gebruik Microsofts DSAR-tool om toegang te krijgen tot de Diagnostische Gegevens, en vergelijk die af en toe met een analyse van het netwerkverkeer	Verbeter de inzagetool voor de Diagnostische Gegevens
		Ondersteun een specifieke audit door SLM Rijk op Microsoft's verzameling en gebruik van de *Required Service Data*	Geef een duidelijke en begrijpelijke uitleg over de inhoud van de Required Service Data
			Laat een onafhankelijke audit uitvoeren op de uitleg waarom de inzagetool zeer beperkte toegang biedt tot *Required Service Data*: omdat gegevens maar heel kort bewaard worden, of omdat Microsoft geen persoonsgegevens zou verzamelen
6.	Gebrek aan controle: verstrekking van persoonsgegevens aan Microsoft en derde partijen die verwerkings-verantwoorde-lijken zijn	Schakel de Aanvullende Optionele Verbonden Ervaringen uit	Zorg ervoor dat eind Q2 2022 al het verkeer naar Bing is verwijderd van SharePoint Online
		Schakel de toegang uit tot apps van derde partijen in de Teams appstore	
		Instrueer eindgebruikers om geen gebruik te maken van Bing zoekopdrachten voor afbeeldingen in SharePoint Online (totdat functionaliteit is verwijderd)	Stuur geen verkeer naar Cloudflare op Microsoft helppagina's die worden aanbevolen in hyperlinks in het Teams-instellingenmenu op de verschillende platforms
7.	Personeelsvolgsysteem: chilling effect	Schakel de functionaliteit *Teams Analytics & rapporten* uit, gebruik pseudonimisering: schakel *Viva Insights* niet in	Voldoe aan art. 25 AVG (gegevensbescherming door ontwerp en standaardinstellingen): schakel Teams Analytics & rapporten standaard uit
		Voer een DPIA uit voorafgaand aan gebruik van deze analytische tools, zeker bij gebruik in combinatie met andere Microsoft Windows & Office analytische diensten	Informeer beheerders wat de gevolgen zijn voor de ruwe data onder beheer van Microsoft bij een keuze voor het pseudonimiseren van de gegevens in *Teams Analytics & reports*.
		Maak een beleid om te voorkomen dat *Teams Analytics & reports* wordt gebruikt als tool om werknemers te monitoren	

Conclusies

Sinds juni 2019 heeft Microsoft, als gevolg van de onderhandelingen met SLM Rijk en SURF, veel juridische, technische en organisatorische maatregelen getroffen om de risico's voor betrokkenen te beperken bij de verwerking van persoonsgegevens door het gebruik van Teams, OneDrive, SharePoint en de Azure AD. In antwoord op de aanvankelijke bevindingen van deze DPIA heeft Microsoft een aantal tekortkomingen verholpen en uitleg gegeven over haar gegevensverwerking.

Gelet op het Schrems-II arrest en de technische bevindingen moet Microsoft nog meer aanpassingen en verbeteringen doorvoeren om het resterende hoge risico en de zes lage risico's te verhelpen. Microsoft moet een duidelijke termijn communiceren voor de toepassing van E2EE op alle Teams-gesprekken. Bovendien moet Microsoft transparanter worden over de inhoud van de Required Service Data, en via een onafhankelijke audit laten controleren dat zij de overeengekomen doelbinding en bewaartermijnen naleeft voor deze specifieke telemetriegegevens. Microsoft moet beheerders in staat stellen om te kiezen voor opt-in voor alle

nieuwe analytische diensten, op basis van duidelijke informatie over de gevolgen voor de gegevensverwerking.

Als overheidsorganisaties en universiteiten alle aanbevolen maatregelen uitvoeren, zijn er geen bekende hoge risico's voor de gegevensverwerking.

Waarschuwing

Het is onzeker hoe de nationale gegevensbeschermingsautoriteiten de risico’s van doorgifte gaan beoordelen in hun gezamenlijk onderzoek naar het gebruik van clouddiensten door publieke sector organisaties. De resultaten worden eind 2022 verwacht. Voor deze DPIA zijn de doorgifterisico's streng beoordeeld. Er is ook een aparte DTIA uitgevoerd, een Data Transfer Impact Assessment. Indien nodig zullen deze DPIA en DTIA in 2023 worden geactualiseerd.