# Handleiding privacyvriendelijke instellingen Microsoft 365 voor beheerders

Versie 2.0

| | |
|---|---|
| Datum | 14 November 2023 |
| Status | Definitief |

# Colofon


| | |
|---|---|
| Afzendgegevens | **Directie Informatievoorziening en Inkoop**<br>**Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services**<br><br>Turfmarkt 147<br>2511 DP  Den Haag<br>Postbus 20301<br>2500 EH  Den Haag<br>www.rijksoverheid.nl/jenv |
| Contact | SLMMicrosoft@minjenv.nl |
| Projectnaam | M365 instellingen |
| Auteurs | Privacy Company (www.privacycompany.eu)<br>Sjoera Nas, Floor Terra and Johannes van 't Hart<br>Eindredactie: SLM |

# Inhoudsopgave

1. Geolocatiekeuze ..... 3
2. Tonen intern privacybeleid aan medewerkers en gastgebruikers ..... 4
3. Pseudonimisering accountgegevens medewerkers ..... 8
4. Instellen authenticatiemiddelen Entra (voorheen Azure AD) ..... 8
5. Versiebeheer van Windows, Office ProPlus en mobiele Office applicaties ..... 11
6. Telemetrieniveau Office 365 ..... 12
7. Microsoft verwerker voor de telemetrie uit Windows 10 ..... 15
8. Telemetrieniveau Windows en Feedback vragen ..... 15
9. Gebruik van Verbonden Ervaringen (Connected Experiences) ..... 19
10. Windows activiteitenoverzicht ..... 21
11. LinkedIn-integratie voor Microsoft accounts ..... 23
12. Customer Experience Improvement Program (CEIP) ..... 25
13. Automatische geolocatie in Outlook Agenda ..... 26
14. Analytische diensten Microsoft 365 ..... 27
15. Pseudonimisering gebruikersrapporten Teams ..... 29
16. Uitschakelen Delve ..... 31
17. Omgang met spam in Defender ..... 32
18. Pseudonimiseren gebruikersnamen in Defender voor Cloud Apps ..... 33
19. Gebruik Giphy in Teams en Outlook ..... 35
20. Toegang tot apps in de app-store in Teams ..... 35
21. E2EE in Teams ..... 36
22. Customer Key, Customer Lockbox en Double Key Encryption ..... 36
23. Indienen van inzageverzoeken door systeembeheerders ..... 38

# Inleiding

Dit document is een technische handleiding voor beheerders bij de Rijksoverheid om Microsoft 365 zo privacyvriendelijk mogelijk in te stellen.

Strategisch leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (hierna: SLM Rijk) heeft in 2019 een scherp contract met Microsoft onderhandeld voor het Rijk voor alle online diensten, inclusief een uitgebreide verwerkersovereenkomst. Op grond van die overeenkomst mag Microsoft als verwerker de verschillende soorten persoonsgegevens alleen voor drie specifieke en legitieme doelen verwerken. Zie voor meer informatie de openbare DPIA's en controle-onderzoeken op de verschillende Microsoft diensten.[1]

Voor verwerkingen die buiten deze overeenkomst vallen, kan Microsoft optreden als zelfstandige verantwoordelijke. Dan kan Microsoft de persoonsgegevens ook voor haar eigen commerciële doelen verwerken. In de doorlopende gesprekken met Microsoft heeft SLM Rijk aangedrongen op technische mogelijkheden voor beheerders om dat soort verdere verwerkingen te voorkomen, en mogelijkheden om de gegevensverwerking te minimaliseren. Daarnaast kunnen organisaties zelf maatregelen nemen medewerkers en participanten van buiten te informeren over de privacy spelregels, en maatregelen treffen om mogelijke privacyrisico's te voorkomen.

Deze handleiding beschrijft de verschillende keuzemogelijkheden die systeembeheerders hebben om Windows 10/11 en Microsoft 365 zo privacyvriendelijk mogelijk in te stellen. In deze handleiding worden deze keuzemogelijkheden afzonderlijk en stapsgewijs behandeld, met screenshots, zodat beheerders die eenvoudig op een goede manier kunnen instellen. In totaal gaat het om 23 opties. Eén van de opties is vervallen, omdat Microsoft inmiddels maatregelen heeft getroffen waardoor de privacy-onvriendelijke verwerkingen niet meer plaatsvinden.[2]

Deze handleiding beschrijft geen organisatorische maatregelen die organisaties zelf kunnen treffen, en biedt ook geen overzicht van alle mogelijke technische privacykeuzes. Microsoft 365 omvat een zeer uitgebreid pakket aan diensten. SLM Rijk laat regelmatig DPIA's uitvoeren en controle onderzoeken. Voor de nabije toekomst staan DPIA's op stapel voor Microsoft Purview (informatie labeling, inclusief Double Key Encryption) en de browser Edge. Als uit die DPIA's extra aanbevelingen volgen voor technische privacykeuzes, wordt deze handleiding aangevuld.

[1] SLM Microsoft, Google Cloud en Amazon Web Services, gehuisvest bij het Ministerie van Justitie en Veiligheid, URL: https://slmmicrosoftrijk.nl/.

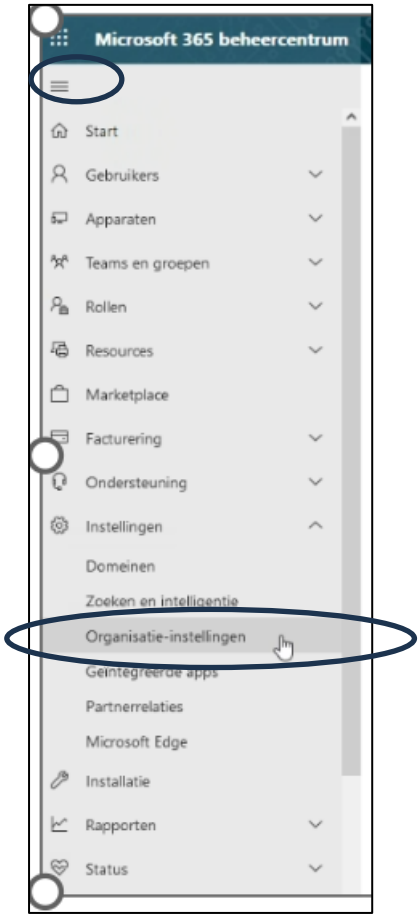
[2] Dit betrof de integratie van een Feedback knop en een Twitter/X feed in de Defender homepage voor beheerders.

# 1. Geolocatiekeuze

Gebruikers in de EU kunnen ervoor kiezen inhoudelijke gegevens op te slaan in de EU, in plaats van in de VS. Deze optie zorgt er ook voor dat de verwerking van de meeste diagnostische en supportgegevens in de EU plaatsvindt. Zie de website van Microsoft voor meer informatie over de uitvoering en planning van de *EU Data Boundary*.[3]

Let op: "Instellingen" komt twee keer voor op admin.microsoft.com. De instellingen bedoeld in deze handleiding zijn te vinden onder de drie horizontale lijntjes in het verticale menu **(de *hamburger*)** links in beeld van het Microsoft 365 beheercentrum, zoals te zien in Figuur 1 hieronder.

*Figuur 1: Instellingenmenu Microsoft 365*

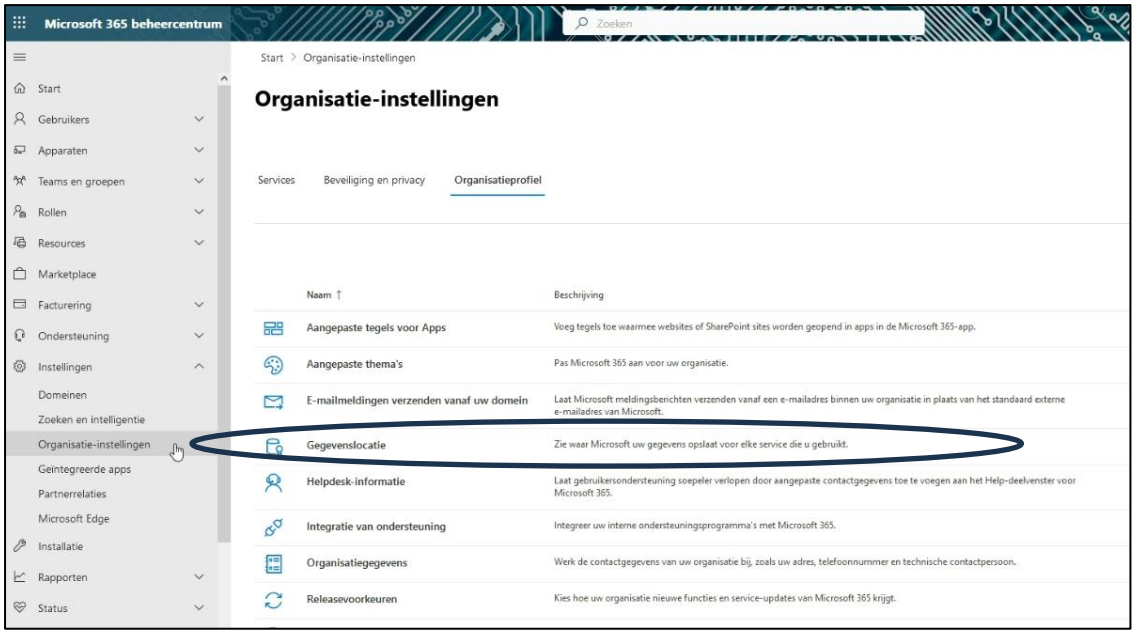



Privacyvriendelijke instelling kiezen

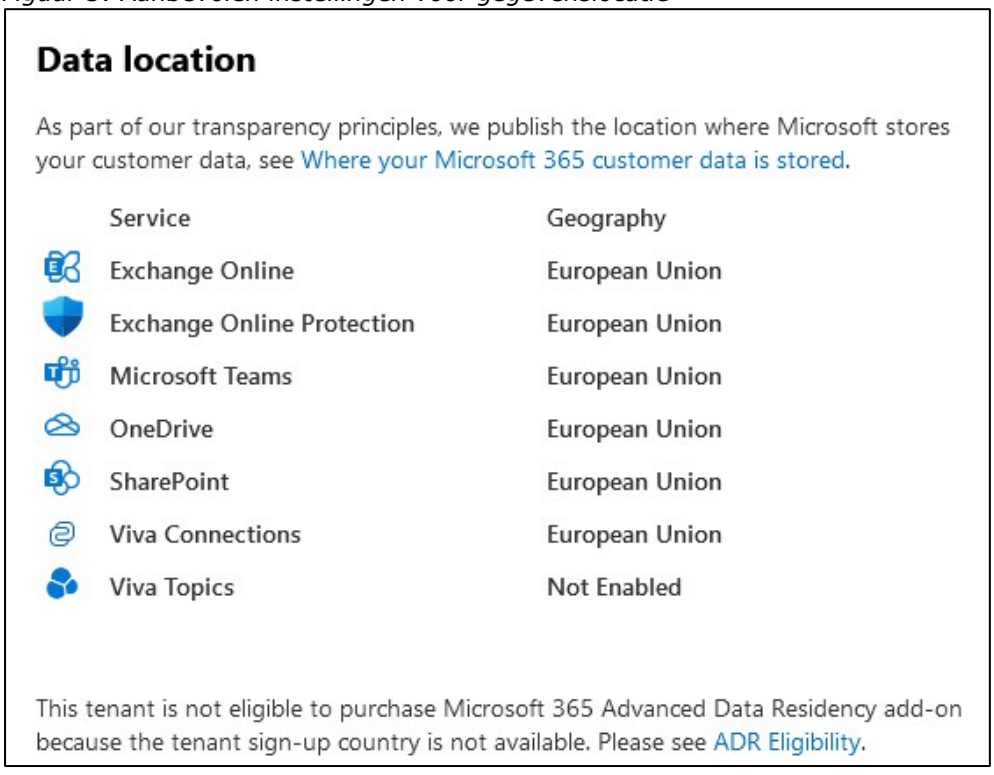
- Ga via https://admin.microsoft.com **- ->** Instellingen **- ->** Organisatieinstellingen **- ->** Organisatieprofiel **- ->** Gegevenslocatie. Zie Figuur 2 hieronder.

[3] Microsoft, What is the EU Data Boundary? 8 februari 2023, URL: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn

*Figuur 2: Schermafbeelding instelling geolocatie*




*Figuur 3: Aanbevolen instellingen voor gegevenslocatie*




## 2. Tonen intern privacybeleid aan medewerkers en gastgebruikers

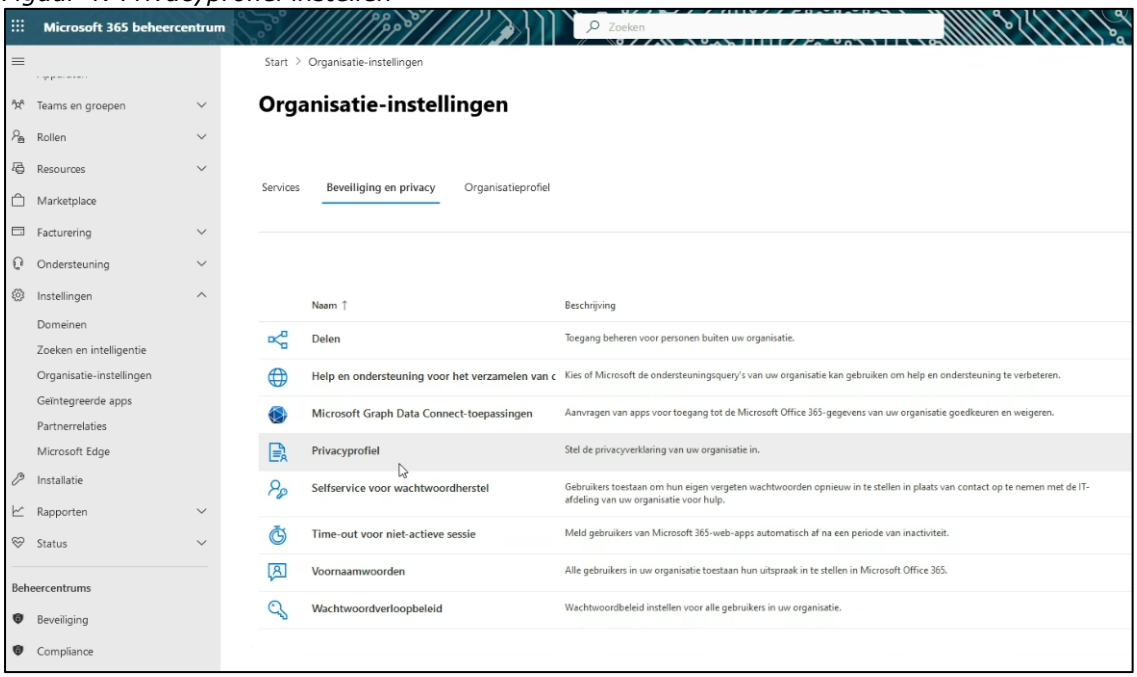
Organisaties verwerken heel veel persoonsgegevens via Microsoft 365. Via een intern privacybeleid kan de organisatie uitleggen wat medewerkers wel en niet mogen doen met de verschillende Office

applicaties, en uitleggen hoe de organisatie omgaat met de grote hoeveelheid informatie over hun dagelijkse werkzaamheden. Microsoft biedt de mogelijkheid om het interne privacybeleid te tonen op de inlogpagina, en om acceptatie van dat interne privacybeleid af te dwingen via Conditional Access opties in Entra (die nieuwe naam voor de Azure Active Directory), ook voor bijvoorbeeld gastgebruikers in Teams.

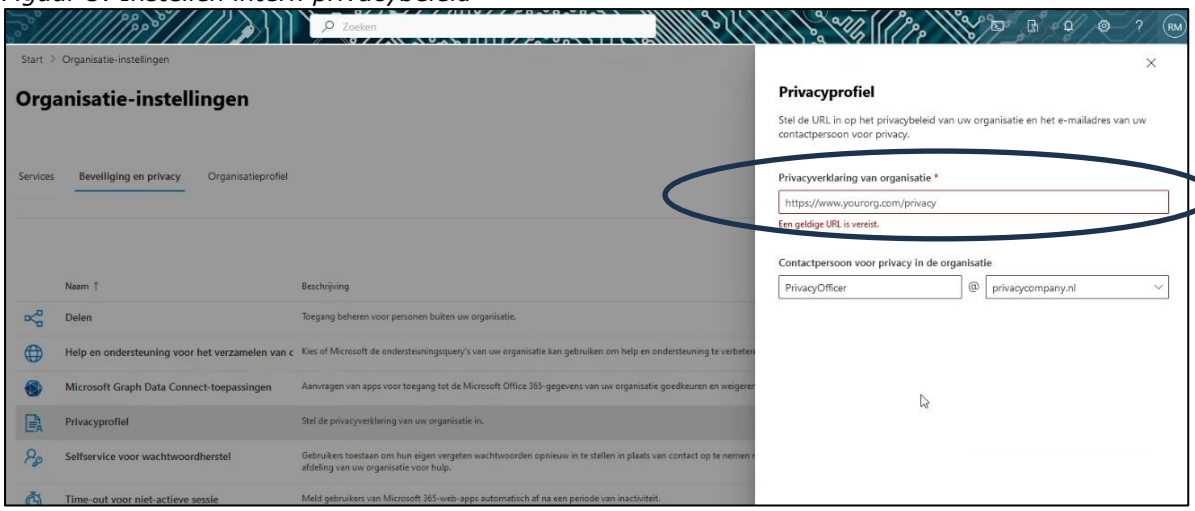
Privacyvriendelijke instelling kiezen

- Ga via https://admin.microsoft.com **- ->** Instellingen **- ->** Organisatieinstellingen **- ->** Beveiliging en privacy **- ->** Privacyprofiel.
- Plaats een link op de inlogpagina voor medewerkers naar het eigen privacybeleid, om medewerkers informatie te geven over het beleid, inclusief de regels voor het gebruik van logsbestanden (zie Figuur 4 en 5 hieronder).
- Dwing acceptatie van het interne privacybeleid af via de Entra ID. Ga naar portal.azure.com **- ->** type "Conditional access" in de zoekbalk **- ->** "Terms of use" links **- ->** new terms. Zie Figuur 6 tot en met Figuur 8 hieronder.
- Controleer de Conditional Access optie. Zie Figuur 9

*Figuur 4: Privacyprofiel instellen*

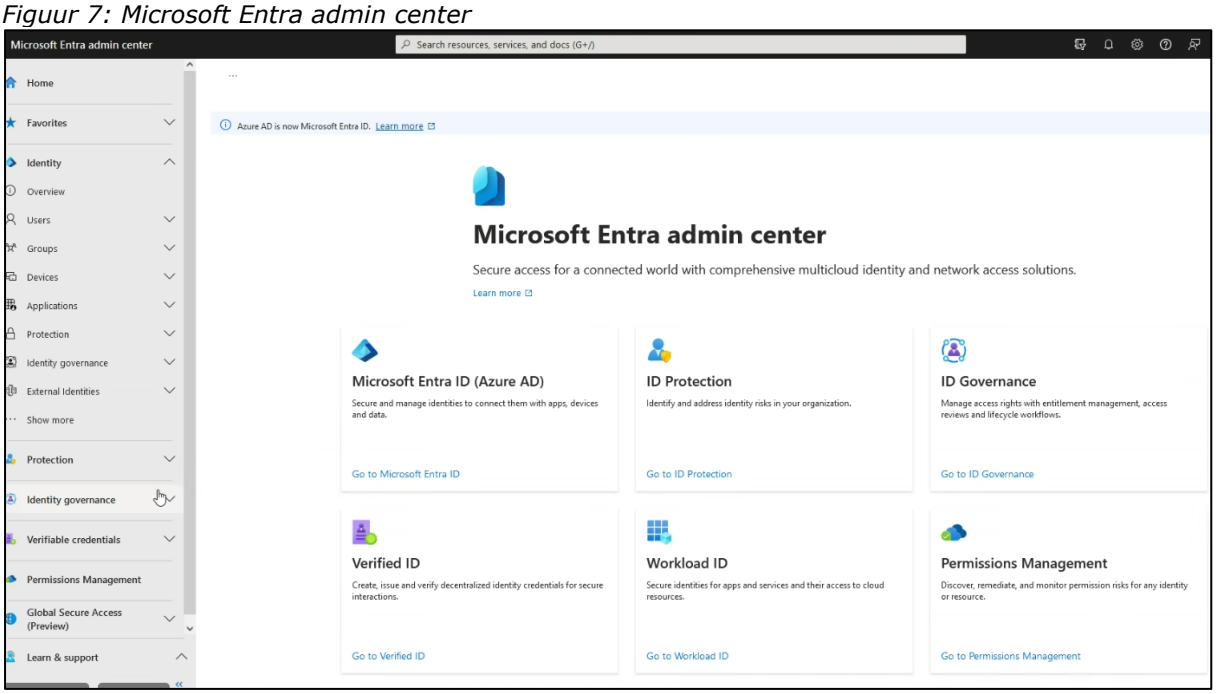


*Figuur 5: Instellen intern privacybeleid*

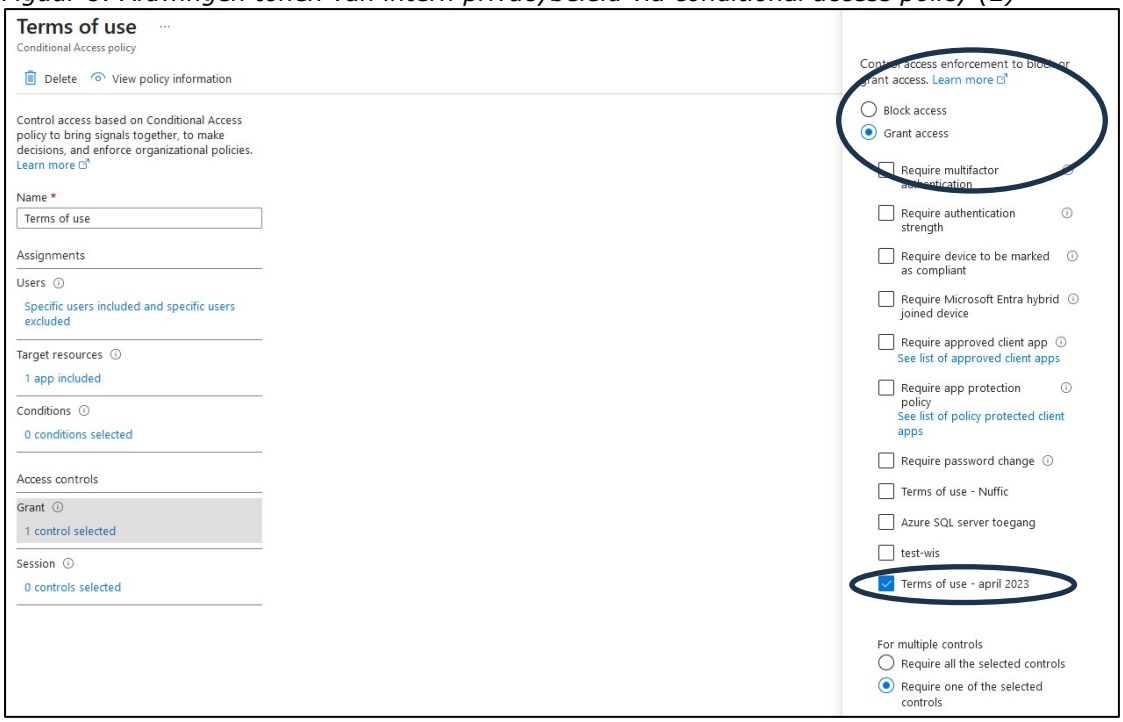



*Figuur 6: Microsoft Entra*

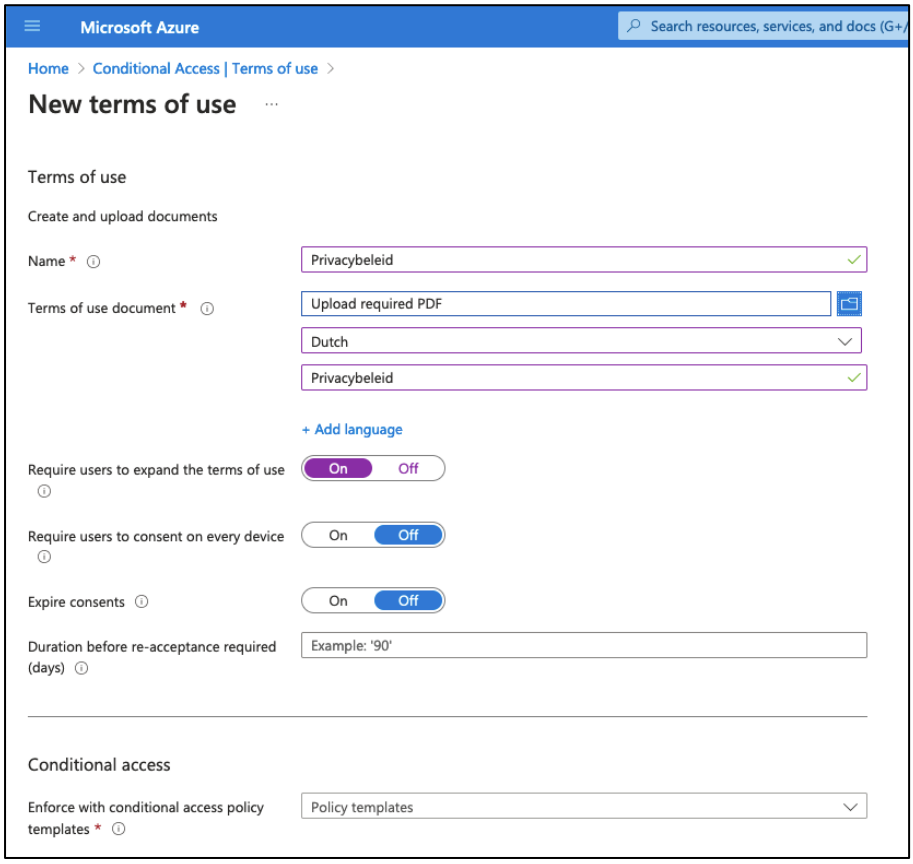

*Figuur 7: Microsoft Entra admin center*



*Figuur 8: Afdwingen tonen van intern privacybeleid via conditional access policy (2)*




*Figuur 9: Conditional Access regels zichtbaar in Azure*



## 3. Pseudonimisering accountgegevens medewerkers

Kies ervoor om accountgegevens van systeembeheerders of andere medewerkers te pseudonimiseren. Dat is zeker van belang als ze met gevoelige gegevens werken. Dan kan het uitlekken van hun naam, in combinatie met het feit dat ze voor een bepaald overheidsorganisatie werken, al tot een hoog risico leiden.

Dat pseudonimiseren kan in de Azure AD, ook als die gebruikt wordt als Single Sign On naar diensten van andere bedrijven. De organisatie kan er ook voor kiezen om generieke accounts aan te maken voor systeembeheerders (systeembeheerder1@minjenv, etc.).

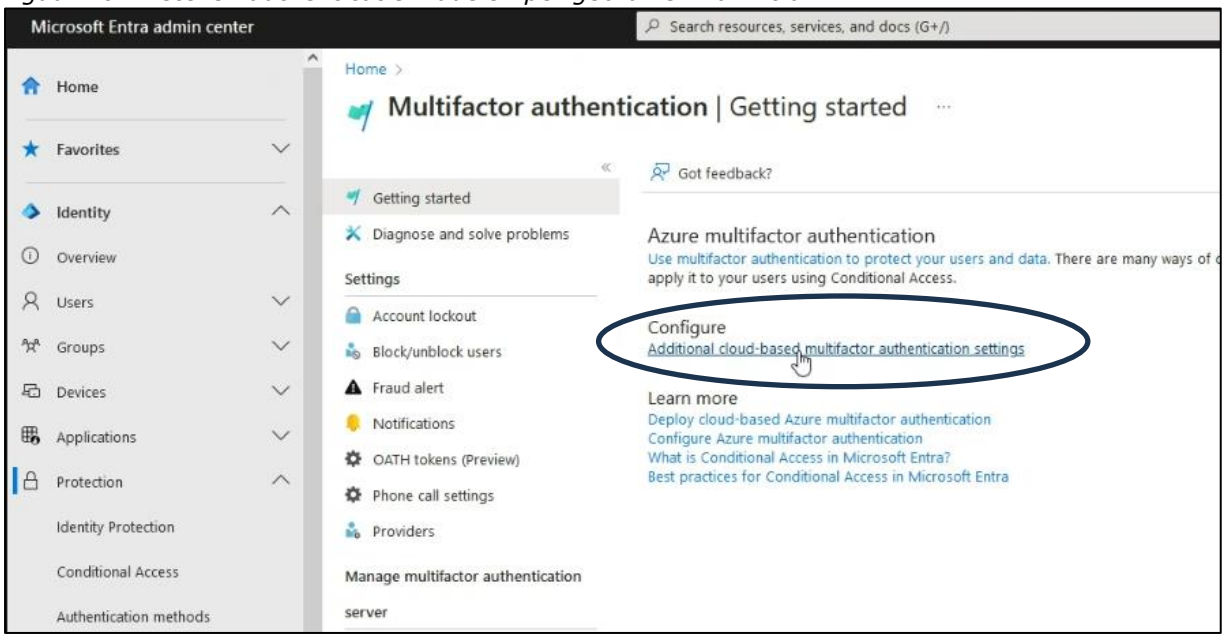
## 4. Instellen authenticatiemiddelen Entra (voorheen Azure AD)

Gebruik van multifactor authenticatie is een belangrijke beveiligingsmaatregel om ongeautoriseerde toegang tot persoonsgegevens te voorkomen.

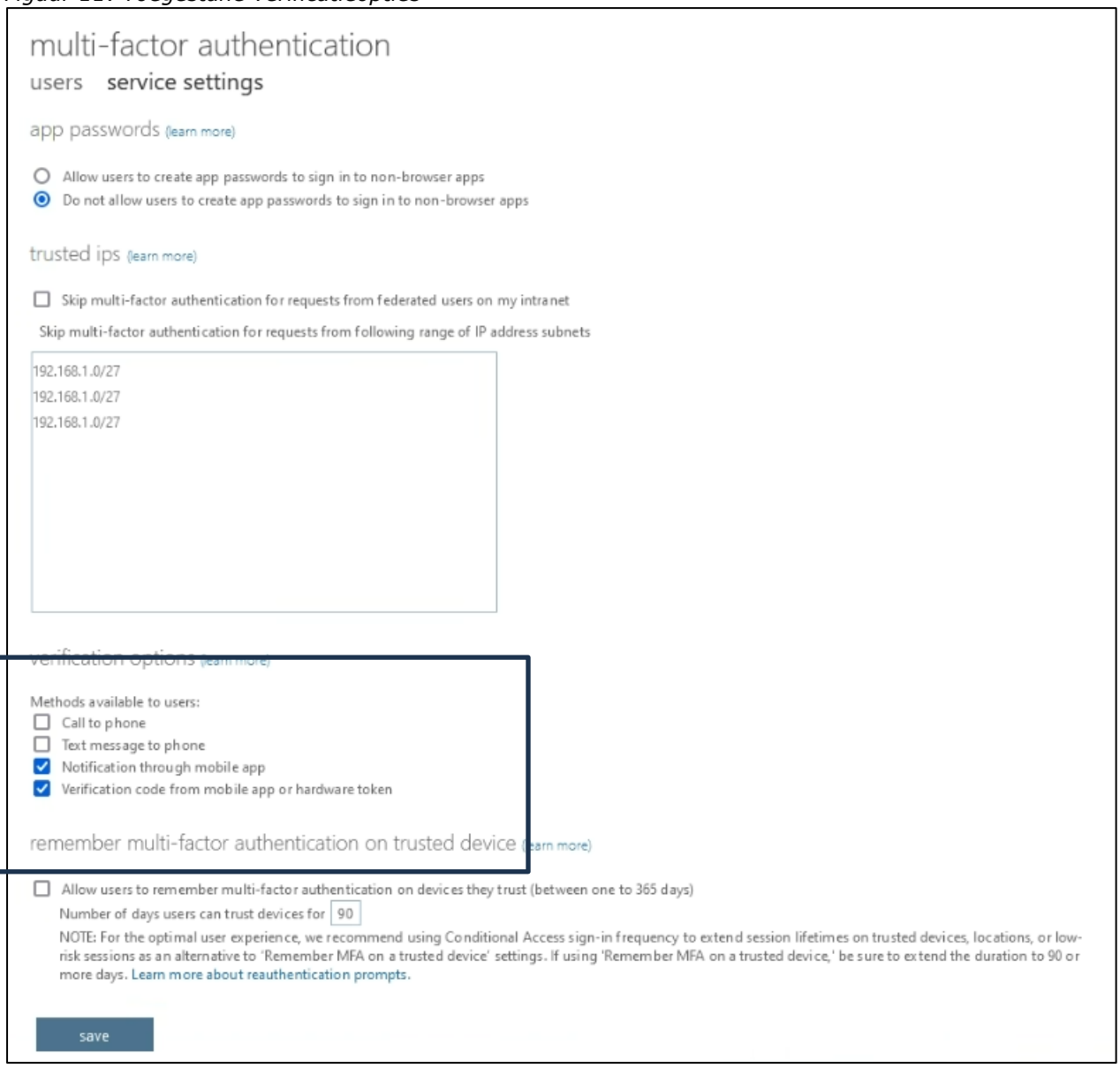
Privacyvriendelijke instelling kiezen

- Kies een authenticatiemiddel voor multifactor authenticatie in Entra, zoals de Authenticator app of een hardware token. Er bestaat ook een mogelijkheid om te kiezen voor het versturen van een code per SMS, maar daarbij vindt doorgifte plaats van onversleutelde mobiele nummers maar de VS. Gebruik de SMS optie dus niet.
- Multi-factor authenticatie is te vinden in het Entra admin center. Ga naar https://portal.azure.com/, zoek naar "Multifactor authenticatie". Onder "Getting started" staat een link naar "Additional cloud-based multifactor authentication settings" waarin in te stellen is welke middelen beschikbaar zijn voor multi-factor authenticatie. Zie Figuur 10 en Figuur 11: hieronder.
- Het gebruik van MFA wordt ten zeerste aanbevolen. Het is mogelijk om MFA toe te laten, of af te dwingen. (Zie Figuur 12 hieronder).

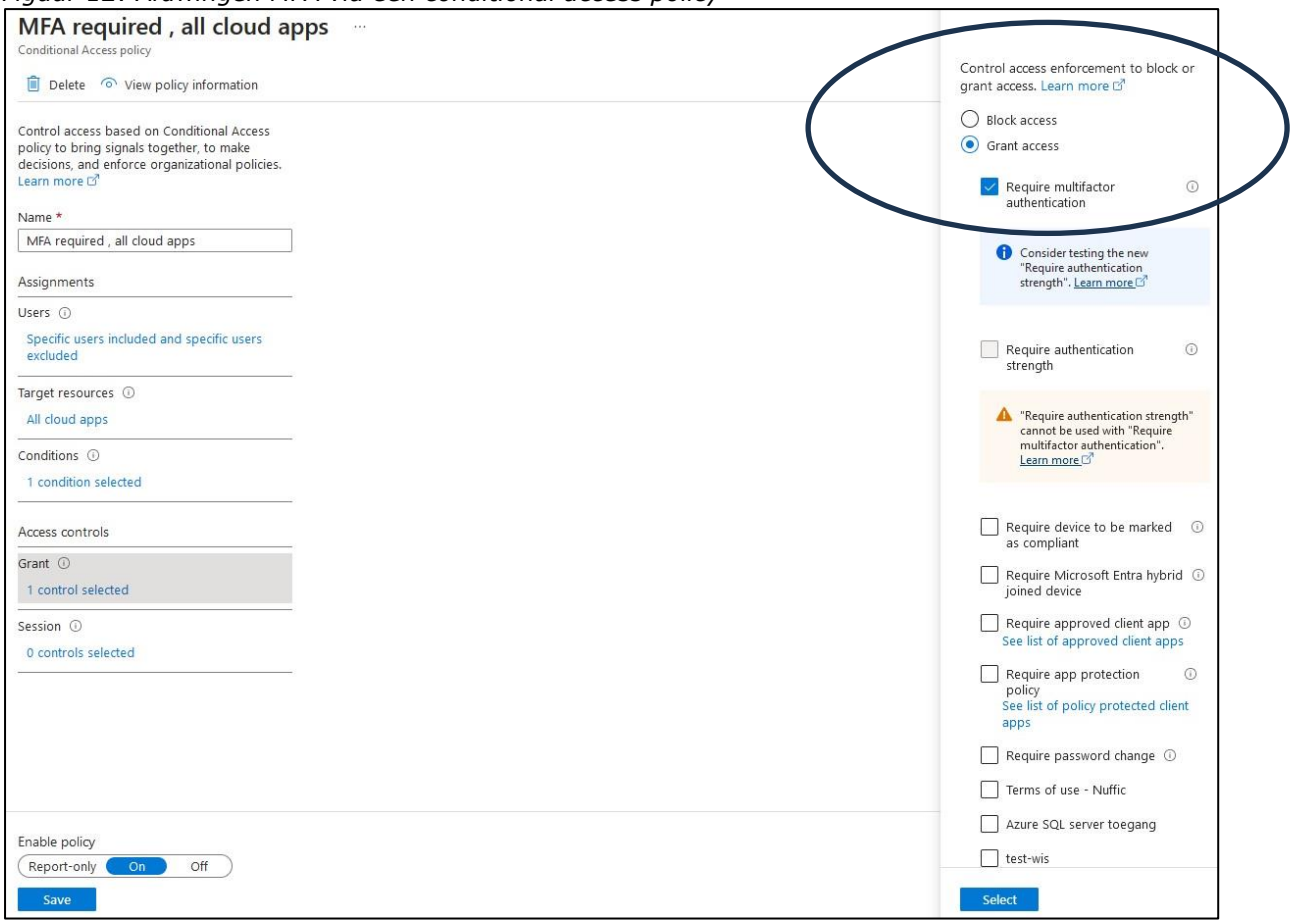
*Figuur 10: Instellen authenticatiemiddelen per gebruiker via Entra*



*Figuur 11: Toegestane verificatieopties*

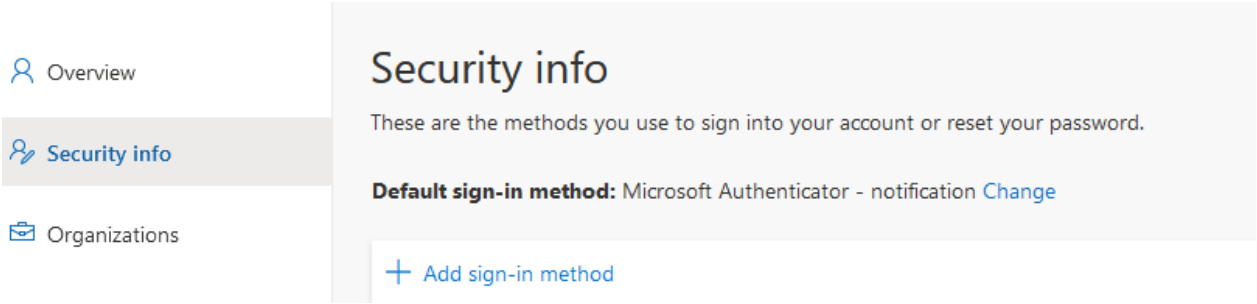


*Figuur 12: Afdwingen MFA via een conditional access policy*

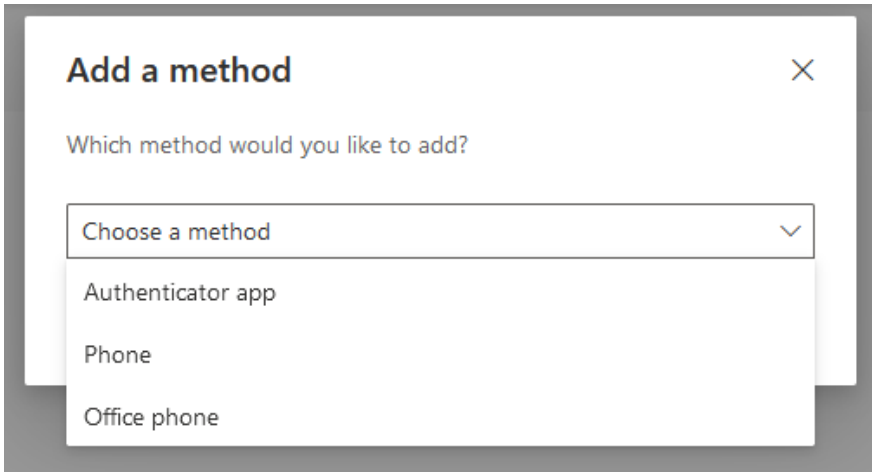



Het is ook mogelijk om op individueel gebruikersniveau MFA-voorkeuren aan te passen. Dat kan via https://mysignins.microsoft.com/security-info (zie Figuur 13 en Figuur 14 hieronder).

*Figuur 13: MFA-instellingen op gebruikersniveau*



*Figuur 14: MFA opties op gebruikersniveau*




## 5. Versiebeheer van Windows, Office ProPlus en mobiele Office applicaties

Om beveiligingsrisico's te voorkomen, is het belangrijk om goed in beeld te hebben welke versies van Windows en Office ProPlus in gebruik zijn. Centraal versiebeheer van de software verdient de voorkeur. Veel grote overheidsorganisatie zullen gebruik maken van centraal gemanagede werkplekken, waarbij ze images uitrollen van de benodigde Microsoft software. Inmiddels werken ook veel organisaties met Microsoft Intune.

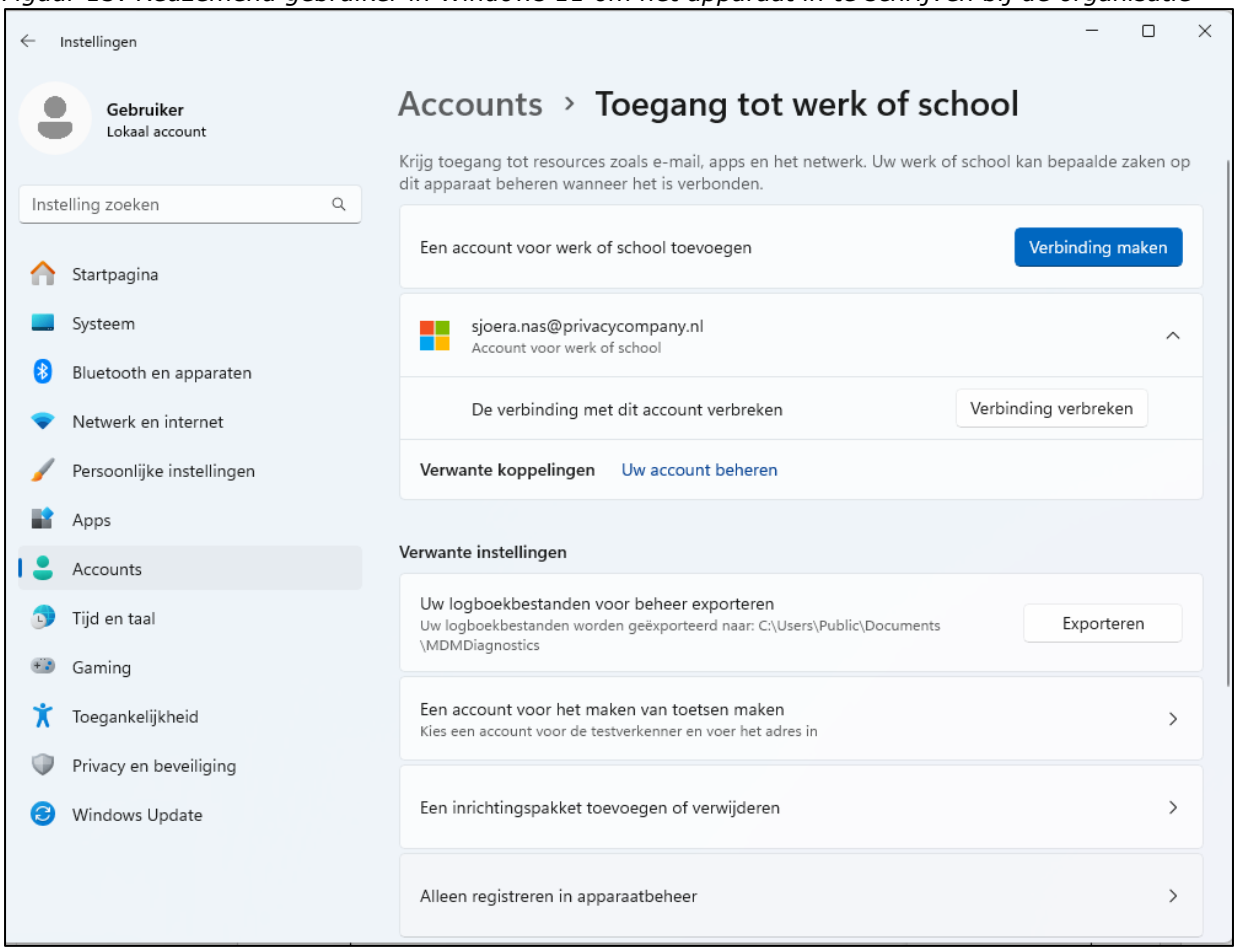
Als de organisatie werkt met Windows 10 of 11, en wil regelen dat de apparaten geregistreerd worden in de tenant, kunnen zij alvast een centrale keuze maken in de image van Windows, of de gebruiker zelf nog een keuzemenu geven. Zie Figuur 15 hieronder. Microsoft publiceert uitleg welke stappen een gebruiker zelf moet ondernemen om zich met het werkaccount aan te melden.[4]

Voor het managen van de versies van de Office applicaties op de mobiele devices is Mobile Device Management vereist, bijvoorbeeld met Microsoft Intune. Daar heeft SLM Rijk in 2020 een paraplu DPIA op laten uitvoeren.[5]

[4] Microsoft, Uw werkapparaat deelnemen aan uw werk- of schoolnetwerk, URL: https://support.microsoft.com/nl-nl/account-billing/uw-werkapparaat-deelnemen-aan-uw-werk-of-schoolnetwerk-ef4d6adb-5095-4e51-829e-5457430f3973.

[5] Rijksoverheid, Data protection impact assessment Intune, 30 juni 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-intune.

*Figuur 15: Keuzemenu gebruiker in Windows 11 om het apparaat in te schrijven bij de organisatie*




Versiebeheer is niet mogelijk en niet nodig voor de browser-diensten (Office Online), omdat Microsoft die applicaties zelf automatisch updatet.

## 6. Telemetrieniveau Office 365

Via telemetriegegevens verzamelt Microsoft pseudonieme persoonsgegevens over de apparaten waarmee gebruikers Microsoft 365 gebruiken, en over het individuele gebruik van haar diensten. Microsoft noemt deze gegevens 'diagnostische gegevens'.

Microsoft legt uit: "*Diagnostische gegevens worden gebruikt om Office veilig en up-to-date te houden, problemen te detecteren, te diagnosticeren en op te lossen, en om producten te verbeteren. Deze gegevens bevatten niet de naam of het e-mailadres van de gebruiker, de inhoud van de bestanden van de gebruiker of informatie over apps die niet verwant zijn aan Office.*"[6]

Het gaat om een gegevensstroom die in de browser, of in het apparaat van de gebruiker (desktop, laptop en smartphone) wordt aangemaakt. De telemetriegebeurtenissen worden zeer regelmatig gebundeld naar Microsoft verstuurd. Via de telemetriegegevens verzamelt Microsoft op een tweede manier persoonsgegevens over de apparaten en het gebruik van haar diensten. Deze verzameling

[6] Microsoft, Verplichte diagnostische gegevens voor Office, 11 mei 2023, URL: https://learn.microsoft.com/nl-nl/deployoffice/privacy/required-diagnostic-data.

staat los van de persoonsgegevens die Microsoft als cloudleverancier automatisch al in de logbestanden op haar cloudservers registreert.

Microsoft biedt drie mogelijkheden om telemetrieniveau in te stellen:

1. Vereist (Required)
2. Optioneel (Optional)
3. Geen van beide (Neither)[7]

Zelfs op het minimumniveau 'Neither' verzamelt Microsoft nog steeds telemetriegegevens. Microsoft noemt die gegevens 'Vereiste servicegegevens voor Office'.[8] Deze gegevensstroom bevat informatie over het gebruik van 'Verbonden Ervaringen' (in het Engels: 'Connected Experiences') die de organisatie gebruikt, en informatie over essentiële diensten van Office, zoals de licentieservice die Microsoft vertelt of een gebruiker de juiste licentie heeft om Office te gebruiken.

SLM Rijk adviseert om het gegevensverkeer via telemetrie uit de Office diensten te minimaliseren door de telemetrie in te stellen op het niveau 'Neither.' Door deze optie te kiezen (in plaats van 'Required') verwerkt Microsoft minder gevoelige gegevens. Het is mogelijk de datastroom te minimaliseren met een Group Policy via User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center.[9]

Privacyvriendelijke instelling kiezen

- Ga naar https://config.office.com **->** Kies 'Office policies' (Figuur 16) **->** Ga naar Microsoft 365 Cloud Policy **->** Zoek naar de policy *Configure the level of client software diagnostic data sent by Office to Microsoft (*Figuur 17) **->** Enabled (Figuur 18).
- Stel het telemetrieniveau in op 'Neither' (Figuur 19).
- Controleer af en toe zelf de informatie die Microsoft geeft over de telemetrie in de Diagnostic Data Viewer op een Windows apparaat.[10]

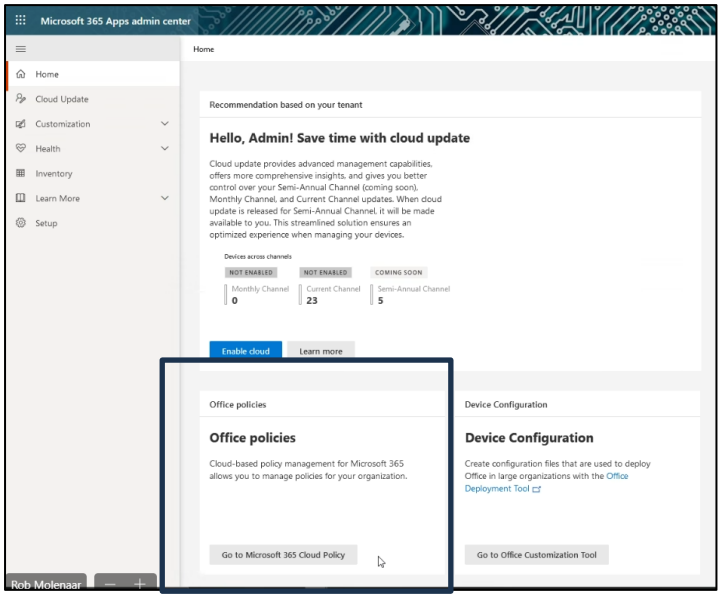
[7] Microsoft, 28 maart 2023, Diagnostische gegevens die van Microsoft 365-apps voor ondernemingen naar Microsoft worden verzonden, URL: https://learn.microsoft.com/nl-nl/deployoffice/privacy/overview-privacy-controls#diagnostic-data-sent-from-microsoft-365-apps-for-enterprise-to-microsoft.

[8] Microsoft, Vereiste servicegegevens voor Office, 4 april 2023, URL: https://learn.microsoft.com/nl-nl/deployoffice/privacy/required-service-data

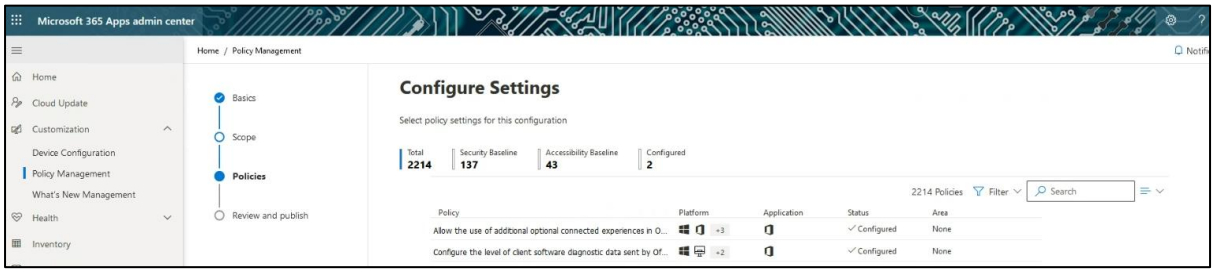
[9] Microsoft, Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise, 27 maart 2023, URL: https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls.

[10] Microsoft, Gebruik van de Viewer diagnostische gegevens met Office, URL: https://support.microsoft.com/nl-nl/office/gebruik-van-de-viewer-diagnostische-gegevens-met-office-cf761ce9-d805-4c60-a339-4e07f3182855

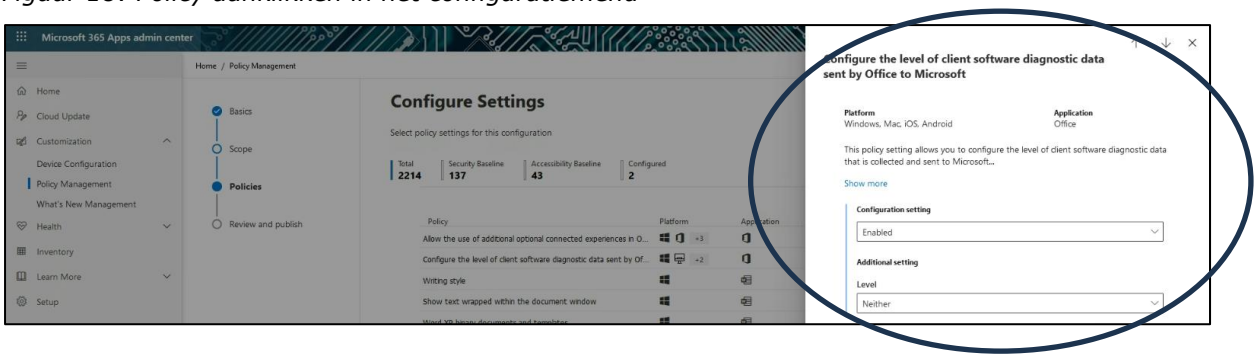
*Figuur 16: Office Policies in het Microsoft 365 Apps admin center*



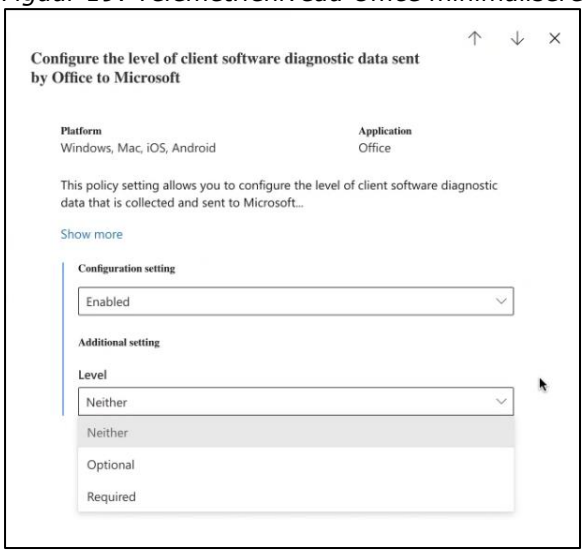

*Figuur 17: Kies Configure the level of client software diagnostic data sent by Office*




*Figuur 18: Policy aanklikken in het configuratiemenu*



*Figuur 19: Telemetrieniveau Office minimaliseren*




## 7. Microsoft verwerker voor de telemetrie uit Windows

Vanaf Windows 10 Enterprise versie 1809 met (tenminste) de update van juli 2021 is het mogelijk voor Enterprise klanten van Microsoft om Microsoft als verwerker te laten optreden voor de gegevensverwerking via de Windows telemetriegegevens, in plaats van als zelfstandige verantwoordelijke.[11]

Dat kan door de Windows apparaten toe te voegen aan de Entra-tenant. Voor Nederlandse overheidsklanten, met een factuuradres in Nederland, registreert Microsoft automatisch dat zij de telemetriegegevens van elk ingeschreven apparaat alleen als verwerker mag verwerken. De telemetriegegevens worden dan ook automatisch in Europa opgeslagen.[12]

Let op: als een organisatie het apparaat niet aanmeldt in Entra, verwerkt Microsoft de telemetriegegevens uit Windows 10 als zelfstandige verantwoordelijke.
Vanaf Windows 11 Enterprise treedt Microsoft automatisch op als verwerker voor de telemetriegegevens. Maar let op: Microsoft blijft verantwoordelijk voor alle andere gegevensverwerkingen via Windows 11. Zie de toelichting bij maatregel 10: het Windows activiteitenoverzicht.

.

## 8. Telemetrieniveau Windows en Feedback vragen

De standaardinstelling voor telemetrie uit Windows is dat zowel de vereiste als de optionele diagnostische gegevens 'aan' staan, maar dat gebruikers zelf nog een keuze krijgen om de optionele diagnostische gegevens uit te zetten.

Beheerders kunnen centraal de gegevensverwerking via Windows telemetriegegevens beperken.

Microsoft biedt, net als in Office, drie keuzemogelijkheden:

[11] Microsoft blog (alleen Engelstalig), Introducing a new option for customers to control their Windows 10 diagnostic data, 23 juli 2020, URL: https://blogs.microsoft.com/eupolicy/2020/07/23/introducing-new-option-customers-control-windows-10-diagnostic-data/.
[12] Microsoft, Diagnostische Windows-gegevens in uw organisatie configureren, 4 augustus 2023, URL: https://learn.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization

1. Uit
2. Vereist
3. Optioneel

Bij een hoger telemetrieniveau in Windows, kan Microsoft ook meer gegevens verzamelen over het gebruik van Office applicaties.

*Figuur 20: Uitleg Microsoft opties telemetrie Windows 10 en Windows 11 (Hernoemd beleid)*[13]

| Beleidstype | Huidige beleid | Hernoemd beleid |
|---|---|---|
| Groepsbeleid | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Telemetrie toestaan**<br>• 0 - Beveiliging<br>• 1 - Basis<br>• 2 - Uitgebreid<br>• 3 - Volledig | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Diagnostische gegevens toestaan**<br>• Diagnostische gegevens uit (niet aanbevolen)<br>• Vereiste diagnostische gegevens verzenden<br>• Optionele diagnostische gegevens verzenden |
| Groepsbeleid | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Configureer de gebruikersinterface van opt-in-instellingen voor telemetrie** | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Configureer de gebruikersinterface van opt-in-instellingen voor diagnostische gegevens** |
| Groepsbeleid | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Configureer opt-in-wijzigingsmeldingen voor telemetrie** | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > **Configureer opt-in-wijzigingsmeldingen voor diagnostische gegevens** |

*Figuur 21: Keuzemogelijkheden Windows telemetrie*[14]

| Categorie | Waarde |
|---|---|
| Diagnostische gegevens uit (beveiliging) | 0 |
| Vereist (basis) | 1 |
| Uitgebreid | 2 |
| Optioneel (volledig) | 3 |

ⓘ Notitie

Als het beleid Computerconfiguratie en het beleid Gebruikersconfiguratie beide zijn ingesteld, wordt het meest beperkende beleid gebruikt.

Microsoft vraagt ook via Windows om 'Feedback' aan gebruikers. Microsoft is zelfstandig verantwoordelijk voor de gegevensverwerking via de Feedback-hub

[13] Microsoft, Wijzigingen in het verzamelen van diagnostische Windows-gegevens, 4 septembert 2023, URL: https://docs.microsoft.com/nl-nl/windows/privacy/changes-to-windows-diagnostic-data-collection#gedragswijzigingen

[14] Microsoft, Diagnostische gegevens beheren met groepsbeleid en MDM, 4 augustus 2023, URL: https://learn.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization#manage-diagnostic-data-using-group-policy-and-mdm

die opent als een gebruiker feedback wil geven in Windows. De rol van Microsoft blijkt uit de verwijzing naar het eigen privacybeleid van Microsoft, gericht op consumenten.

*Figuur 22: Microsoft uitleg Feedback-hub op Windows*


Privacyvriendelijke instelling kiezen

Als organisaties gebruik maken van centraal gemanagede apparaten met images van de benodigde software, kunnen ze het telemetrieniveau als volgt instellen in het keuzemenu van de eindgebruiker:

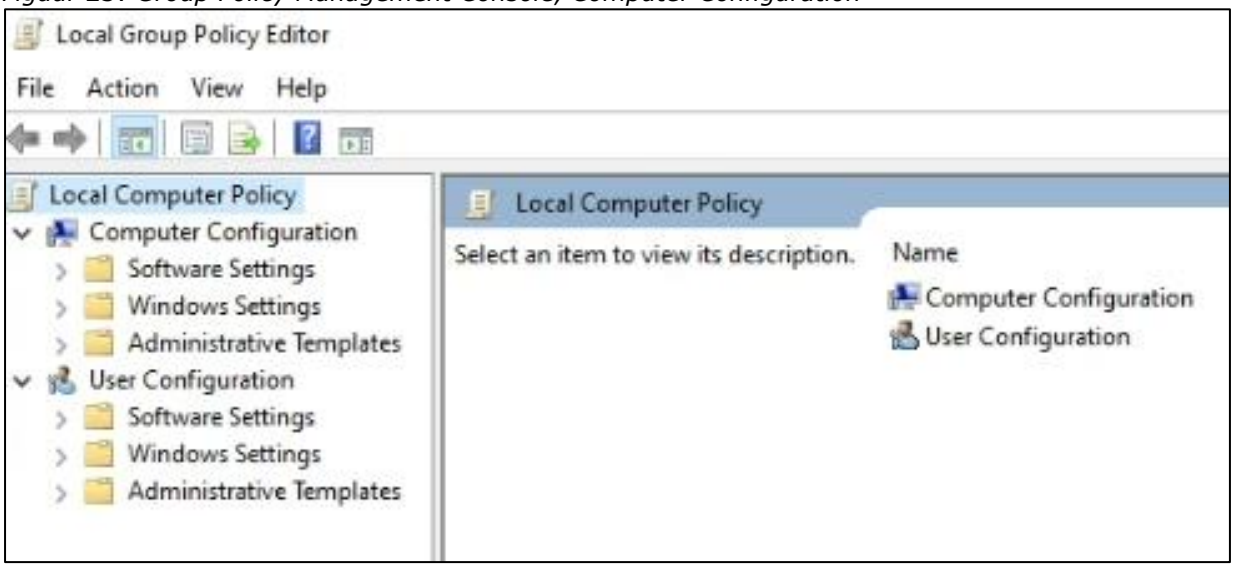
- In Windows 10, **->** Settings **->** Privacy **->** Diagnostics & feedback.
- In Windows 11 **->** Settings **->** Privacy & security **->** Diagnostics & feedback.

Het is ook mogelijk om het telemetrieniveau via de Registry Editor of via een Group Policy in te stellen

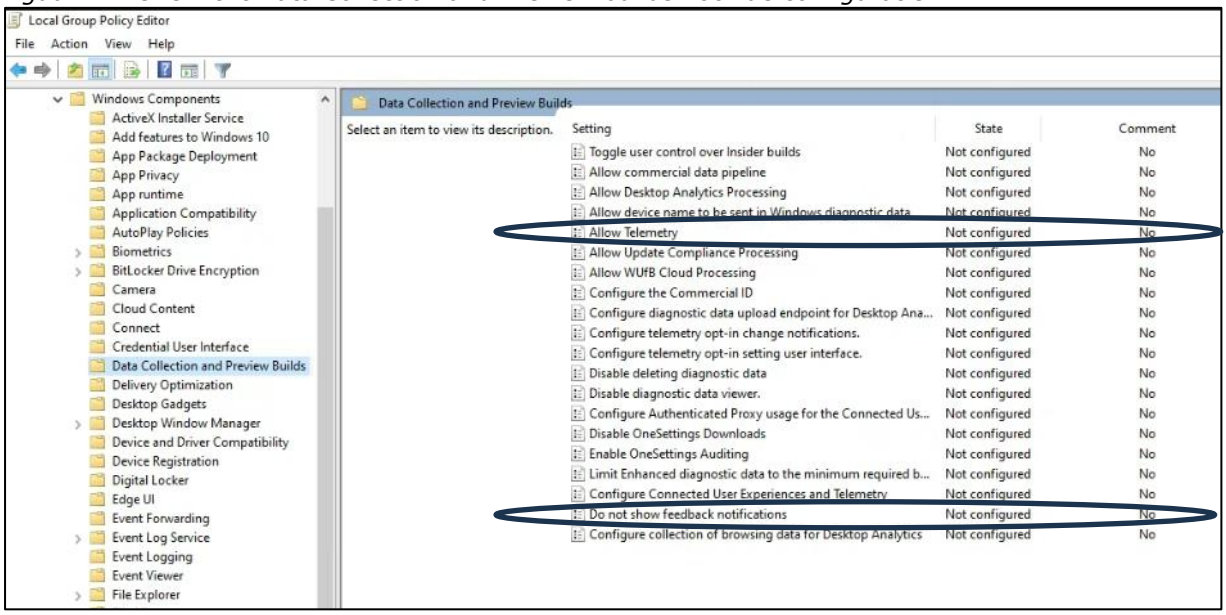
- Ga vanuit de Group Policy Management Console (gpmc), naar Computer Configuration **->** Administrative Templates **->** Windows Components **->** Data Collection and Preview Builds. Zie Figuur 23 en Figuur 24 hieronder.

- Dubbelklik op Allow Telemetry (of Allow diagnostic data on Windows 11 and Windows Server 2022) en kies 'uit' of '0'.[15] Zie Figuur 25 hieronder.
- Zet in hetzelfde menu ook de policy aan 'Do not show feedback notifications'. Zie de onderste omrande policy in Figuur 24.

*Figuur 23: Group Policy Management Console, Computer Configuration*

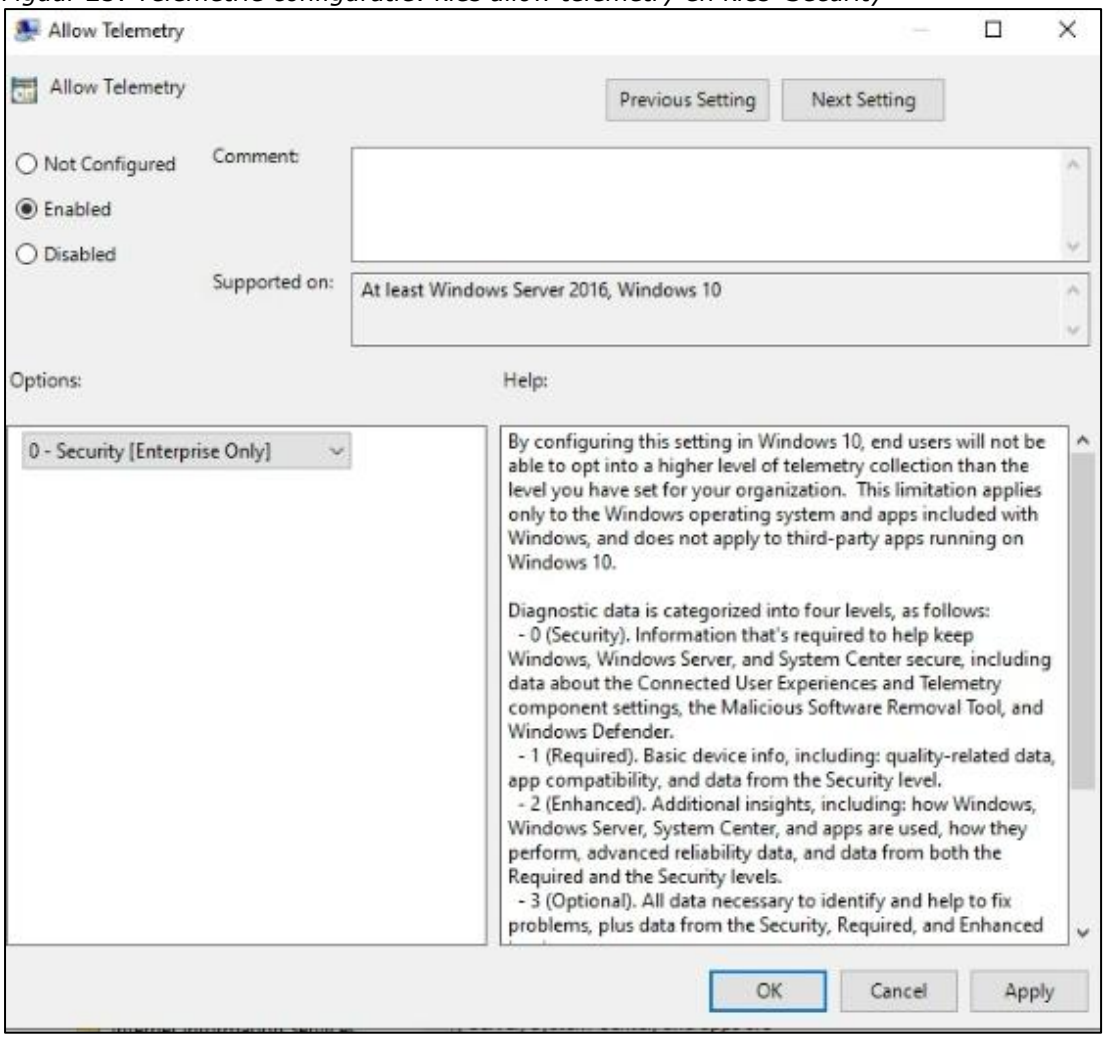



*Figuur 24: Overzicht Data Collection and Preview builds vóór de configuratie*




[15] Microsoft, Groepsbeleid gebruiken om het verzamelen van diagnostische gegevens te beheren, 4 augustus 2023, URL: https://learn.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization#use-group-policy-to-manage-diagnostic-data-collection

*Figuur 25: Telemetrie configuratie: kies allow telemetry en kies 'Security'*




## 9. Gebruik van Verbonden Ervaringen (Connected Experiences)

De Verbonden Ervaringen (Connected Experiences) zijn mini-clouddiensten waarmee Microsoft gegevens levert in Office zoals een spellingcheck of ontwerpen voor dia's.

Microsoft onderscheidt vier soorten Connected Experiences. Microsoft treedt op als zelfstandige verantwoordelijke voor de gegevensverwerking in 22 diensten in de vierde categorie, de *Additional Optional Connected Experiences.* Voor de andere drie categorieën treedt Microsoft op als verwerker.

SLM Rijk adviseert om de toegang tot deze *Additional Optional Connected Experiences* centraal uit te schakelen op alle platforms. Microsoft heeft ook de externe dienst Giphy toegevoegd aan de instellingen voor Optional Connected Experiences in Teams.[16] Het uitzetten van deze diensten kan met een Group Policy of via de Registry, voor alle Office 365-services.

[16] Microsoft, Overview of optional connected experiences in Microsoft Teams, 4 oktober 2023, URL: https://learn.microsoft.com/en-us/microsoftteams/teams-privacy-oce-overview.

*Figuur 26: Uitleg Microsoft over instellingen in de Registry*[17]

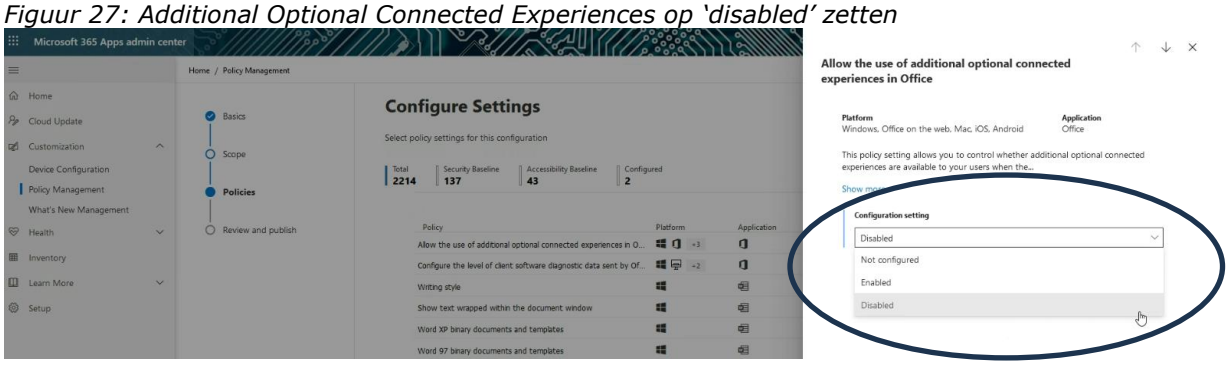
| Policy setting | Registry setting | Values |
|---|---|---|
| Configure the level of client software diagnostic data sent by Office to Microsoft | SendTelemetry | 1=Required<br>2=Optional<br>3=Neither |
| Allow the use of connected experiences in Office that analyze content | UserContentDisabled | 1=Enabled<br>2=Disabled |
| Allow the use of connected experiences in Office that download online content | DownloadContentDisabled | 1=Enabled<br>2=Disabled |
| Allow the use of additional optional connected experiences in Office | ControllerConnectedServicesEnabled | 1=Enabled<br>2=Disabled |
| Allow the use of connected experiences in Office | DisconnectedState | 1=Enabled<br>2=Disabled |

Privacyvriendelijke instelling kiezen

Voor het instellen van een Group Policy zijn de volgende stappen nodig:

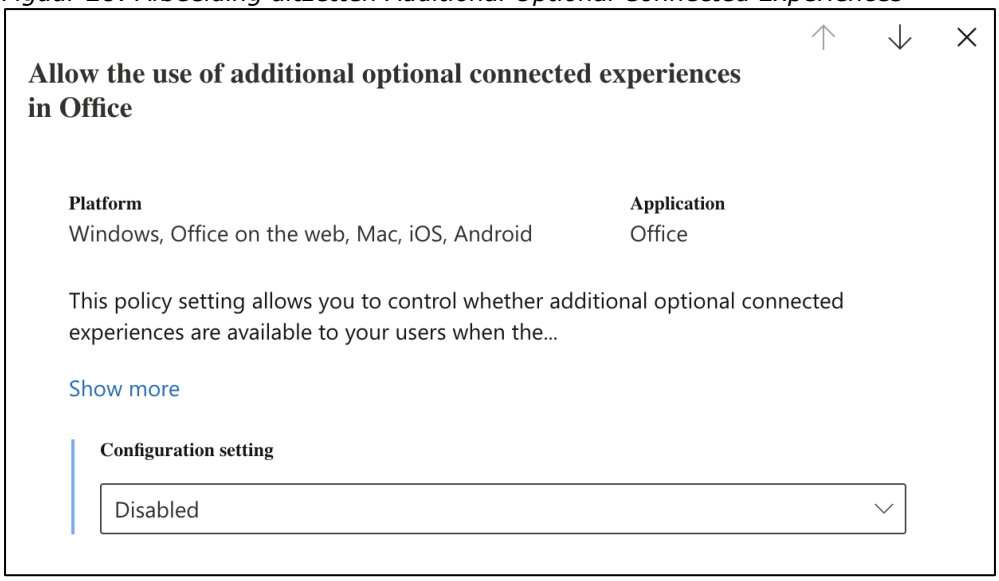
- Ga naar https://config.office.com/officeSettings
- Kies *Office Policies* en kies de beleidsconfiguratie die voor de hele organisatie geldt.
- Zet op die pagina de policy *Allow the use of additional connected experiences in office* op Disabled. Zie de uitvergroting in Figuur 28 hieronder.

*Figuur 27: Additional Optional Connected Experiences op 'disabled' zetten*




[17] Microsoft, Control privacy settings by editing the registry, https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls#control-privacy-settings-by-editing-the-registry.

*Figuur 28: Afbeelding uitzetten Additional Optional Connected Experiences*




## 10. Windows activiteitenoverzicht

Microsoft biedt de mogelijkheid via het activiteitenoverzicht in Windows om alle gebruikersactiviteiten lokaal bij te houden op het apparaat. Dit overzicht bevat gedetailleerde informatie welke apps en diensten gebruikers gebruiken, welke bestanden ze openen en welke websites ze bekijken. Gebruikers kunnen toestemming geven om deze informatie op te slaan in de Microsoft cloud. Microsoft gebruikt deze gegevens vervolgens ook om persoonlijke ervaringen te bieden (zoals het ordenen van activiteiten op basis van de gebruiksduur) en suggesties te doen (zoals anticiperen op wat de gebruiker nodig heeft op basis van diens activiteitengeschiedenis).[18]

Microsoft legt uit dat ze de activiteitengeschiedenis gebruikt "*om Microsoft-producten en -services te verbeteren wanneer de instelling voor het verzenden van uw activiteitengeschiedenis naar Microsoft is ingeschakeld. We doen dit door technieken voor Machine Learning toe te passen zodat we beter begrijpen hoe klanten in het algemeen onze producten en services gebruiken. We onderzoeken bovendien waar klanten fouten tegenkomen en helpen hen vervolgens deze op te lossen.*"[19]

Omdat deze verwerkingen niet onder de overeenkomst met SLM Rijk vallen, is het advies om het gebruik van internetsynchronisatie in Windows centraal te verhinderen, door de Windows Activity Feed uit te zetten, zowel in Windows 10 als Windows 11.

De Activity Feed staat ook standaard aan in Windows 11. Hoewel Microsoft optreedt als verwerker voor de telemetriegegevens uit Windows 11 voor klanten met factuuradres in de EU, blijft Microsoft als verantwoordelijke optreden voor alle andere verwerkingen via Windows 11, ook voor het activiteitenoverzicht.

Microsoft schrijft: "*For Windows 10/11 Enterprise, Pro, and Education editions that support a Windows diagnostic data processor configuration, Microsoft is the processor for Windows diagnostic data collected from a device where such configuration is set. (…) Except as provided above, Microsoft*

[18] Microsoft Support, Geschiedenis van Windows-activiteiten en uw privacy, ongedateerd, URL: https://support.microsoft.com/nl-nl/windows/-geschiedenis-van-windows-activiteiten-en-uw-privacy-2b279964-44ec-8c2f-e0c2-6779b07d2cbd .
[19] Idem.

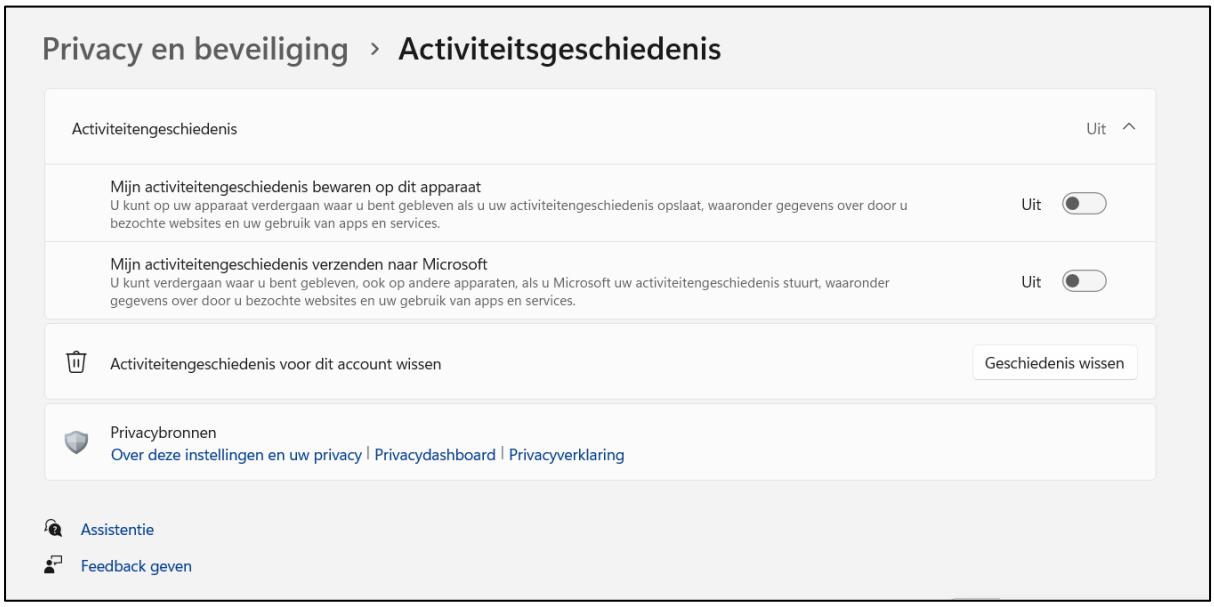
*will continue to be a controller of Personal Data processed in connection with your use of Windows, including data processed by Microsoft in connection with Customer's use of service-based capabilities. When Microsoft is a controller, Microsoft will handle the Personal Data in accordance with the Microsoft Privacy Statement (www.aka.ms/privacy), and the Data Protection Addendum (www.aka.ms/DPA) terms do not apply.*[20]

Privacyvriendelijke instelling kiezen

Beheerders kunnen het Windows activiteitenoverzicht op twee manieren uitzetten: via het eindgebruikersmenu als ze images centraal uitrollen (zie Figuur 29 hieronder), of via de Registry.

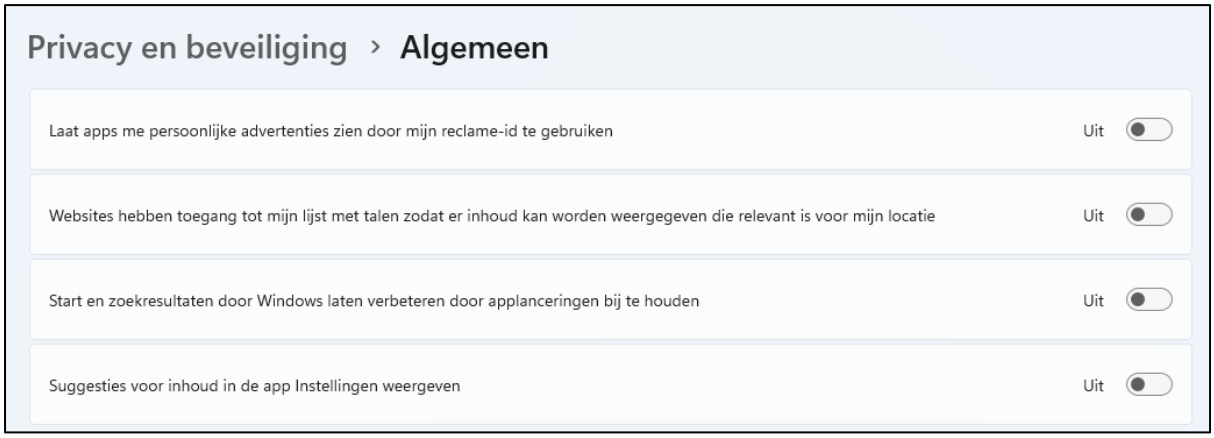
- Eindgebruikersmenu: Ga naar 'Instellingen', Privacy en beveiliging **->** Activiteitsgeschiedenis **->** Mijn activiteitengeschiedenis verzenden naar Microsoft **->** Uit.
- Kijk ook de overige privacy-instellingen voor Windows na. Zie Figuur 30 hieronder.
- Registry: Ga naar Registry Path Software\Policies\Microsoft\Windows\System **->** Value Name EnableActivityFeed **->** Value Type REG_DWORD **->** Disabled Value 0.

*Figuur 29: Uitzetten verzending activiteitsgeschiedenis naar Microsoft (Windows 11)*




[20] Microsoft Product Terms, Software, Windows desktop, URL: https://www.microsoft.com/licensing/terms/productoffering/WindowsDesktopOperatingSystem/eaeas.

*Figuur 30: Algemene privacy-instellingen Windows 11*




## 11. LinkedIn-integratie voor Microsoft accounts

Microsoft is zelfstandig verantwoordelijk voor de gegevensverwerkingen via LinkedIn, en mag de persoonsgegevens over het gebruik van deze dienst dus gebruiken voor haar eigen commerciële doelen.

Microsoft zet standaard LinkedIn-integratie aan voor Microsoft-medewerkersaccounts in Office 365.[21] De instellingen voor de Connected Experiences hebben geen invloed op LinkedIn integraties.

Als medewerkers toestemming geven om hun LinkedIn account te koppelen aan hun Microsoft 365 account, kunnen zij LinkedIn-gegevens en -middelen toepassen op verschillende locaties binnen de Office-toepassingen.

SLM Rijk adviseert om de LinkedIn-integratie centraal uit te schakelen en om te voorkomen dat Microsoft via Office alsnog LinkedIn features toont aan gebruikers.

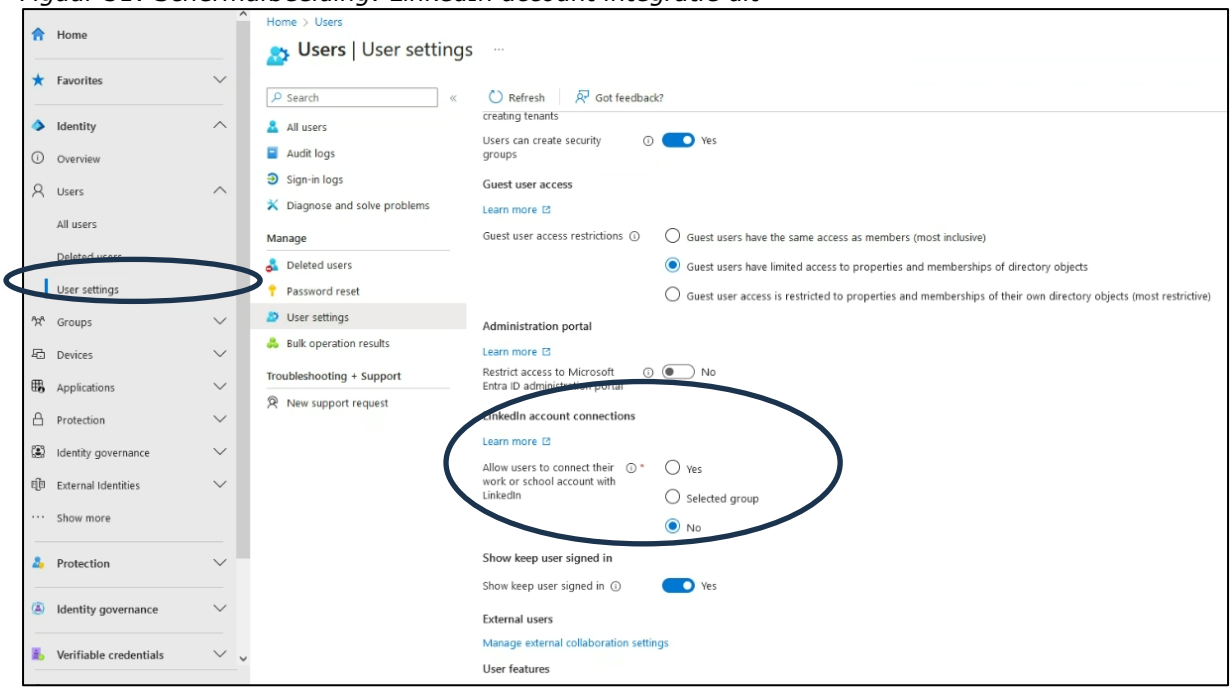
Privacyvriendelijke instelling kiezen

- Ga naar https://entra.microsoft.come **->** typ in de zoekbalk "users" of "gebruikers" **->** user settings / gebruikersinstellingen **->** LinkedIn-integratie uitzetten. Zie Figuur 31 hieronder.
- Gebruik volgens de aanwijzingen van Microsoft Group Policies om twee andere LinkedIn integraties uit te zetten: 'Show LinkedIn features in Office applications' en 'LinkedIn Resume Assistant in Word'. Microsoft schrijft:
- Download de Office 2016-beheersjabloonbestanden (ADMX/ADML) **->** Pak de ADMX-bestanden uit en kopieer ze naar uw centrale archief **->** Open Groepsbeleidsbeheer **->** Maak een groepsbeleid-object met de volgende instelling: Gebruikersconfiguratie >Beheersjablonen>Microsoft Office 2016>Diversen>LinkedIn-functies weergeven in Office-toepassingen.[22] Zie Figuur 32 en Figuur 33 hieronder.

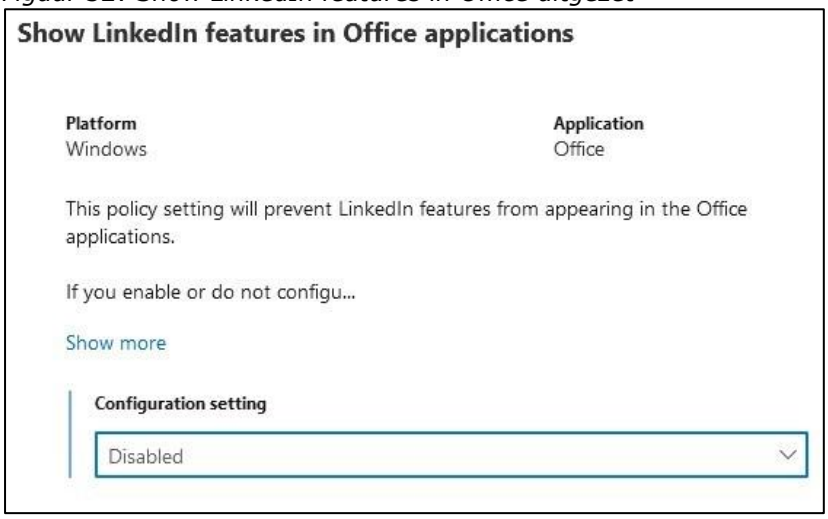
[21] Integrate LinkedIn account connections in Microsoft Entra ID, 23 october 2023, URL: https://learn.microsoft.com/en-us/entra/identity/users/linkedin-integration.

[22] Microsoft, Gebruik groepsbeleid om LinkedIn-accountverbindingen in te schakelen, 28 oktober 2023, URL: https://learn.microsoft.com/nl-nl/entra/identity/users/linkedin-integration#use-group-policy-to-enable-linkedin-account-connections.

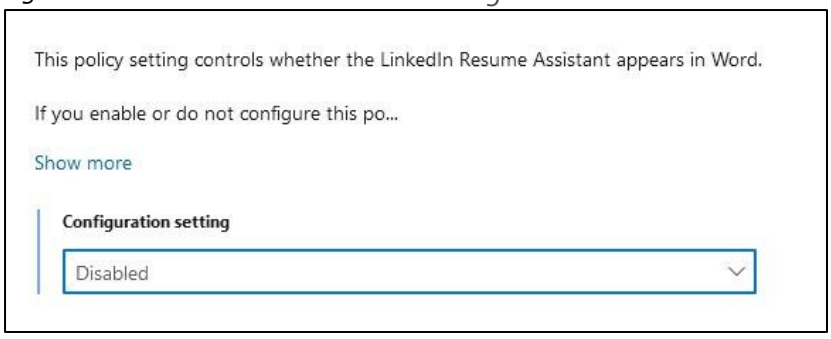
*Figuur 31: Schermafbeelding: LinkedIn account integratie uit*




*Figuur 32: Show LinkedIn features in Office uitgezet*




*Figuur 33: LinkedIn Resume Assistant uitgezet*



## 12. Customer Experience Improvement Program (CEIP)

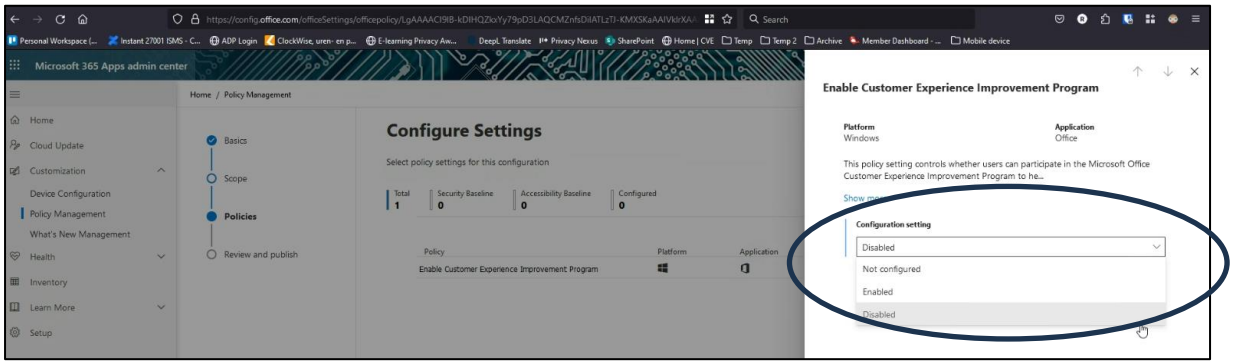
Via het Customer Experience Improvement Program (CEIP) verwerkt Microsoft diagnostische gegevens voor kwaliteitsverbetering van zowel Office als Windows 10/11. Microsoft gebruikt de gegevens om problemen op te lossen en om de producten en functies die klanten het vaakst gebruiken te verbeteren. Microsoft zegt geen namen, adressen of andere direct identificeerbare persoonsgegevens van gebruikers te verzamelen, alleen IP-adressen, maar Microsoft geeft geen inzage in deze gegevensstroom. Standaard staat deze verwerking aan, zowel voor Office ProPlus als in Windows 10/11.

Vanwege het gebrek aan transparantie adviseert SLM Rijk om deze verwerking uit te zetten.

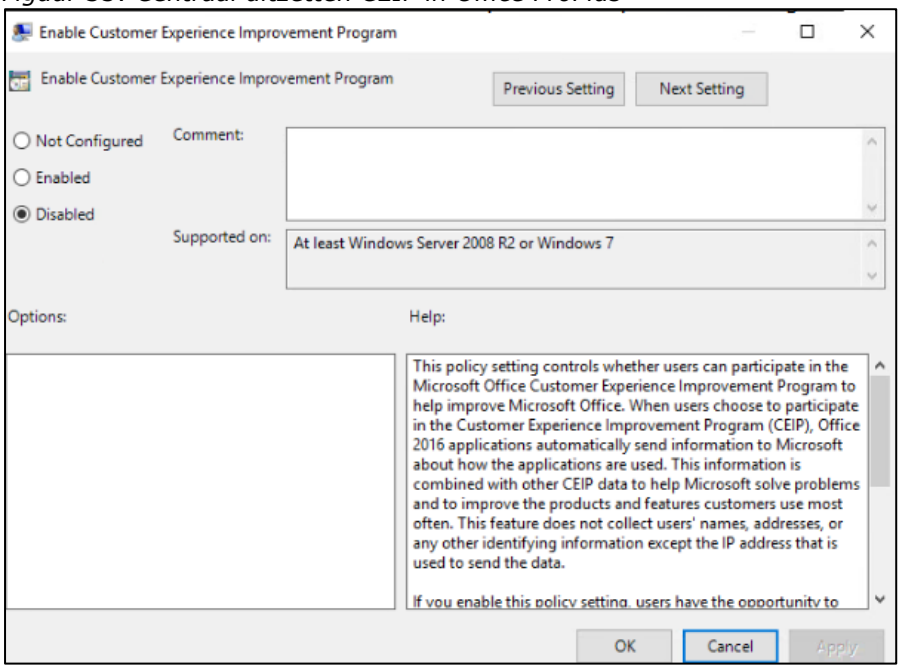
Privacyvriendelijke instelling kiezen

- Ga naar https://config.office.com **- ->** Microsoft 365 Cloud Policy **->** Kies een policy onder "name" **->** Policies **->** Zoek op "Enable Customer Experience Improvement Program" **- >** Disabled. Zie Figuur 34 hieronder.
- Of schakel CEIP centraal uit via de Group Policy Editor in Office en Windows: zie Figuur 35 en Figuur 36 hieronder.

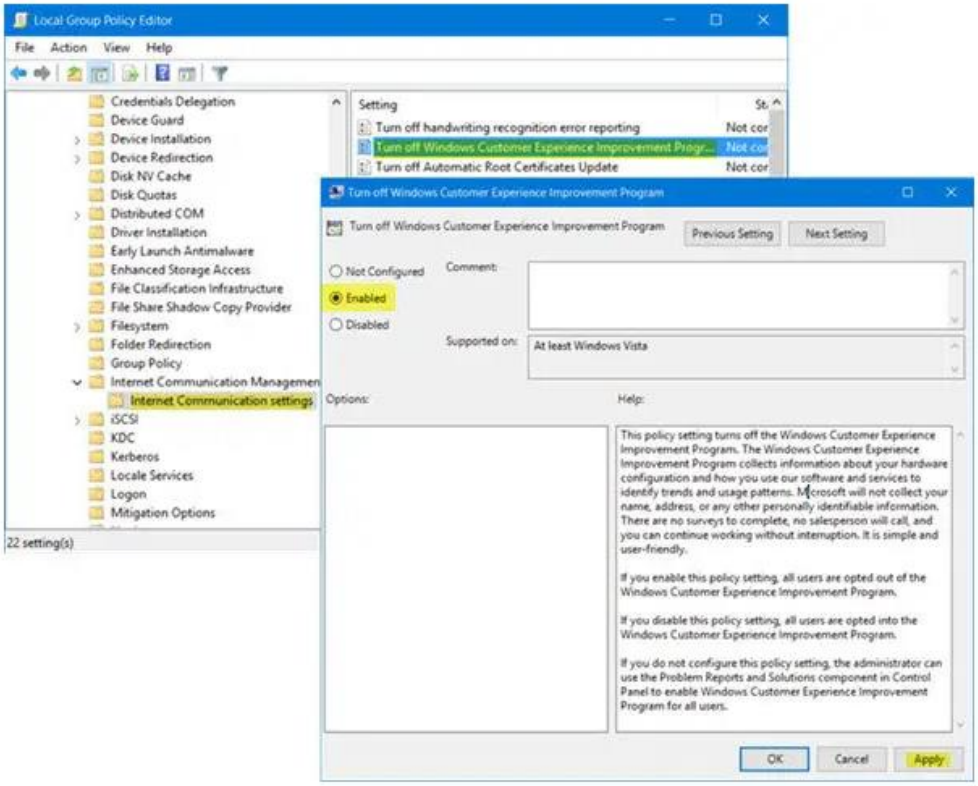
*Figuur 34: Centraal uitschakelen CEIP in via config.office.com*




*Figuur 35: Centraal uitzetten CEIP in Office ProPlus*



*Figuur 36: Centraal uitzetten CEIP in Windows*[23]




## 13. Automatische geolocatie in Outlook Agenda

Zelfs als een organisatie alle *Additional Optional Connected Experiences* centraal heeft uitgezet, gaat er nog verkeer via de Outlook Agenda naar Bing om automatisch de locatie in te vullen van een afspraak. Microsoft is zelfstandige verantwoordelijke voor Bing, en staat zichzelf toe om de gegevens die ze via Bing verkrijgt voor haar eigen commerciële doelen gebruiken.

SLM Rijk adviseert om deze gegevensstroom te blokkeren via Windows Powershell, zoals aanbevolen door Microsoft.[24]

<u>Privacyvriendelijke instelling kiezen</u>

- Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -PlacesEnabled $false

*Figuur 37: Geolocatie in Outlook uitgeschakeld*


[23] Schermafbeeldingen van The Windows Club, URL: https://www.thewindowsclub.com/disable-windows-customer-experience-improvement-program.
[24] Microsoft specifiek Powershell script voor Outlook on the Web, URL: https://learn.microsoft.com/en-us/powershell/module/exchange/set-owamailboxpolicy?view=exchange-ps#-placesenabled

# 14. Analytische diensten Microsoft 365

Microsoft biedt een aantal analytische diensten, waarmee gedrag van medewerkers inzichtelijk wordt gemaakt. Medewerkers kunnen via Viva Insights bijvoorbeeld persoonlijke aanbevelingen krijgen om 'gezondere gewoonten op het werk' te ontwikkelen. Door metingen hoeveel tijd ze aan e-mail of vergaderingen besteden, of door aanbevelingen om mindfulness oefeningen te doen. Microsoft nodigt medewerkers uit om aan te geven op emoji's hoe ze zich die dag voelen. Microsoft biedt ook gedetailleerde analyses aan medewerkers over hun e-mailgedrag, bijvoorbeeld hoeveel mensen hun mail hebben geopend en hoeveel tijd ze hebben besteed aan het lezen van de mail (als de mail aan meer dan 5 personen is gestuurd). Voor gedetailleerde e-mailanalyses is een aparte Outlook add-in vereist. Microsoft claimt met deze diensten de productiviteit en het welzijn van medewerkers te vergroten, maar deze claims zijn niet onderbouwd.

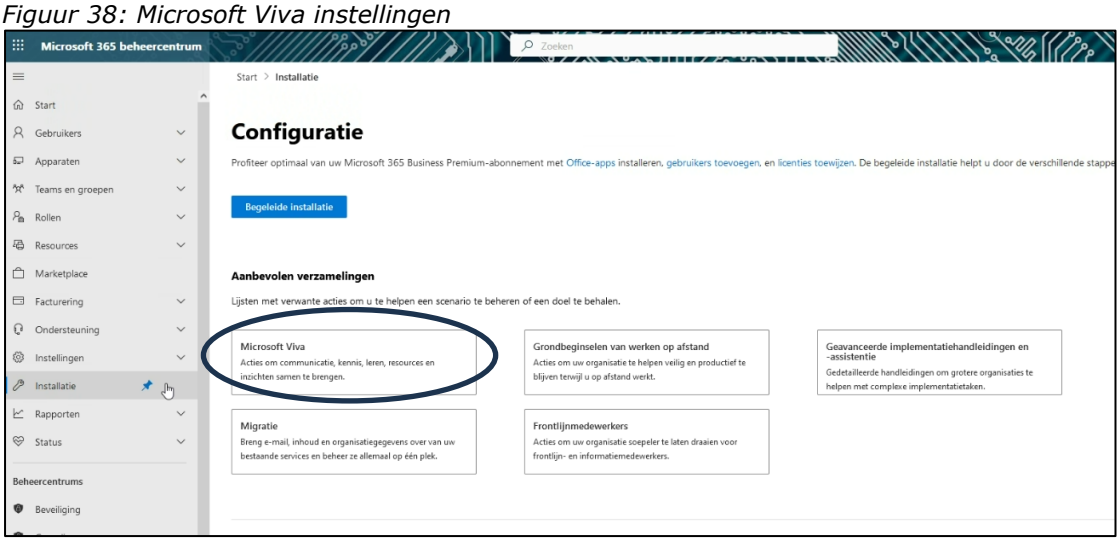
Er zijn wel privacyrisico's verbonden aan het gebruik van de diensten, als de informatie ingezet wordt bij beoordelingen, of als onderdeel van een personeelsvolgsysteem.

Viva Insights staat standaard uit. Als een beheerder Viva Insights aanzet, kan een gebruiker de dienst nog steeds individueel uitzetten. Hoewel Microsoft de dienst Viva Briefings emails tijdelijk heeft gepauzeerd (sinds 15 januari 2023), raadt SLM Rijk nog steeds aan om die dienst uit te zetten. Zie Figuur 41 hieronder.

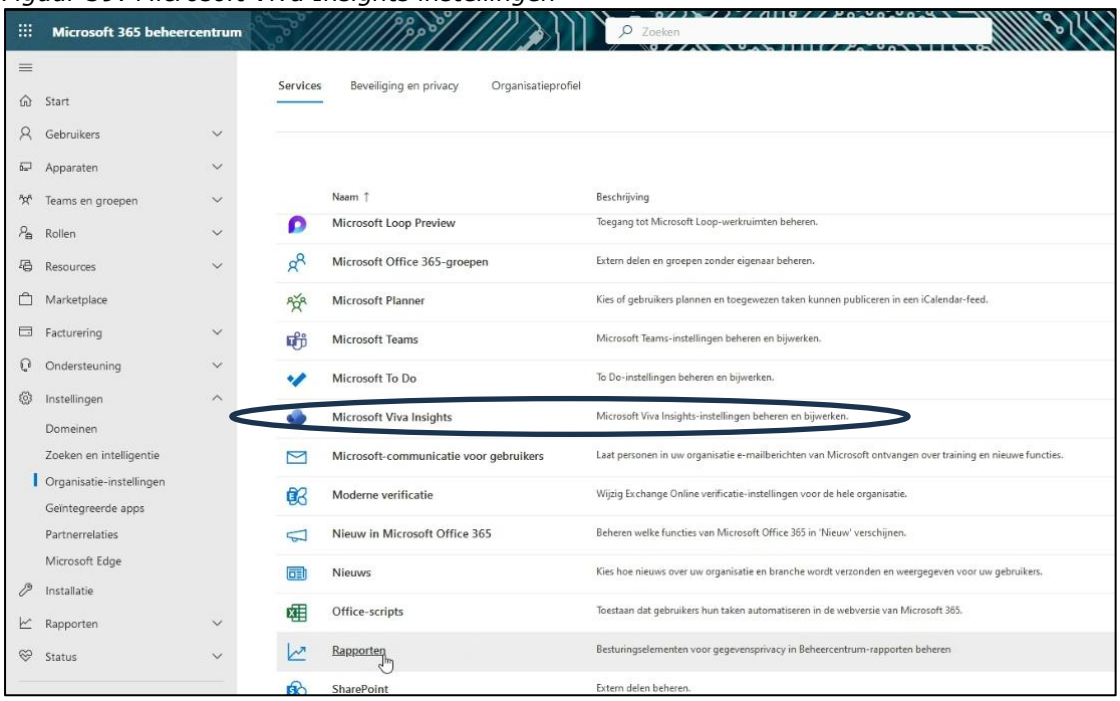
Privacyvriendelijke instelling kiezen

- Controleer dat Viva Insights mail briefings uitstaan: Ga naar https://admin.microsoft.com **->** Installatie **->** Microsoft Viva **->** Viva Insights **->** Manage settings (Zie x)
- Controleer ook dat Viva Insights uitstaan in Outlook

*Figuur 38: Microsoft Viva instellingen*

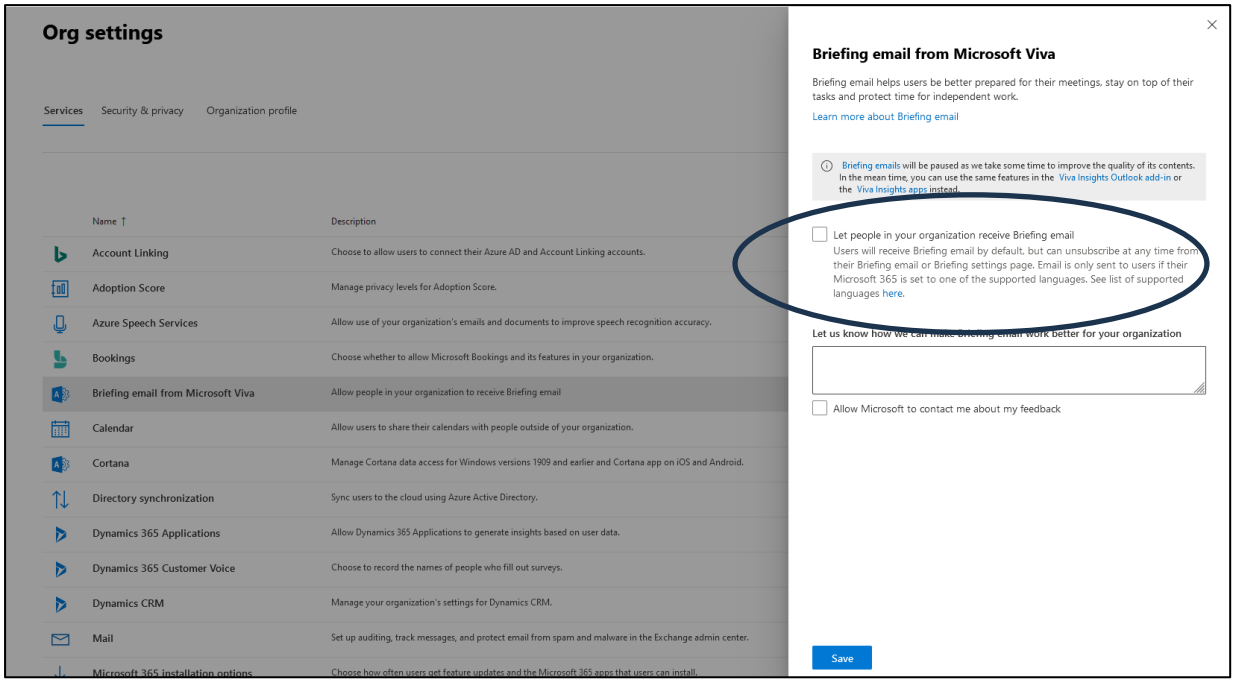


*Figuur 39: Microsoft Viva Insights instellingen*




*Figuur 40: Privacy vriendelijke instellingen Viva Insights*

*Figuur 41: Viva mail briefing uitgezet*



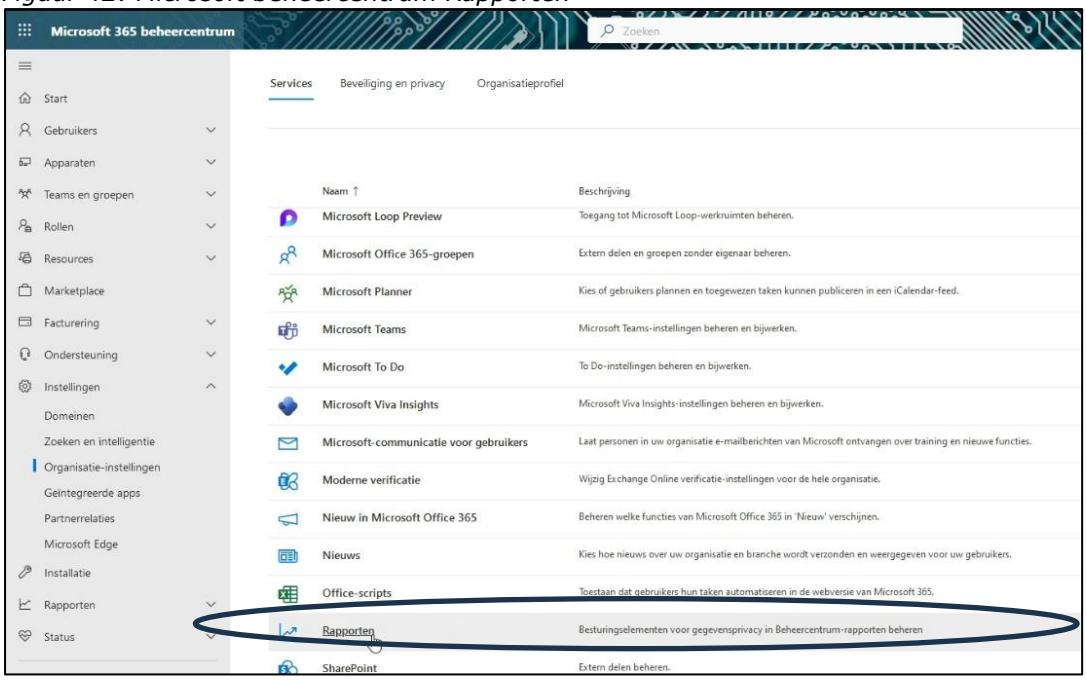

## 15. Pseudonimisering gebruikersrapporten Teams

Voor Teams Analytics & reports bestaat er geen uitschakelmogelijkheid, alleen een pseudonimiseringsoptie voor de beheerder. Het is niet aannemelijk dat pseudonieme weergave in gebruiksrapporten invloed heeft op de ruwe data in de onderliggende cloudlogs bij Microsoft, maar de maatregel beschermt tegen ongewilde inzage door beheerders of managers in persoonlijk gedrag van collega's.

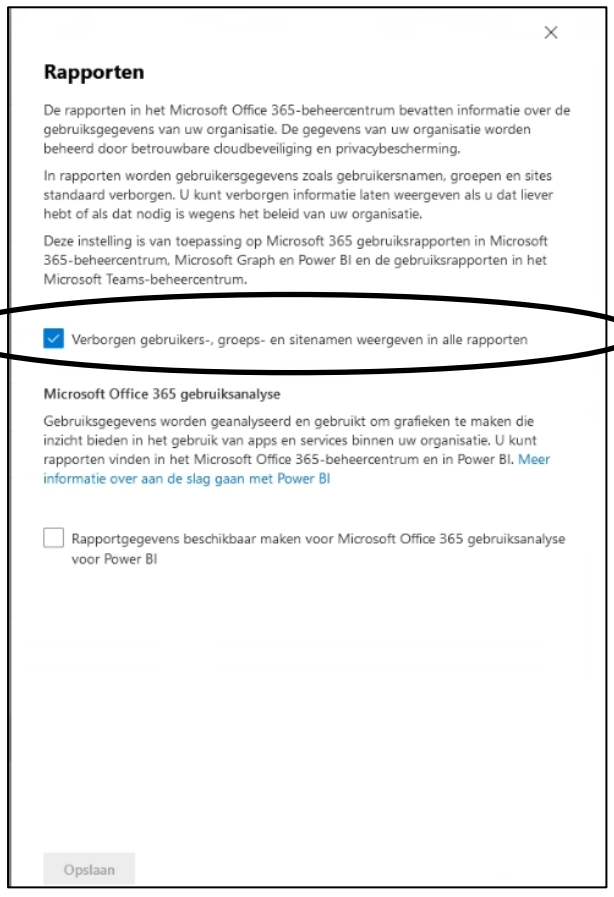
<u>Privacyvriendelijke instelling kiezen</u>

- Kies de pseudonimiseringsoptie in Teams Analytics & Reports, via het Microsoft Admin Center **->** Settings **->** Org Settings **->** kies 'Reports' op het Services tabblad **->** kies 'Display anonymous identifiers' **->** Save changes.

*Figuur 42: Microsoft beheercentrum Rapporten*




*Figuur 43: Standaard pseudonimiseringsoptie Teams Analytics & Reports*



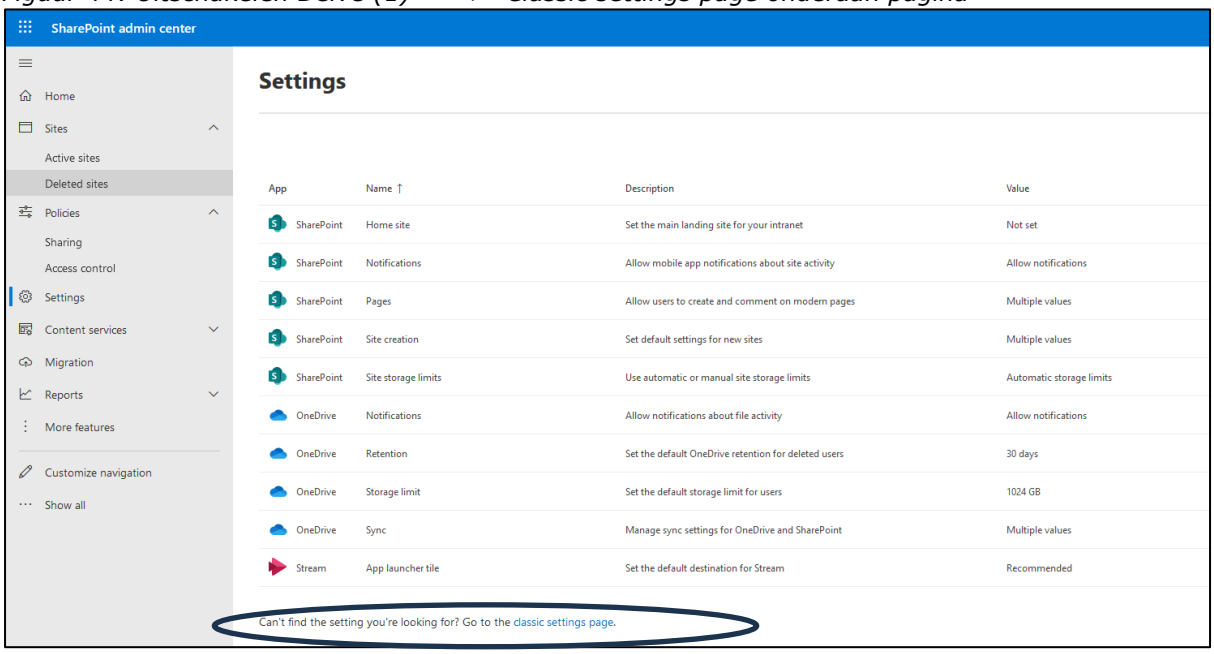
# 16. Uitschakelen Delve

De standaardinstelling is dat Delve aan staat. Systeembeheerders kunnen Delve uitschakelen, zie Figuur 44 en Figuur 45 hieronder. Uitzetten voorkomt het risico dat medewerkers intern via SharePoint onbedoelde toegang krijgen tot documenten waar collega's aan werken.

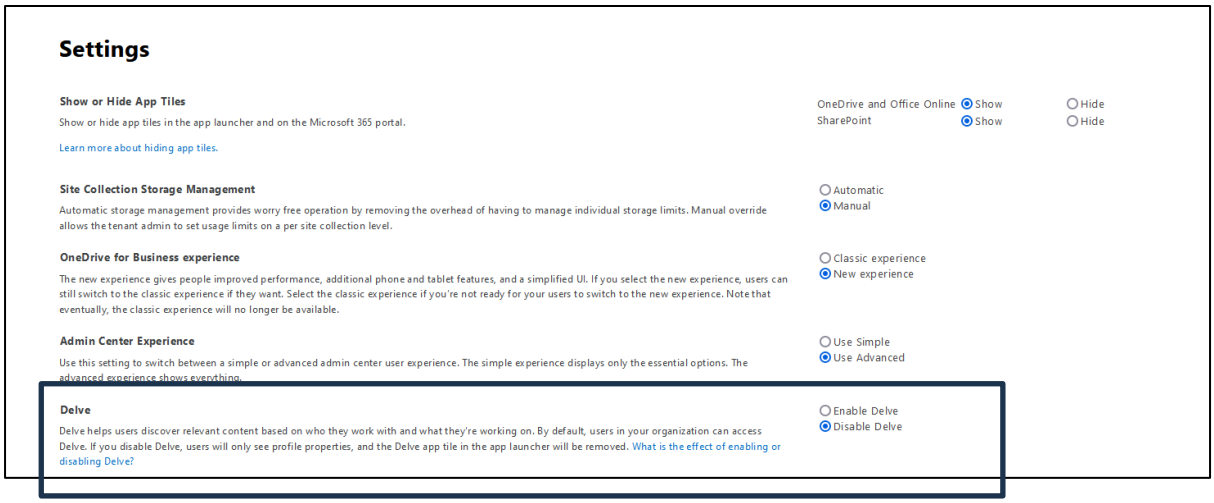
Privacyvriendelijke instelling kiezen

- Schakel Delve uit: Ga naar https://admin.microsoft.com/sharepoint?page=sharing&modern=true **->** Settings **->** Classic settings page (onderaan de pagina) **->** Disable Delve

*Figuur 44: Uitschakelen Delve (1) -- **->** Classic settings page onderaan pagina*




*Figuur 45: Uitschakelen Delve (2)*



# 17. Omgang met spam in Defender

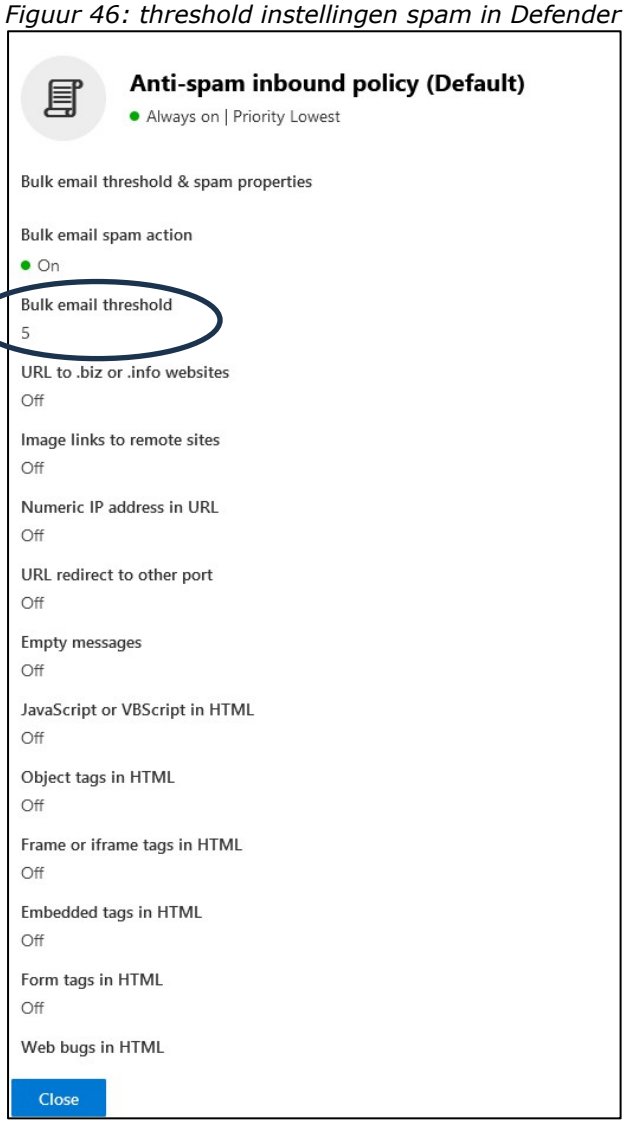
Microsoft kan in Defender mail classificeren als spam, en automatisch weggooien. Dat kan leiden tot een dataprotectierisico, als bijvoorbeeld een sollicitatiebrief of bezwaarschrift niet bij de ontvanger aankomen, terwijl ze wel (tijdig) zijn verzonden.

Beheerders kunnen ervoor kiezen om eindgebruikers toegang te bieden tot mails die door Defender als spam worden gekwalificeerd, zodat gebruikers zelf de *false positives* kunnen herstellen.

Privacyvriendelijke instelling kiezen

- Bepaal zorgvuldig hoe streng de 'threshold' is voor spam en malware. Zie Figuur 46 hieronder.
- Neem steekproeven op mail die als spam is gemarkeerd, of gebruik een third party e-mail threat protection-product waarbij de gebruiker zelf toegang heeft tot de onderschepte spamberichten.

*Figuur 46: threshold instellingen spam in Defender*



# 18. Pseudonimiseren gebruikersnamen in Defender voor Cloud Apps

Microsoft biedt een pseudonimiseringsoptie in de dashboards van Defender voor Cloud Apps voor de gebruikersnamen. In de dashboards wordt de gebruikersnaam dan vervangen door een versleutelde gebruikersnaam. Microsoft noemt dit '*anonimisering*', maar wijst er ook op dat de beheerders de echte gebruikersnaam kunnen opzoeken als dat nodig is voor een specifiek beveiligingsonderzoek. Er is dus geen sprake van anonimisering, maar van pseudonimisering. Het is een goede privacymaatregel om te voorkomen dat beheerders onnodig gedrag van collega's herkennen.

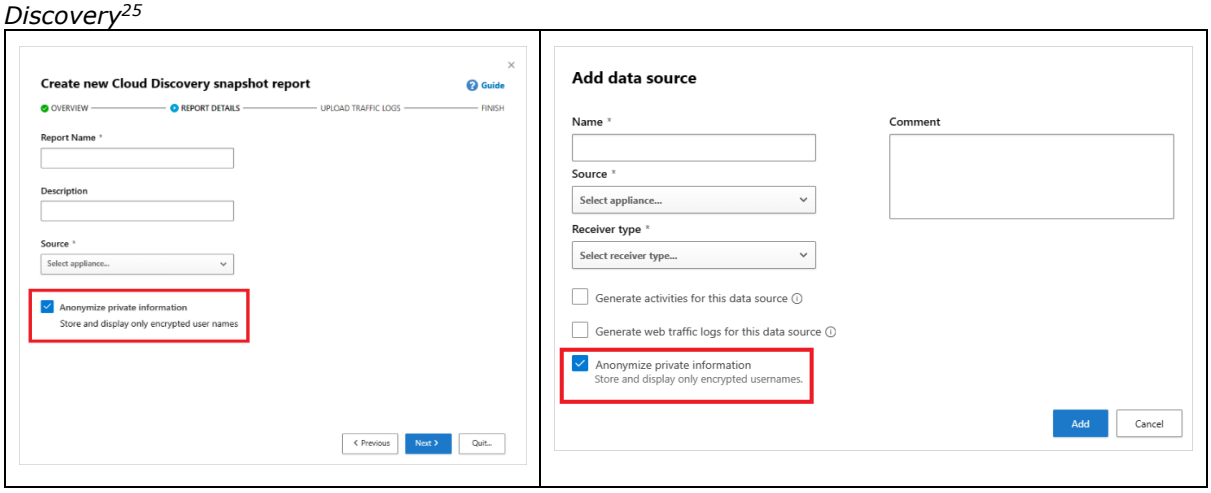
De lookups/conversies worden gelogd in het Governance-logboek. Met dit log kunnen organisaties controleren of beheerders de gebruiker terecht hebben geheridentificeerd, in overeenstemming met het interne privacybeleid.

Privacyvriendelijke instelling kiezen

Microsoft biedt instellingen voor pseudonimisering in de dashboards van Defender voor Cloud Apps voor gebruikersnamen, voor nieuwe snapshotrapporten en voor rapporten van nieuwe gegevensbronnen.

- Ga naar https://security.microsoft.com **->** Settings **->** Cloud Apps **->** Snapshot Reports (onder Cloud Discovery) **->** Create snapshot report **->** Onder Report Details, kies Anonymize private information. Zie Figuur 47 hieronder.
- Ga naar https://security.microsoft.com **->** Settings **->** Cloud Apps **->** Automatic Log Upload (onder Cloud Discovery) **->** Add data source **->** Anonymize private information

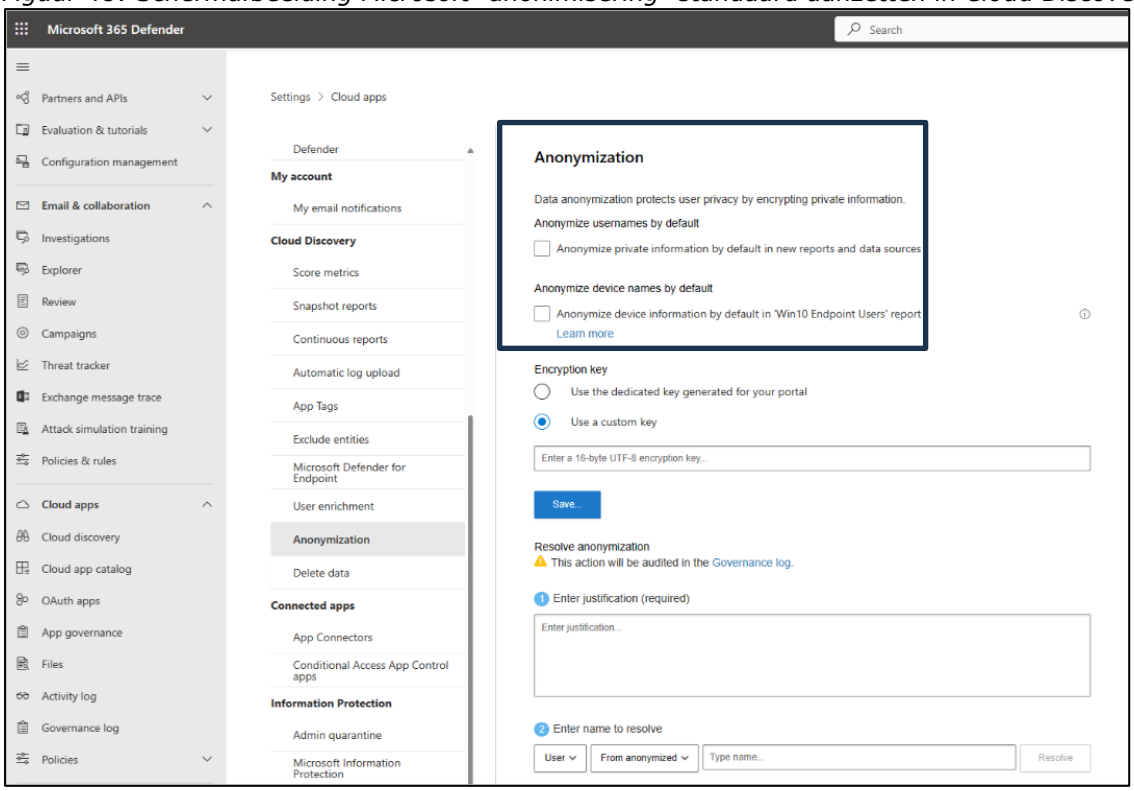
*Figuur 47: Schermafbeeldingen "anonimiseren" in nieuwe rapporten en nieuwe bronnen in Cloud Discovery*[25]




- Het is ook mogelijk om standaard de pseudonimisering in te stellen voor alle dashboards in Cloud Discovery: Ga naar https://security.microsoft.com **->** Settings **->** Cloud Apps **->** Anonymization (onder Cloud Discovery)

[25] Microsoft, Cloud Discovery-gegevens anoniem maken, 24 april 2023, URL: https://learn.microsoft.com/nl-nl/defender-cloud-apps/cloud-discovery-anonymizer

*Figuur 48: Schermafbeelding Microsoft "anonimisering" standaard aanzetten in Cloud Discovery*[26]




Microsoft biedt ook een omgekeerde mogelijkheid tot het automatisch verrijken van Cloud Discovery-gegevens met Azure AD gebruikersnamen. Microsoft legt uit:

"*Cloud Discovery-gegevens kunnen nu worden verrijkt met Azure Active Directory-gebruikersnaamgegevens. Wanneer u deze functie inschakelt, wordt de gebruikersnaam, die wordt ontvangen in de logboeken voor detectieverkeer, vergeleken en vervangen door de Azure AD gebruikersnaam. Met Cloud Discovery-verrijking worden de volgende functies ingeschakeld:*

- *U kunt schaduw-IT-gebruik onderzoeken door Azure Active Directory-gebruiker. De gebruiker wordt weergegeven met de UPN.*
- *U kunt het gebruik van de gedetecteerde cloud-app correleren met de verzamelde API-activiteiten.*

*Vervolgens kunt u aangepaste logboeken maken op basis van Azure AD gebruikersgroepen. Bijvoorbeeld een schaduw-IT-rapport voor een specifieke marketingafdeling*."[27]

Het is goed mogelijk dat een organisatie deze optie tijdelijk aanzet om individueel gebruik op te sporen van gebruik dat niet strookt met het beleid van de organisatie, zoals schaduw ICT. De organisatie moet hier wel beleid voor maken, omdat het haaks staat op de aanbeveling om de accountnamen juist te pseudonimiseren.

[26] Idem.

[27] Microsoft, Cloud Discovery-gegevens verrijken met Azure AD gebruikersnamen, 25 april 2023, URL: https://learn.microsoft.com/nl-nl/defender-cloud-apps/cloud-discovery-aad-enrichment.

## 19. Gebruik Giphy in Teams en Outlook

Voorheen adviseerde SLM Rijk om het gebruik van Giphy in Outlook en Teams apart centraal uit te zetten, omdat organisaties hiermee persoonsgegevens van hun werknemers doorgeven aan een derde partij. Het Amerikaanse bedrijf Giphy biedt een grote verzameling afbeeldingen aan, GIF's en geanimeerde GIF's, die gebruikers kunnen invoegen in allerlei chatprogramma's en sociale media. Op het gebruik van de dienst zijn de voorwaarden en het privacybeleid van Giphy van toepassing.

Giphy legt in zijn privacyverklaring uit dat het van elke gebruiker van zijn diensten automatisch het IP-adres, de unieke apparaatidentificatie, cookie-informatie en de specifieke advertentie-identificatienummers uit Android en iOS verzamelt. Giphy behoudt zich het recht voor om het IP-adres te gebruiken voor gerichte reclame. Bovendien staat Giphy zichzelf toe om geheime pixels van reclamenetwerken via de afbeeldingen te versturen. Voor gebruikers in de EU schrijft Giphy dat zij geen verwerker is, maar verantwoordelijke.

Het apart uitzetten van Giphy is niet meer nodig, omdat Microsoft Giphy heeft toegevoegd aan de lijst *Additional Optional Connected Experiences*. Dus als een organisatie het advies onder 9 over de verbonden ervaringen heeft opgevolgd, staat Giphy ook uit.

## 20. Toegang tot apps in de app-store in Teams

Teams heeft een ingebouwde appstore, met apps van Microsoft en apps van derde partijen.

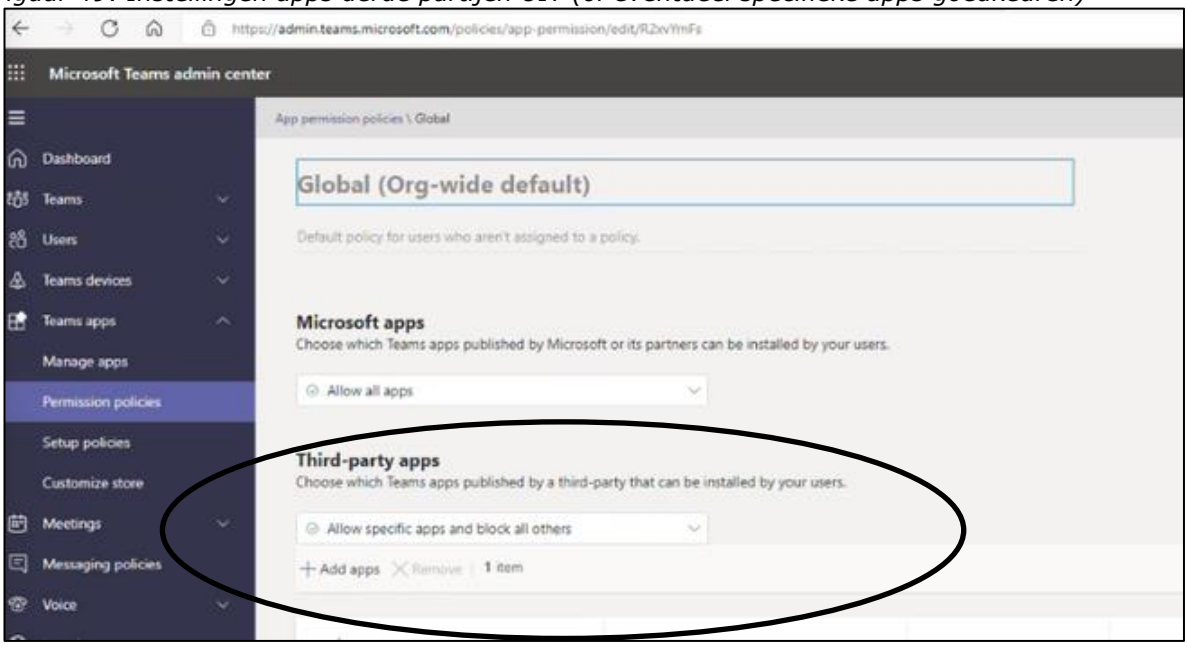
Beheerders kunnen de toegang van medewerkers tot apps beperken om het risico te mitigeren dat via de apps persoonsgegevens van de organisatie uitlekken aan derde partijen.

SLM Rijk adviseert om in beginsel de toegang tot apps van derde partijen in de Teams app-store uit te zetten, evenals de toegang tot persoonsgegevens door apps, tenzij de toegang noodzakelijk is voor de organisatie, en er goede afspraken zijn over de gegevensverwerking.

Privacyvriendelijke instelling kiezen

- Ga naar https://admin.teams.microsoft.com **->** Team apps **->** Permission policies **->** Global **->** Disable third-party apps

*Figuur 49: Instellingen apps derde partijen UIT (of eventueel specifieke apps goedkeuren)*



# 21. E2EE in Teams

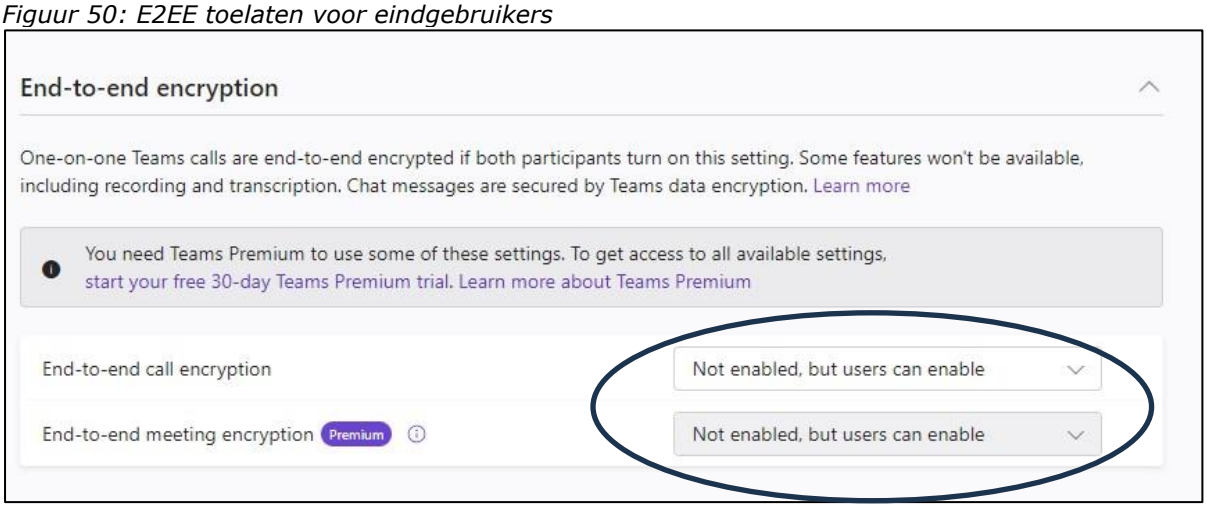
Teams-gegevens worden onderweg (in transit) en als ze opgeslagen zijn (at rest) versleuteld in de datacentra van Microsoft met behulp van standaardtechnologieën zoals TLS en SRTP. Dit omvat oproepen, berichten, bestanden, vergaderingen en andere inhoud. Beheerders kunnen voor extra versleuteling kiezen door E2EE in Teams aan te zetten. Microsoft biedt die versleuteling niet aan voor alle Teams-gesprekken, maar alleen voor 1 op 1 gesprekken tussen eindgebruikers. Met E2EE wordt informatie versleuteld bij de oorsprong, op het apparaat van de gebruiker, en ontsleuteld op de beoogde bestemming, het apparaat van de ontvanger, zodat tussen die punten geen informatie kan worden ontsleuteld. De sleutel is ook niet toegankelijk voor Microsoft.

Microsoft heeft een aparte dienst ontwikkeld, Teams Premium, met allerlei AI-diensten. In die dienst zou het wel mogelijk moeten zijn om E2EE voor alle Teams gesprekken aan te zetten, maar dan werken alle AI-diensten niet meer. SLM Rijk laat een DPIA en HRIA uitvoeren op Teams Premium.

Privacyvriendelijke instelling kiezen

- Schakel E2EE standaard in voor 1-op-1 gesprekken in Teams **->** https://admin.teams.microsoft.com **->** Enhanced encryption **->** Global **->** Not enabled, but users can enable
- Instrueer eindgebruikers om E2EE ook in te schakelen

*Figuur 50: E2EE toelaten voor eindgebruikers*




# 22. Customer Key, Customer Lockbox en Double Key Encryption

De dienst *Customer Key* is gebouwd op service-encryptie en stelt organisaties in staat om zelf encryptiesleutels aan te maken en te beheren. Microsoft 365 gebruikt deze sleutels vervolgens om de opgeslagen gegevens in OneDrive, SharePoint en Exchange Online te versleutelen. Microsoft weliswaar toegang tot de sleutel bij het verwerken van de gegevens, maar Customer Key vermindert wel de mogelijkheden die Microsoft heeft om toegang te krijgen tot de onversleutelde inhoudelijke gegevens

De dienst *Customer Lockbox* stelt beheerders in staat om een extra niveau van versleuteling in te schakelen voor gegevens die zijn opgeslagen in Exchange Online (inclusief Teamgegevens), SharePoint en OneDrive. Hierdoor kunnen de Microsoft engineers en support medewerkers niet meer bij de inhoud van bestanden zonder aparte toestemming van de klant. De klant kan wel toegang geven, maar dan voor beperkte tijd, voor specifieke doeleinden.

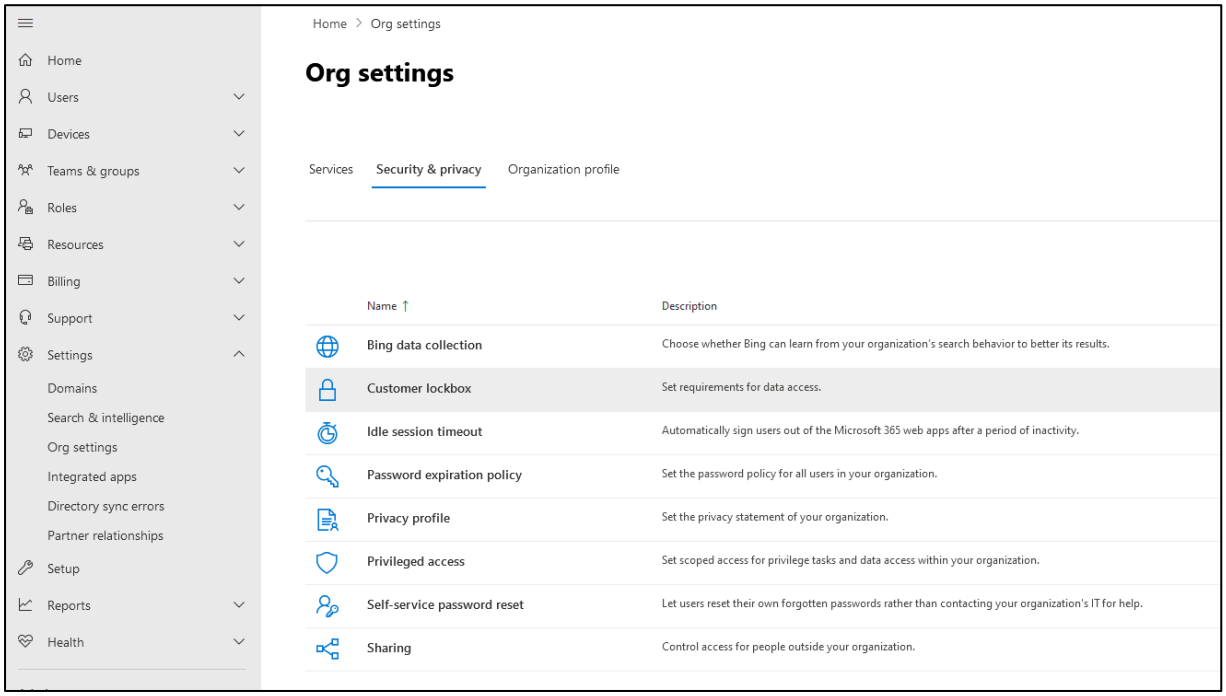
De dienst *Double Key Encryption* stelt organisaties in staat om bestanden te versleutelen met een sleutel onder eigen beheer. SLM Rijk werkt aan een DPIA over deze dienst en zal daarin, indien nodig, aparte instructies opnemen voor privacyvriendelijke instellingen.

SLM Rijk adviseert om Customer Lockbox in te schakelen zolang de EU Data Boundary nog niet is voltooid (voor support gegevens eind 2024).

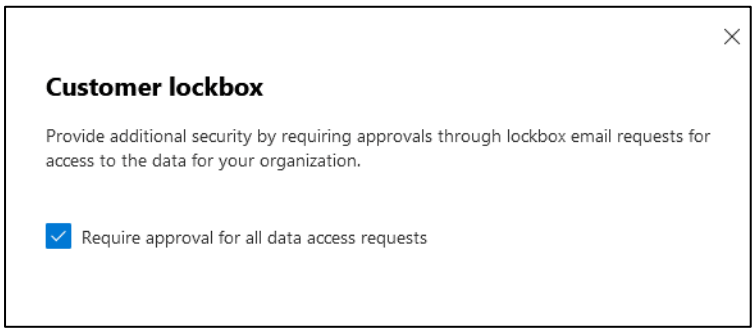
Privacyvriendelijke instelling kieze

- Ga via https://admin.microsoft.com- -> Instellingen- -> Organisatieinstellingen- -> Beveiliging en privacy
- Selecteer Customer Lockbox in de rechter kolom. Schakel het selectievakje in *Goedkeuring vereisen voor alle verzoeken om toegang tot gegevens* en sla de wijzigingen op om de functie in te schakelen.

*Figuur 51: Instellingen Customer Lockbox (1)*




*Figuur 52: Instellingen Customer Lockbox (2)*



# 23. Indienen van inzageverzoeken door systeembeheerders

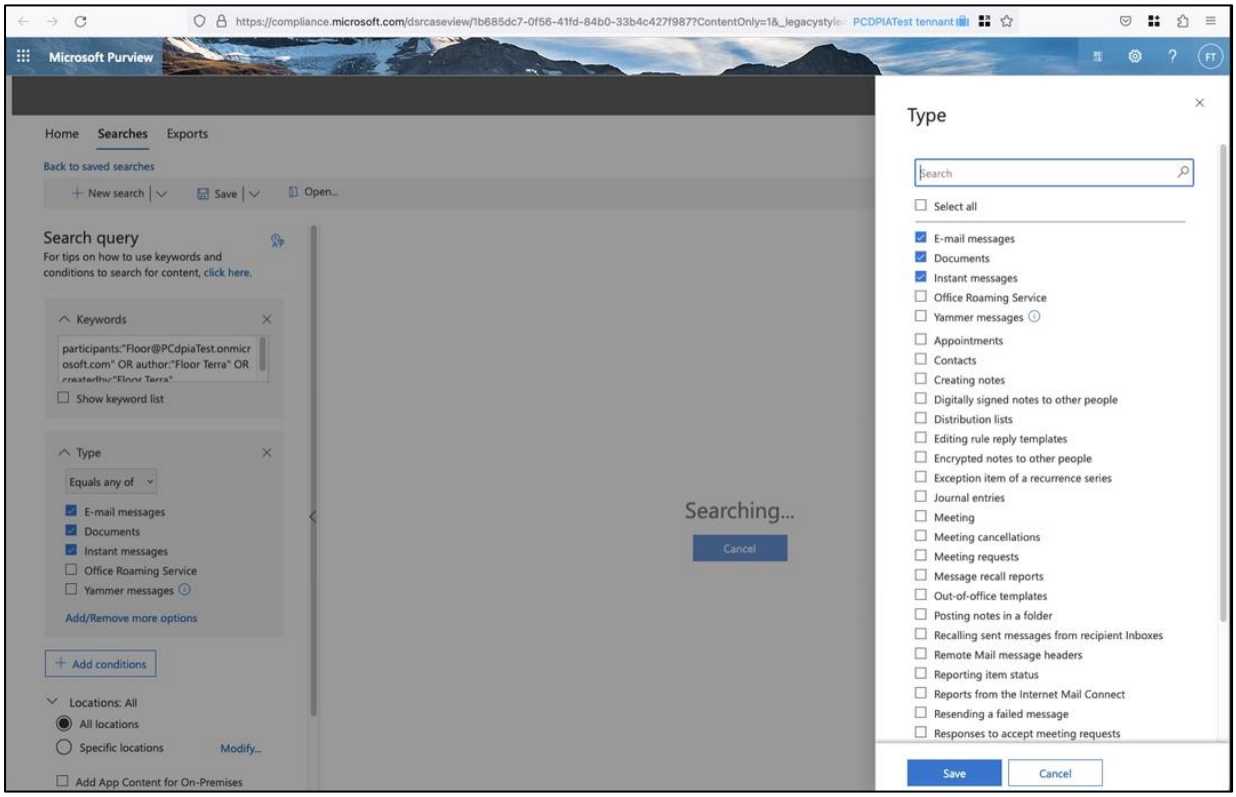
Systeembeheerders kunnen op twee manieren een inzageverzoek indienen bij Microsoft als een medewerker een inzageverzoek bij hen indient: enerzijds voor de inhoudelijke gegevens (zoals e-mails en bestanden), anderzijds voor alle diagnostische data.

**Inzage in inhoudelijke gegevens**

Beheerders kunnen via het compliance portal van Microsoft een inzageverzoek indienen voor de inhoudelijke gegevens.[28]

- Zorg dat de systeembeheerder geautoriseerd is voor content export door hem lid te maken van de eDiscovery Manager rol groep.
- Log in op https://compliance.microsoft.com/
- Kies Ediscovery **->** User data search **->** Create a Case (een UDS case)
- Voer als zoekterm de account naam van de gebruiker in om bijvoorbeeld alle e-mails van, aan, cc en bcc een persoon te vinden.
- Selecteer vervolgens het Type data waarvoor inzage wordt gevraagd. Standaard vinkt Microsoft alleen drie categorieën inhoudelijke persoonsgegevens aan: e-mails, documenten en instant messages. Maar er zijn veel meer soorten gegevens op te halen.

*Figuur 53: Microsoft Inzage portaal voor inhoudelijke gegevens*




[28] Microsoft, Office 365 Data Subject Requests for the GDPR and CCPA, 11 February 2023, URL: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-office365.

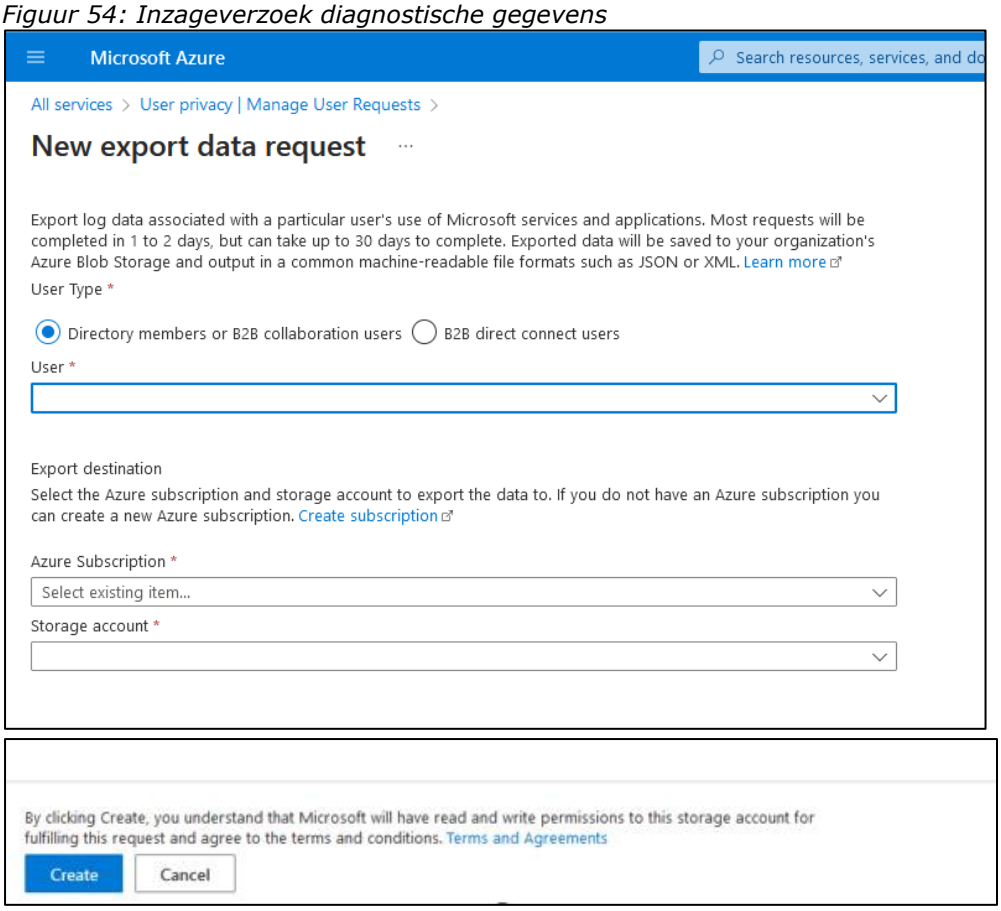
### Inzage in diagnostische gegevens

De topbeheerder (tenant admin) kan ook inzage vragen voor een medewerker in de diagnostische gegevens.[29]

Via het Azure portaal geeft Microsoft inzage in de product- en dienstgebruiksgegevens zoals user activity logs, zoekopdrachten en andere gegevens die gegenereerd worden door producten en diensten als onderdeel van de systeemfunctionaliteit en interactie van gebruikers met de diensten of systemen. Microsoft waarschuwt dat een exportverzoek lang kan duren. Meestal zou het in één of twee dagen voltooid moeten zijn, maar het kan tot 30 dagen duren.

- Meld u aan bij het Azure-portaal als tenant admin en selecteer Alle services.
- Zoek op User Privacy **->** Manage User Requests **->** Add export request
- Vul de details in van het verzoek, met het e-mailadres van de Azure Active Directory-gebruiker die de export heeft aangevraagd, het abonnement en de locatie van het Azure opslagaccount.
- Maak een nieuwe container als opslaglocatie voor de geëxporteerde privacygegevens van de gebruiker.
- Selecteer Create.

*Figuur 54: Inzageverzoek diagnostische gegevens*




[29] Microsoft, Part 3: Responding to DSRs for system-generated Logs (alleen Engelstalig), 11 February 2023, URL: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-system-generated-log-data.