



Ministerie van Justitie en Veiligheid

## **Handleiding privacyvriendelijke instellingen Microsoft 365 - voor beheerders**

Versie 1.0

|        |             |
|--------|-------------|
| Datum  | 9 juni 2023 |
| Status | Definitief  |



## Colofon

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



## Inhoud

Colofon 3

Inleiding 7

1. Geolocatiekeuze 8
2. Tonen intern privacybeleid aan medewerkers en gastgebruikers 10
3. Pseudonimisering accountgegevens medewerkers 14
4. Instellen authenticatiemiddelen Azure AD 15
5. Versiebeheer van Office ProPlus en mobiele Office-applicaties 17
6. Telemetrieniveau Office 365 18
7. Microsoft verwerker voor de telemetrie uit Windows 10 21
8. Telemetrieniveau Windows 22
9. Gebruik van Verbonden Ervaringen (Connected Experiences) 24
10. Windows 10 activiteitenoverzicht 26
11. LinkedIn-integratie voor Microsoftaccounts 28
12. Customer Experience Improvement Program (CEIP) 29
13. Automatische geolocatie in Outlook Agenda 31
14. Analytische diensten Microsoft 365 32
15. Omgang met spam in Defender 36
16. Pseudonimiseren gebruikersnamen in Defender voor Cloud Apps 37
17. Toegang tot Feedback en Twitter in Defender portal 40
18. Het gebruik van Giphy in Teams en Outlook 41
19. Toegang tot apps in de app-store in Teams 42
20. E2EE in Teams 43
21. Customer Key, Customer Lockbox en Double Key Encryption 44
22. Indienen van inzageverzoeken door systeembeheerders 46



## Inleiding

Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (hierna: SLM) heeft in 2019 een contract met Microsoft onderhandeld voor het Rijk voor alle online diensten, inclusief een verwerkersovereenkomst. Op grond van deze overeenkomst mag Microsoft als verwerker verschillende soorten persoonsgegevens alleen voor drie specifieke en legitieme doelen verwerken. Lees hier meer informatie over de openbare DPIA's en controle-onderzoeken op de verschillende Microsoftdiensten.<sup>1</sup>

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

Deze handleiding beschrijft de verschillende opties die systeembeheerders hebben om Microsoft365 zo privacyvriendelijk mogelijk in te stellen. De mogelijkheden worden afzonderlijk en stapsgewijs behandeld, met screenshots, zodat beheerders die eenvoudig op een goede manier kunnen instellen. In totaal gaat het om 22 opties.

Deze handleiding beschrijft niet de organisatorische maatregelen die organisaties kunnen treffen en biedt ook zeker geen totaaloverzicht van alle mogelijke technische privacykeuzes. Microsoft365 omvat een zeer uitgebreid pakket aan diensten. SLM laat regelmatig DPIA's en controle-onderzoeken uitvoeren. Voor de nabije toekomst staan DPIA's op stapel voor Microsoft Purview (informatie labeling, inclusief Double Key Encryption), Dynamics en de webbrowser Edge. Als uit die DPIA's extra aanbevelingen volgen voor technische privacykeuzes, wordt deze handleiding aangevuld.

---

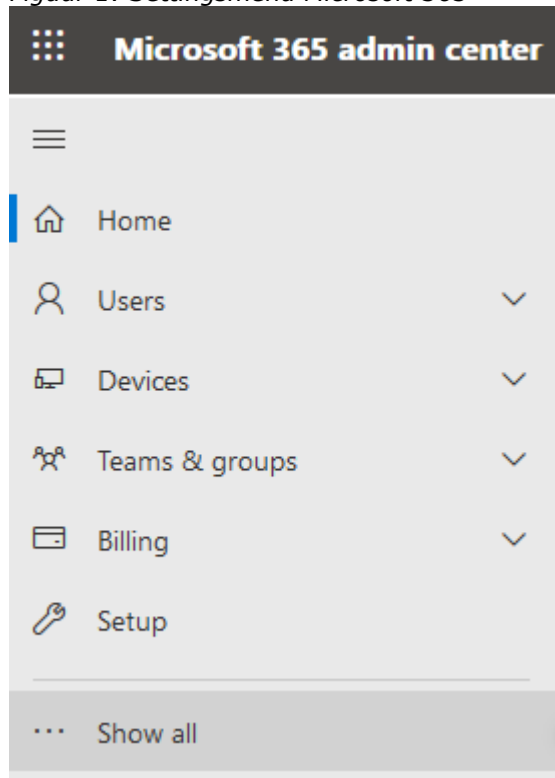
<sup>1</sup> SLM Microsoft, Google Cloud en Amazon Web Services, gehuisvest bij het Ministerie van Justitie en Veiligheid, URL: <https://slmmicrosoftrijk.nl>

## 1. Geolocatiekeuze

Klanten 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. Bekijk de website van Microsoft voor meer informatie over de uitvoering en planning van de *EU Data Boundary*.<sup>2</sup>

Let op: "Settings" komt twee keer voor op admin.microsoft.com. De correcte "settings" voor deze instellingen is te vinden onder de drie horizontale lijntjes in het verticale menu (**de hamburger**) links in beeld, zoals te zien in onderstaande figuur 1.

Figuur 1: Settingsmenu Microsoft 365



- Ga via <https://admin.microsoft.com> -> Settings -> Org settings -> Organisation profile -> Data location

<sup>2</sup> Microsoft, What is the EU Data Boundary? 8 februari 2023, URL: <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn>  
Pagina 8 van 50

Figuur 2: Schermafbeelding instelling geolocatie



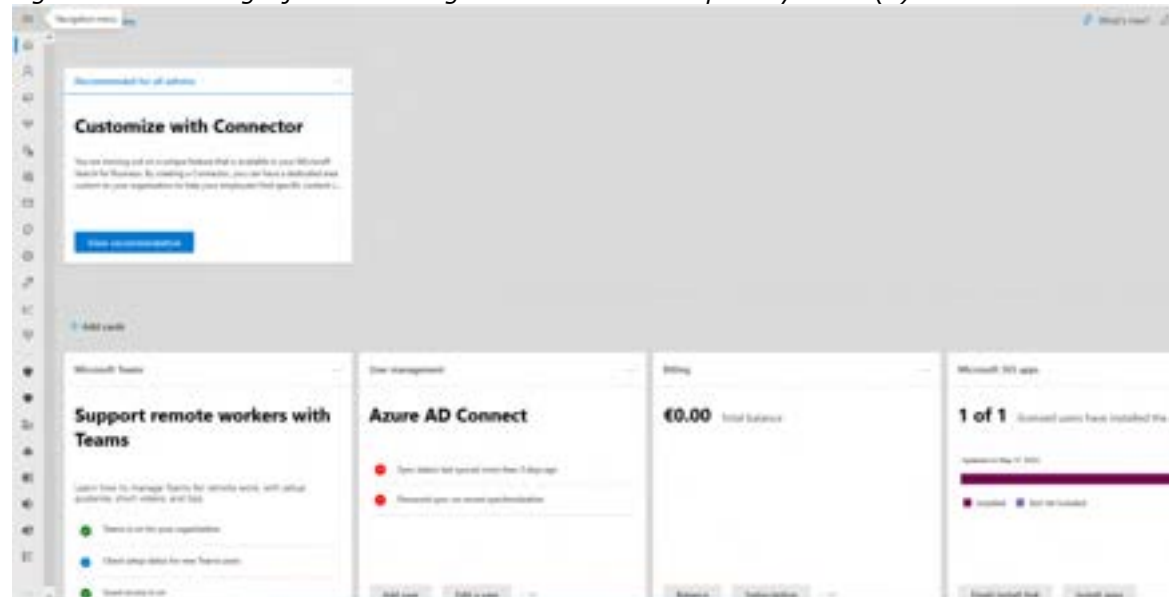
## 2. Tonen intern privacybeleid aan medewerkers en gastgebruikers

Organisaties verwerken veel persoonsgegevens via Microsoft 365. Via een intern privacybeleid kan de organisatie uitleggen wat medewerkers wel en niet mogen doen met de verschillende Officeapplicaties en 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 de Azure AD, ook voor bijvoorbeeld gastgebruikers in Teams.

- Ga via <https://admin.microsoft.com> -> Settings -> Org Settings -> Security & privacy -> Privacy Profile.
- 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 tot en met
- 
- 

- Figuur 6\_hieronder).
- Dwing acceptatie via de Azure AD af (zie Figuur en Figuur hieronder).

Figuur 3: Keuzemogelijkheid afdwingen tonen van intern privacybeleid (1)



Figuur 4: Keuzemogelijkheid afdwingen tonen van intern privacybeleid (2)



*Figuur 5: Keuzemogelijkheid afdwingen tonen van intern privacybeleid (3)*

**Privacy profile**

Set the URL to your organization's privacy policy, and the email address of your privacy contact.

Organization privacy statement \*

A valid URL is required

Organization privacy contact

*Figuur 6: Keuzemogelijkheid afdwingen tonen van intern privacybeleid (4)*

**Org settings**

Security & privacy Organization profile

Name 1

Big data collection

Customer feedback

Site search history

Personalization policy

Privacy profile

Privileged access

Self-service password reset

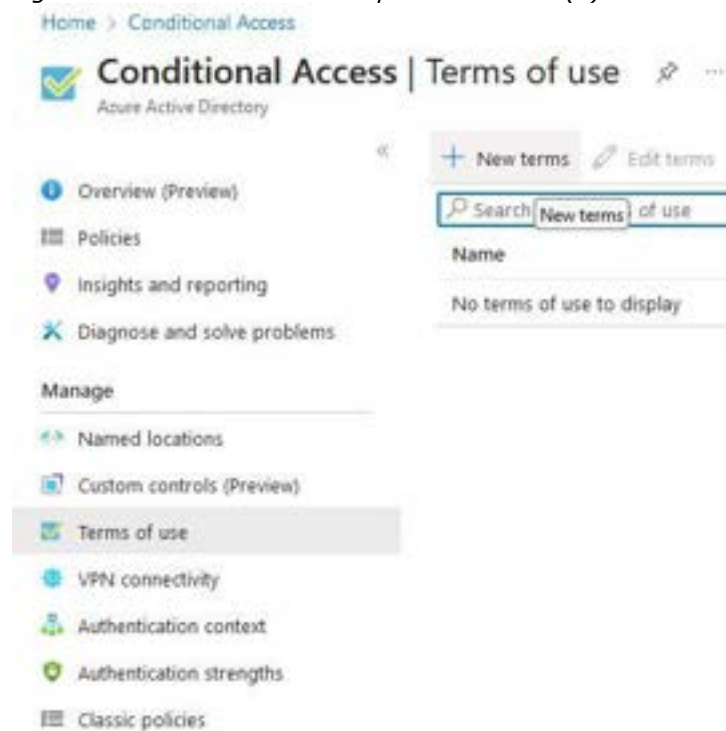
Sharing

Als onderdeel van de Conditional Access opties kan de Azure AD worden geïnstrueerd om eindgebruikers, inclusief gastgebruikers, te dwingen het interne

privacybeleid van de organisatie te accepteren. Zo'n Conditional Access policy kan worden afgedwongen nadat first-factor authenticatie is voltooid. Beheerders kunnen op die manier ook bewustwording afdwingen van relevante privacyregels bij gastgebruikers.

- Ga naar <https://portal.azure.com/> -> typ "Conditional access" in de zoekbalk -> "Terms of use" links -> new terms.
- Stel de Conditional Access opties in voor de Azure AD.

*Figuur 7: Conditional Access opties Azure AD (1)*



Figuur 8: Conditional Access opties Azure AD (2)

**Microsoft Azure** Search resources, services, and docs (5+)

Home > Conditional Access > Terms of use >

## New terms of use

**Terms of use**

Create and upload documents

Name \*

Terms of use document \*

+ Add language

Require users to expand the terms of use ☒

Require users to consent on every device ☒

Expire consents ☒

Duration before re-acceptance required (days)

---

**Conditional access**

Enforce with conditional access policy templates \*

### 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 Azure AD

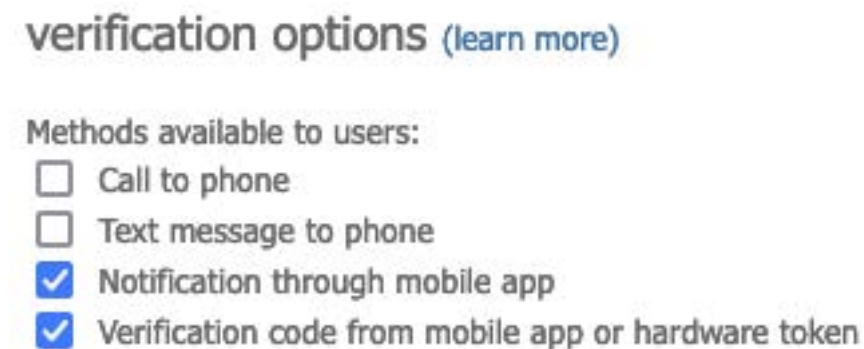
Gebruik van multifactorauthenticatie (MFA) is een belangrijke beveiligingsmaatregel om ongeautoriseerde toegang tot persoonsgegevens te voorkomen.

- Kies een authenticatiemiddel voor multifactorauthenticatie in de Azure AD, zoals de Authenticator-app of een hardwaretoken. Nota bene: 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 naar de VS. Gebruik deze optie dus niet.
- Multifactorauthenticatie is te vinden in <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 multifactorauthenticatie. Zie [Figuur 2](#) hieronder.

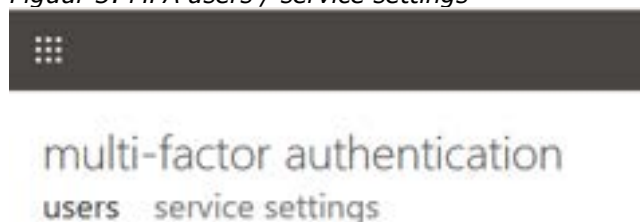
Let op: de opties om in te stellen welke authenticatiemiddelen zijn toegestaan, staan onder *service settings* (zie [Figuur 3](#) hieronder).

Het is mogelijk om MFA toe te laten, of af te dwingen. (Zie [Figuur 4](#) en [Figuur 5](#) hieronder).

*Figuur 2: Verificatieopties toestaan*



*Figuur 3: MFA users / service settings*



*Figuur 4: Instellen authenticatiemiddelen Azure AD per gebruiker*



*Figuur 5: Multi-factor authenticatieopties*

## Multi-factor authentication

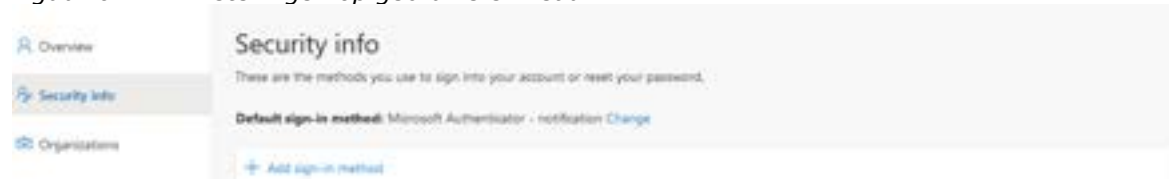
Multi-factor authentication provides a second layer of security by requiring users to sign in with more than just their username and password.

[Configure multi-factor authentication](#)

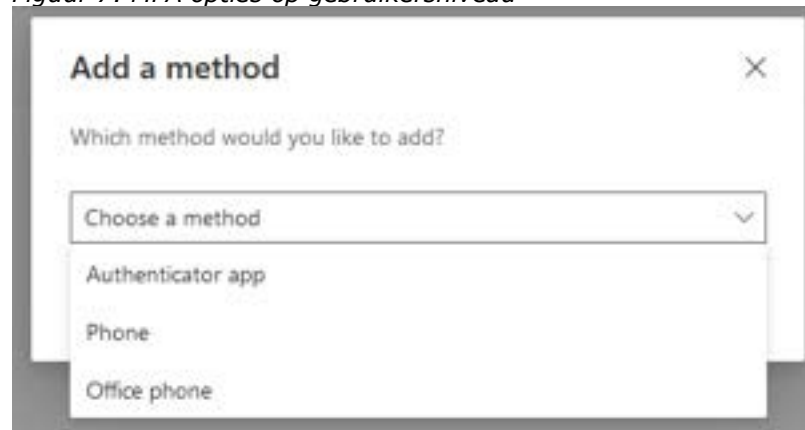
[Learn more about Azure multi-factor authentication](#)

Het is ook mogelijk om op individueel gebruikersniveau MFA-voorkeuren aan te passen. Dat kan via <https://mysignins.microsoft.com/security-info> (zie [Figuur 6](#) en [Figuur 7](#) hieronder).

*Figuur 6: MFA-instellingen op gebruikersniveau*



*Figuur 7: MFA opties op gebruikersniveau*



## 5. Versiebeheer van Office ProPlus en mobiele Office-applicaties

Om beveiligingsrisico's te voorkomen, is het belangrijk om goed in beeld te hebben welke versies van Office ProPlus in gebruik zijn. Centraal versiebeheer van Office ProPlus en mobiele applicaties heeft de voorkeur. Veel grote overheidsorganisatie zullen gebruik maken van centraal gemanagede werkplekken, waarbij ze images uitrollen van de benodigde Microsoftsoftware.

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 8](#) hieronder. Op deze pagina geeft Microsoft een uitleg welke stappen een gebruiker zelf moet ondernemen om zich met het werkaccount aan te melden.<sup>3</sup>

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 in 2020 een DPIA op laten uitvoeren.<sup>4</sup>

*Figuur 8: Keuzemenu gebruiker 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.

<sup>3</sup> 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>.

<sup>4</sup> Rijksoverheid, Data protection impact assessment Intune, 30 juni 2020, URL: <https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-intune>.

## 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."*<sup>5</sup>

Het gaat om een gegevensstroom die in de browser of in het apparaat van de gebruiker (desktop, laptop en/of smartphone) wordt aangemaakt. Deze telemetriegebeurtenissen worden zeer regelmatig gebundeld naar Microsoft verstuurd. Hiermee verzamelt Microsoft op een tweede manier persoonsgegevens over de apparaten en het gebruik van haar diensten. Deze verzameling staat los van de persoonsgegevens die Microsoft als cloudleverancier automatisch al in de logbestanden op haar cloud servers registreert.

Microsoft biedt drie mogelijkheden om telemetrieniveau in te stellen:

1. Vereist (Required)
2. Optioneel (Optional)
3. Geen van beide (Neither)<sup>6</sup>

Zelfs op het minimumniveau 'Neither' verzamelt Microsoft nog steeds telemetriegegevens. Microsoft noemt deze 'Vereiste servicegegevens voor Office'.<sup>7</sup> Deze gegevensstroom bevat informatie over het gebruik van 'verbonden ervaringen' 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 adviseert 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.<sup>8</sup>

<sup>5</sup> Microsoft, Verplichte diagnostische gegevens voor Office, 11 mei 2023, URL: <https://learn.microsoft.com/nl-nl/deployoffice/privacy/required-diagnostic-data>.

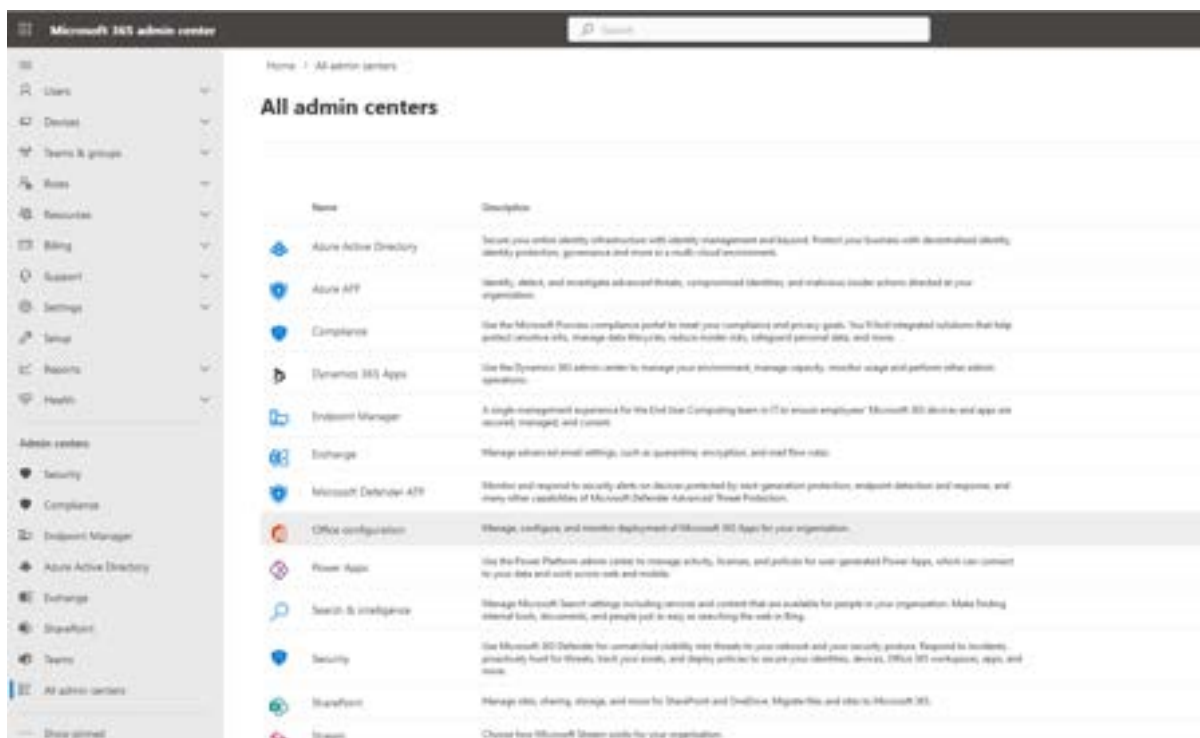
<sup>6</sup> Microsoft, 28 maart 2023, Diagnostische gegevens die van Microsoft 365-apps voor ondernemingen naar Microsoft worden verzonden, URL: <https://learn.microsoft.com/nl-nl/deployoffice/privacy/overview-privacy-controls#diagnostic-data-sent-from-microsoft-365-apps-for-enterprise-to-microsoft>.

<sup>7</sup> Microsoft, Vereiste servicegegevens voor Office, 4 april 2023, URL: <https://learn.microsoft.com/nl-nl/deployoffice/privacy/required-service-data>

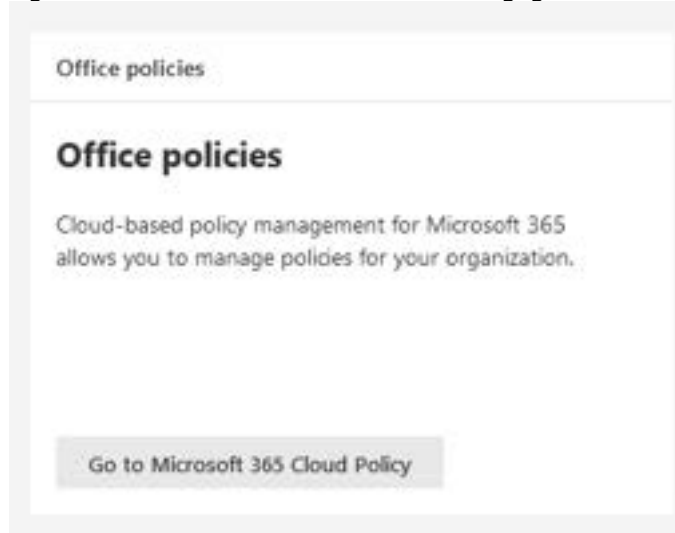
<sup>8</sup> Microsoft, Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise, 27 maart 2023, URL: <https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls>.

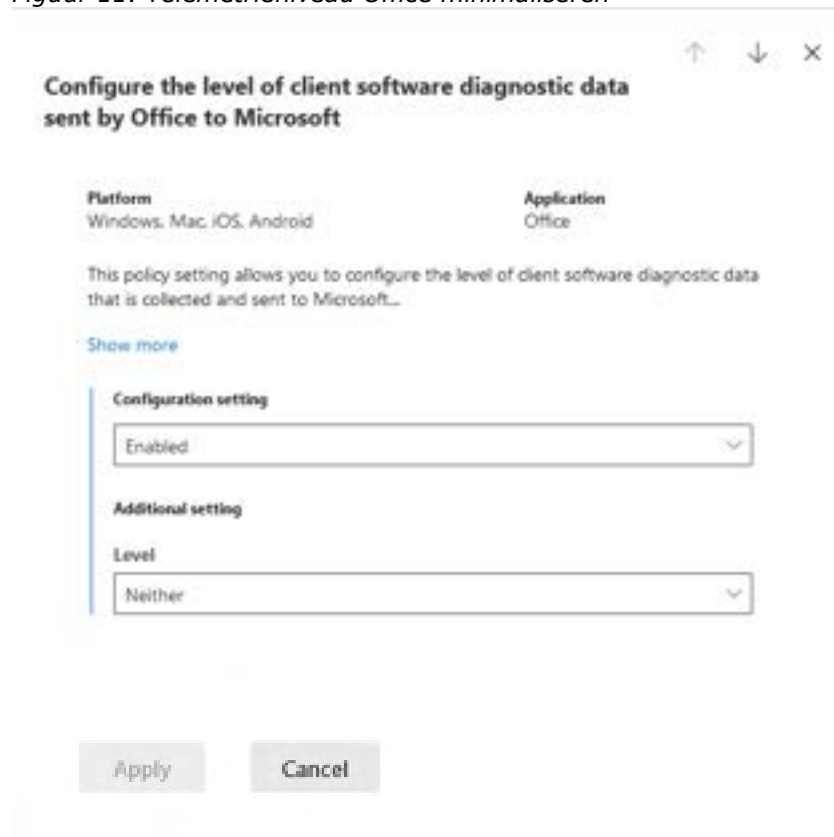
- Ga naar <https://config.office.com>, Kies 'Office policies' -> Ga naar Microsoft 365 Cloud Policy -> Zoek naar de policy *Configure the level of client software diagnostic data sent by Office to Microsoft* -> Enabled.

Figuur 9: Verzamelen Office telemetrie gegevens uitzetten (1)



Figuur 10: Verzamelen Office telemetrie gegevens uitzetten (2)



*Figuur 11: Telemetrieniveau Office minimaliseren*

- Controleer af en toe zelf de informatie die Microsoft geeft over de telemetrie in de Diagnostic Data Viewer op een Windowsapparaat.<sup>9</sup>

<sup>9</sup> 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>

## 7. Microsoft verwerker voor de telemetrie uit Windows 10

Vanaf Windows 10 Enterprise versie 1809 met (tenminste) de update van juli 2021 is het mogelijk voor Enterprise klanten om Microsoft als verwerker te laten optreden voor de gegevensverwerking van de Windows telemetriegegevens in plaats van als zelfstandige verantwoordelijke.<sup>10</sup>

Dat kan door de Windows 10 apparaten toe te voegen aan de Azure AD-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.<sup>11</sup>

Let op: als een organisatie het apparaat niet aanmeldt in de Azure AD, verwerkt Microsoft de telemetriegegevens uit Windows als zelfstandige verantwoordelijke.

Opmerking: Vanaf Windows 11 Enterprise treedt Microsoft automatisch op als verwerker.

---

<sup>10</sup> 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/>.

<sup>11</sup> Microsoft, Diagnostische Windows-gegevens in uw organisatie configureren, 18 maart 2023, URL: <https://learn.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization>

## 8. Telemetrieniveau Windows

De standaardinstelling voor telemetrie in 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:

1. Uit
2. Vereist
3. Optioneel

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

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 een group policy in te stellen

- Ga vanuit de Group Policy Management Console, naar Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds.
- Dubbelklik op Allow Telemetry (of Allow diagnostic data on Windows 11 and Windows Server 2022) en kies 'uit'.<sup>12</sup>

---

<sup>12</sup> Microsoft, Groepsbeleid gebruiken om het verzamelen van diagnostische gegevens te beheren, 18 maart 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 12: Opties telemetrie Windows 10 en Windows 11 (Hernoemd beleid)<sup>13</sup>*

| Beleidstype  | Huidige beleid                                                                                                                                                                                                                                                | Hernoemd beleid                                                                                                                                                                                                                                                                                                                              |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Groepsbeleid | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > Telemetrie toestaan <ul style="list-style-type: none"> <li>0 - Beveiliging</li> <li>1 - Basis</li> <li>2 - Uitgebreid</li> <li>3 - Volledig</li> </ul> | Computerconfiguratie > Beheersjablonen > Windows-onderdelen > Gegevensverzameling en preview-versies > Diagnostische gegevens toestaan <ul style="list-style-type: none"> <li>Diagnostische gegevens uit (niet aanbevolen)</li> <li>Vereiste diagnostische gegevens verzenden</li> <li>Optionele diagnostische gegevens verzenden</li> </ul> |
| 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                                                                                                                                                                    |

<sup>13</sup> Microsoft, Wijzigingen in het verzamelen van diagnostische Windows-gegevens, 18 maart 2023, URL: <https://docs.microsoft.com/nl-nl/windows/privacy/changes-to-windows-diagnostic-data-collection#gedragswijzigingen>

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

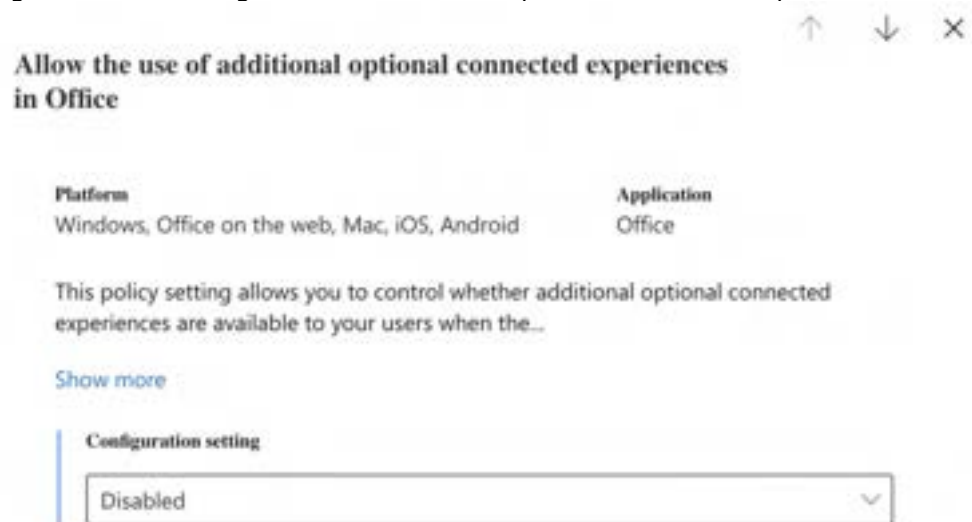
De Verbonden Ervaringen (Connected Experiences) zijn mini clouddiensten waarmee Microsoft gegevens levert in Office zoals een spelling- en grammaticacontrole of ontwerpen voor PowerPoint-slides.

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 adviseert de toegang tot deze *Additional Optional Connected Experiences* centraal uit te schakelen op alle platforms. Dat kan met een Group Policy of via de Registry, voor alle Office 365-services. Voor de 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.

Figuur 13: Afbeelding uitzetten Additional Optional Connected Experiences



*Figuur 14: Uitleg Microsoft over instellingen in de Registry<sup>14</sup>*

| 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                 |

<sup>14</sup> 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>.

## 10. Windows 10 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).<sup>15</sup>

Microsoft legt uit dat ze de activiteitengeschiedenis gebruikt *om Microsoftproducten 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.*<sup>16</sup>

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

Dat kan via het menu bij centraal uitgerold images of via de Registry. Zie [Figuur 15](#) hieronder

- Ga naar 'Instellingen', Privacy en beveiliging > Activiteitengeschiedenis -> Mijn activiteitengeschiedenis verzenden naar Microsoft -> Uit.

*Figuur 15: Uitzetten verzending activiteitengeschiedenis naar Microsoft (Windows 11)*



<sup>15</sup> 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> .

<sup>16</sup> Idem.

- Ga naar Registry Path `Software\Policies\Microsoft\Windows\System`
- Value Name `EnableActivityFeed`
- Value Type `REG_DWORD`
- Disabled Value `0`

## 11. LinkedIn-integratie voor Microsoftaccounts

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

Als medewerkers toestemming geven om hun LinkedIn-account te koppelen aan hun Microsoft365-account, kunnen zij LinkedIn-gegevens en -middelen toepassen op verschillende locaties binnen de Officetoepassingen.

SLM adviseert de LinkedIn-integratie centraal uit te schakelen.

- Ga naar <https://portal.azure.com/#home> -> typ in de zoekbalk "users" of "gebruikers" -> user settings / gebruikersinstellingen -> LinkedIn-integratie uitzetten

*Figuur 16: Schermafbeelding: LinkedIn-integratie uit*



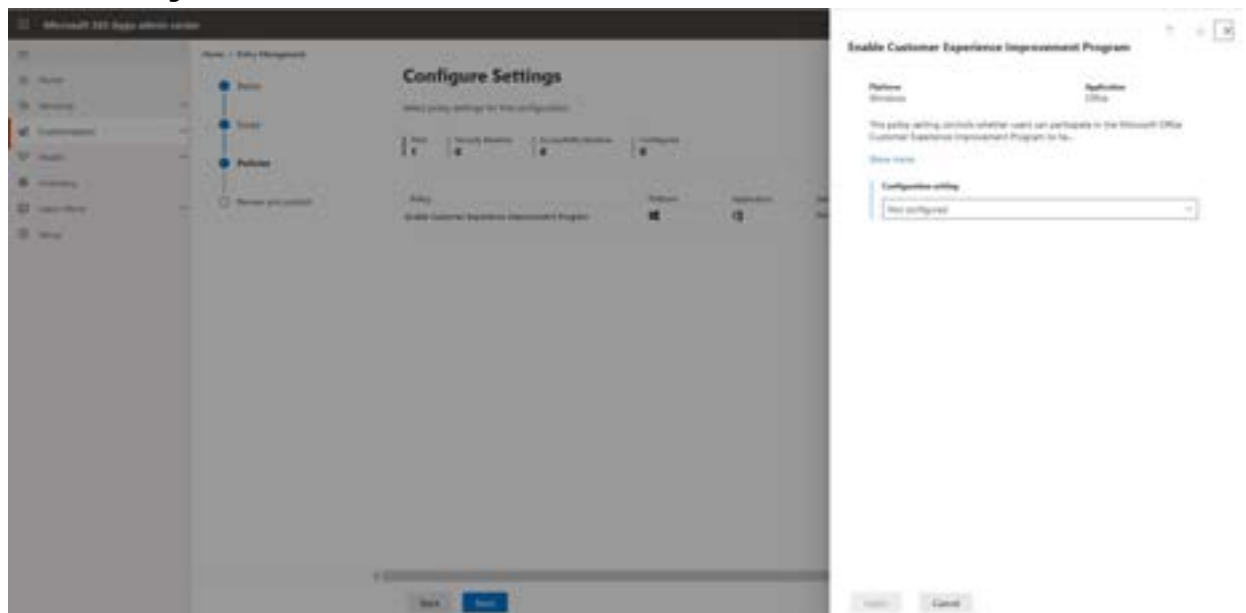
## 12. Customer Experience Improvement Program (CEIP)

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 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.

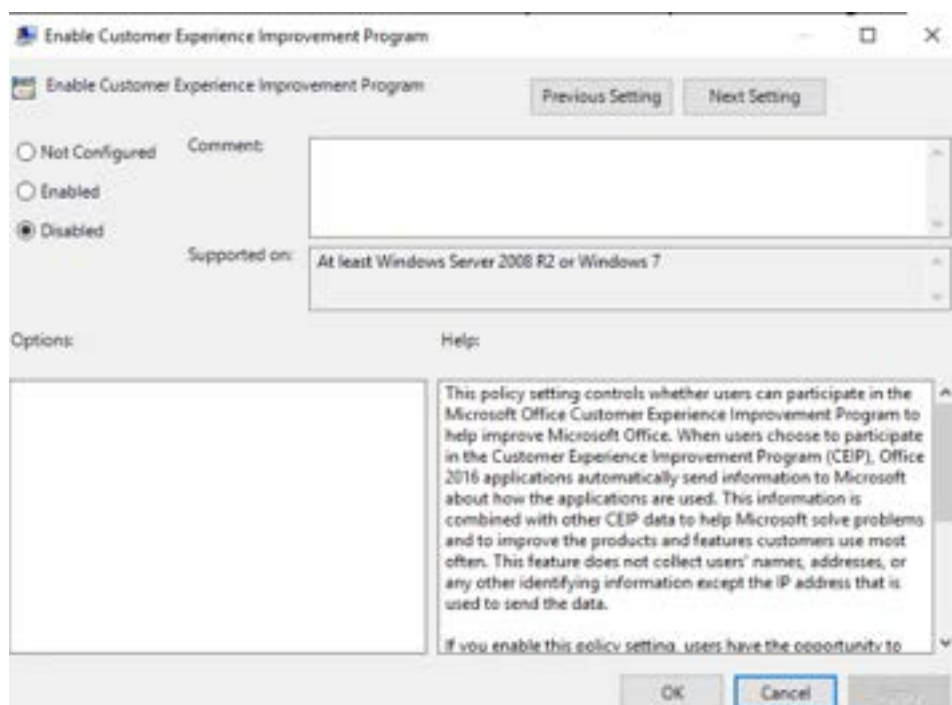
Vanwege het gebrek aan transparantie adviseert SLM deze verwerking uit te zetten.

- Schakel CEIP centraal uit via de Group Policy Editor in Office en Windows: zie Figuur 17,
- 
- 
- *Figuur 18*, en
- *Figuur 19* hieronder.
- Ga naar <https://config.office.com/> -> Microsoft 365 Cloud Policy -> Kies een policy onder "name" -> Policies -> Zoek op "Enable Customer Experience Improvement Program" -> Disabled
-

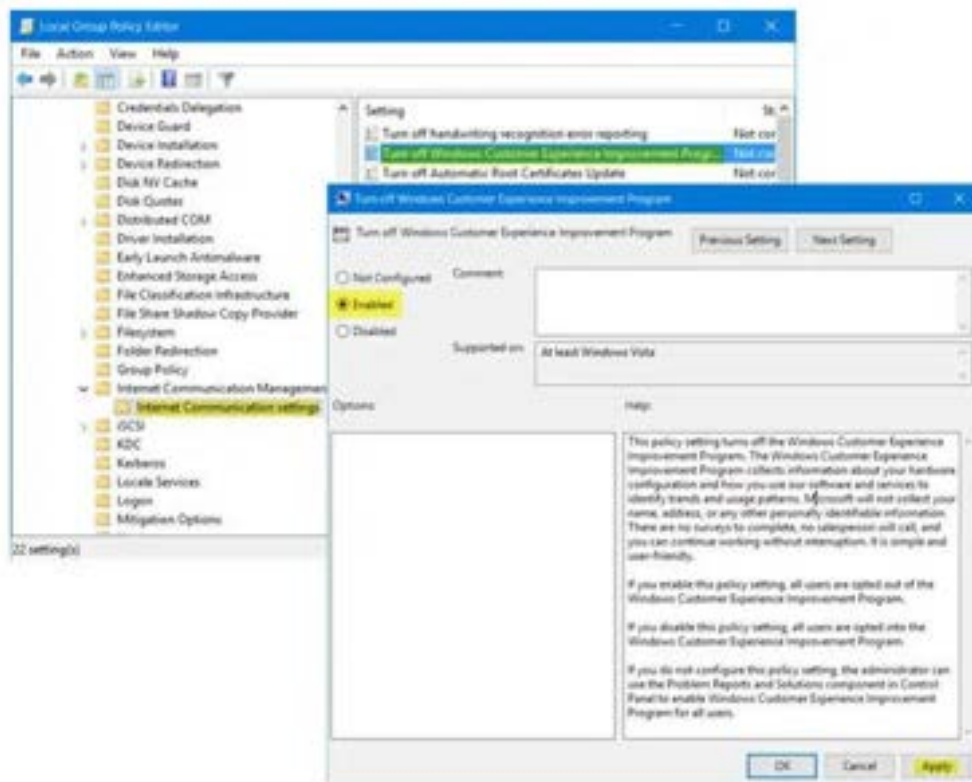
*Figuur 17: Centraal uitschakelen CEIP in Office*



*Figuur 18: Centraal uitzetten CEIP in Office ProPlus*



Figuur 19: Centraal uitzetten CEIP in Windows<sup>17</sup>



<sup>17</sup> Schermafbeeldingen van The Windows Club, URL:

<https://www.thewindowsclub.com/disable-windows-customer-experience-improvement-program>.

## 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 zelfstandig verantwoordelijk voor Bing en mag de gegevens die ze via Bing verkrijgt voor haar eigen commerciële doelen gebruiken.

SLM adviseert deze gegevensstroom te blokkeren met een group policy via Powershell.

- `Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -PlacesEnabled $true`<sup>18</sup>

---

<sup>18</sup> Microsoft specifiek Powershell commando 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. Zij 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.

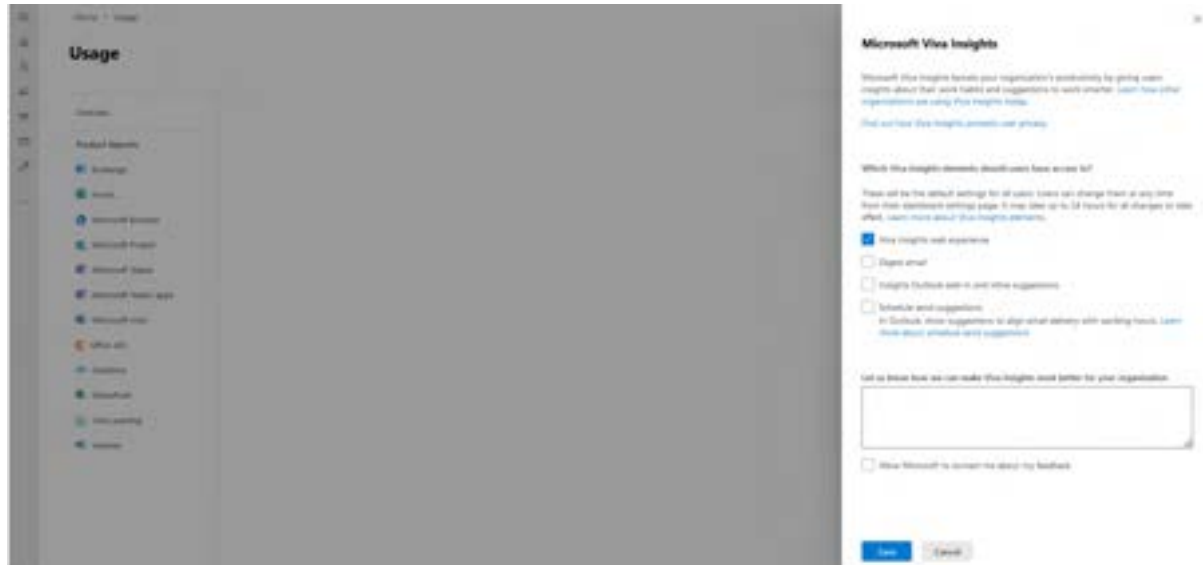
Er zijn wel privacyrisico's verbonden aan het gebruik van de diensten, als de informatie ingezet wordt bij beoordelingen of als onderdeel van een personeelsvolgsysteem.

De standaardinstelling voor de analytische diensten Delve en Teams Analytics & reports is dat ze aan staan. Viva Insights staat standaard uit. Als een beheerder Viva Insights aanzet, kan een gebruiker de dienst nog steeds individueel uitzetten.

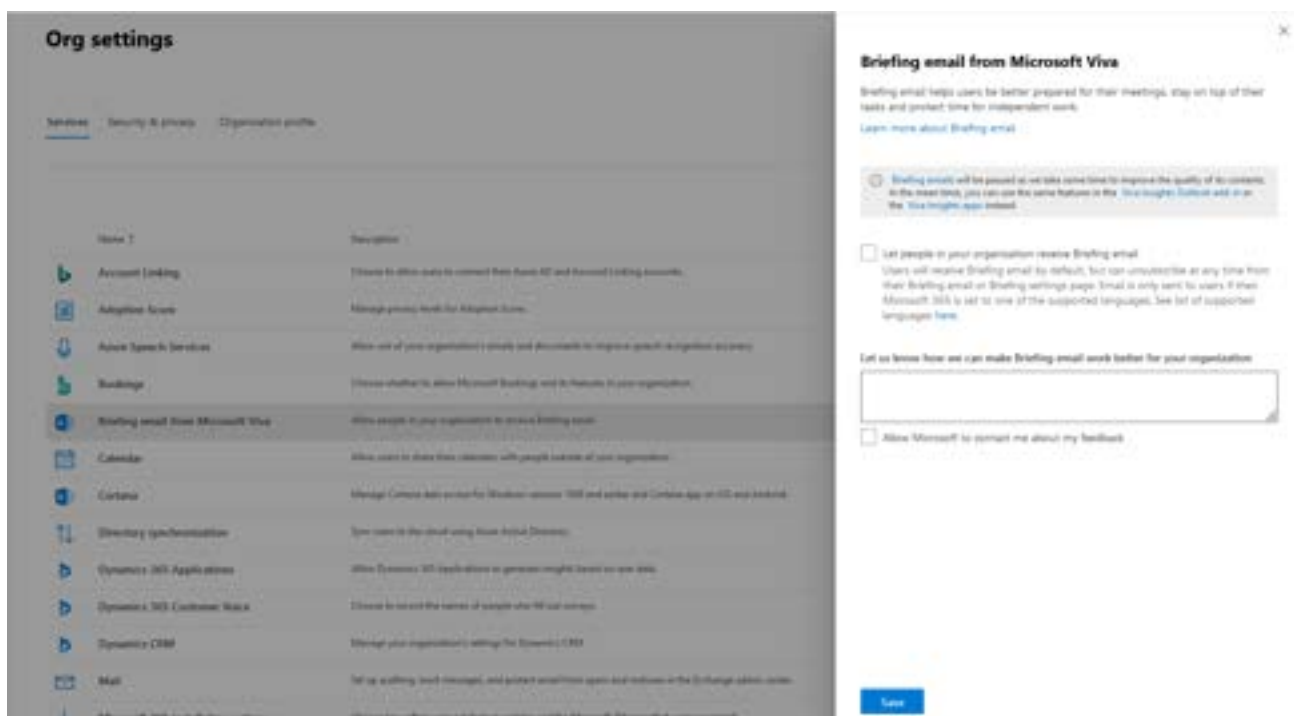
Systeembeheerders kunnen Delve uitschakelen. Voor Teams Analytics & reports bestaat er geen uitschakelmogelijkheid, alleen een pseudonimiseringsoptie voor de beheerder. Het is niet aannemelijk dat pseudonieme weergave in gebruiksrapporten invloed heeft op de ruwe data in de onderliggende cloudlogs bij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

- Controleer dat Viva Insights mail briefings uitstaan: Home -> Setup -> Microsoft Viva -> Viva Insights -> Manage settings
- Controleer ook dat Viva Insights uitstaan in Outlook
- 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.
- Schakel Delve uit: Ga naar <https://admin.microsoft.com/sharepoint?page=sharing&modern=true> -> Settings -> Classic settings page (onderaan de pagina) -> Disable Delve

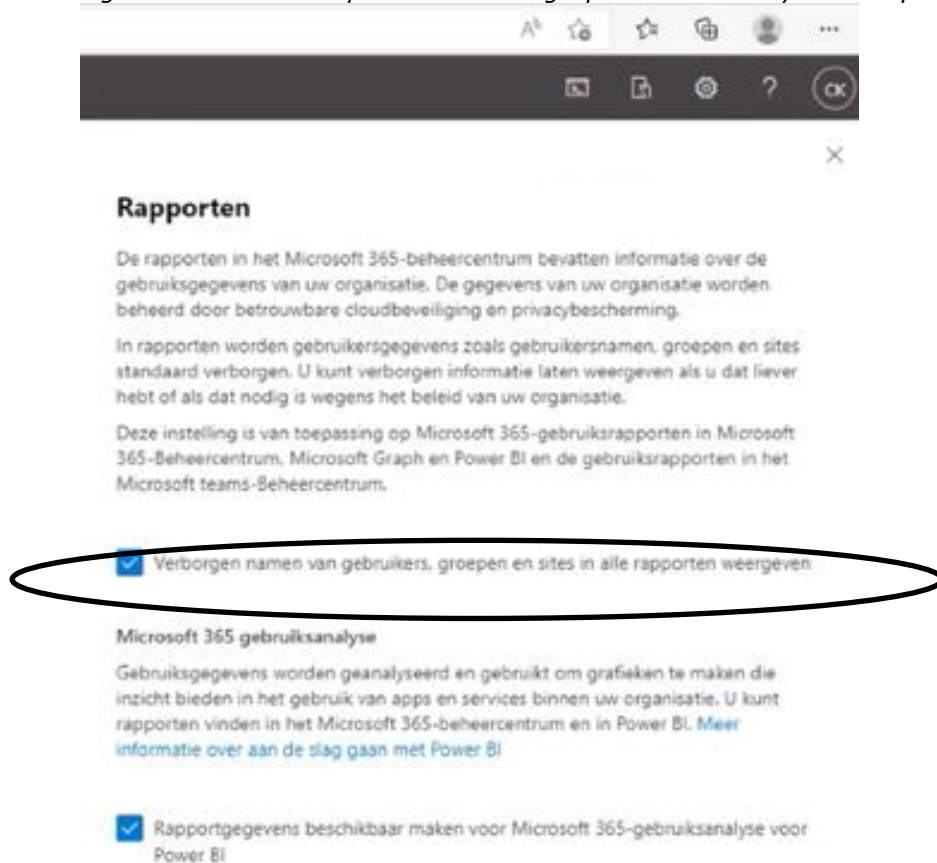
Figuur 20: Standaardinstellingen Viva Insights



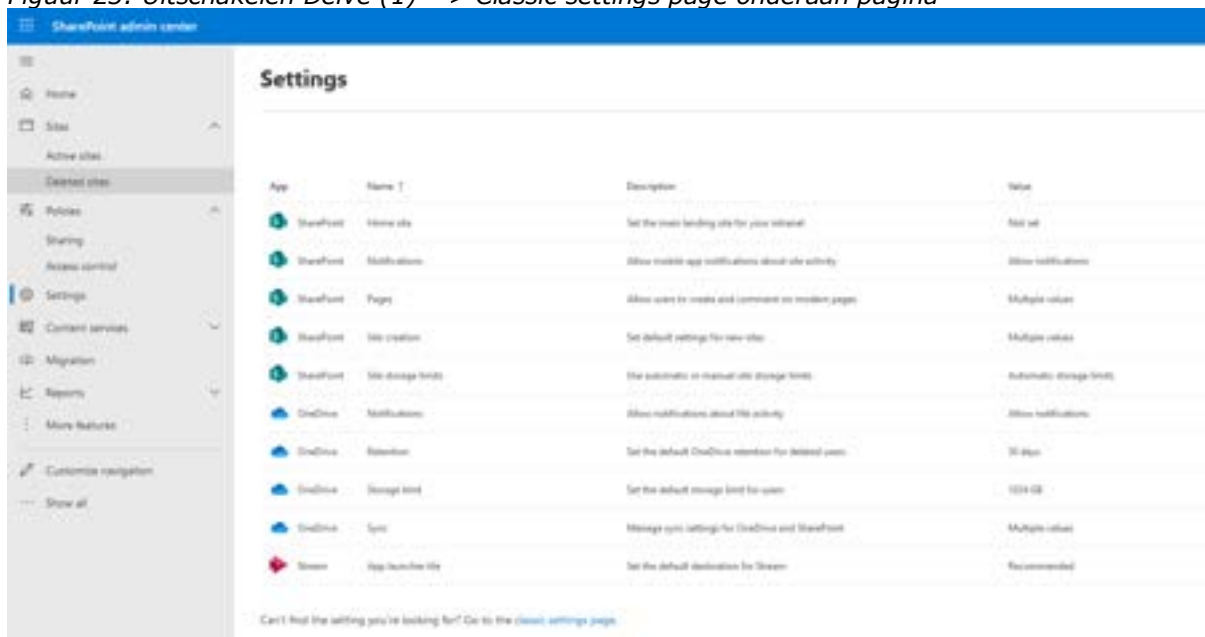
Figuur 21: Instellingen Viva Insights: mail briefings uit



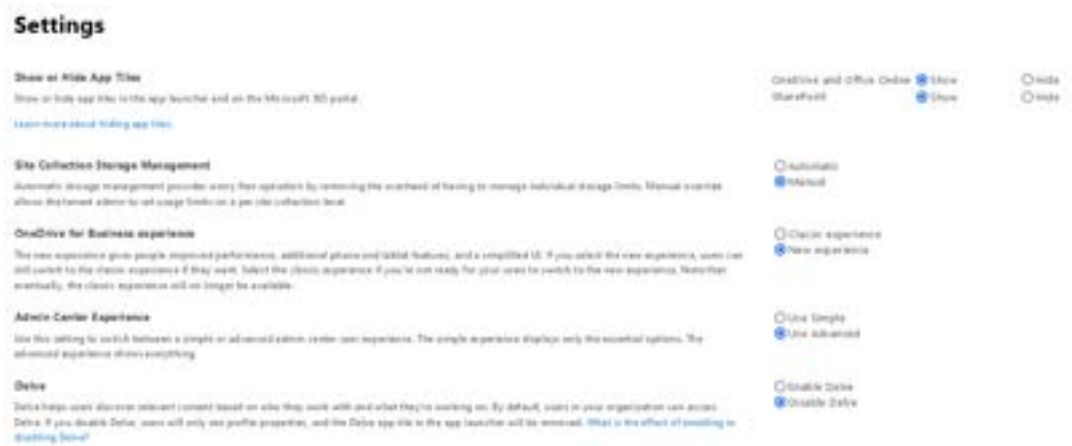
Figuur 22: Standaard pseudonimiseringsoptie Teams Analytics &amp; Reports



Figuur 23: Uitschakelen Delve (1) --&gt; Classic settings page onderaan pagina



Figuur 24: Uitschakelen Delve (2)



## 15. Omgang met spam in Defender

Microsoft kan in Defender mail classificeren als spam en automatisch weggooien. Dat kan leiden tot een dataproctierisico, 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.

- Een afweging kan zijn om een third party e-mail threat protection-product te gebruiken waarbij de gebruiker zelf toegang heeft tot de onderschepte spamberichten.

## 16. Pseudonimiseren gebruikersnamen in Defender voor Cloud Apps

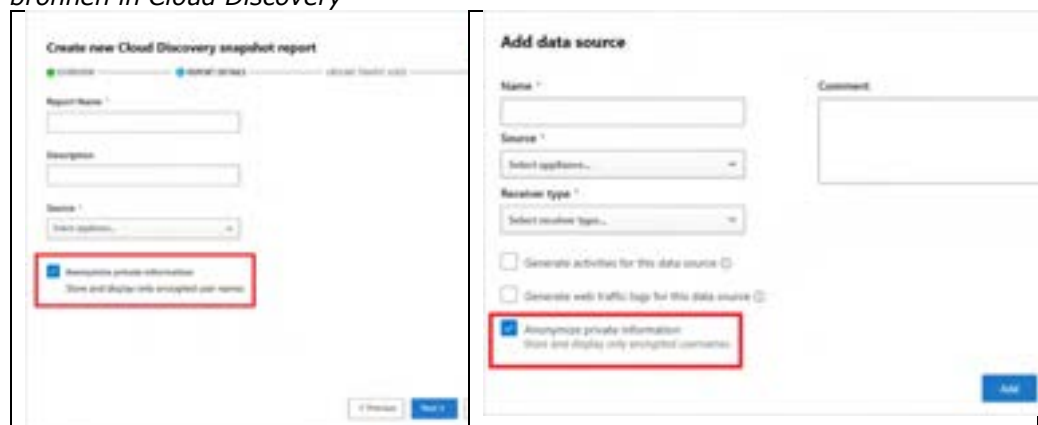
Microsoft biedt een pseudonimiseringsoptie in de dashboards van Defender voor Cloud Apps voor de gebruikersnamen. In de dashboards wordt de gebruikersnaam dan vervangen door een versleutelde gebruikersnaam. Microsoft noemt dit 'anonymisering', maar wijst er ook op dat de beheerders de echte gebruikersnaam 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 deze log kunnen organisaties controleren of beheerders de gebruiker terecht hebben geheridentificeerd, in overeenstemming met het interne privacybeleid.

Microsoft beschrijft drie manieren voor pseudonimisering in de dashboards van Defender voor Cloud Apps voor gebruikersnamen, voor nieuwe snapshotrapporten of rapporten van nieuwe gegevensbronnen.

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

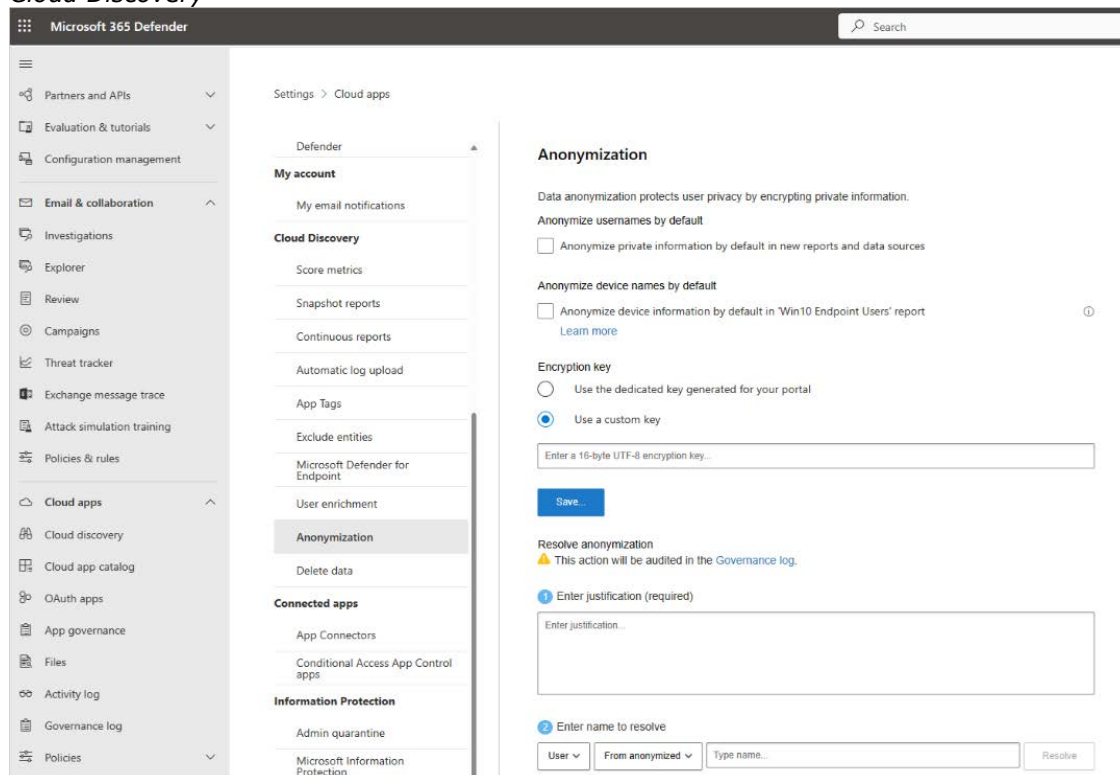
Figuur 25: Schermafbbeeldingen "anonimiseren" in nieuwe rapporten en nieuwe bronnen in Cloud Discovery<sup>19</sup>



3. 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)

<sup>19</sup> Microsoft, Cloud Discovery-gegevens anoniem maken, 24 april 2023, URL: <https://learn.microsoft.com/nl-nl/defender-cloud-apps/cloud-discovery-anonymizer>

**Figuur 26: Schermafbeelding Microsoft "anonimisering" standaard aanzetten in Cloud Discovery<sup>20</sup>**



**Let op:** Microsoft biedt ook een omgekeerde mogelijkheid tot het automatisch verwijderen 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."*<sup>21</sup>

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

<sup>20</sup> Idem.

<sup>21</sup> 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>.

staat op de aanbeveling om de accountnamen juist gepseudonimiseerd te tonen aan de beheerders.

## 17. Toegang tot Feedback en Twitter in Defender portal

Als een beheerder inlogt op het hoofdportaal van Defender, stuurt Microsoft gegevens naar zichzelf als verantwoordelijke en naar Twitter. Dat komt doordat er een Twitterintegratie is en een mogelijkheid voor beheerders om feedback te geven aan Microsoft. Omdat zowel Microsoft als Twitter optreden als zelfstandige verantwoordelijken, is er sprake van derdenverstrekking.

Microsoft heeft SLM toegezegd op korte termijn instellingen te ontwikkelen voor beheerders om de integratie van Twitter met het Defender-portal uit te zetten en om centraal te voorkomen dat medewerkers persoonsgegevens delen met Microsoft via Feedback.

- Schakel Twitter en Feedback uit in Defender zodra Microsoft dat mogelijk maakt.

## 18. Het gebruik van Giphy in Teams en Outlook

Zelfs als een organisatie alle *Additional Optional Connected Experiences* centraal heeft uitgezet, kunnen er via Teams en Outlook (onbedoeld) nog persoonsgegevens worden doorgegeven aan het Amerikaanse bedrijf Giphy. Giphy biedt een grote verzameling afbeeldingen aan, GIF's en geanimeerde GIF's, die gebruikers kunnen invoegen in allerlei chatprogramma's en sociale media.

Giphy is gevestigd in New York met een vertegenwoordiger in Hamburg. Op het gebruik van de dienst zijn de voorwaarden en het privacybeleid van Giphy van toepassing.

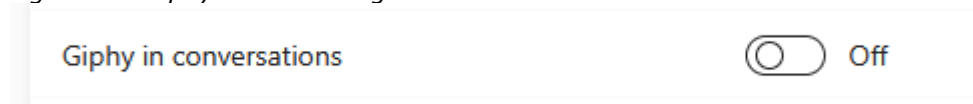
Giphy legt in zijn privacyverklaring uit dat het van elke gebruiker van zijn diensten automatisch het IP-adres, de unieke apparaatidentificatie, cookie-informatie en de specifieke advertentie-identificatienummers uit Android en iOS verzamelt. Giphy behoudt zich het recht voor om het IP-adres te gebruiken 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.

Om toegang tot Giphy te blokkeren kunnen beheerders een apart groepsbeleid toepassen in Teams en een PowerShell commando toepassen op Outlook. Dit beleid voorkomt overigens niet dat gastgebruikers Giphy-plaatjes opnemen in hun gesprekken op Teams en mailtjes naar medewerkers van de overheidsorganisatie. Hierdoor kunnen alsnog persoonsgegevens van medewerkers naar Giphy worden gestuurd, op het moment dat zij de getoonde plaatjes aanklikken.

SLM adviseert Giphy uit te schakelen in Teams.

- Ga naar <https://admin.teams.microsoft.com>
- Kies Messaging Policies > Global
- Schakel Gebruik Giphys in gesprekken uit.

*Figuur 27: Giphy in Teams uitgeschakeld*



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

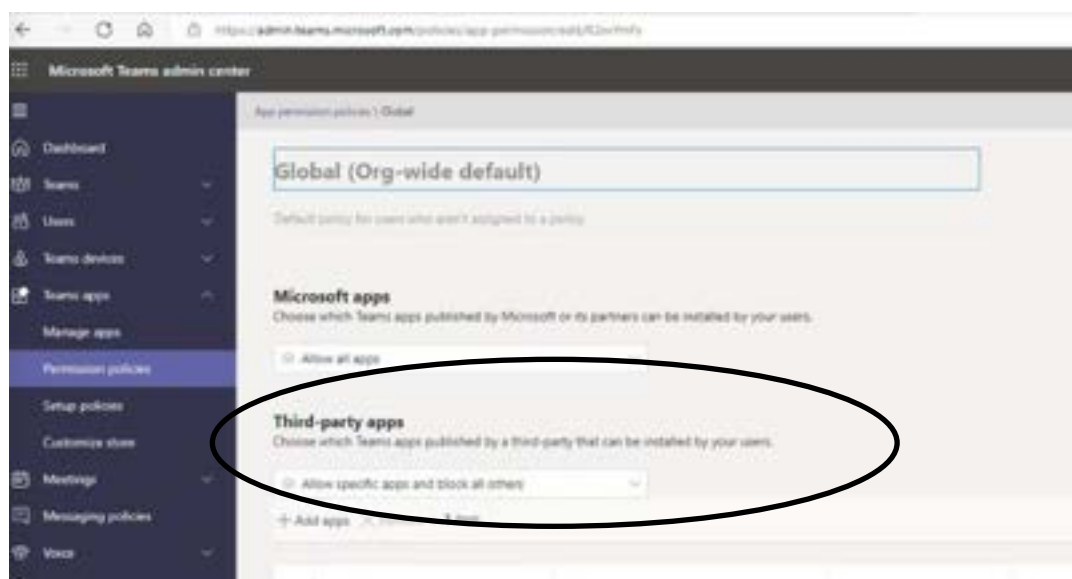
Teams heeft een ingebouwde appstore met apps van Microsoft en apps van derde partijen.

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 adviseert 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.

- Ga naar [https://admin.teams.microsoft.com](https://admin.teams.microsoft.com/policies/app-permissions/global/default) -> Team apps -> Permission policies -> Global -> Disable third-party apps

*Figuur 28: Instellingen apps derde partijen UIT (eventueel specifieke apps goedkeuren)*



## 20. E2EE in Teams

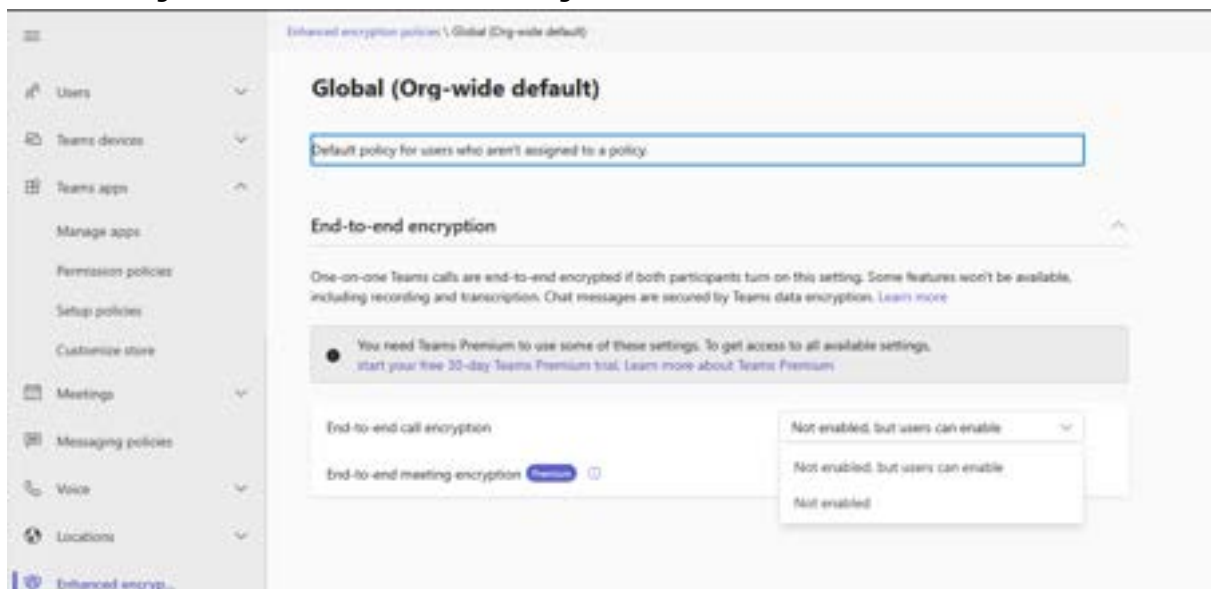
Teams-gegevens worden onderweg (in transit) en als ze opgeslagen zijn (at rest) versleuteld in de datacentra van Microsoft met behulp van standaardtechnologieën, zoals TLS en SRTP. Dit omvat oproepen, berichten, bestanden, vergaderingen en andere inhoud. Beheerders kunnen voor extra versleuteling kiezen 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 adviseert E2EE standaard in te schakelen voor 1-op-1 gesprekken in Teams.

- Ga naar <https://admin.teams.microsoft.com> -> Enhanced encryption -> Global -> Not enabled, but users can enable
- Instrueer eindgebruikers om E2EE ook in te schakelen

*Figuur 29: E2EE toelaten voor eindgebruikers*



## 21. 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. Microsoft365 gebruikt deze sleutels vervolgens om de opgeslagen gegevens in OneDrive, SharePoint en Exchange Online te versleutelen. Microsoft heeft 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

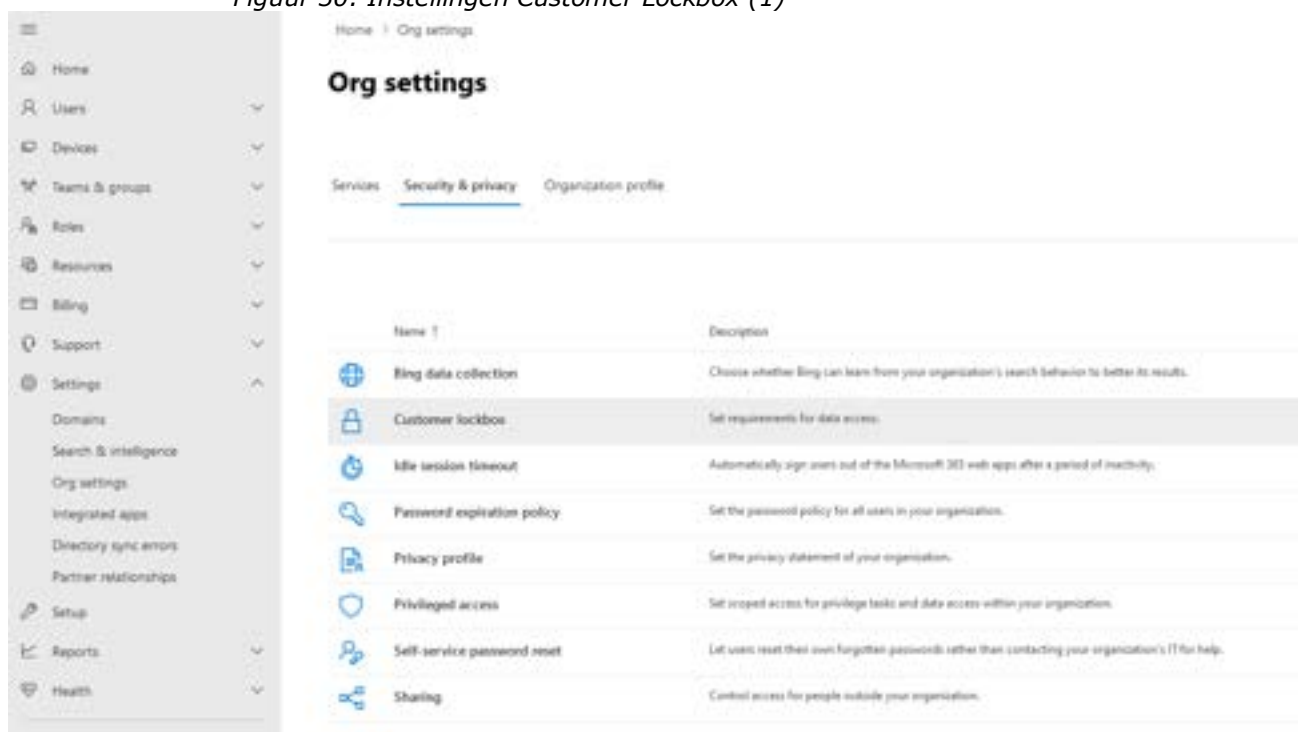
De dienst *Customer Lockbox* stelt beheerders in staat om een extra niveau van versleuteling in te schakelen voor gegevens die zijn opgeslagen in Exchange Online (inclusief Teamgegevens), SharePoint en OneDrive. Hierdoor kunnen de Microsoftengineers en supportmedewerkers niet meer bij de inhoud van bestanden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

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

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

- Ga naar <https://admin.microsoft.com/Adminportal/Home>
- Kies Settings > Org Settings > Security & Privacy
- Selecteer Customer Lockbox in de linker 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 30: Instellingen Customer Lockbox (1)



Figuur 31: Instellingen Customer Lockbox (2)



## 22. 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**

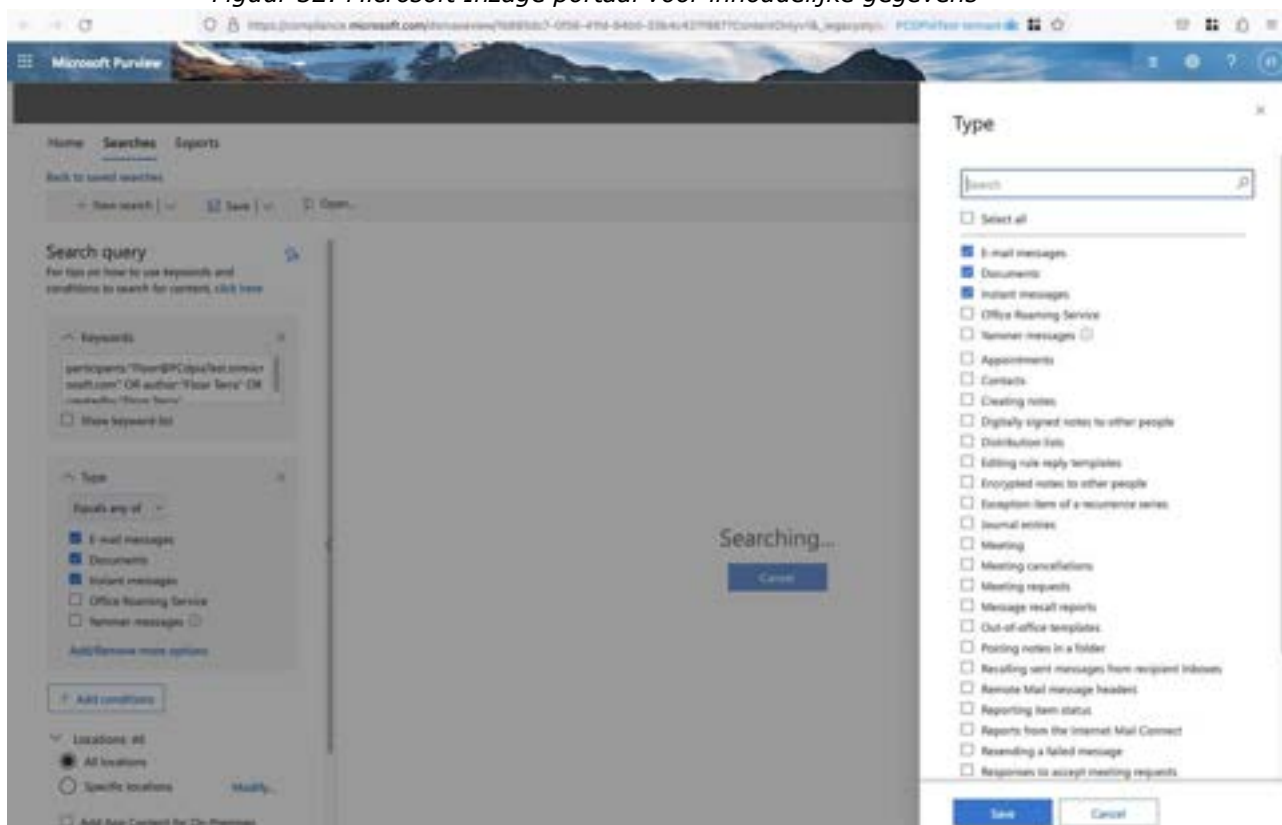
Beheerders kunnen via het complianceportal van Microsoft een inzageverzoek indienen voor de inhoudelijke gegevens.<sup>22</sup>

- Zorg dat de systeembeheerder geautoriseerd is voor contentexport door hem lid te maken van de eDiscovery Managerrolgroep.
- Log in op <https://compliance.microsoft.com/>
- Kies Ediscovery > User data search > Create a Case (een UDS case)
- Voer als zoekterm de accountnaam 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.

---

<sup>22</sup> 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>  
Pagina 48 van 50

Figuur 32: Microsoft Inzage portaal voor inhoudelijke gegevens



### Inzage in diagnostische gegevens

De topbeheerder (tenant admin) kan ook inzage vragen voor een medewerker in de diagnostische gegevens.<sup>23</sup>

Via het Azure-portaal geeft Microsoft inzage in de product- en dienstgebruiksgegevens zoals user-activitylogs, 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.

<sup>23</sup> 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>

Figuur 33: Inzageverzoek diagnostische gegevens

**Microsoft Azure** Search resources, services, and do

[All services](#) > [User privacy](#) | [Manage User Requests](#) >

## New export data request ...

Export log data associated with a particular user's use of Microsoft services and applications. Most requests will be completed in 1 to 2 days, but can take up to 30 days to complete. Exported data will be saved to your organization's Azure Blob Storage and output in a common machine-readable file formats such as JSON or XML. [Learn more](#)

User Type \*

☒ Directory members or B2B collaboration users ☐ B2B direct connect users

User \*

Export destination

Select the Azure subscription and storage account to export the data to. If you do not have an Azure subscription you can create a new Azure subscription. [Create subscription](#)

Azure Subscription \*

Storage account \*

By clicking Create, you understand that Microsoft will have read and write permissions to this storage account for fulfilling this request and agree to the terms and conditions. [Terms and Agreements](#)

**Create** Cancel