HANDLEIDING: MICROSOFT 365 EN DE AVG

Richt Microsoft 365 zo veilig mogelijk in

Datum	20 april 2022
Versie	2
Aantal pagina's inclusief voorblad	33

Handleiding: Microsoft 365 en de AVG

Waarom deze handleiding?

Privacy is een gezamenlijke verantwoordelijkheid van de leverancier én de school. Dit document biedt scholen ondersteuning om Microsoft 365 zo veilig mogelijk in te richten. Het is bedoeld voor FG-ers, tenantbeheerders, bovenschoolse ICT-coördinatoren (BIC-ers) en netwerkbeheerders.
We beschrijven een aantal stappen die je kunt nemen voor het beveiligen en beschermen van de privacy bij het gebruik van Microsoft producten en diensten in je onderwijsorganisatie. Ook bespreken we verschillende instellingen binnen de tenant. Daarnaast gaan we in op de achtergrond en vertellen we wat de eventuele gevolgen zijn bij het uitschakelen van bepaalde functionaliteiten.

Tot slot bespreken we een aantal specifieke afwegingen die je als onderwijsorganisatie moet maken tussen privacy, beveiliging en gebruiksgemak. Zo proberen we je te helpen bij het maken van weloverwogen keuzes en het inrichten van je omgeving naar de wensen van je onderwijsorganisatie.
Dit document is voor het eerst opgesteld in juni 2020 naar aanleiding van de toen sterk verbeterde privacyvoorwaarden van Microsoft. In april 2022 hebben we de handleiding bijgewerkt naar aanleiding van de DPIA op Teams, SharePoint en OneDrive (gepubliceerd in februari 2022). Dit document geeft de stand van zaken, zowel juridisch als technisch, van het moment dat hij voor het laatst is bijgewerkt weer. Ga naar de website van APS IT-diensten voor de laatste ontwikkelingen of lees meer informatie over de veiligheid van de Microsoft licenties via APS IT-diensten.

Disclaimer

Dit document is met grote zorgvuldigheid samengesteld. APS IT-diensten B.V. is echter niet aansprakelijk voor enige directe of indirecte schade die zou kunnen ontstaan door het gebruik van de hierin aangeboden informatie. Aan de inhoud van dit document kunnen op geen enkele wijze rechten worden ontleend of aanspraken worden gemaakt.

Dit document geeft de scholen inzicht in een aantal mogelijkheden die Microsoft in haar omgeving biedt voor beveiliging en de bescherming van de privacy en adviseert de scholen in hoofdlijnen hoe zij die producten en diensten in kunnen richten om zo goed mogelijk te voldoen aan wet- en regelgeving.

Inhoudsopgave: Microsoft 365 en de AVG

Microsoft en de AVG

Inleiding

Vanaf 2018 heeft de Nederlandse overheid in samenwerking met SURF, APS IT-diensten en SLBdiensten een aantal Data Privacy Impact Analyses (of DPIA's) laten uitvoeren op Office 365, Office Pro Plus (Microsoft 365 Apps for Enterprise), Office Online, Office mobile apps, Intune, Windows 10 en meest recentelijk de DPIA op Teams, OneDrive en SharePoint. Naar aanleiding van deze DPIA's heeft Microsoft technische en juridische verbeteringen doorgevoerd in haar producten en voorwaarden. Deze verbeterde voorwaarden en functionaliteiten zijn vanaf januari 2020 ook van toepassing verklaard op de Microsoft 365 diensten die worden afgenomen via de contracten die SURF, APS IT-diensten en SLBdiensten voor het Nederlandse onderwijs met Microsoft hebben gesloten.

Wij hebben deze voorwaarden bestudeerd en vergeleken met de voorwaarden die het onderwijs door middel van de model verwerkersovereenkomst uit het Privacyconvenant Onderwijs stelt aan leveranciers. De analyse hiervan staat op onze website.

Vanuit AVG-perspectief zien wij geen bezwaren om te werken met de diensten Microsoft 365 en/of Azure wanneer je die via ons afneemt.

Onze adviezen in het kort

- Sluit je Microsoft overeenkomst via APS IT-diensten, SLBdiensten of SURF;
- Gebruik de laatste versies van de software;
- Zorg in de basis voor een veilige inrichting;
- Minimaliseer het versturen van diagnostische gegevens in Windows 11;
    - Telemetrie (Telemetric), stel deze in op het niveau **Beveiliging**
    - Timeline sync, zet deze **Uit (Alleen van toepassing op Windows 10)**
- Minimaliseer het versturen van diagnostische gegevens in Microsoft 365 Apps for Enterprise (Office 365 ProPlus);
    - Beperk diagnostische gegevens Office, zet de functionaliteit op **Geen van beiden (Neither)**
    - Optionele verbonden ervaringen (Optional connected experiences), zet enkel de **optionele verbonden ervaringen uit**, waar Microsoft de verwerkingsverantwoordelijke is
- Zet End to End Encryption aan in Microsoft Teams;
- Blokkeer het gebruik van 3th party apps in Microsoft Teams;
- Zet Giphy uit in Microsoft Teams;
- Zet Microsoft Viva Insights uit;
- Maak een disclaimer die gastgebruikers eerst moeten accepteren voordat ze kunnen samenwerken.

Deze adviezen werken we in dit document verder uit.

Microsoft overeenkomst via APS IT-diensten

Goed om te weten: ons Microsoft contract biedt scholen extra veiligheid.

In de basis heeft Microsoft duidelijke voorwaarden om privacy te borgen. Daarbovenop zijn er speciale aanvullende afspraken met Microsoft vastgelegd. Wanneer je de Microsoft overeenkomst via een van de Nederlandse onderwijspartners (APS IT-diensten, SLBdiensten of SURF) afneemt, maak je gebruik van dit contract met extra afspraken. De extra voordelen van de Microsoft overeenkomst bovenop de standaardvoorwaarden voor scholen, zijn:

- Microsoft mag geen reclame maken met gegevens van scholen en schoolbesturen.
- Je krijgt mogelijkheden om het delen van diagnostische gegevens met Microsoft te beperken.
- Microsoft beperkt de bewaartermijn voor diagnostische gegevens tot maximaal 18 maanden.
- Jaarlijks zal namens ons onderwijsconsortium in samenwerking met de Rijksoverheid een strenge controle (audit) plaatsvinden waarvan we de bevindingen publiceren op onze website.

Wij zullen dit document en eventuele adviezen verwerken, wanneer na de volgende controle blijkt dat dat nodig is.

Gebruik de laatste versies van de software

In iedere nieuwe versie zitten oplossingen voor mogelijke beveiligingsrisico's. Door altijd gebruik te maken van de nieuwste versie, ben je up-to-date als het gaat om veiligheid. Microsoft 365 Apps for Enterprise zorgt er automatisch voor dat je werkt met de meest recente versie. Als je een Office 2016 of 2019 versie gebruikt, moet je zelf zorgen dat je deze updatet wanneer er nieuwe beveiligingsupdates beschikbaar zijn. Dit staat los van eventuele features.

Wat betreft de AVG policies zijn in juni 2020 ieder geval deze versies van belang:

- Office voor Windows: werk minimaal met versie 1904 van Microsoft 365 apps voor ondernemingen (voorheen Office 365 ProPlus), de click-to-run versie.
- Office voor Mac: werk minimaal met versie 16.28 of hoger van de Office voor Mac toepassingen.
- Windows 10: werk minimaal met versie 1903 en gebruik enkel de Enterprise of Education versie.

Indien je met andere versies werkt, beschik je niet over de functionaliteit om telemetrie en diagnostische gegevens uit te zetten of beperken.

Zorg in de basis voor een veilige inrichting

Met de 'Microsoft 365 A3 voor onderwijsmedewerkers' licentie uit het Microsoft basispakket heb je vele producten binnen handbereik die het mogelijk maken om veilig te werken. Al heb je de duurste kluis in je huis; als je hem open laat staan, helpt hij niet tegen diefstal. Kortom, je Microsoft 365 omgeving moet in de basis goed ingericht worden. Een aantal zaken waar je meteen mee kan beginnen wanneer je met Microsoft 365 werkt, zijn:

- **Azure Active Directory**
  Zorg dat je Azure AD op orde is. Een juiste en up-to-date Active Directory is belangrijk. Deze kun je eventueel syncen vanuit andere systemen. Geef enkel de juiste personen toegang tot de -voor hen- geschikte data. Werk daarbij bijvoorbeeld met (dynamische) groepen zodat je niet alle gebruikers handmatig toegang hoeft te geven, maar enkel iemand in- of uit een bepaalde groep hoeft te halen met de juiste rechten.
- **Rollen en rechten**
  Het is belangrijk dat je nadenkt over rollen en rechten die je je gebruikers geeft. Via rollen kun je specifieke personen meer rechten geven. Weet dat een beheeraccount gewilder is voor

hackers en geef deze niet zomaar aan iedereen uit. Zet hier extra beveiligingen op om misbruik te voorkomen. Neem ook mee dat als je externe partijen beheerrechten geeft, zij ook toegang hebben tot alle data.

- **Self service password reset**
  Laat gebruikers zelf hun wachtwoord resetten. Dit zorgt voor minder werk bij ICT en de medewerker is hierdoor zelf verantwoordelijk voor het onthouden en/of wijzigen van het wachtwoord.
- **Multi Factor Authentication** (MFA, ook wel 2FA of 2-factor authenticatie)
  Naast het inloggen met een wachtwoord is er nog een andere verificatie nodig om in te kunnen loggen. Dit kan bijvoorbeeld via een code die per sms naar de gebruiker wordt gestuurd of via de authenticator app. Er bestaan ook externe tokengenerators.

  Het voordeel is dat de gebruiker maar één wachtwoord hoeft te onthouden en dat er een extra beveiligingslaag is wanneer een wachtwoord is geraden. Je kunt als beheerder instellen dat Microsoft binnen het eigen netwerk niet iedere keer (wanneer een pc in slaapstand gaat) opnieuw vraagt om een extra authenticatie, of dat dit eenmalig wordt gevraagd. Zo wordt het inloggen met MFA tijdens het lesgeven niet als hinderlijk ervaren. Er is dan extra verificatie nodig zodra er een verbinding via een andere locatie wordt gemaakt. Deze extra verificatie op andere locaties kan echter dan wel weer als extra belasting ervaren worden. Je kunt er zelfs voor kiezen om MFA binnen het eigen netwerk helemaal uit te zetten, maar besef dan dat hacken ook gewoon binnen je eigen schoolomgeving kan gebeuren. Het moet uiteindelijk voor iedereen een werkbare situatie zijn, maar deze mag uiteraard niet ten koste van de veiligheid gaan.

  Je hebt als organisatie dus meerdere opties om MFA passend bij het beleid van jullie organisatie in gebruik te nemen. Het advies is om MFA zeker voor beheeraccounts te gebruiken. Wanneer hier ongeautoriseerde personen toegang tot krijgen, kan dit grote gevolgen hebben.

- **Microsoft Defender for Office 365**
  Binnen het Microsoft basispakket heb je de beschikking over Microsoft Defender for Office 365. Wanneer je deze tool op de juiste manier inricht, zullen gebruikers veel minder geconfronteerd worden met mailtjes die leiden naar malware en virussen. Linkjes met malware worden gefilterd en komen niet meer aan. Maar ook zullen zij onveilige bijlagen niet meer kunnen ontvangen of uploaden. Microsoft Defender for Office 365 werkt voor e-mail, maar ook binnen OneDrive, SharePoint en Teams.

Deze functionaliteiten zijn onderdeel van het Microsoft basispakket.

Diagnostische gegevens beperken in Windows 10

Het beheren van diagnostische gegevens is pas mogelijk vanaf Windows 10 versie 1903 en hoger. Zorg er daarom voor dat minimaal deze versie aanwezig is binnen jullie organisatie. Zo kun je het geadviseerde beveiligingsniveau aanzetten.

Goed om te weten!

Microsoft is transparant over wat er naar hen wordt verzonden. Vanaf Windows 10 versie 1803 kun je als gebruiker via de app Viewer voor diagnostische gegevens inzien wat er van jou als gebruiker is verstuurd. Zo kun je een keuze maken om functionaliteiten aan te passen. Ben je klaar met de viewer? Schakel de gegevensweergave weer uit om niet onnodig veel gegevens op je pc te hebben staan.

In Windows 10 kun je verschillende dingen doen om te voorkomen dat er gebruikersinhoud, zoals gebruikersbestanden of communicatie, wordt verzameld. Daarnaast treft Microsoft extra maatregelen om te voorkomen dat er gegevens worden verzameld die een bedrijf of gebruiker direct identificeren, zoals naam, e-mailadres of account-id.

- **Telemetrie setting:** Stel deze in op het niveau **Beveiliging (Security)**
  Door voor de optie 'beveiliging' te kiezen worden er alleen gegevens verzonden die zijn bedoeld om je Windows-pc en andere Windows-pc's veiliger te maken.
- **Timeline sync:** Zet deze **Uit (Off)**
  De cloudsynchronisatie-functionaliteit in Timeline (Timeline sync) houdt een chronologisch overzicht bij van de activiteiten die op de pc worden uitgevoerd. Denk hierbij aan bezochte websites, alle bewerkte Office-documenten en gebruikte multimediabestanden.
  In Windows 11 is deze functionaliteit verwijderd. Je hoeft dit dus alleen maar uit te zetten als er nog apparaten met Windows 10 aanwezig zijn.

Zie deze pagina voor meer informatie over diagnostische gegevens in Windows 10/11.

Gevolgen wanneer je de telemetrie beperkt en timeline uitzet

- **Telemetrie setting:** wanneer je de telemetrie gegevens op de setting **Beveiliging** zet, heeft dit geen gevolgen voor de werking van producten. Standaard staat Windows 10/11 op **Volledig**. Het niveau **Beveiliging** is alleen te vinden in de Windows 10/11 Enterprise en Education variant.
- **Timeline sync:** Microsoft raadt af om deze uit te schakelen. Het biedt namelijk voordelen voor jou als gebruiker. Met de tijdlijn zie je een overzicht van dingen waaraan je eerder hebt gewerkt en wat je aan het doen was, zodat je op een later moment makkelijk schakelt tussen activiteiten en items om er verder aan te werken. Door dit uit te zetten kunnen gebruikers er geen gebruik meer van maken.

Instellingen via Microsoft Endpoint Manager (voorheen Intune) aanpassen

Om via Microsoft Endpoint Manager (Microsoft Device Management, MDM, voorheen: Intune) de instellingen aan te passen, heb je minimaal de rol *Intune beheerder* nodig in de tenant van je organisatie. Deze methode werkt alleen als je je apparaten ook daadwerkelijk beheert via Microsoft Endpoint Manager.

Om dit te kunnen doen, moet je omgeving in ieder geval aan de volgende eisen voldoen:
- Gebruikersaccounts moeten in de Azure Active Directory (AAD) staan (eventueel gesynchroniseerd).
- Beveiligingsgroepen moeten met de juiste gebruikers in de Azure Active Directory (AAD) staan (eventueel gesynchroniseerd).
- Om een *policy* in te stellen moet je ingelogd zijn in de tenant met één van de volgende rollen in de AAD: Globale beheerder, Security Administrator of Office App Admin.

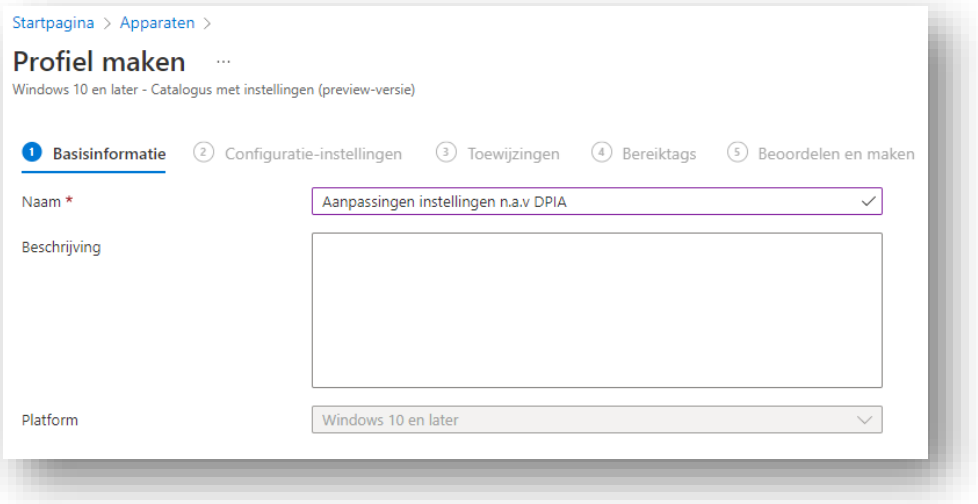
Je kunt de instellingen vervolgens aanpassen.

Aanpassen Telemetrie instelling en Timeline sync

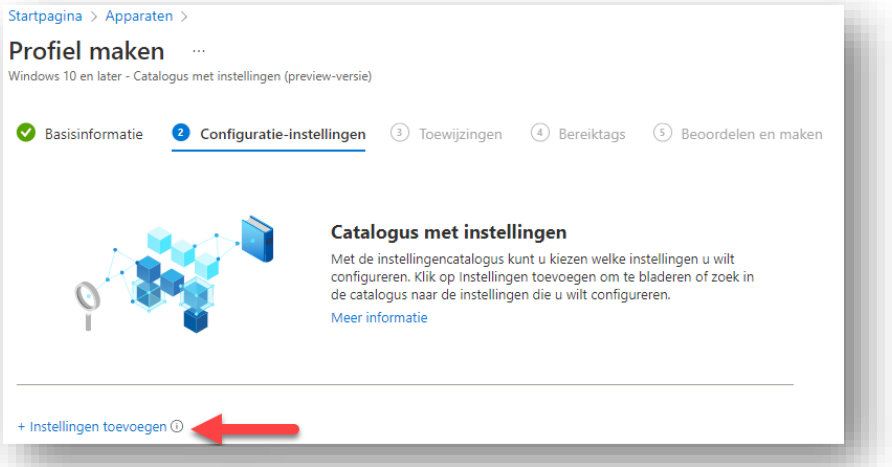
1. Ga binnen het Microsoft Endpoint Manager Admin center naar **Apparaten (Devices)** > **Configuratie profielen (Configuration profiles)**
2. Klik vervolgens bovenin op **+ Profiel maken (+ Create profile)**
3. Voer nu de volgende gegevens in:
   - Platform: **Windows 10 en later**

- Profieltype: **Catalogus met instellingen (preview versie)**

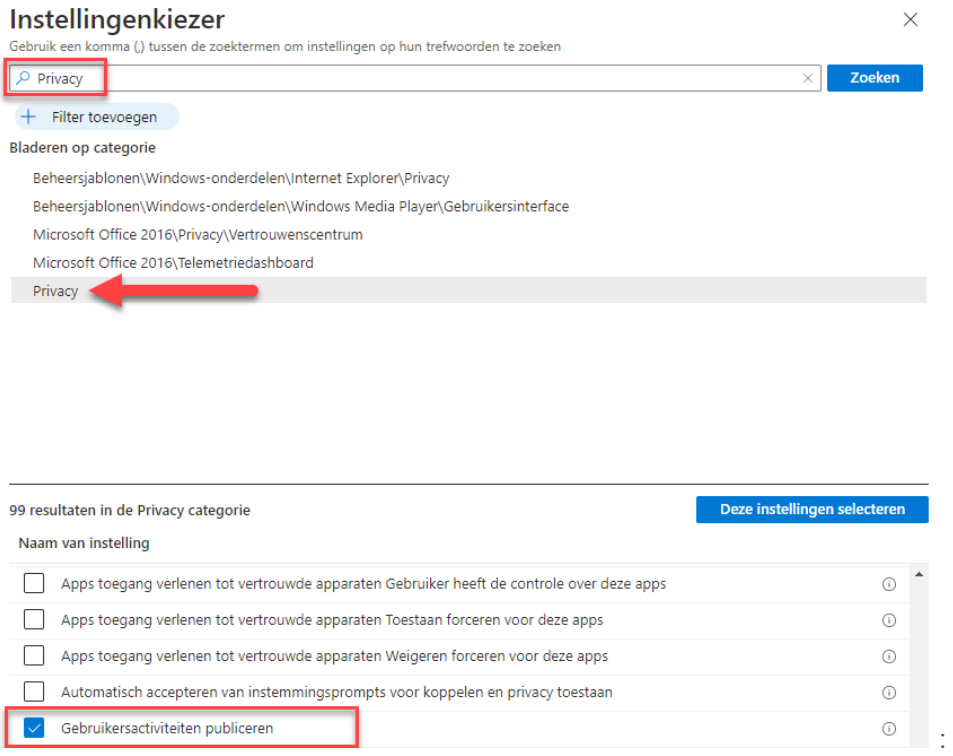
4. Klik onderin op de blauwe knop **Profiel maken (Create)**
5. Geef het profiel een duidelijke herkenbare naam (*bijvoorbeeld: Aanpassingeninstellingen n.a.v. DPIA*) en klik op **Volgende (Next)**



6. Klik bij **Configuratie instellingen (Configuration settings)** op **Instellingen toevoegen**

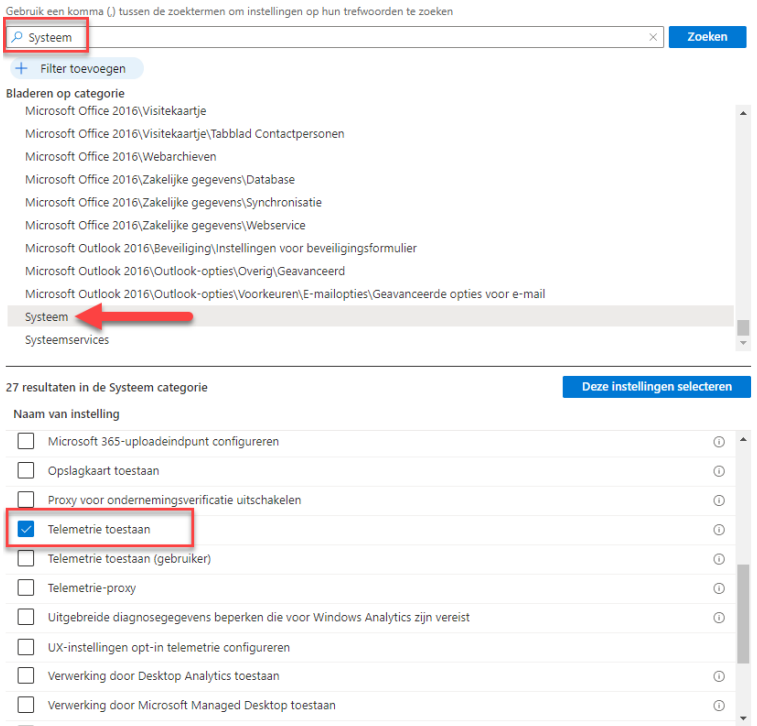


7. Zoek nu de instelling: **Privacy**
   Selecteer de optie **Privacy** en zoek naar de instelling *Gebruikersactiviteiten publiceren.* Vink deze optie aan.

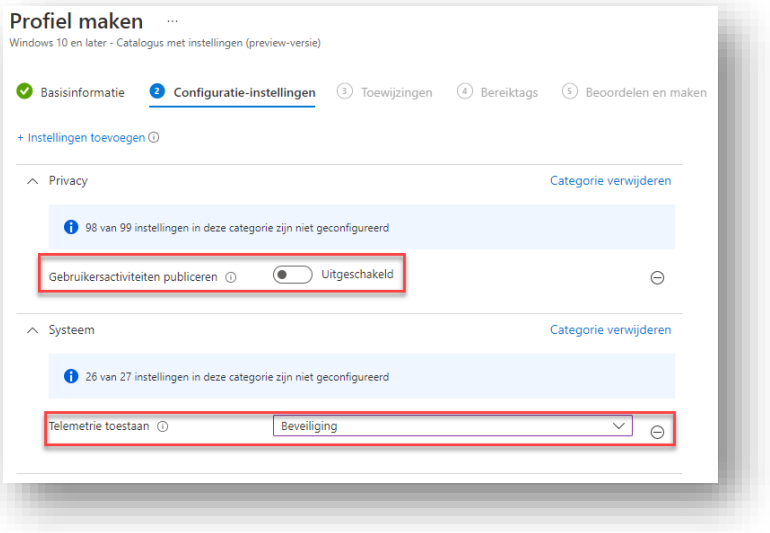


:

8. Zoek nu de optie **Systeem**
   Selecteer de optie **Systeem** en selecteer de instelling *Telemetrie toestaan.*



9. Klik nu als laatste dit rechterscherm weg via het kruisje rechtsboven
10. Stel de twee instellingen nu op de juiste manier in:
    Gebruikersactiviteiten: *Uitgeschakeld*
    Telemetrie toestaan: *Beveiliging*



11. Klik op **Volgende**
12. Wijs het profiel toe aan de juiste apparaatgroepen en klik op **Volgende**
13. Maak het profiel af door als laatste op **Maken** te klikken

Het profiel is voltooid. De instellingen worden naar de apparaten gesynchroniseerd.

Diagnostische gegevens beperken in Microsoft 365-apps voor ondernemingen

De nieuwe (verbeterde) privacy instellingen voor het beheren van diagnostische gegevens binnen Office zijn beschikbaar vanaf **Microsoft 365-apps voor ondernemingen** (voorheen Office 365 ProPlus) versie 1904 en hoger. Daarom moet je minimaal deze versie gebruiken binnen je organisatie, zodat je het beveiligingsniveau kunt aanzetten.

Goed om te weten!

Microsoft is transparant over wat er naar hen wordt verzonden. Je kunt als gebruiker via de app Viewer voor diagnostische gegevens, waar je standaard de Windows diagnostische gegevens in kan zien, ook diagnostische gegevens van Office weergeven door deze functie in te schakelen. Ben je klaar met het bekijken? Schakel dan de gegevensweergave uit om niet onnodig veel gegevens op je pc te hebben staan.

In **Microsoft 365-apps voor ondernemingen** (OfficeProPlus) kun je het verschillende dingen doen om te voorkomen dat er gebruikersinhoud, zoals gebruikersbestanden of communicatie, wordt verzameld. Ook treft Microsoft extra maatregelen om te voorkomen dat er gegevens worden verzameld die een bedrijf of gebruiker identificeren, zoals naam, e-mailadres of account-id.

- **Diagnostische data:** Stel deze in op het niveau **Geen van beide (Neither)**
  Dit gaat om diagnostische gegevens over de gebruikte Office-clientsoftware die wordt uitgevoerd op het apparaat van de gebruiker.

- **Verbonden ervaringen (Connected experiences):** *Dit zijn alle diensten binnen Office die persoonlijke informatie ophalen van het internet om efficiënter te (be)werken, communiceren en samenwerken.*
  Het advies vanuit de DPIA is om de optionele connected experiences **Uit (Off)** te zetten. Ze adviseren zo min mogelijk gebruik te maken van de optionele connected services, waarvoor Microsoft de verwerkeringsverantwoordelijke is en niet de verwerker.
  Ons advies is om goed te kijken of de beperkingen die hierdoor ontstaan niet noodzakelijk zijn voor je organisatie.

Er zijn op dit moment drie soorten beleidsinstellingen en deze zijn als volgt onder te verdelen:

1. **Het gebruik van verbonden ervaringen in Office toestaan waarmee inhoud wordt geanalyseerd** (Allow the use of connected experiences in Office that analyze content)
   Deze ervaringen maken gebruik van je Office-inhoud om je te voorzien van ontwerpaanbevelingen, bewerksuggesties, inzichten in gegevens en dergelijke.
2. **Het gebruik van verbonden ervaringen in Office toestaan waarmee online-inhoud wordt gedownload** (Allow the use of connected experiences in Office that download online content)
   Met deze ervaringen kun je online inhoud zoeken en downloaden, zoals sjablonen, afbeeldingen, 3D-modellen, video's en referentiemateriaal waarmee je documenten kunt verfraaien.
3. **Het gebruik van aanvullende, optionele verbonden ervaringen in Office toestaan** (Allow the use of additional optional connected experiences in Office)
   Naast de hierboven genoemde verbonden ervaringen die met Office worden meegeleverd, zijn er enkele optionele verbonden ervaringen, waartoe gebruikers toegang hebben. Bijvoorbeeld de LinkedIn-functies van de cv-assistent in Word of de functie 3D-kaarten in Excel, die gebruikmaakt van Bing.
   Handig om te weten: Deze instelling bevat slechts een subset van alle verbonden ervaringen die er zijn en dit betreft enkel de connected services waar Microsoft geen verwerker voor is.

Het is mogelijk alle drie bovenstaande opties in één keer uit te schakelen. Wij adviseren dit niet te doen. Hierbij schakel je alle verbonden ervaringen uit en dit heeft negatieve en beperkende gevolgen voor online samenwerken en de werking van het Office-pakket voor gebruikers. Zie hieronder wat de impact is als je ervoor kiest om ook de andere opties uit te schakelen.

Ons advies is om alleen de optionele verbonden ervaringen in Office uit te schakelen. Het uitschakelen van deze functionaliteit heeft de minste impact op de gebruikers.

Gevolgen wanneer je diagnostische data beperkt en optionele verbonden ervaringen uitzet

- **Diagnostische data:** Deze kan zonder problemen uitgezet worden en dit heeft geen gevolgen voor het werken met Office. Er worden via deze instelling geen diagnostische gegevens meer verzameld en verzonden over de Office-clientsoftware die wordt uitgevoerd op het apparaat van de gebruiker. Dit betekent wel dat Microsoft geen data meer ontvangt om de programma's beter te maken. Deze optie beperkt op aanzienlijke wijze mogelijkheden voor Microsoft om problemen te detecteren, diagnosticeren en oplossen bij gebruikers. Lees meer informatie over welke diagnostische gegevens worden verzonden naar Microsoft.
- **Verbonden ervaringen (Connected experiences):** Het gevolg van het beperken van diagnostische data is dat de lintopdracht of de menuopdracht voor de gebruiker grijs wordt weergegeven. Of zij krijgen een foutmelding wanneer ze gebruikmaken van een verbonden ervaring.

Hieronder bespreken we alle mogelijke opties van de verbonden ervaringen:

Het gebruik van aanvullende optionele verbonden ervaringen toestaan in Office

Bij het uitschakelen van deze functie zullen optionele verbonden ervaringen waarbij Microsoft niet de verwerker is, worden uitgeschakeld. Maak hierbij de overweging dat wanneer je dit uitzet, gebruikers mogelijk alternatieven zoeken. En hoe veilig zijn die? Om een voorbeeld te geven: Zodra Bing Search wordt uitgeschakeld, gaan gebruikers wellicht Google gebruiken. Het kan een keuze zijn om een functie niet uit te schakelen, omdat de alternatieven minder goed zijn.

Enkele voorbeelden van deze functies zijn:
- Invoegtoepassingen (zoals Bing Search of LinkedIn koppelingen);
- Outlook uservoice;
- CV-assistent.

Bekijk welke expliciete ervaringen hieronder vallen. Let op: het gaat slechts om een subset van deze lijst. Wanneer je deze functie uitschakelt, doe je dit enkel voor de functies in de lijst waar een sterretje achter staat.

Het gebruik van verbonden ervaringen waarmee inhoud wordt geanalyseerd toestaan in Office
Bij het uitschakelen van deze functie zullen gebruikers een aantal functies missen die een meerwaarde kunnen bieden.

Enkele voorbeelden van deze functies zijn:
- Handschrift naar tekst omzetten;
- Presentaties als film publiceren naar Stream;
- Het vertalen van de inhoud van een Word-document in een andere taal;
- Dicteren;
- Live-ondertitels en bijschriften (in bijvoorbeeld PowerPoint).

Bekijk welke expliciete ervaringen hieronder vallen.

Het gebruik van verbonden ervaringen waarmee online-inhoud wordt gedownload toestaan in Office
Bij het uitschakelen van deze functie kunnen gebruikers geen extra opties gebruiken binnen diensten die soms wel gewenst zijn.

Enkele voorbeelden van deze functies zijn:
- Sjablonen voor bestanden gebruiken (inclusief downloaden);
- Interessante agenda's (via internet) toevoegen;
- Tekenen en schrijven met inkt in Office;
- Pictogrammen (online opzoeken) invoegen in Office;
- Microsoft Forms (formulier of toets) invoegen in PowerPoint;

Bekijk welke expliciete ervaringen hieronder vallen.

Het gebruik van verbonden ervaringen in Office toestaan
Via deze instelling zet je alle functies die bij bovengenoemde ervaringen vermeld worden, in één keer uit, inclusief functies vernoemd in onderstaande link*. Bij het uitschakelen van deze functie krijgen gebruikers aanzienlijk functieverlies. Gebruikers zullen hun manier van werken moeten aanpassen. Het is een situatie waarbij je het werken in de cloud haast onmogelijk maakt.

Enkele voorbeelden van functies die niet meer zullen werken zijn:
- Samenwerken (realtime) aan een document;
- Documenten online opslaan (SharePoint en OneDrive);
- Veilige koppelingen (ATP);
- Vertrouwelijkheidslabels (Sensitivity Labels);
- Het delen van bestanden;

- Versiegeschiedenis vanuit het bestand zelf;

* Alle verbonden ervaringen vermeld (ook zonder sterretje) zullen niet meer werken.

Tip!

Ervaar je als gebruiker dat bepaalde functies niet meer werken? Kijk dan via de volgende stappen na of een beheerder bepaalde zaken voor jou heeft uitgezet:

Ga naar **Bestand** > **Account** > **Accountprivacy** en selecteer **Instellingen beheren**.

Zie je hier een bericht met de tekst 'De beheerder van uw organisatie beheert uw privacyinstellingen en heeft besloten de optionele verbonden ervaringen uit te schakelen'? Dan weet je dat dit functieverlies te maken heeft met verbonden ervaringen die voor je uitgezet zijn.

Instellingen via Microsoft Endpoint Manager (voorheen Intune) aanpassen

Om via Microsoft Endpoint Manager (Microsoft Device Management, MDM, voorheen: Intune) de instellingen aan te passen heb je minimaal Intune beheerrechten nodig in de tenant van jullie organisatie.

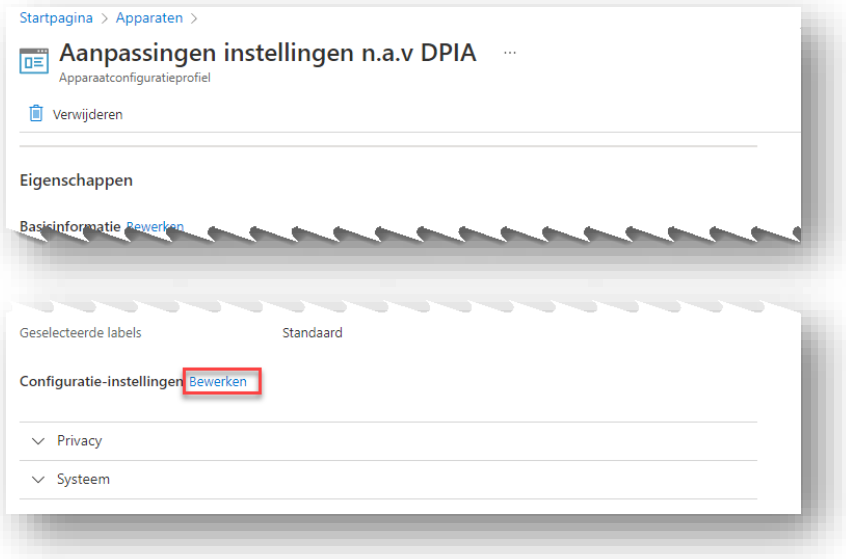
Let op: deze methode werkt alleen als je je devices ook daadwerkelijk beheert via Microsoft Endpoint Manager (Intune) en wanneer de gebruikers de Microsoft 365 voor ondernemingen (Office 365 Proplus) gebruiken.

Om de instellingen aan te passen, moet je in ieder geval aan de volgende eisen voldoen:
- Gebruikersaccounts moeten in de Azure Active Directory (AAD) staan (eventueel gesynchroniseerd).
- Beveiligingsgroepen moeten met de juiste gebruikers in de Azure Active Directory (AAD) staan (eventueel gesynchroniseerd).
- Om een policy in te stellen moet je ingelogd zijn in de tenant met een van de volgende rollen in de AAD: Globale beheerder, Security Administrator of Office App Admin.

Je kunt de instellingen vervolgens als volgt aanpassen:

Uitzetten van diagnostische data tegelijk met de optionele verbonden ervaringen
De onderstaande wijzigingen kunnen worden opgenomen in hetzelfde profiel als hierboven is aangemaakt. Open dus als eerste de beleidsregel *Aanpassingen instellingen n.a.v DPIA*.

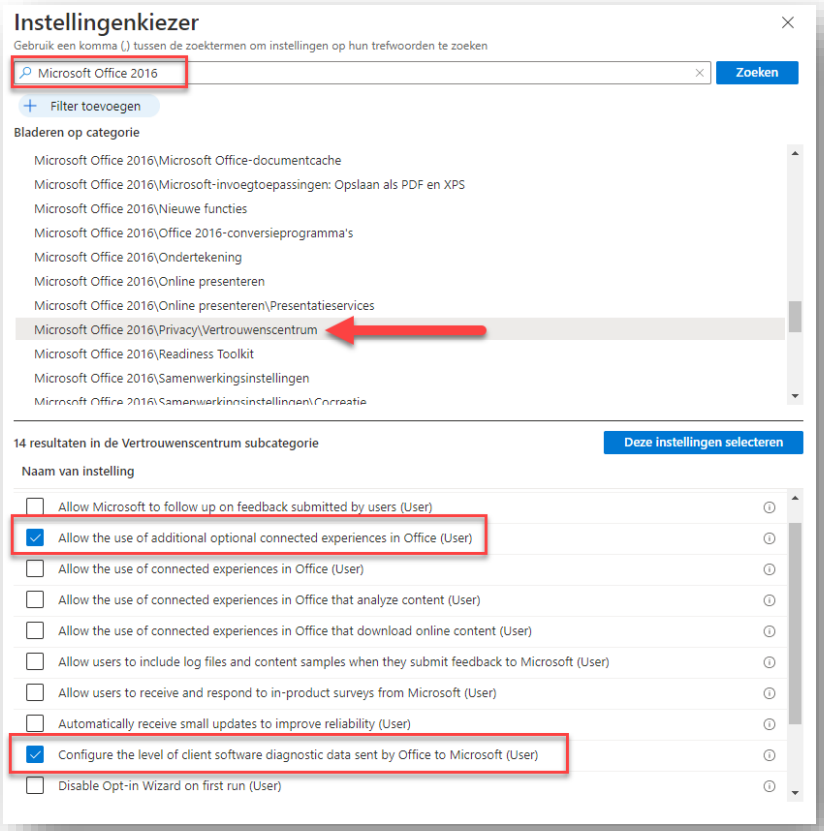
1. Klik in het overzichtsscherm onderaan op **Bewerken** bij de Configuratie-instellingen



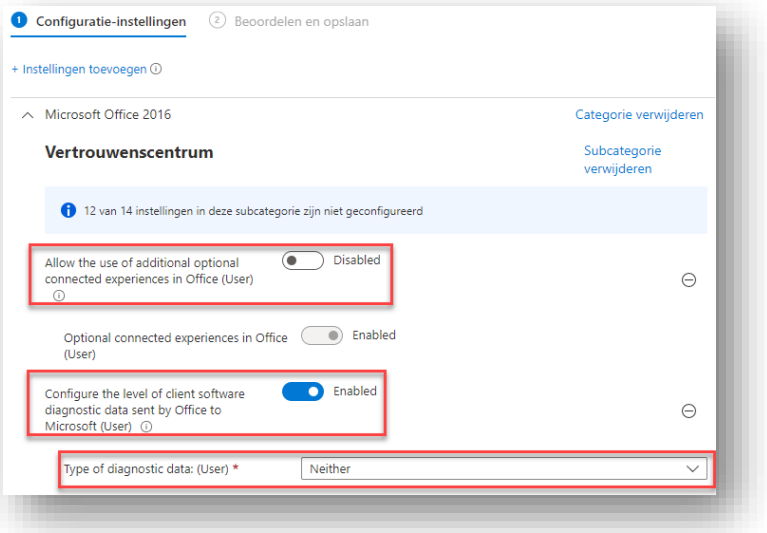
2. Klik op **Instellingen toevoegen**

3.

3. Zoek nu de optie **Microsoft Office 2016\Privacy\Vertrouwenscentrum** en selecteer deze categorie. Selecteer nu de juiste instellingen:
    a. Configure the level of client software diagnostic data sent by Office to Microsoft (user)
    b. Allow the use of additional optional connected experiences in Office (User)



4. Klik op het kruisje rechtsboven om dit scherm weer af te sluiten
5. Stel de twee instellingen op de juiste manier in



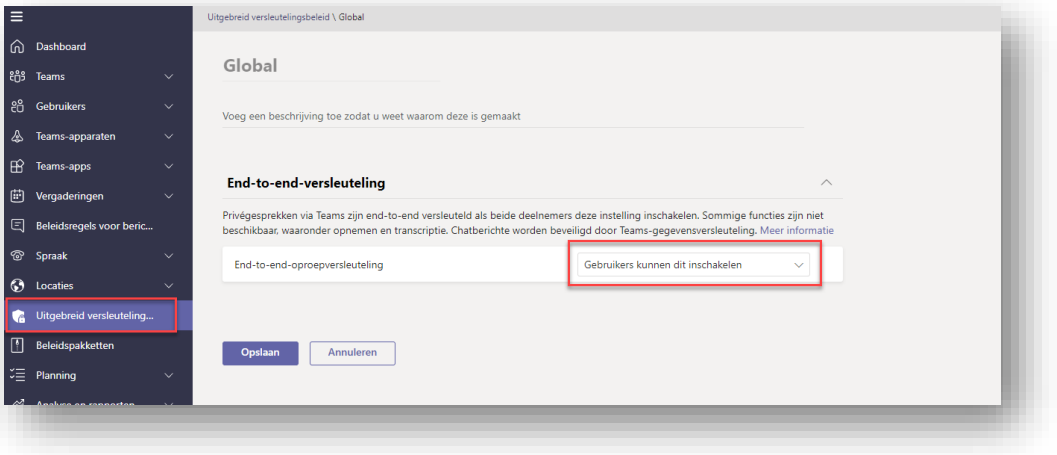
6. Sla de instellingen weer op en ook deze set aan instellingen wordt doorgezet naar de gekoppelde apparaten

Extra aanpassingen in de Microsoft 365 omgeving

Zet End-to-End Encryption aan in de omgeving

Door het aanzetten van End-to-End Encryption kunnen een-op-een vergaderingen extra worden versleuteld.

1. Ga naar het **Teams Admin Centrum**.
2. Ga naar het onderdeel **Uitgebreid versleutelingsbeleid**.
3. Open de **Standaard global policy** en pas daar de setting aan dat End-to-End-oproepversleuteling door iedereen aan te zetten is.

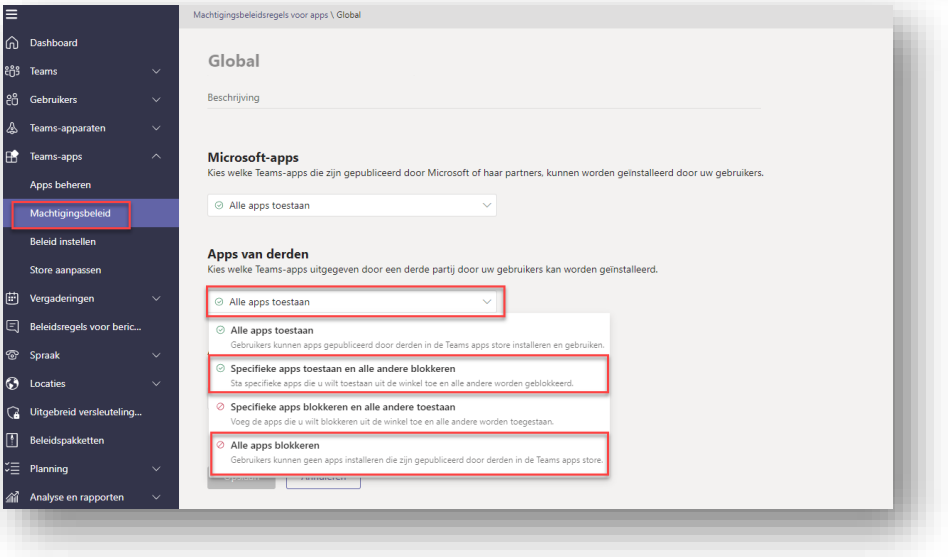


4. Sla de nieuwe policy op. Deze wordt nu automatisch naar iedereen doorgevoerd.
5. Als medewerkers nu deelnemen aan een een-op-een Teamsvergadering kunnen zij het beleid aanzetten. Dit doen zij via de instellingen van de Teams app.

Blokkeer het gebruik van 3th party apps in Microsoft Teams

Standaard kunnen alle gebruikers binnen Microsoft Teams apps gebruiken. Dit kunnen apps van Microsoft zijn, maar ook van buiten de organisatie en Microsoft. Het gebruik van deze apps moet worden geblokkeerd voor alle apps. Eventueel kunnen er apps worden uitgezonderd waar met de makers een verwerkersovereenkomst voor is afgesloten.

1. Ga naar het **Teams Admin Centrum**.
2. Op het onderdeel **Teams apps**, ga naar **Machtigingsbeleid** en open de **Global policy**.

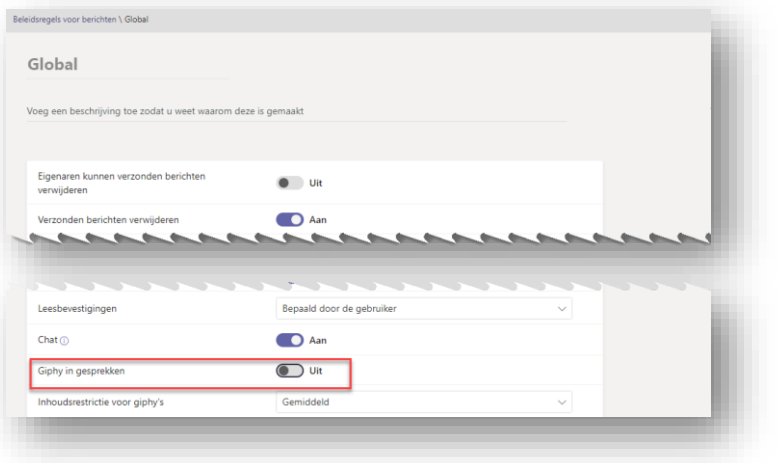


3. Kies hier bij **Apps van derden** voor de optie **Alle apps blokkeren**. Heb je bepaalde apps die je wel zou willen gebruiken? Kies dan voor de optie **Specifieke apps toestaan en alle andere blokkeren**.
4. Sla de nieuwe policy op. Deze wordt nu automatisch naar iedereen doorgevoerd.

Uitzetten van Giphy in Microsoft Teams

Het gebruiken van Giphy binnen Microsoft Teams mag ook niet. Binnen de beleidsregels van berichten is deze functionaliteit uit te zetten.

1. Ga naar het **Teams Admin Centrum**.
2. Ga naar **Beleidsregels voor berichten** en open de **Global policy**.
   Heb je specifieke beleidsregels voor leerlingen? Voer de onderstaande stappen dan ook voor de andere regels uit.
3. Schakel de optie **Giphy in gesprekken** uit.



4. Sla de nieuwe policy op. Deze wordt nu automatisch naar iedereen doorgevoerd.

Zet Microsoft Viva Insights uit

Het advies is om Microsoft Viva Insights in zijn geheel uit te zetten. Zo geef je medewerkers niet de indruk dat zij worden gevolgd, of dat hun informatie wordt gedeeld.

1. Navigeer naar het **Microsoft 365 beheercentrum**
2. Ga naar **Organisatie-instellingen ➔ Services ➔ Microsoft Viva Insights**
3. Deselecteer op deze pagina alle instellingen.

4. Sla de instellingen op. Deze worden nu doorgevoerd naar de gebruikers.

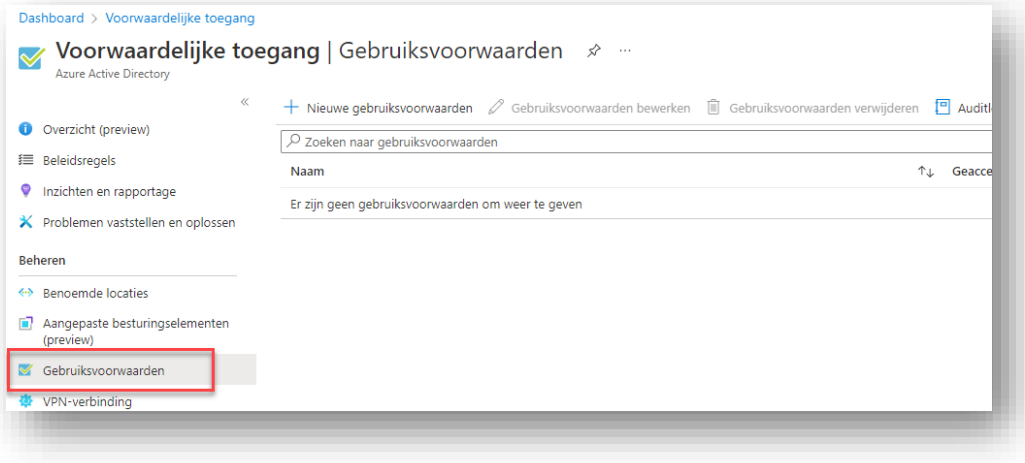
Maak een disclaimer die gastgebruikers eerst moeten accepteren voordat ze kunnen samenwerken

Als je gasten toegang geeft tot je omgeving, kun je deze gasten eerst een disclaimer presenteren. Hierin staat hoe je als organisatie omgaat met persoonlijke en gevoelige data. Na accepteren van deze disclaimer kunnen gasten daadwerkelijk aan de slag.

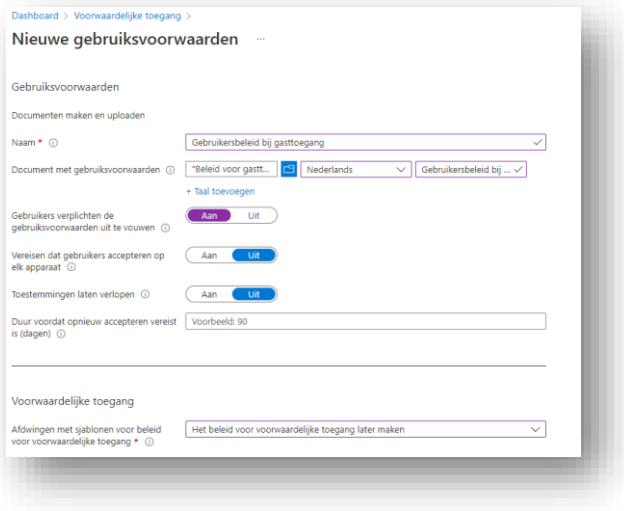
Je zal eerst zo'n disclaimer in een PDF document moeten vormgeven. Hierna kun je via de voorwaardelijke toegang deze disclaimer aan gastgebruikers tonen.

Aanmaken van de disclaimer

1. Navigeer naar de Voorwaardelijke toegang.
2. Open het onderdeel **Gebruiksvoorwaarden**.



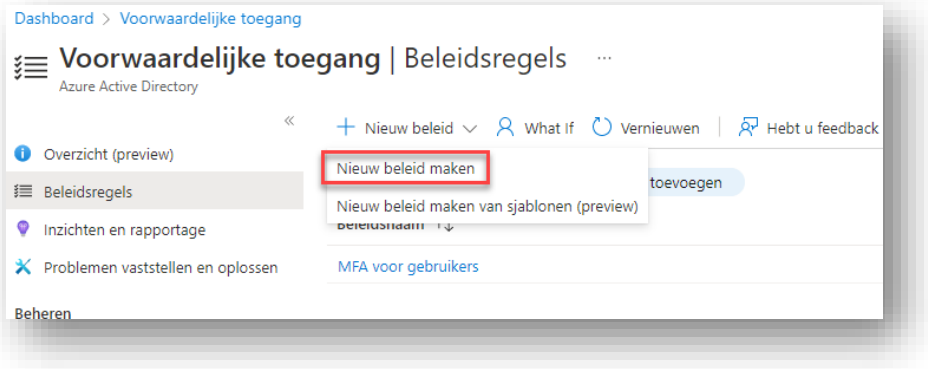
3. Klik op **Nieuwe gebruikersvoorwaarden**.
   Vul nu de juiste gegevens in bij dit beleid. Of neem het over zoals hieronder staat.



4. Klik nu als laatste op **Maken** en de nieuwe gebruikersvoorwaarden worden gemaakt.

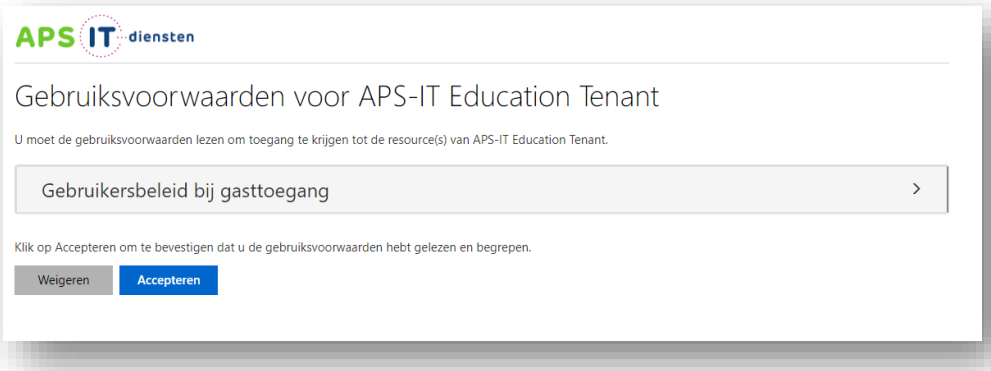
Aanmaken van de voorwaardelijke toegangsregel

1. Navigeer weer naar het onderdeel Voorwaardelijke toegang.
2. Er zal nu een beleidsregel moeten worden gemaakt die deze gebruikersvoorwaarden moet tonen tijdens het aanmelden.
3. Klik op **Nieuw beleid**.



4. Geef het beleid als eerste een duidelijke naam **Gebruikersvoorwaarden bij gasttoegang**.
5. Vul dan bij de afzonderlijke onderdelen de juiste informatie in.
   a. Gebruikers of werkbelastingsidentiteiten.
      Selecteer daar de groep **Alle gastgebruikers en externe gebruikers**.
   b. Cloud-apps of acties
      Selecteer de app **Office 365**.
   c. Verlenen
      In dit onderdeel kun je nu de net gemaakte beleidsregel **Gebruikersbeleid bij gasttoegang** aanvinken.
6. Schakel nu als laatste het beleid in.

Het beleid is direct actief. Als vanaf nu een gast wordt uitgenodigd, dan zal het onderstaande scherm worden getoond. De gast moet de gebruikersvoorwaarden lezen en accepteren om zo toegang te krijgen.



Extra diensten en functies

Een veilige inrichting is niet zwart-wit. Er zijn grijze gebieden. Als je de AVG heel strikt wilt volgen, geven we hieronder voor diverse diensten en functies het advies. Het strikt opvolgen van deze adviezen kan leiden tot verminderde functionaliteit. Je moet hierin dus afwegingen maken. De AVG eist dat je dit bewust doet en ook documenteert. In het tweede deel van dit hoofdstuk gaan we dieper in op de afwegingen die helpen een keus te maken.

DLP binnen Teams: werkt jouw organisatie met externen? Weet dan hoe DLP zijn werk doet en onderneem gepaste actie.
- Strikt advies is: *schakel de mogelijkheid uit om met externe gebruikers te chatten*.

Previews: wees bewust van het gebruik van previews en van waar je gegevens zich bevinden.
- Strikt advies zou zijn: *gebruik geen previews of gratis evaluatieversies.*

Retentiebeleid (retention policies): zorg dat data niet zomaar verwijderd kan worden of juist verwijderd wordt wanneer dat strikt genomen zou moeten.
- Strikt advies is: *stel een bewaar- en verwijderbeleid op en implementeer dat met retention policies.*

Litigation Hold: gebruik Litigation Hold op de juiste manier. Het is bedoeld voor rechtszaken in combinatie met het verzamelen van bewijs.
- Strikt advies is: *blokkeer het gebruik van Litigation Hold.*

Power BI: pas een aantal standaardinstellingen aan binnen Power BI om te voldoen aan de AVG.
- Strikt advies is: *schakel 'Inhoud delen met externe gebruikers', 'Gegevens exporteren' en 'Publiceren op internet' uit.*

Zoeken in auditlogboek (Audit Log Search): zet auditlogboek aan om als beheerder - na een eventuele hack -belangrijke zaken vast te stellen of uit te sluiten.
- Strikt advies is: *schakel 'Audit Log Search' in.*

Klanten-lockbox (Customer Lockbox): maak je gebruik van serviceaanvragen bij Microsoft? Denk dan na over de Customer Lockbox.
- Strikt advies is: *zet Customer Lockbox aan.*

Privileged Acces Management: beheert een externe partij jullie omgeving? Houd dan met Privileged Acces Management (PAM) de controle over het beheer.
- Strikt advies is: *maak gebruik van PAM.*

Double Key Encryption (DKE): om strikt aan de AVG te voldoen, zijn er experts die adviseren DKE te gebruiken om *bijzondere* persoonsgegevens te beschermen. DKE is echter een erg complex product met serieuze kanttekeningen. Vanuit APS IT-diensten adviseren we daarom andere oplossingen te gebruiken dan DKE. Zie ook verderop in dit document
- Strikt juridisch advies zou zijn: *maak gebruik van DKE voor bijzondere persoonsgegevens. Zie verderop voor onze kanttekeningen bij dit juridische advies.*

Customer Key: de organisatie kan een eigen encryptiesleutel inbrengen waarmee de data op de servers van Microsoft wordt versleuteld. Op deze manier heeft enkel de organisatie de sleutel voor de encryptie van de data in de cloud. Op basis van de DPIA in februari 2022 wordt geadviseerd 'normale' persoonsgegevens die worden opgeslagen in SharePoint Online of OneDrive met Customer Key te beschermen.
- Strikt advies is: *data moet versleuteld zijn. Als het redelijkerwijs mogelijk is, mag deze sleutel niet bij anderen bekend zijn.*

Information Barriers: denk na over mogelijke scheiding(en) tussen bijvoorbeeld zorg en onderwijs of leerkrachten en leerlingen.

- Strikt advies is: *gebruikers mogen elkaars gegevens niet zomaar zien en/of vinden zonder toestemming vooraf. Zorg daarom voor een scheiding tussen adresboeken.*

Vertrouwelijkheidslabels (Sensitivity Labels): bescherm je belangrijke documenten met labels om te voorkomen dat niet geverifieerde gebruikers de documenten inzien.

- Strikt advies is: *label alle documenten zodat gebruikers alleen die gegevens in kunnen zien die zij nodig hebben voor het werk.*

Back-up: denk na over een back-up strategie en weet wat Microsoft zelf doet aan dataherstel. Maak daarnaast een risico-analyse en bekijk of dit voldoende is.

- Strikt advies is: *maak een back-up (of documenteer waarom je dat niet doet).*

Wij zullen deze punten nader toelichten zodat je een weloverwogen keuze kunt maken. Daarbij zul je zien dat het belangrijk is om goed na te denken over wat voor jouw organisatie het beste is.

DLP binnen Microsoft Teams

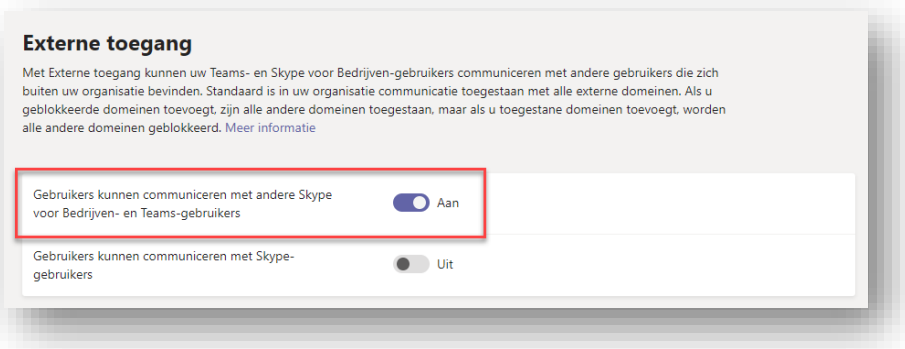
Werk je met DLP? Onderstaande informatie is dan erg interessant. Deze vertrouwelijkheidslabels zijn één van de manieren om te voorkomen dat (gevoelige) data je organisatie verlaat.

DLP kan gevoelige informatie blokkeren binnen Teams wanneer je samenwerkt met externe gebruikers. Op deze manier zien zij de inhoud niet, ook al maken ze gebruik van het team of kanaal. Wees je ervan bewust dat als je met externen werkt in een team, zij mogelijk bepaalde documenten die beveiligd zijn met DLP niet kunnen openen.
Er is één beperking. DLP werkt namelijk niet in losse chats binnen Teams. Er is wel een aanvullende dienst die dit mogelijk maakt: Communications DLP*. Hiermee zorg je dat de DLP-policies ook intact blijven in Teams chats.

Dit werkt enkel met externe gebruikers als beide tenants in de Teams only modus zitten. DLP voor Teams blokkeert geen berichten als de externe gebruiker Skype voor Bedrijven als voorkeursapp gebruikt. Het bovengenoemde strikte advies komt daaruit voort. Je weet namelijk niet waarin externe gebruikers chatten, tenzij je dit navraagt bij de beheerder.

Het uitzetten van chatten met externen doe je als volgt:

- Ga naar het Teams beheercentrum
- Ga vervolgens naar **Instellingen voor de gehele organisatie** > **Externen**
- Zet hier het schuifje op **Aan** bij de optie **Gebruikers kunnen communiceren met andere Skype voor Bedrijven- en Teams-gebruikers**



Besef dat als je dit uitschakelt, de gebruikers niet meer kunnen chatten met mensen buiten de organisatie. In sommige gevallen is dat niet wenselijk. Je kunt beslissen om bepaalde domeinen (waarvan je weet dat deze in *Teams only* werken) wél toe te staan. Dit doe je bij dezelfde instellingen door een specifiek Domein toe te voegen en toe te staan.

**DLP heb je standaard tot je beschikking met A3. Het werkt met OneDrive en SharePoint en indirect met Teams. Wil je DLP ook binnen chats in Teams laten werken? Dan heb je een aanvullende licentie (Communication Compliance) nodig. Deze zit in de volgende A5 bundels: Microsoft 365 A5 volledige Suite; Office 365 A5; Microsoft 365 A5 Compliance; Microsoft 365 A5 Information Protection & Governance.*

Lees meer informatie over DLP binnen Teams.

Previews

De previews van nieuwe onderdelen* van Microsoft 365 draaien standaard op een datacenter buiten Europa. Dat betekent dus dat als er via een preview versie informatie-uitwisseling plaatsvindt, deze informatie wordt opgeslagen buiten Europa. Zodra een onderdeel *General Available* (GA) wordt, verandert dit en zal de informatie in hetzelfde datacenter als jouw omgeving komen te staan. Het advies is hier zorgvuldig mee om te gaan en preview versies van producten voorzichtig in gebruik te nemen.

**Denk hierbij aan Forms (Pro), Stream en Bookings die beschikbaar kwamen en eerst in preview werkten. Deze kon je via de website alvast bestellen en uitproberen.*

Toch kan het soms handig zijn om als beheerder of ICT'er nieuwe onderdelen vooraf uit te proberen voordat de rest van je organisatie deze ontvangt. Het is het goed dat je je hiervan bewust bent, zodat je een weloverwogen keuze kunt maken.

Retentiebeleid (Retention Policies)

Een retentiebeleid stel je in om onbedoelde of opzettelijke verwijdering of wijziging van belangrijke data en/of e-mail te voorkomen. Dit beleid blijft onopgemerkt zijn werk doen op de achtergrond en is volgens jullie eigen beleid in te stellen.

Simpel gezegd beschermt het data door een reservekopie op te slaan in een 'veilige ruimte' gedurende een vooraf ingestelde periode. De nieuwste inhoud blijft beschikbaar om te bewerken. De veilige reservekopie blijft behouden zoals deze was op het moment dat deze werd verwijderd of gewijzigd.

De lengte van de bewaarperiode kun je zelf bepalen en na deze periode wordt alles definitief uit de mailbox en/of bibliotheek verwijderd. Je kunt inhoud ook onbepaalde tijd bewaren (oneindige bewaarplicht) of totdat de bewaarplicht is verlopen.

Omdat verschillende soorten gegevens, verschillende perioden van bewaren vereisen, heb je waarschijnlijk meer dan één bewaarbeleid nodig om de basis te dekken. Het is goed hier zorgvuldig over na te denken.

Documenten automatisch laten verwijderen en/of onbeperkt bewaren hebben ieder ook zijn risico's:

- Komt er een geschil (denk aan een juridische claim), dan loop je met automatisch verwijderen een risico en ben je hier niet voor beschermd. Wanneer dit het geval is, denk dan na over Litigation Hold (zie het volgende kopje).
- Bij een oneindige periode loop je mogelijk een groter risico op een claim vanwege mogelijke datalekken.

Daarom is het over het algemeen aan te raden gegevens vóór verwijdering te beoordelen.

Wees ervan bewust dat alle inhoud van een e-mailbox, dus ook de OneDrive (na verwijderen van bijvoorbeeld een uit dienst tredende medewerker), zonder ingestelde bewaartermijn na 30 dagen definitief weg is. Als iemand (al dan niet per ongeluk) data uit een SharePoint-bibliotheek verwijdert, is dit na 90 dagen definitief weg. Het verwijderen van belangrijke gegevens kan de continuïteit van de organisatie flink in de weg staan.

Besef daarom goed dat financiële documenten, zorgdossiers en/of contracten etc. een langere verplichte bewaartermijn hebben - meestal tussen 7-10 jaar. E-mailboxen van medewerkers die dit soort gegevens kunnen bevatten zou je langer in moeten stellen. Belangrijk is dat je de juiste bewaartermijnen uit je bewaarbeleid instelt op zowel SharePoint-sites als e-mailboxen en zo ook deze data veilig stelt.

Op basis van alle informatie denken wij dat het verstandig is om na te denken over de gevolgen en/of continuïteit wanneer een mailbox van een specifieke gebruiker definitief verwijderd wordt. Ook is het goed stil te staan bij SharePoint-bibliotheken die belangrijke gegevens bevatten en wat de gevolgen zijn als deze gegevens wegvallen. Onthoud ook dat zakelijke data altijd op centrale SharePoints staat en niet op de OneDrive van afzonderlijke gebruikers.

Maak daarnaast duidelijk hoe je als organisatie omgaat met (het bewaren van) zakelijke data, zoals bijvoorbeeld e-mail, en leg dit vast. Bijvoorbeeld in het arbeidsvoorwaardenreglement of in een ICT- en internetreglement.

Retention policies kun je als volgt instellen binnen je tenant:
- Ga naar het Compliance centrum.
- Klik op **Beleid (Policies)** in het linkernavigatie-deel en vervolgens rechts op **Retentie** (**Retention).**
- Stel hier de gewenste bewaar- of verwijdertermijnen in met de gewenste periodes.

Bekijk meer informatie over het instellen en hoe je dat voor je hele organisatie doet.

Het is ook goed om te weten dat een Retention Policy door een beheerder verwijderd kan worden. Daarom is het goed na te denken over de rechten van gebruikers en extra bescherming op beheeraccounts. Mocht deze in verkeerde handen vallen, kun je belangrijke data verliezen.

Bekijk meer informatie over Retention Policies.

Litigation Hold (in-place bewaring)

Litigation Hold is ontworpen om zeer specifieke data die je wilt behouden vast te zetten vanwege een mogelijke of lopende juridische procedure*. En zo mogelijke verwijdering van bewijs te voorkomen.

Met Litigation Hold kun je een bewaarperiode op een mailbox met Exchange Online Plan 2 plaatsen om de mailboxinhoud te behouden. Dit is inclusief verwijderde items en originele versies van gewijzigde items. Inhoud in het archiefpostvak (indien ingeschakeld) wordt dan zelfs bewaard.

Het advies vanuit de AVG (*blokkeer het gebruik van Litigation Hold*) komt tot stand omdat een Litigation Hold het onmogelijk maakt om te voldoen aan verwijderverzoeken (ook bekend als het 'recht om te worden vergeten/ te wissen') op grond van de AVG en dat is strikt genomen niet toegestaan. Maar wanneer je met juridische zaken te maken hebt, wil je niet dat er bewijs verloren gaat. Gebruik Litigation Hold niet (standaard) om aan een bewaarplicht te voldoen of ter voorkoming van data-verlies. Het is bedoeld voor rechtszaken in combinatie met het verzamelen van bewijs. Voor een bewaarplicht zijn eventuele Retention Policies beter geschikt (zie het kopje hierboven). Weet dat deze functie bestaat en zet hem tijdig en op de juiste manier in.

Litigation Hold werkt niet met terugwerkende kracht. Alles dat is gewijzigd of verwijderd voordat de Litigation Hold werd ingesteld, wordt niet beschermd. Tenzij het al op een andere manier wordt beschermd zoals met een Retention Policy. Het is belangrijk Litigation Hold op tijd in te zetten en goed te kijken naar jullie Retention Policies en hoe deze elkaar kunnen aanvullen. Een Litigation Hold heeft voorrang op elk ander ingesteld bewaarbeleid.

Zodra de Litigation Hold is opgeheven, hebben de Retention Policies opnieuw voorrang en worden alle acties (zoals automatische verwijdering) die eerder hadden moeten plaatsvinden, onmiddellijk ondernomen.

**Als je gericht informatie wilt beschermen en verzamelen, bijvoorbeeld voor een juridisch conflict, kan je ook een eDiscovery openen. Hierbij kun je een georganiseerde zoekactie maken op delen van je Microsoft 365 tenant.*

Wat gebeurt er bij het verwijderen van mail uit een mailbox, waar een Litigation Hold op zit?
De verwijderde items worden verplaatst van de Deletions-submap naar de speciale Discovery Holds-submap. Deze worden bewaard totdat de mailbox wordt vrijgegeven uit de eDiscovery-bewaarplicht. Besef goed dat als je geen Litigation Hold hebt ingesteld en de gebruiker meer dan 90 dagen geleden verwijderd is, een eDiscovery niets op zal leveren.

Litigation Hold kun je als volgt terugvinden binnen je tenant:
- Ga naar het Exchange Beheercentrum Admin Center
- Klik op **Geadresseerden** in het linkernavigatievenster
- Dubbelklik op de mailbox waar je een bewaartermijn voor wilt opgeven
- Ga naar **Postvakgemachtigden**
- Scroll naar **Bewaren vanwege juridische procedure**
- Schakel deze in en geef een gewenste tijdperiode op

Lees meer over Litigation Hold.

Power BI

Met Power BI kunnen gebruikers dashboards, rapporten en apps delen met externen en deze publiceren op internet. Hiermee maken zij het rapport en de gegevens die het bevat, beschikbaar voor mensen buiten de organisatie.

Naast het delen is het ook mogelijk gegevens uit een Power BI Dashbord te exporteren. Denk hierbij aan: analyses maken in Excel, exporteren naar een CSV-file, downloaden van een gegevensset (PBIX) en de functies van Power BI Service Live Connect bedienen.

Let op!
Als je inhoud wilt delen (of exporteren), hebben zowel de maker als ontvanger een Power BI Pro-licentie nodig, ongeacht of je de inhoud binnen of buiten jullie organisatie deelt.

Ook is het zo dat iedereen met een Power BI licentie (die beschikbaar is via de Cloudbundel) zijn gemaakte dashboards op internet kan publiceren. Hiermee is het via een openbare URL voor iedereen beschikbaar.

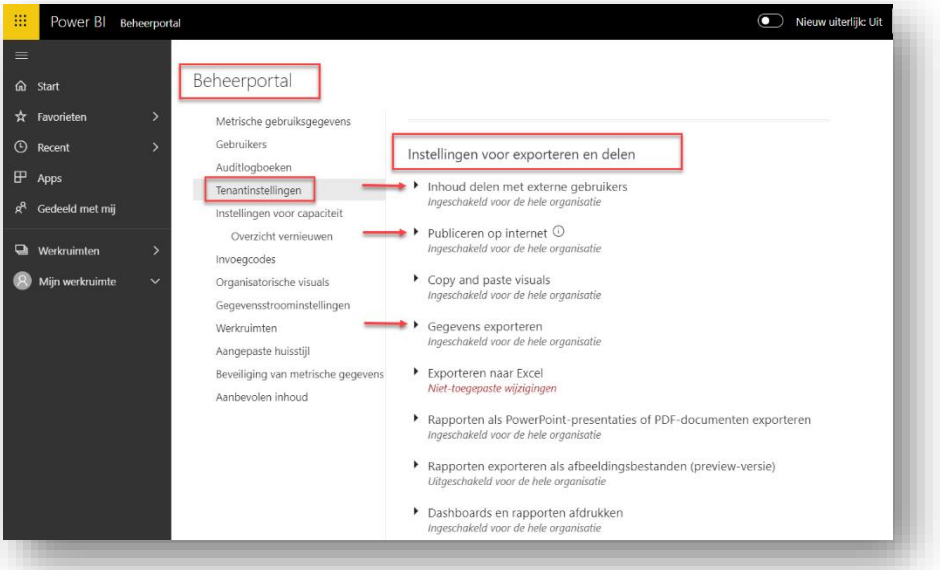
Of je nu deelt, publiceert of exporteert: deze gegevens kunnen gevoelige informatie bevatten en vormen dus een risico. Daarom is het advies vanuit de AVG: zet onderstaande drie opties uit, of zet deze gereguleerd open voor een geselecteerde groep gebruikers. Zo kun je deze specifieke mensen trainen hoe ze moeten delen en op welke manier dit veilig is.

- Inhoud delen met externe gebruikers;
- Publiceren op internet;
- Gegevens exporteren.

Je kunt ervoor kiezen om de Vertrouwelijkheidslabels (sensitivity labels) binnen Power BI aan te zetten. Op deze manier voorkom je dat inhoud te zien is voor gebruikers waar het niet voor is bestemd. Deze licentie is onderdeel van de Cloudbundel en kun je zonder extra kosten inzetten. Lees hoe je dit instelt.

Het uitschakelen van bovenstaande drie opties binnen Power BI doe je als volgt:

- Ga naar de Power BI beheerportal. Deze is ook te vinden via het tandwieltje (na inloggen) rechtsboven in de balk.
- Om in de portal te komen heb je Admin rechten nodig.
- Klik links op **Tenantinstellingen.**
- Onder **Instellingen voor exporteren en delen** kun je alle drie de opties vinden die hierboven besproken zijn. Stel het vervolgens in zoals wenselijk is.



Zoeken in auditlogboek

In het auditlogboek worden gebruikers- en systeemhandelingen vastgelegd voor latere referentie of verantwoording. Dit is met name wenselijk als je wilt voldoen aan een goed archiefbeheer.

Zodra je auditlogboek aanzet, registreert het activiteiten, waar je als beheerder uitgebreid op kan zoeken. Denk bijvoorbeeld aan Office 365-aanmeldingen, wijzigingen in instellingen, wachtwoordherstel en het downloaden of delen van documenten.

Naast het registreren kun je ook waarschuwingen instellen voor verdachte activiteiten. Denk bijvoorbeeld aan een waarschuwing voor inlogpogingen uit andere landen, het downloaden van meerdere bestanden in korte tijd of massale verwijderingen op SharePoint.

Doordat je activiteiten registreert kun je alert zijn op verdachte activiteiten. Hierdoor houd je meer grip op je omgeving en data en kun je verbeteringen doorvoeren om nog beter te voldoen aan de regelgevingen.

Als een account bijvoorbeeld gehackt is, wil je als organisatie nagaan welke bestanden benaderd zijn, om onrechtmatige toegang vast te stellen of uit te sluiten. Hierdoor kun je direct gepaste actie ondernemen.

Auditlogboeken kunnen voor een ICT-er ook erg handig zijn om problemen op te lossen. Vraagt een medewerker bijvoorbeeld naar een onvindbaar bestand, dan kun je via een auditlogboek zien waar het bestand is. Ook kun je terugzien door wie een bestand verwijderd is. Stel dat het vaker voorkomt dat er bestanden gewist worden, kun je mogelijk met een gebruiker in gesprek gaan over de procedure van bestanden verwijderen. Maar als hetzelfde bestand meerdere keren moet worden hersteld, is er mogelijk een dieper liggend probleem.

Auditlogboeken zijn niet standaard ingeschakeld. Wil je deze gebruiken, dan moet je dit inschakelen en configuraties instellen wanneer je waarschuwingen wilt ontvangen. Heb je een vrij recente Microsoft 365 tenant, dan staat het mogelijk standaard ingeschakeld.

Het is goed erover na te denken wie auditlogboeken mogen inzien. Dit vergt mogelijk een nieuw gesprek over Microsoft 365 Governance en wie toegang moeten krijgen tot de Microsoft 365 beheeromgeving(-en).Diegene die toegang hebben tot de logboeken kunnen steeksproefgewijs ook onderzoeken of de juiste mensen toegang hebben gehad tot gevoelige documenten.

Goed om te weten:

- Auditlogboeken worden standaard 90 dagen bewaard*. Heb je geen waarschuwingen aanstaan, controleer dan regelmatig je auditlogboeken op verdachte activiteiten.
- Auditlogboeken, rapporteren niet automatisch Power BI activiteiten. Deze moet je handmatig instellen.
- Met een auditlogboek kan je aan de Autoriteit Persoonsgegevens aantonen dat je een goed werkend Privacy Management Systeem hebt en dus op dat vlak voldoet aan de AVG regelgeving

* Met een A5-abonnement is dit zelfs tot 365 dagen.

Klanten-Lockbox (Customer Lockbox)

In de AVG wordt gesteld dat je enkel gebruikers toegang mag verlenen tot jouw gevoelige data (medische en persoonlijke dossiers) wanneer zij deze nodig hebben om hun werk goed uit te voeren. En dat dit vervolgens altijd gelogd moet worden. Bijvoorbeeld: IB-ers mogen alléén maar de gegevens

van hun ‘eigen’ leerlingen zien en bij een eventuele controle moet dit aantoonbaar zijn. Het loggen is in je omgeving al reeds terug te vinden (kijk hier). Houd dit dus in de gaten.

Wat betreft je data: niemand bij Microsoft heeft standaard (permanent) toegang tot inhoud binnen jullie Microsoft 365 gegevens. Alle diensten binnen Microsoft 365 zijn zo ontworpen dat de mensen die serviceactiviteiten uitvoeren nooit zomaar toegang hebben tot jullie gegevens. Bijna alle serviceactiviteiten die door Microsoft worden uitgevoerd, zijn geautomatiseerd.

Het zal je vast opgevallen zijn dat de technici bij een service aanvraag weleens mee willen kijken op je scherm. Zij geven dan duidelijk aan dat je geen gevoelige data open mag hebben staan en dat zij niks uitvoeren, enkel doorgeven wat jij moet doen. Dit zijn strikte regels waar zij zich aan moeten houden.

Het is goed om je hierbij het volgende te beseffen: maak je gebruik van een serviceaanvraag binnen je tenant, kan er zich een scenario voordoen waarbij een Microsoft technici wél toegang tot inhoud nodig heeft. In deze zeldzame gevallen moet een Microsoft-technicus namelijk toegang hebben tot jullie inhoud om de oorzaak te achterhalen en het probleem op te lossen. Denk hierbij aan een gebruiker die problemen ervaart in zijn mailbox of documentinhoud.

Als dit scenario zich voordoet, is er geen akkoord van jouw kant nodig. Microsoft is in deze gevallen van mening dat de zeldzame scenario’s waarin een Microsoft-technicus toegang tot klantinhoud nodig heeft, enkel het geval is wanneer de klant hier zelf om vraagt.

Voor dit soort (uitzonderlijke) scenario’s bestaat er ‘Customer Lockbox’ (een toegangscontroletechnologie). Via deze dienst heb je als organisatie de volledige controle over jouw gegevens. Customer Lockbox voegt dus in dit geval een extra zekerheid toe: Microsoft kan alleen bij de data ná expliciete toestemming. Customer Lockbox wordt momenteel ondersteund in Exchange Online, SharePoint Online en OneDrive for Business.

Het gebruik van de Customer Lockbox-functie zorgt er letterlijk voor dat de technicus van Microsoft geen toegang krijgt tot de inhoud zonder uitdrukkelijke toestemming. Wanneer je het verzoek om toegang krijgt, kan je dit verzoek onderzoeken en goedkeuren of afwijzen. Zolang het verzoek niet is goedgekeurd, wordt aan de Microsoft-technicus geen toegang verleend, ook niet meer wanneer de toestemming is verlopen.

Daarnaast dwingt het meerdere goedkeuringsniveaus binnen Microsoft af en geef je hen realtime toegang met beperkte en tijdgebonden autorisatie. Bovendien worden alle toegangscontroleactiviteiten in de service geregistreerd en gecontroleerd en is dit in te zien via de audit log in het Security & Compliance center.

Wil je gebruik maken van Klanten Lockbox (Customer Lockbox)? Dan heb je een aanvullende licentie (Communication Compliance) nodig. Deze zit in de volgende A5 bundels: Microsoft 365 A5 volledige Suite; Office 365 A5; Microsoft 365 A5 Compliance; Microsoft 365 A5 Insider Risk Management. Meer informatie over Klanten Lockbox (Customer Lockbox) binnen Teams vind je hier.
Iedere gebruiker aan wie de beheerdersrol ‘Customer Lockbox access approver’ is toegewezen kan ‘customer lockbox-aanvragen’ goedkeuren.

Privileged Access Management (PAM)

Wanneer een externe partij jullie omgeving beheert, hebben ze waarschijnlijk een Global Admin account en kunnen ze de gehele omgeving benaderen en beheren. Dat externe partijen toegang hebben tot jullie (gevoelige) data is strijdig met de AVG. Als je een externe partij toegang geeft, heb je een log in-plicht. Er moet gelogd worden zodat te herleiden valt wie wanneer toegang heeft gehad tot data.

Om grip te houden op de werkzaamheden van deze externe partijen, kun je gebruikmaken van Privileged Acces Management. Net zoals bij Customer Lockbox zou zo'n externe partij toegang moeten vragen om werkzaamheden uit te voeren. Voordeel is dat al deze aanvragen gelogd worden en er altijd inzicht is wie er wanneer toegang heeft gehad.

Bij PAM kun je instellen dat een externe beheerder die Intune van een stichting beheert, eerst toestemming moet vragen. Deze toegang kan geautomatiseerd plaatsvinden. Als de externe beheerder iets in Azure moet aanpassen, moet er wederom om toestemming gevraagd worden. Toestemming kun je geven met een bepaald tijdsbestek en na verloop van tijd vervallen de rechten.

Wil je gebruik maken van Privileged Acces Management (PAM), heb je een aanvullende licentie (Privileged Acces Management) nodig. Deze zit in de volgende A5 bundels: Office 365 A5; Microsoft 365 A5 Compliance; Microsoft 365 A5 Insider Risk Management.

Meer informatie over Privileged Acces Management (PAM) vind je hier.

Customer Key en Double Key Encryption (DKE)

Waar je met BitLocker een versleuteling op je harde schijf kunt doen, is je data in de cloud standaard versleuteld door Microsoft. Wanneer je zelf de controle wilt over deze sleutel, dan bestaat er de Customer Key. Hiermee voldoe je aan wettelijke of nalevingsverplichtingen voor het beheren van basissleutels.

Data die op de servers bij Microsoft staat, kan je versleutelen met een zelf ingebrachte Customer Key (sleutel). Customer Key biedt extra bescherming tegen het bekijken van data door niet-geautoriseerde systemen of personeel en vormt een aanvulling op de BitLocker-schijfversleuteling. Op deze manier voorkom je dat een cloudleverancier zomaar data kan ontsleutelen.

Let op: hiermee voorkom je niet dat Microsoft-personeel toegang heeft tot jouw data wanneer je hierom vraagt via een serviceaanvraag. Bekijk hiervoor de informatie over de Customer Lockbox op pagina 24 van deze handleiding. Wanneer je met Microsoft 365 werkt, geef je bepaalde diensten toestemming om jouw coderingssleutel te gebruiken om cloudservices met toegevoegde waarde te bieden, zoals eDiscovery, antimalware, antispam en zoekindexering. Dit heeft te maken met het feit dat documenten geïndexeerd worden voor zoekresultaten.

Wil je gebruik maken van Customer Key, dan heb je een aanvullende licentie (Customer Key) nodig. Deze zit in de volgende A5 bundels: Office 365 A5; Microsoft 365 A5 Compliance; Microsoft 365 A5 Info Protection & Governance.

Meer informatie over Customer Key vind je hier.

Er zijn uitzonderlijke situaties waarin gebruik van Customer Key niet leidt tot AVG compliance voor bijzondere persoonsgegevens. In dat geval wordt, om strikt aan de AVG te voldoen, het gebruik van Double Key Encryption (DKE) geadviseerd. Bij DKE worden er twee encryptiesleutels aangemaakt waarvan een door de school buiten de Microsoft cloud wordt bewaard. Daardoor kunnen ook opsporingsdiensten geen toegang meer krijgen tot data. Er kleven echter grote nadelen aan het gebruik van DKE omdat het een complex product is dat om een hoge ICT en Privacy volwassenheid vraagt van de organistie en de individuele gebruiker. DKE vraagt om:

- veel kennis rond beheer en inrichting van Microsoft 365 in je organisatie,
- heldere afspraken over governance op je tenant (wie is waarvoor verantwoordelijk),
- goed ingerichte processen rond toegang voor mensen en beheer van sleutels,
- een hoog privacy bewustzijn bij collega's,
- misschien wel de belangrijkste: een hoge privacy discipline van collega's (anders geformuleerd: iedereen moet zich ook echt 'veilig' gedragen).

Als je deze zaken niet op orde hebt is de kans erg groot dat het gebruik van DKE juist leidt tot een lager niveau van informatiebeveiliging en privacy. Voor meer informatie over de afweging van het gebruik van DKE, bekijk je ons visie document over het gebruik van DKE. In de kern komt dat advies erop neer dat scholen een plan moeten maken om hun informatiebeveiliging naar een heel hoog niveau te brengen. In dat plan zijn de opgesomde punten belangrijk en prioritair. Als die op orde zijn, is de implementatie van DKE de volgende stap.

Information Barriers

Wanneer je met verschillende onderwijsinstellingen in één omgeving werkt, staat standaard alles open en kan iedereen met elkaar communiceren. Op basis van groepen bepaal je uiteindelijk wie waar toegang tot heeft.

Als je de communicatie tussen twee groepen wilt beperken (bijvoorbeeld uit veiligheidsoverweging) kun je gebruikmaken van Powershell-scripts. Maar je kunt ook eens kijken naar Information Barriers. Dit is een vrij nieuwe dienst, die werkt binnen Microsoft Teams.

Je kunt met Information Barriers een scheiding maken tussen bijvoorbeeld onderwijs en zorg of tussen leerkrachten en leerlingen. De dienst voorkomt dat mensen bellen of chatten met gebruikers waar dat niet mee mag. Onderling communiceren of elkaar opzoeken wordt hiermee onmogelijk gemaakt.

Een ander voorbeeld is een organisatie met verschillende scholen in één tenant, waarbij je wilt voorkomen dat leerlingen van de ene school via de chat de leerlingen van de andere school benaderen. Iedere vorm van ongeoorloofde communicatie wordt door middel van Information Barriers geblokkeerd. Leerlingen kunnen hierdoor andere leerlingen (van een andere school) niet toevoegen. Wil je gebruik maken van Information Barriers, dan heb je een tegenwoordig geen aanvullende licentie meer nodig. De functionaliteit van Information Barriers zit tegenwoordig in de standaard A3 bundel. Meer informatie over Information Barriers vind je hier.

Vertrouwelijkheidslabels (Sensitivity labels)

Data kan zich bij (samen)werken in de cloud overal bevinden. Op verschillende apparaten, apps en services. Natuurlijk wil je alle data zo goed mogelijk beschermen. Met vertrouwelijkheidslabels classificeer je gegevens en bescherm je de toegang, zonder dat het de samenwerking belemmert.

Medewerkers kunnen handmatig een label aan een document koppelen. Een label kan een koptekst toevoegen of een watermerk, ook kun je in een label aangeven of bepaalde gebruikers deze documenten mogen openen of bewerken.

Als er een label op een document zit dat alleen internen dit document mogen openen, zal een externe, zelfs wanneer het bestand per ongeluk verstuurd wordt, deze niet kunnen openen. Het label blijft intact, ongeacht waar deze zich bevindt. Bij openen wordt gecontroleerd of de gebruiker toegang heeft, of zal zijn inloggegevens moeten invoeren. Heeft hij die niet, dan zal het document niet te openen zijn.

Met de Cloudbundel heb je de mogelijkheid om vertrouwelijkheidslabels in te stellen zodat gebruikers deze handmatig kunnen toevoegen. In combinatie met DLP (ook in de Cloudbundel) kun je zelfs instellen dat de gebruiker advies krijgt om de inhoud te labelen.

Wil je dat dit automatisch gebeurt, dan heb je een aanvullende licentie (rules-based auto classification) nodig. Als iets gevoelige informatie bevat, wordt het bestand herkend en automatisch gelabeld. Deze zit in de volgende A5 bundels: Office 365 A5; EM+S A5; Microsoft 365 A5 Compliance; Microsoft 365 A5 Info Protection & Governance.

Lees meer over vertrouwelijkheidslabels.

Zie de stappen voor gebruikers, hoe zij deze labels op documenten en e-mails kunnen toepassen.

Let op!

Werkt jouw organisatie al met vertrouwelijkheidslabels en ook met Power BI Pro? Zorg dan dat je de labels ook binnen Power BI aanzet. Hier is een aparte handeling voor nodig. Deze labels werken als volgt:
Wanneer Power BI-gegevens met een vertrouwelijkheidslabel worden geëxporteerd naar een Excel-, PowerPoint- of PDF-bestand, wordt het vertrouwelijkheidslabel meegestuurd. Als je geen toestemming hebt om iets te openen door dit label, kun je dit ook niet buiten Power-BI (in Excel-, PowerPoint- of PDF-apps) openen. Het label blijft dan intact.

Back-up

Microsoft heeft een aantal opties om dataverlies te voorkomen. Maar kun je dit ook zien als back-up? In de Microsoft Serviceovereenkomst staat onder paragraaf 6b letterlijk: *We raden aan dat u regelmatig een back-up maakt van Uw Inhoud en de Gegevens die u opslaat in de Diensten of opslaat door middel van Apps en Diensten van derden.*

Dit geeft duidelijk aan dat je zelf verantwoordelijk bent voor de inhoud van je tenant. Het is belangrijk om duidelijk te hebben hoe jullie als organisatie met bepaalde risico's van gegevensverlies om willen omgaan.

Microsoft biedt een aantal mogelijkheden om data te herstellen (de prullenbak van 90 dagen, retentielabels, etc.) die misschien voor jullie organisatie voldoende worden geacht. Maar standaard zit er géén back-up functie in Microsoft 365. Het is daarom de vraag of de dataherstel functie voor je organisatie voldoende is om je data te herstellen.

De mogelijkheden die Microsoft biedt om dataverlies te voorkomen

Standaard back-up: je kunt tot 14 dagen data (compleet) terug laten zetten. Dit duurt vaak enkele dagen. Het is niet mogelijk om een zogenaamde *point in time restore* uit te voeren. Ook is dit niet mogelijk voor enkele items (bricklevel restores), zoals een individuele mailbox.
Besef ook: deze back-up is bedoeld voor Disaster Recovery (voor Microsoft om aan SLA te voldoen, niet specifiek voor onderwijsorganisaties, dit voldoet mogelijk niet aan jullie behoefte).

Prullenbak: Er zijn meerdere prullenbakken. Wil je een verwijdering ongedaan maken, dan heb je de 2e prullenbak. Hier zit wel een limiet aan met betrekking tot het aantal dagen. Verwijderde SharePoint items worden maximaal 93 dagen bewaard. E-mail blijft beschikbaar tot de prullenbak geleegd wordt. De 2e prullenbak zal maximaal 30 dagen worden bewaard.
Goed om te weten: leegt een beheerder bewust de 2e prullenbak, dan is alles definitief weg.

Retentiebeleid: Hiermee stel je een bewaartermijn in (of een verwijdertermijn). Standaard is deze (zoals hierboven ook aangegeven) beperkt. E-mail blijft 30 dagen bewaard en SharePoint 93 dagen. Een medewerker die uit dienst gaat en waarvan de data wordt verwijderd, is dus binnen 30 dagen

alles kwijt wat in zijn/haar OneDrive en e-mail staat. In sommige gevallen is dat niet handig. Denk aan overname van werkzaamheden of wanneer je er later achterkomt dat zakelijke documenten in de OneDrive opgeslagen waren. Je kunt dit zelf verlengen en wij raden aan dit te doen. Goed om te onthouden: mocht je beheeraccount worden gehackt, dan is deze verlenging ook weer uit te zetten.

Als oplossing bestaat hier de **Preservation Lock** voor**.** Dit is een extra lock (bovenop het retentiebeleid) die niet meer te verwijderen is, een retentiebeleid daarentegen wel. Kijk goed waar je de Preservation Lock gebruikt**.** Besef ook dat je met een Preservation Lock niet kan voldoen aan de verwijderplicht van de AVG. Onthoud ook dat het retentiebeleid geen echte hersteloplossing of back-up is.

Versiebeheer: Versiebeheer kan maar 500 versies opslaan. Herstel je een item uit de prullenbak, dan heb je slechts één versie terug en kun je niet zien wie wat gedaan heeft in eerdere versies. Versiebeheer is een risico als je het hebt over de compliance. Maar is erg handig tijdens samenwerken.

Het kiezen voor het wel/niet maken van een (externe) back-up heeft alles te maken met de risico's en hoe je je omgeving ingeregeld hebt. De mogelijkheden die Microsoft standaard biedt voor dataverlies zijn voor sommige onderwijsorganisatie voldoende en bij andere juist niet.

Extra back-up: Als je tot de conclusie komt dat je een extra back-up wenst, denk dan ook na over de volgende vragen: van welke clouddiensten maken we gebruik (Parnassys, CITO)? Neemt de back-up oplossing dit ook mee? Zo nee, leg deze vraag bijvoorbeeld eens bij deze partijen neer om te horen wat zij hiervoor geregeld hebben.

Sommige documenten hebben een bewaarplicht, maar besef ook dat er een verwijderplicht* is. Hoe gaat je back-up daarmee om? Als een document niet meer in je bezit mag zijn, maar het is wel onderdeel van je back-up, is er dan een AVG-probleem? Denkt je back-up ook na over instellingen, versies en groepen? Wordt de back-up versleuteld opgeslagen?

Kortom: genoeg vragen om mee te nemen in de overweging. En besef ook: de ontwikkeling van Microsoft gaat in hoog tempo door. Evalueer de risico's elk jaar opnieuw. Waar je nu wel een externe back-up voor wenst, kan misschien in de toekomst geregeld worden binnen de omgeving.

**Volgens CNIL, de Franse toezichthouder op de AVG, hoeven organisaties geen back-ups te verwijderen als ze voldoen aan het recht om te wissen. Desalniettemin moeten ze de betrokkene duidelijk uitleggen dat back-ups gedurende een bepaalde tijd worden bewaard (zoals beschreven in het bewaarbeleid). Aan de verwijderplicht kun je ook voldoen met een procedure door niets uit de back-up te verwijderen, maar dit enkel te doen direct na het herstel het de data. Je moet dan uitleggen dat je technisch niet in staat bent om je back-upbestanden aan te passen waardoor je een procedure hebt om verwijderde gegevens te verwijderen na een herstel.*

Vragen?

Heb je nog vragen of opmerkingen? Neem dan gerust contact op met onze Servicedesk. Wij zijn iedere werkdag bereik via 030 – 28 56 870 of info@apsitdiensten.nl.

Tip!

Bekijk ook onze meestgestelde vragen in onze FAQ over Microsoft en de AVG, naar aanleiding van ons webinar hierover.

APS IT-diensten
Zwarte Woud 2
3524 SJ Utrecht

www.apsitdiensten.nl

T 030 2856 870
M info@apsitdiensten.nl