SIVON

Overzicht van te nemen maatregelen om de privacyrisico's uit de DPIA Microsoft Teams, OneDrive en SharePoint te beperken

In de onderstaande tabel zijn de maatregelen die scholen moeten nemen overgenomen uit het DPIA rapport zoals vermeld in hoofdstuk 17.1.2 “Measures government organisations and universities must take to mitigate the risks”. De 7 risico’s kunnen met 20 maatregelen gemitigeerd worden.

Risico	L/ H*	Maatregel uit DPIA	In het Nederlands	Implementatie
Structural transfer of Telemetry Data to the USA (until December 2022)	L	Accept the temporary risk of the transfer of the pseudonymised Telemetry Data while Microsoft is building its EU Data Boundary.	Verlies van controle en heridentificatie van pseudonieme persoonsgegevens door de structurele doorgifte van telemetriegegevens naar de VS.	SIVON gaat de voortgang monitoren en scholen informeren wanneer Microsoft deze aanpassing doorgevoerd heeft. SIVON doet dit in samenwerking met SURF/APS IT-diensten/SLBdiensten/SLMrijk. Accepteer het tijdelijke risico. Meer informatie over data boundery
Content Data processed in the EU accessible for	H	Enable E2EE in Teams for 1-on-1 conversations	Risico’s van doorgifte van persoonsgegevens naar de VS bij spontane 1 op 1	Deze maatregelen zijn alleen nodig bij de uitwisseling van gevoelige of bijzondere persoonsgegevens. Mitigeren kan door: • Geen gevoelige en bijzondere persoonsgegevens uit te wisselen (behalve via spontane 1 op 1 gesprekken in Teams waarbij E2EE aan staat)

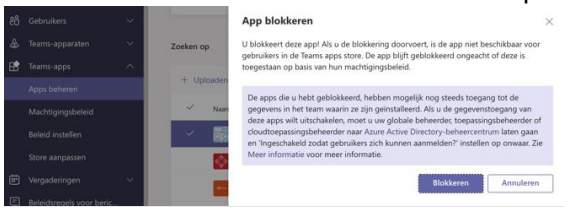
Microsoft if not E2EE		Do not exchange sensitive or special categories of data via Teams calls that are not end-to-end encrypted	gesprekken via Teams	• E2EE implementeren zoals hieronder beschreven voor 1-op-1 gesprekken in Teams • Een andere applicatie gebruiken of "live" gesprek voeren **Voor implementatie van de maatregelen kunt u extra licenties nodig hebben**
Content Data processed in the EU accessible for Microsoft if not E2EE	H	Enable E2EE in Teams for all meetings and chats as soon as Microsoft makes this available. Do not exchange sensitive or special categories of data via Teams calls that are not end-to-end encrypted	Risico's van doorgifte van persoonsgegevens naar de VS bij geplande gesprekken via Teams	Deze maatregelen zijn alleen nodig bij de uitwisseling van gevoelige of bijzondere persoonsgegevens. Mitigeren kan door: • Geen gevoelige en bijzondere persoonsgegevens uit te wisselen via Teams (behalve via spontane 1 op 1 gesprekken in Teams waarbij E2EE aan staat) • Een andere applicatie gebruiken of "live" gesprek voeren Het is pas veilig om gevoelige en bijzondere persoonsgegevens uit te wisselen als E2EE beschikbaar en geimplementeerd is. SIVON informeert u wanneer Microsoft E2EE in Teams doorgevoerd heeft. Monitoring van de voortgang bij Microsoft doet SIVON in samenwerking met SURF/APS IT-diensten/SLBdiensten/SLMrijk. **Voor implementatie van de maatregelen kunt u extra licenties nodig hebben.**
Ongoing incidental transfer of usernames / e-mail addresses	L	Consider the use of pseudonyms in the Azure AD for employees whose work	Overweeg het gebruik van pseudoniemen voor werknemers waarvan de	Stel beleidsregels op voor het niet gebruiken van persoonsgegevens in bestands- en padnamen. Dit is een algemeen advies. Dit advies zou u ook kunnen toepassen bij andere Amerikaanse leveranciers.

/ pathnames OneDrive to the USA		identity must remain confidential. Use pseudonyms when the Azure AD is used for Single Sign On with external suppliers for employees whose work identity must remain confidential.	identiteit vertrouwelijk is, ook bij gebruik van de Azure AD als Single Sign On naar diensten van andere bedrijven.	
Ongoing incidental transfer of usernames / e-mail addresses / pathnames on OneDrive to the USA	L	Create a Teams and OneDrive privacy policy for internal users and guest users, establish a policy for the sharing of files and images. Make employees and guest users accept these rules through Terms &	Gebruik Azure AD functionaliteit om gebruikers te wijzen op het geldende beleid.	Zorg ervoor dat gebruikers relevante disclaimers voor juridische vereisten of nalevingsvereisten te zien krijgen. Dit kunt u instellen met Azure AD.

		Conditions imposed by Azure AD.		
Loss of control, loss of confidentiality: undue access by US government authorities to Content Data	H	Use Double Key Encryption for documents with sensitive and special categories of data stored in SharePoint/OneDrive (including Teams recordings). Use Customer Lockbox for other stored personal data.	Er bestaat een hoog risico voor het delen van gevoelige en bijzondere persoonsgegevens via Microsoft Teams, SharePoint of OneDrive Online.	Deze maatregelen zijn alleen nodig bij de opslaan van gevoelige of bijzondere persoonsgegevens in OneDrive en SharePoint. U kunt verschillende dingen doen • Sla geen gevoelige of bijzonder persoonsgegevens op in SharePoint of OneDrive. • Implementeer een andere vorm van “bring your own key”. • Implementeer DKE van Microsoft voor (een beperkte groep) gebruikers en voor een specifieke set gevoelige data. SIVON is in overleg met partijen over uitleg en werking van double-key encryption oplossingen en DKE van Microsoft. Onder deze tabel wordt een toelichting gegeven op double-key encryption.
Possible accessfrom the USA to audit logs, Azure AD and Telemetry Data processed	L	Do not use SMS for authentication to prevent the transmission of unencrypted cell phone numbers. Instead, use	Gebruik geen SMS voor authenticatie om de overdracht van onversleutelde mobiele telefoonnumm	Handleiding voor het instellen van Authenticator

and stored in the EU after 2022		the Authenticator app or a hardware token.	ers te voorkomen.	
Difficulty to exercise data subject access rights to Required Service Data	L	Regularly use the Data Viewer Tool when and where available, and compare the results with Microsoft's public documentation.	Voor het correct uitvoeren van rechten van betrokkenen (recht op inzage etc.), kan de Data Viewer Tool gebruikt worden. Advies is om deze tool regelmatig te testen zodat beheerders op de hoogte zijn van de mogelijkheden.	Voor het correct uitvoeren van rechten van betrokkenen (recht op inzage etc.), kan de Data Viewer Tool gebruikt worden. Advies is om deze tool regelmatig te testen zodat beheerders op de hoogte zijn van de mogelijkheden.
Lack of transparency Telemetry Data	L	Use Microsoft's DSAR* tool to obtain access to diagnostic	Voor het correct uitvoeren van rechten van betrokkenen	Voor het correct uitvoeren van rechten van betrokkenen (recht op inzage etc.), kan de Data Viewer Tool gebruikt worden. Advies is om deze tool regelmatig te testen zodat beheerders op de hoogte zijn van de mogelijkheden.

		data, and compare with an occasional network traffic analysis. * data subject access request	(recht op inzage etc.), kan de Data Viewer Tool gebruikt worden. Advies is om deze tool regelmatig te testen zodat beheerders op de hoogte zijn van de mogelijkheden.	
Difficulty to exercise data subject access rights to Required Service Data	L	Support a specific audit by SLM Rijk on Microsoft's collection and use of the *Required Service Data*.		Deze audit komt ter zijnder tijd beschikIbaar op het portaal van SLMrijk. In samenwerking met SLMrijk/APS IT-diensten/SURF/SLBdiensten houdt SIVON u op de hoogte houden van de uitkomst van deze audit.
Lack of control: personal data shared with Microsoft	L	Disable the Additional Optional Connected Experiences in Office365.	Oneigenlijke verdere verwerking door derde partijen zoals Bing giphy en Linkedin.	Zie beschrijving hoe u deze maatregel moet implementeren In de handleiding van APS IT-diensten staat een uitgebreide uitleg.

and third parties as controllers				
Lack of control: personal data shared with Microsoft and third parties as controllers	L	Disable access to third party applications in the app store in Teams.	Oneigenlijke verdere verwerking door derde partijen.	In admin.teams.microsoft.com kunt u third party apps blokkeren. 
Lack of control: personal data shared with Microsoft and third parties as controllers	L	Warn end users not to insert images into SharePoint via the built-in Bing search engine for the next six months. Make sure that no traffic is sent to third parties when the admin has disabled the Controller	Oneigenlijke verdere verwerking door derde partijen.	Actie voor scholen om gebruikers te informeren. SIVON gaat scholen informeren wanneer Microsoft deze aanpassing doorgevoerd heeft. Monitoring van de voortgang bij Microsoft doet SIVON in samenwerking met SURF/APS IT-diensten/SLBdiensten/SLMrijk.

		Connected Experiences. By the end of Q2 2022 all traffic to Bing should be removed from SharePoint Online when the organisation has disabled the Controller Connected Experiences. Microsoft must still take action to prevent any traffic to Cloudflare on Microsoft support pages that are accessed from links in Teams settings on the different platforms.		
Employee monitoring system:	L	Disable most of the functions in	Personeelsvolg-systeem: chilling effect.	In admin.microsoft.com gaat u naar instellingen -> organisatie instellingen -> selecteer Microsoft Viva insight en disable alle opties. (zie ook afbeelding hieronder). Indien u deze functionaliteit toch (deels) wilt gebruiken: voer dan eerst een DPIA uit

chilling effect		Teams Analytics & reports, and turn on the pseudonymisation option: do not enable Viva Advanced Insights.		
Employee monitoring system: chilling effect	L	Create a policy to prevent use of Teams Analytics & reports as an employee monitoring tool. Conduct a DPIA prior to use of these analytic tools, certainly when used in combination with another Microsoft Windows & Office Analytical services.	Personeelsvolg-systeem: chilling effect.	Zie hierboven

Lack of transparency Telemetry Data	L	Set the telemetry collection in installed applications to the lowest “Neither” level.	Verlies van controle en gebrek aan transparantie over de telemetriegegevens	Telemetry instellingen Zie handleiding van APS IT-diensten https://apsit.sharepoint.com/sites/externen/Docs/Microsoft/Handleidingen/Microsoft%20365%20en%20AVG/Microsoft%20365%20en%20AVG.pdf
Lack of transparency Telemetry Data	L	Set telemetry collection in Windows to the lowest "security" level.	Verlies van controle en gebrek aan transparantie over de telemetriegegevens	Dit is een oude - hopelijk reeds door scholen geïmplementeerde - maatregel. Zie https://aanpakibp.kennisnet.nl/app/uploads/DPIAs-Microsoft.pdf en https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization Of https://apsit.sharepoint.com/sites/externen/Docs/Microsoft/Handleidingen/Microsoft%20365%20en%20AVG/Microsoft%20365%20en%20AVG.pdf
Minimise data and risk of acces to data outside EU	L	Disclose retention period policies and enforce compliance, delete outdated data (to mitigate the risks of access from the U.S.A.)	Maak bewaartermijnen-beleid bekend en dwing naleving af, verwijder verouderde gegevens (om de risico's van toegang vanuit de VS te beperken).	De scholen moet haar eigen bewaartermijnenbeleid opstellen en dan toetsen of de bewaartermijnen van Microsoft voldoen aan haar beleid. Zo nodig iets regelen om de data lang genoeg te bewaren. Denk er bijvoorbeeld aan dat er kortere Microsoft bewaartermijnen gelden na het opzeggen van je Microsoft contract. Scholen moeten betrokkenen informeren over bewaartermijnen. In de tabel hieronder staan de standaard bewaartermijn die Microsoft hanteert.
Ongoing incidental	L	Establish policies to	Geen namen van leerlingen	Stel beleidsregels op voor het niet gebruiken van persoonsgegevens in bestands- en padnamen. Dit is een algemeen advies. Dit advies zou u ook kunnen toepassen bij andere Amerikaanse leveranciers.

transfer of usernames / e-mail addresses / pathnames OneDrive to the USA		prevent file names and file paths from containing personal data.	of medewerkers opnemen in de bestandsnaam of directorynaam.	
Lack of transparency Telemetry Data	L	Inform employees about their access possibilities via the Data Viewer tool, or by filing a DSAR with the admin of their organisation.	Informeer medewerkers over de inzagemogelijkheden via de Data Viewer tool en door een inzageverzoek in te dienen bij de beheerder(s) van de organisatie	Informeer leerlingen, hun ouders en medewerkers over hun rechten, zoals het recht op inzage. Dit staat doorgaans al in het privacyreglement van de school.

*L= laag risico H= hoog risico

Double Key Encryption (DKE)

DKE is een vorm van encryptie waarbij u zelf de sleutel beheert. Met dubbele sleutelversleuteling worden uw gegevens versleuteld met twee sleutels. Uw versleutelingssleutel is in uw beheer en de tweede sleutel wordt opgeslagen in Microsoft Azure
https://docs.microsoft.com/nl-nl/microsoft-365/compliance/double-key-encryption-overview
De implementatie en gebruik van DKE is vrij complex.

Voor double key encryption zijn aanvullende Microsoft licenties nodig, te weten een compliance add-on of een A5 pakket.

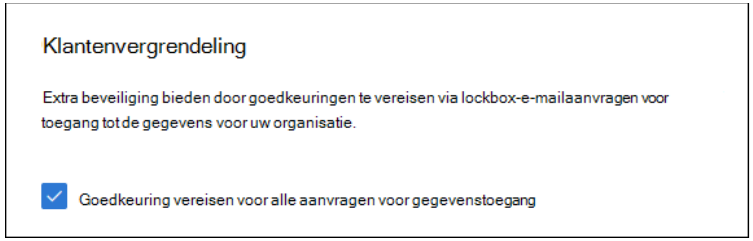
DKE is alleen te gebruiken op de geïnstalleerde desktop versies van Word, PowerPoint en Excel op Windows.
Met DKE werkt content search in onedrive en sharepoint niet.
Virusscanners kunnen bijlagen blokkeren omdat ze de encrypted file niet kunnen scannen
Meer info over DKE.

LET OP: wees voorzichtig met volledige implementatie van DKE. Dit geeft weer nieuwe risico's. Als u systemen te veel dichttimmert ontwijken gebruikers de maatregelen. DKE is complex voor gebruikers. Gaat er iets mis met de encryptie codes dan is er geen enkele mogelijkheid om de data terug te halen. Daarnaast is delen van bestanden niet (volledig) mogelijk en levert het scannen van versleutelde bestanden problemen op. https://blogs.microsoft.com/datalaw/our-practices/

Customer lockbox
Customer Lockbox is geen oplossing om toegang tot data door de Amerikaanse veiligheidsdiensten te blokkeren. Customer lockbox is gericht op service ondersteuning door Microsoft. Customer Lockbox zorgt ervoor dat Microsoft geen toegang heeft tot uw inhoud om servicebewerkingen uit te voeren zonder uw expliciete goedkeuring. Met Customer Lockbox wordt u betrokken bij het goedkeuringsproces dat door Microsoft wordt gebruikt om ervoor te zorgen dat alleen geautoriseerde aanvragen toegang tot uw inhoud verlenen.
U heeft twee opties

1) U zet customer lockbox aan zoals hier beschreven
2) U voorkomt in uw beleid dat gebruikers zelf support gaan aanvragen bij Microsoft

Ga naar admin.microsoft.com Kies Instellingen > Org Instellingen > Security & Privacy.
Selecteer Beveiligingsgegevens & privacy en selecteer vervolgens Klantenvergrendeling in de linkerkolom. Schakel het selectievakje Goedkeuring vereisen voor alle aanvragen voor gegevenstoegang in en sla de wijzigingen op om de functie in te zetten.
Voor customer lockbox is een A5 licentie nodig.



End to End Encryptie (E2EE)

Om E2EE encryptie te gebruiken moet deze eerst geactiveerd worden in de tenant voordat gebruikers zelf een slotje op het gesprek kunnen zetten.

Volg deze instructies voor tentant instellingen om E2EE de activeren Vóór het gesprek moeten beide personen het volgende doen:

1. Selecteer in Teams meer opties naast uw profielafbeelding en selecteer vervolgens Instellingen.

2. Selecteer Privacy aan de linkerkant en selecteer vervolgens de schakelknop naast End-to-end versleutelde oproepen om deze in te schakelen.

Voor implementatie van de maatregelen kunt u extra licenties nodig hebben

Wat zijn bijzondere en gevoelige persoonsgegevens in teams gesprekken?
In de Toelichting over de DPIA [Toelichting DPIA op Microsoft Teams, OneDrive en SharePoint - SIVON], wordt uitgelegd wat bijzondere en gevoelige persoonsgegevens zijn. De hoge risico's die in de DPIA genoemd worden, gelden voor gevoelige en bijzondere persoonsgegevens. Bij het gebruik van 'gewone' persoonsgegevens is het oordeel in de DPIA dat dit minder impact heeft op de privacy van de gebruikers. Bij gevoelige en bijzondere persoonsgegevens is dat anders. Het gebruik van bijzondere persoonsgegevens is standaard niet toegestaan tenzij je een beroep kunt doen op een uitzondering. Voor het onderwijs geldt bijvoorbeeld dat gezondheidsgegevens alleen gebruikt mogen worden als dat noodzakelijk is voor het leren en begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands privacy ernstig kan beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lid van een vakbond, ras of etnische afkomst. Bij gevoelige gegevens op school gaat het volgens de Autoriteit Persoonsgegevens (AP) om gegevens die snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie,

gezondheid of zelfs mishandeling. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden volgens de AP zwaardere eisen gesteld aan de beveiliging van de gegevens.

Het is dus niet de bedoeling om ziektelijstjes of roddels over bijzondere kenmerken van mensen uit te wisselen in Teams, maar dat mag ook niet op het prikbord in de kantine, en ook niet in mails aan alle leden van een afdeling. Er verandert dus niet zo heel veel.

Het kan voorkomen dat er zichtbare gezondheids- of geloofskenmerken zichtbaar zijn van deelnemers aan een Teams-overleg. De Autoriteit Persoonsgegevens past een doelcriterium toe bij de uitleg wanneer foto's bijzondere persoonsgegevens zijn. Kort samengevat: als het niet de bedoeling is om onderscheid te maken naar bijzondere kenmerken, zijn het géén bijzondere persoonsgegevens.

De AP schrijft op haar website dat er situaties zijn waarin door het maken en publiceren van foto's of filmpjes wel bijzondere persoonsgegevens worden verwerkt. Als voorbeeld noemt de AP een leraar die foto's maakt van een sessie waarin kinderen aan het bidden zijn en deze foto's deelt op de website om aan de buitenwereld te laten zien hoe de school het geloof naleeft. Een school verwerkt geen géén bijzondere persoonsgegevens in beeldmateriaal als alle 3 de volgende punten gelden:

- Het beeldmateriaal is niet gericht op bijzondere persoonsgegevens of het maken van onderscheid op basis van deze gegevens.
- Het is voor redelijkerwijs ook niet te voorzien dat iemand onderscheid zal maken op basis van het beeldmateriaal.
- Het is onvermijdelijk dat bijzondere persoonsgegevens in beeld komen in het beeldmateriaal.

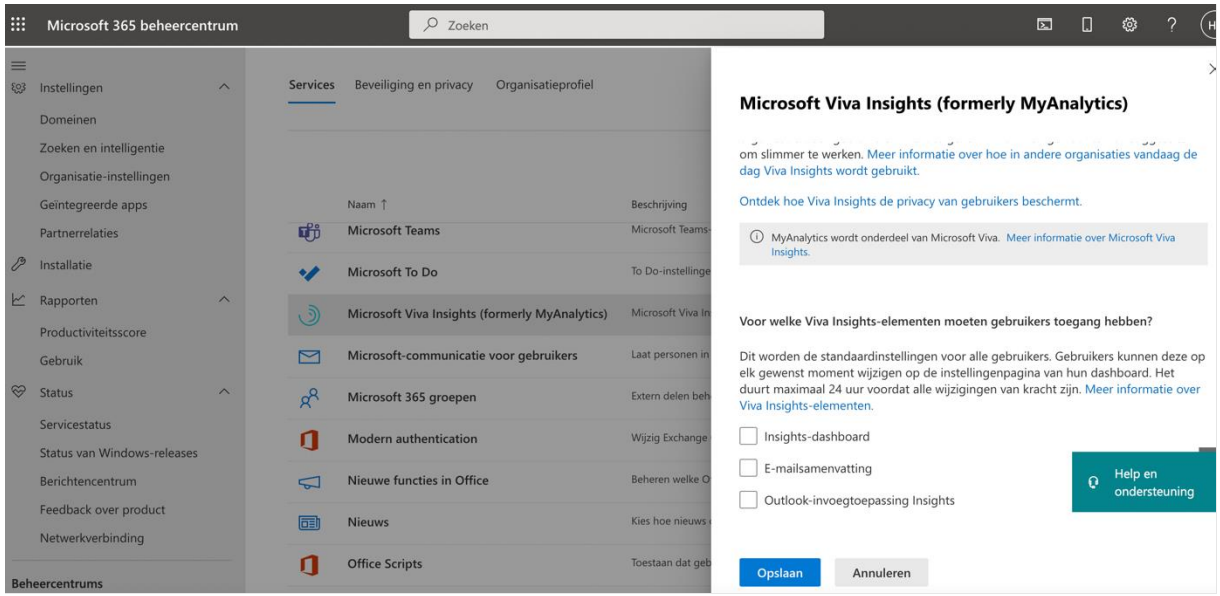
Om te zorgen dat instellingen deze drie spelregels naleven geven wij organisaties de volgende adviezen:

- Schotel nieuwe of externe deelnemers een pop-up voor met spelregels die de deelnemers moeten accepteren, over de omgang met persoonsgegevens. Bijvoorbeeld: deel niet ongevraagd persoonsgegevens in de chat, deel geen vertrouwelijke bestanden, gebruik geen persoonsgegevens in pad- of bestandsnamen. Dat kan via de Azure AD. Dat is de laatste tip bij het eerste hoge risico: *Create a Teams and OneDrive privacy policy for internal users and guest users, set rules for sharing of files and images. Make employees and guest users accept these rules through Terms & Conditions imposed by Azure AD.*
- Wijs deelnemers voor de meeting op de mogelijkheid om hun camera uit te zetten als zij het vervelend vinden om zichtbaar in beeld te komen, tenzij het absoluut nodig is dat deelnemers in beeld zijn.
- Maak beleid of, en in welke gevallen, het noodzakelijk is om de vergadering op te nemen, en bepaal een bewaartermijn. Microsoft schrijft op https://docs.microsoft.com/en-us/microsoftteams/cloud-recording dat het volgens haar klanten bijna nooit gebeurt dat opnames ouder dan 60 dagen worden teruggekeken. Microsoft schrijft: "*Customers have provided overwhelming feedback that they want more controls to reduce storage clutter created from Teams meeting recordings, 99% of which, on average, are never rewatched after 60 days.*"
- Neem bij een opname niet de galerij met deelnemers op, en niet de chats.

Deze afwegingen over de grondslagen van de gegevensverwerking gaat vooraf aan de risico-afweging over de doorgifte van bijzondere persoonsgegevens via Teams, OneDrive of SharePoint Online.

Als het toch nodig is om bijzondere persoonsgegevens uit te wisselen, of hele gevoelige informatie zoals informatie over kinderen, locatiegegevens of financiële gegevens, dan moet de organisatie end-to-end-encryptie gebruiken om (de hele kleine kans) uit te sluiten dat de Amerikaanse opsporings- en inlichtingendiensten toegang krijgen tot de data. Die versleuteling-met-eigen-sleutel bestaat al wel voor spontane (niet via Outlook geplande) 1-op-1-Teams gesprekken, maar nog niet voor groepsgesprekken. Dat gaat Microsoft wel op termijn mogelijk maken, maar daar is nog geen deadline voor bekend.

Afbeelding voor het uitzetten van MyAnalytics aka Viva Insights



Bewaartermijnen

Informatie over het aanpassen van bewaartermijnen staat in de handleiding van APS IT-diensten
https://apsit.sharepoint.com/sites/externen/Docs/Microsoft/Handleidingen/Microsoft%20365%20en%20AVG/Microsoft%20365%20en%20AVG.pdf

Type data	Bewaartermijn
Gebruikers data	30 dagen nadat de beheerder de data verwijderd heeft of 180 dagen na het verlopen van de licentie.
Chats in Teams	6 maanden. Deze periode kan aangepast worden door de beheerder. https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide#retention-policy-for-teams-locations
Persoonsgegevens	180 dagen
Tot persoon herleidbare gegevens	30 tot 180 dagen. In OneDrive 30 dagen
Azure AD MFA slaat geen persoonsgegevens op, maar UserObjectId is te herleiden tot inlog poging van een persoon	Logging data wordt 30 dagen bewaard.

Versie 1.0 (3 maart 2022)