**Checklist maatregelen**

**Naar aanleiding van DPIA Microsoft Teams-OneDrive-Sharepoint**

Versie: 1.1 (12 mei 2022)

*Let op: Deze versie wordt regelmatig herzien, download de laatste versie op www.privacyopschool.nl*

Naam schoolbestuur:

*Invullen*

Datum:

*Invullen*

Naam invuller:

*Invullen*

## Uitleg checklist

Uit een nieuwe Data Protection Impact Assessment (DPIA) uitgevoerd door SURF, SLM Rijk en Privacy Company zijn privacy risico’s naar voren gekomen bij het gebruik van Microsoft Teams, Onedrive en Sharepoint. Naar aanleiding hiervan heeft SIVON een handleiding beschikbaar gesteld met te nemen maatregelen. Deze checklist van Privacy op School is een middel voor onderwijsinstellingen om vast te leggen welke van deze maatregelen genomen zijn of wat de status is. De onderwijsinstelling kan deze checklist zelf aanvullen/wijzigen en vervolgens gebruiken om bijvoorbeeld de eigen Functionaris voor de Gegevensbescherming te informeren.

De checklist is opgesteld naar aanleiding van informatie gepubliceerd door SIVON in maart 2022. De checklist van Privacy op School is geenszins bedoeld als uitputtende lijst met maatregelen, adviesdocument of vervanging van de SIVON informatie. Het is aan te bevelen dat de onderwijsinstelling de gebruikte bronnen zelf nog raadpleegt voor de laatste informatie. Zie hiervoor de bronvermelding.

## Geconstateerde risico's

Uit de DPIA komt een aantal privacy risico’s naar voren met betrekking tot de uitwisseling en opslag van gevoelige en bijzondere persoonsgegevens. Namelijk:

1. Doorgifte van bijzondere en gevoelige gegevens buiten de EER, waar een lager beschermingsniveau geldt dan AVG (met als theoretisch mogelijk gevolg inzage in de gegevens door Amerikaanse overheidsdiensten)
2. Verlies van controle en her- identificatie van pseudonieme persoonsgegevens door de structurele doorgifte van telemetriegegevens[[1]](#footnote-2) naar de VS.
3. Verlies van controle en oneigenlijke verdere verwerking vanwege de incidentele verwerking van padnamen, gebruikersnamen en e-mailadressen in specifieke telemetrieberichten over OneDrive.
4. Verlies van controle en gebrek aan transparantie over de telemetriegegevens uit de browser, en over het gebruik van zogenaamde ‘Verbonden Ervaringen’ (Connected Experiences’).
5. Beperkingen op het recht van inzage voor betrokkenen.
6. Oneigenlijke verdere verwerking door derde partijen.
7. Personeelsvolgsysteem: chilling effect.

## Organisatiespecifieke risico’s (zelf aan te vullen)

Het is mogelijk dat er nog meer privacy risico’s spelen bij het gebruik van Microsoft Teams, Onedrive en Sharepoint door de onderwijsinstelling. Deze organisatiespecifieke risico’s kunnen hier worden toegevoegd. Er kunnen bijvoorbeeld risico’s ontstaan doordat:

* Er geen backup wordt gemaakt van informatie;
* Er geen goedgekeurd en geïmplementeerd toegang- of autorisatiebeleid is;
* Tweefactorauthenticatie niet in gebruik is;
* Er geen gebruik gemaakt wordt van beveiligd mailen;
* *Etc.*

Aanvullende risico’s bij de onderwijsinstelling zijn:

*Invullen*

## Te nemen organisatorische maatregelen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Omschrijving** | **Kruis aan indien uitgevoerd** | **Toelichting hoe maatregel wordt uitgevoerd of motivatie waarom deze (nog) niet wordt uitgevoerd** | **Datum uitgevoerd of plandatum uitvoering** |
| **O-1** | Activeer centraal[[2]](#footnote-3) de mogelijkheid om end-to-end encryption (E2EE) in te schakelen.  *NB. E2EE is alleen in te schakelen voor spontane (niet geplande) één op één gesprekken in Teams.* |  |  |  |
| **O-2** | Instrueer medewerkers om: - (E2EE) in te schakelen voor één-op-één gesprekken in Teams als ze gevoelige en bijzondere persoonsgegevens uitwisselen.  *NB. Dit is alleen mogelijk indien O-1 is uitgevoerd.* - geen gevoelige en bijzondere persoonsgegevens uit te wisselen in geplande bijeenkomsten in Teams. |  |  |  |
| **O-3** | Stel privacy beleidsregels op voor medewerkers en gastgebruikers voor het niet gebruiken van persoonsgegevens in bestands- en mapnamen, het delen van bestanden en afbeeldingen en ten aanzien van het gebruik van gevoelige en bijzondere persoonsgegevens in Teams, OneDrive en Sharepoint (zie ook T-1). |  |  |  |
| Zorg ervoor dat deze gebruikers de privacy beleidsregels te zien krijgen en dit accepteren.  *NB. De beleidsregels kunnen getoond worden aan de gebruiker via een pop-up. Dit is in te stellen via Azure AD.* |  |  |  |
| **O-4** | Informeer leerlingen, ouders, medewerkers over hun privacy rechten, zoals het recht op inzage. Neem dit op in het privacyreglement of de -verklaring.  *NB. Betrokkenen kunnen controleren welke gegevens worden verzameld via de Data Viewer Tool van Microsoft (relevant in geval van inzageverzoek).* | ☐ |  |  |
| **O-5** | Maak beleid voor bewaren, opschonen en verwijderen van verouderde gegevens. |  |  |  |
| **O-6** | Maak beleid om het gebruik van Teams Analytics & Reporting als een controlemiddel voor werknemers te voorkomen. | ☐ |  |  |
| **O-7** | Zorg dat gebruikers van Sharepoint geen afbeeldingen insluiten via de ingebouwde Bing zoekmachine door hier instructies over te geven.  *NB. Dit geldt totdat de functionaliteit in juli 2022 is uitgeschakeld.* | ☐ |  |  |
| **O-8** | Instrueer medewerkers dat Teams gesprekken niet mogen worden opgenomen wanneer er bijzondere of gevoelige persoonsgegevens worden gedeeld. | ☐ |  |  |
| ***O-9*** | *Zelf aan te vullen o.b.v. organisatiespecifieke risico’s* |  |  |  |
| **…** | *…* |  |  |  |

## Te nemen technische maatregelen**[[3]](#footnote-4)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Omschrijving** | **Kruis aan indien uit te voeren** | **Toelichting hoe maatregel wordt uitgevoerd of motivatie waarom deze (nog) niet wordt uitgevoerd** | **Datum uitgevoerd of plandatum uitvoering** |
| **T-1** | Sla geen gevoelige en bijzondere persoonsgegevens op in OneDrive en SharePoint. | ☐ |  |  |
| Alternatief: Versleutel documenten met gevoelige of bijzondere persoonsgegevens die zijn opgeslagen in SharePoint en OneDrive met een eigen sleutel (key), zoals Microsoft Double Key Encryption (DKE).  *NB. Dit is alleen mogelijk met A5 licentie of een aanvullend product.* | ☐ |  |  |
| **T-2** | Gebruik twee factor authenticatie via de Microsoft Authenticator-app of een hardware token om toegang te krijgen tot je account, i.p.v. SMS verificatie per telefoon. | ☐ |  |  |
| **T-3** | Schakel centraal de ‘Additional Optional Connected Experiences’ in Office365 uit. | ☐ |  |  |
| **T-4** | Schakel centraal toegang uit tot ‘third party applications’ in the app store in Teams. | ☐ |  |  |
| **T-5** | Zet centraal de functionaliteit van Teams Analytics & Reporting en MS Viva Insights uit. Schakel de pseudonimisering optie in. | ☐ |  |  |
| Alternatief: Mocht er toch besloten worden deze tools te gebruiken voer dan eerst een Data Protection Impact Assessment (DPIA) uit. | ☐ |  |  |
| **T-6** | Stel centraal telemetrie in op het basisniveau. | ☐ |  |  |
| **T-7** | Overweeg om accounts te creëren met een pseudoniem voor medewerkers van wie de identiteit vertrouwelijk moet blijven.  *NB. Dit heeft betrekking op de pseudonimisering in de (Azure) Active Directory.* | ☐ |  |  |
| **T-8** | Maak beleid om te voorkomen dat gebruikers zelf support aanvragen bij Microsoft. | ☐ |  |  |
| Alternatief: Zet centraal ‘Customer lockbox’ aan en schakel de goedkeuring voor alle aanvragen voor gegevenstoegang in.  *NB. Dit is alleen mogelijk met A5 licentie.* | ☐ |  |  |

## Meer informatie en bronnen:

* <https://www.sivon.nl/app/uploads/2022/03/Maatregelen-Microsoft-Teams-OneDrive-SharePoint.pdf>
* <https://www.sivon.nl/actueel/veelgestelde-vragen-over-privacytoets-op-microsoft-teams-onedrive-en-sharepoint/>
* <https://www.sivon.nl/actueel/privacytoets-op-microsoft-teams-onedrive-sharepoint/>

## Definities

*Bijzondere persoonsgegevens:*

Gegevens die apart in de AVG zijn genoemd waarbij het gebruik hiervan standaard is verboden, tenzij je een beroep kunt doen op een uitzondering. Gegevens zijn bijzonder omdat het gebruik hiervan iemands privacy ernstig kan beïnvloeden. Bijvoorbeeld gezondheidsgegevens.

*Gevoelige persoonsgegevens:*

Gegevens die snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Er kunnen conclusies aan worden verbonden met gevolgen voor het latere maatschappelijke leven. Bijvoorbeeld leerresultaten van kinderen, grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie, gezondheid of zelfs mishandeling.

*E2EE:*

End-to-end encryption/ end-to-end-versleuteling. Dit is het versleutelen van berichten zodat een ander dan de zender en ontvanger de inhoud van het bericht niet kan lezen.

*DKE:*

Double Key Encryption / dubbele versleuteling. Met dubbele sleutelversleuteling voor Microsoft 365 kun je zeer gevoelige gegevens beveiligen om te voldoen aan gespecialiseerde vereisten. Het helpt om de volledige controle over de versleutelingssleutels te behouden. Er worden twee sleutels gebruikt om gegevens te beveiligen: een sleutel in het besturingselement en een tweede sleutel die veilig is opgeslagen in Microsoft Azure. Als je gegevens wilt weergeven die zijn beveiligd met dubbele sleutelversleuteling, hebt je toegang tot beide sleutels nodig. Aangezien Microsoft slechts één van deze sleutels kan openen, blijven beveiligde gegevens ontoegankelijk voor Microsoft, zodat je volledige controle hebt over de privacy en beveiliging van uw gegevens.

1. Dit zijn gegevens over de aangesloten hardware (zoals printers of modems), de software op het apparaat (inclusief apps en de browser Edge) en het gebruik van die software. [↑](#footnote-ref-2)
2. Met ‘centraal’ wordt hier(na) bedoeld dat de instelling via de beheeromgeving binnen Microsoft kan worden aangepast. De admin kan deze instelling doorvoeren activeren zodat gebruikers individueel de instelling te zien krijgen en kunnen toepassen (O-2). [↑](#footnote-ref-3)
3. Vraag uw ICT-leverancier om ondersteuning. [↑](#footnote-ref-4)