Veelgestelde vragen DPIA op Microsoft OneDrive, SharePoint en Teams

Wat was de scope van de DPIA?
De DPIA die in opdracht van SURF en het ministerie van Justitie en Veiligheid is uitgevoerd, betrof de online versies van Microsoft Teams, Microsoft SharePoint en Microsoft OneDrive. De resultaten van dit onderzoek betreffen dus alleen deze oplossingen en zeggen daarmee niets over andere oplossingen van Microsoft of de 'on-premises' oplossingen van deze applicaties.

Kan mijn instelling deze oplossingen nog wel blijven gebruiken?
Ja, maar er zullen door de beheerders van uw omgeving wel maatregelen getroffen moeten worden. SURF zorgt voor een gedetailleerde uiteenzetting van deze maatregelen en zet deze online.

Moet mijn instelling zelf iets doen?
De DPIA heeft zes lage risico's en één hoog risico vastgesteld. De zes lage risico's zijn pas 'laag' na het doorvoeren van de maatregelen zoals aanbevolen in de DPIA. Het hoge risico valt momenteel niet technisch op te lossen. Hiervoor dient de beheerder van de instelling een instructie te geven aan de betrokken gebruikers/medewerkers.

Wat is het hoge risico precies?
Het hoge risico doet zich in beperkte gevallen voor bij Teams. Indien men een geplande afspraak in Teams heeft, dan is dat gesprek niet end-to-end encrypted (E2EE). Vanwege de theoretische mogelijkheid dat (Amerikaanse) opsporings- en inlichtingendiensten een inzageverzoek doen, is het voor hen dan vrij eenvoudig deze gesprekken te analyseren. Alleen als het hier gaat om gesprekken met betrekking tot bijzondere persoonsgegevens (zoals beschreven in de AVG artikel 9) doet zich een hoog risico voor, vanwege de gevoeligheid van deze persoonsgegevens. Het wordt dus sterk afgeraden dit soort gesprekken via een geplande meeting te voeren. Dit risico doet zich niet voor bij spontane één-op-één gesprekken via Teams. In dat geval kunnen de gesprekken wel end-to-end versleuteld worden.

Wat doet Microsoft tegen dit hoge risico?
Microsoft heeft aangegeven zich in te spannen om ook bij geplande Teams gesprekken end-to-end encryption toe te passen. Microsoft kan nog geen termijn geven wanneer dit is geïmplementeerd. Dat is mede de reden waarom dit risico op hoog staat, en blijft staan, tot hier meer duidelijkheid over is.

Loopt mijn instelling nu gevaar?
Niet voor zover wij hebben kunnen vaststellen. Het hoge risico betreft de theoretische mogelijkheid dat Amerikaanse opsporings- en inlichtingendiensten inzageverzoeken doen op data van (Nederlandse) burgers. Microsoft heeft gemeld dat het geen verzoeken heeft gehad waarbij het personen uit de Nederlandse publieke sector betrof.

Zijn de resultaten van de Schrems II uitspraak en de nieuwe richtlijnen van de EDPB meegenomen in dit onderzoek?
Ja, die zijn meegenomen. Er is bij dit onderzoek ook een Data Transfer Impact Assessment (DTIA) uitgevoerd. Tevens wordt aan het einde van 2022 een uitspraak van de European Data Protection Board (EDPB) verwacht, die mogelijk invloed kan hebben op de

resultaten van onder andere deze DPIA. Uiteraard blijft SURF dit goed in de gaten houden.

Waar hebben de gevonden risico's betrekking op?
Zowel de hoge als de lage risico's hebben betrekking op de doorgifte van persoonsgegevens naar de VS en de mate van transparantie die Microsoft biedt in het verwerken van persoonsgegevens als verwerker.

Welke lage risico's zijn er gevonden?
Deze 6 lage risico's zijn gevonden:

1. De huidige structurele overdracht van beperkte diagnostische gegevens en de incidentele overdracht van beveiligingsgegevens naar de VS leveren beide gegevensbeschermingsrisico's op.
2. Microsoft is niet volledig transparant over de browser-gebaseerde verzameling van telemetrie gegevens en de telemetrie gebeurtenissen over het gebruik van de verbonden ervaringen.
3. Microsoft heeft toegezegd het programma waarmee de diagnostische gegevens kunnen worden opgehaald, te verbeteren. Dit om beheerders te helpen bij eventuele verzoeken tot toegang van gegevens van individuele werknemers. Dit hulpmiddel is momenteel nog lastig in gebruik.
4. Er is één uitzondering op de garantie van Microsoft dat de 'vereiste servicegegevens' geen direct identificeerbare (leesbare) gebruikersnamen/e-mailadressen adressen of documentnamen bevatten. Microsoft kan de gebruikersnaam en/of het e-mailadres van een werknemer, gezamenlijk met de naam van de tenant en het bestandspad met de volledige naam van het document verzamelen. Dit is noodzakelijk voor bijvoorbeeld het functioneren van OneDrive. Deze gegevens worden niet langer dan 30 dagen bewaard.
5. Microsoft biedt twee verschillende analysediensten voor Teams: Teams Analytics and Reporting en Viva Insights. Deze tools geven inzicht in het gedrag van medewerkers aan de medewerkers zelf, alsmede aan de administrators van de instelling. Teams Analytics & Rapporten is standaard ingeschakeld. Deze optie dient door de administrator van de instelling uitgezet te worden. Viva Insights staat standaard uit. Indien de administrator deze functionaliteit aanzet, kan de gebruiker zich hiervoor afmelden.
6. Microsoft is bezig om ervoor te zorgen dat er geen verkeer vanuit SharePoint naar zijn zoekmachine Bing wordt gestuurd, in situaties waarin een Enterprise of Education klant, de Controller Connected Experiences heeft uitgeschakeld. Momenteel staat Microsoft zichzelf toe om deze gegevens als verantwoordelijke te verwerken voor de 17 genoemde doelen in hun standaard privacy statement. Het verwijderen van verkeer van SharePoint naar Bing moet in juli 2022 zijn afgerond.

Welke maatregelen moet mijn instelling zelf nemen?
Ten aanzien van het hoge risico waarbij content data in de EU worden verwerkt, maar toegankelijk zijn vanuit de VS omdat die gegevens niet zijn versleuteld:

- Geef instructies aan gebruikers om geen bijzondere persoonsgegevens te delen via ingeplande Teams calls, want dergelijke geplande sessies zijn niet end-to-end encrypted. Onder geplande calls verstaan we Teams-meetings die via de agenda zijn opgezet. Spontane calls via Teams zijn wel te versleutelen.

- Maak gebruik van Double Key Encryption voor documenten met gevoelige of bijzondere categorieën persoonsgegevens die zijn opgeslagen in SharePoint en OneDrive. Dit betreft ook opnames van Teams-vergaderingen.
- Gebruik Customer Lockbox voor andere opgeslagen persoonsgegevens.
- Zet de end-to-end encryptie standaard aan bij 1-on-1 calls en instrueer gebruikers om ook end-to-end encryptie in te schakelen. Microsoft beschrijft hier hoe dit aangezet kan worden.
  Een korte beschrijving hiervan: Nadat de beheerder de functie heeft geactiveerd, dient een eindgebruiker het volgende te doen: Ga naar 'Settings' en kies hierna voor de opties 'Privacy'. Selecteer de button naast 'End-to-end encrypted calls' om deze te activeren.
- Maak een privacybeleid voor Teams en OneDrive voor gebruikers en gastgebruikers. Stel regels op voor het delen van bestanden en afbeeldingen. Zorg ervoor dat medewerkers en gastgebruikers deze regels accepteren via de Algemene Voorwaarden van Azure AD.

Ten aanzien van de lage risico's:

- Microsoft ontwikkelt een EU Data Boundary. Hiermee worden vanaf eind 2022 alle EU persoonsgegevens in de EU opgeslagen (inclusief diagnostische en service data). Tot die tijd dient het risico ten aanzien van de huidige structurele overdracht van beperkte diagnostische gegevens en incidentele overdracht van beveiligingsgegevens naar de VS geaccepteerd te worden.
- Gebruik geen SMS-code ter verificatie, om te voorkomen dat er een overdracht van onversleutelde mobiele telefoonnummers naar landen buiten de EER plaatsvindt. Gebruik in plaats daarvan de Microsoft Authenticator-app of een hardware token.
- Stel beleidsregels op voor het gebruik van OneDrive en SharePoint, waarin wordt vastgelegd dat er geen persoonsgegevens opgenomen mogen worden in bestandsnamen en bestandspaden.
- Overweeg om accounts te creëren met een pseudoniem voor werknemers van wie de identiteit vertrouwelijk moet blijven (binnen de eigen AD omgeving of binnen Azure AD als deze gebruikt worden voor Single Sign On.
- Gebruik regelmatig de Data Viewer Tool en vergelijk de resultaten met de openbare documentatie.
- Informeer werknemers over de mogelijkheid van het gebruik van de Data Viewer Tool en informeer ze over de mogelijkheid tot het doen van een inzageverzoek bij de eigen instelling.
- Wanneer de data subject access request (DSAR) tool wordt gebruikt om inzage te krijgen in diagnostische data, vergelijk deze dan met een eigen uitgevoerde technische analyse op het netwerkverkeer.
- Zet de functionaliteit van Teams Analytics and Reporting uit en gebruik pseudonimisering. Schakel Viva Insights niet in. Mocht er toch worden besloten tot het gebruik van deze tooling; voer dan een DPIA uit. Zeker wanneer ze gebruikt worden in combinatie met andere analytische diensten van Microsoft Windows & Office.
- Maak beleid om het gebruik van Teams Analytics & Rapporten als een controlemiddel voor werknemers te voorkomen.
- Om het risico van de data doorgifte van Microsoft naar derde partijen met Microsoft in de rol van verantwoordelijke te mitigeren, wordt aangeraden om de controller Connected Experiences en de third party apps in Teams uit te zetten.

- Instrueer eindgebruikers om niet via SharePoint online naar afbeeldingen te zoeken in de Bing zoekmachine, tot de functionaliteit in juli 2022 is uitgeschakeld.

Welke conclusie is in de DPIA getrokken?
Microsoft heeft naar aanleiding van de onderhandelingen door SLM Rijk en SURF al veel juridische, technische en organisatorische maatregelen genomen. Tekortkomingen zijn verbeterd en garanties zijn gegeven over de gegevensverwerkingen door Microsoft. Hiermee zijn een groot deel van de risico's voor betrokkenen gemitigeerd bij de verwerking van persoonsgegevens door het gebruik van Teams, OneDrive en SharePoint. Echter, Microsoft heeft ook nog een aantal stappen te zetten om de geconstateerde hoge risico en lage risico's te mitigeren. Als instellingen de genoemde aanbevolen maatregelen opvolgen en uitvoeren, dan zijn er op dit moment geen hoge risico's voor het verwerken van (bijzondere) persoonsgegevens.

De risico's worden eind 2022 opnieuw beoordeeld, nadat er meer duidelijkheid is gegeven door de European Data Protection Board (EDPB) omtrent data transfers buiten de EER. SURF houdt deze ontwikkelingen nauwgezet in de gaten en spant zich in om ervoor te zorgen dat technische en contractuele afspraken met leveranciers compliant zijn en dat risico's worden geminimaliseerd.

Hoe zit het met de bedrijfskritische gegevens?
Bij het gebruik van een applicatie dient de verantwoordelijke binnen de instelling te kijken naar de verwerking van persoonsgegevens alsmede andere gegevens die bedrijfsvertrouwelijk kunnen zijn. Een DPIA richt zich alleen op persoonsgegevens en compliancy met de AVG. Derhalve zijn andere vormen van vertrouwelijke c.q. bedrijfskritische informatie niet meegenomen.

Doet het hoge risico zich alleen voor bij Teams?
Bestanden binnen Onedrive en SharePoint kun je wel versleuteld opslaan. Dit is ook de mitigerende maatregel: gebruik Double Key Encryption voor bestanden met gevoelige of bijzondere persoonsgegevens die zijn opgeslagen in SharePoint/OneDrive. Hieronder vallen ook opnames van Teams-gesprekken. Gebruik Customer Lockbox om andere opgeslagen persoonsgegevens te beschermen.

Bij live gesprekken in Teams kan/gebeurt dit vooralsnog niet, met uitzondering van de spontane één-op-één calls. Hier kun je de E2EE maatregel standaard aan zetten. Dit is de reden dat geplande Teams meetings als een hoog risico geclassificeerd zijn. Er is momenteel geen mitigerende maatregel beschikbaar, anders dan de instructie aan medewerkers om geen bijzondere persoonsgegevens te verwerken.

Hoe kan ik gebruik maken van E2EE (end-to-end encryption) bij één-op-één gesprekken?
Het is eerst aan de beheerder van de instelling om de E2EE functie te activeren. Daarna zet iedere gebruiker E2EE aan, in hun Teams applicatie.

Selecteer in Teams de mogelijkheid 'More options' naast je profiel foto. Kies 'Settings' en kies hierna voor de opties 'Privacy' aan de linkerzijde. Selecteer de button naast 'End-to-end encrypted calls' om deze te activeren.