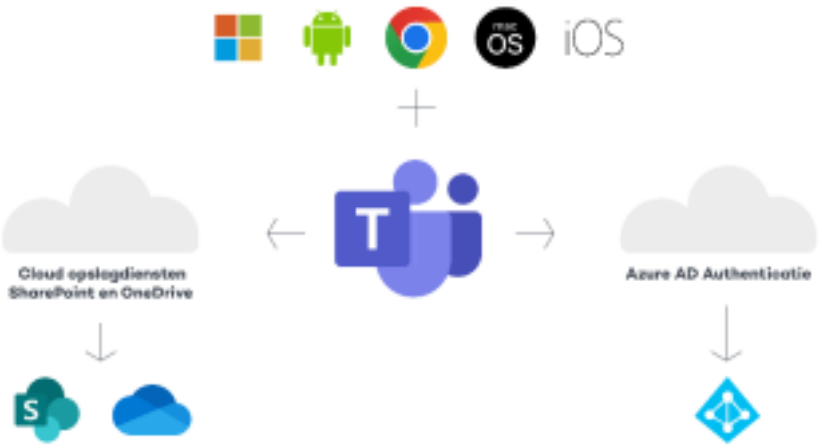
Zusammenfassung

Diese Datenschutz-Folgenabschätzung (DSFA) bewertet die datenschutzrechtlichen Risiken der (beruflichen) Nutzung von Microsoft Teams in Kombination mit OneDrive, SharePoint Online und dem Azure Active Directory.

Teams ist ein Online-Tool für Videoanrufe, Chats und Dateifreigabe. Als Teil von Office 365 stellt Microsoft Endbenutzern zwei Cloud-Speicherdienste bereit: OneDrive und SharePoint Online. Diese Dienste werden häufig verwendet, um auf Dateien zuzugreifen und diese zu speichern, die über Teams freigegeben wurden. Um die Onlinedienste von Microsoft nutzen zu können, müssen sich Endbenutzer und Systemadministratoren sowie Gastbenutzer über den Online-Clouddienst Azure Active Directory authentifizieren.

Umfang der DSFA

Die Datenverarbeitung über Teams und die drei Cloud-Dienste wurde in den drei verschiedenen Versionen der Office-Software getestet, die in der Microsoft 365 Enterprise-Lizenz enthalten sind. Teams, SharePoint und OneDrive können auf den Computern und Laptops der Mitarbeiter (Office 365 ProPlus), auf Smartphones und Tablets (Office Mobile Apps für iOS und Android) und als Online-Anwendungen installiert werden, die in einem Browser ausgeführt werden (Office for the Web, früher bekannt als Office Online).



Diese DSFA ist eine iterative Bewertung der Nutzung von Teams, SharePoint und OneDrive auf zwei Versionen der Office-Software: Office für das Web und die mobilen Office-Apps. Diese DSFA enthält Ergebnisse im Zusammenhang mit der Verarbeitung von Diagnosedaten in Office für das Web und den mobilen Office-Apps vom 31. Mai 2020, wie im September 2021

Diese DSFA wurde von SLM Rijk, dem zentralen Verhandlungsführer für Produkte und Dienstleistungen, in Auftrag gegeben Microsoft, Google und Amazon Web Services für die nationale Regierung und für SURF, die zentrale IT-Einkaufsorganisation für niederländische Hochschulen und Universitäten.

Ergebnis: sechs niedrige Datenschutzrisiken

Das Ergebnis dieser DSFA nach wiederholten Konsultationen mit Microsoft ist, dass keine bekannten hohen Risiken für die Verarbeitung von Diagnosedaten mehr bestehen. Es besteht jedoch ein hohes Risiko, wenn Organisationen Microsoft Teams verwenden, um hochsensible und spezielle Datenkategorien zu verarbeiten, aufgrund des möglichen Zugriffs durch Strafverfolgungsbehörden und Geheimdienste in den USA.

Sechs geringe Datenschutzrisiken bei der Verarbeitung von Diagnosedaten

Die sechs geringen Datenschutzrisiken beziehen sich auf folgende Umstände:

1. Die aktuelle systematische **Übertragung einer begrenzten Menge Diagnosedaten als auch die zufällige Übertragung von Sicherheitsdaten in die USA** bergen Datenschutzrisiken. Organisationen können diese Risiken akzeptieren, da diese Risiken bis Ende 2022 nach Abschluss der EU-Datengrenze von Microsoft behoben sein werden. Ab diesem Zeitpunkt verarbeitet Microsoft alle Inhalts-, Diagnose-, Konto- und Support-Daten von EU-Enterprise- und Education-Kunden ausschließlich in den EU-Rechenzentren von Microsoft. Obwohl Microsoft weiterhin einige personenbezogene Daten in die USA übertragen wird, um Sicherheitsrisiken zu identifizieren und zu beheben, werden diese laufenden Übertragungen zufällig und nicht strukturell sein und im Allgemeinen nur pseudonyme und aggregierte Daten enthalten.
2. Microsoft ist **nicht sehr transparent über die browserbasierte Erfassung von Telemetriedaten** und die Telemetrie-Ereignisse über die Nutzung der sogenannten *Connected* Experiences. Microsoft nennt diese Diagnosedaten *Required Service Data*. Selbst wenn ein Kunde die Erfassung von Office-Telemetriedaten minimiert hat, indem er „keine/keine" ausgewählt hat, wirkt sich diese Einstellung nicht auf die Erfassung der *erforderlichen Dienstdaten*. Laut Microsoft sind diese Daten zu dynamisch oder vertraulich, um sie im Detail zu veröffentlichen, aber Microsoft verspricht, diese Daten nur für die drei vereinbarten Verarbeitungszwecke zu verarbeiten.
3. Microsoft hat zugesagt, sein Tool Diagnostic Data Viewer zu verbessern, um Administratoren bei der Bearbeitung möglicher **Zugriffsanfragen** einzelner Mitarbeiter zu unterstützen. Dieses Instrument ist derzeit schwer zu benutzen.
4. Es gibt **eine Ausnahme** von der Gewährleistung von Microsoft, dass die *erforderlichen Dienstdaten* **keine direkt identifizierbaren (lesbaren) Benutzernamen/Adressen oder Dokumentennamen enthalten**. Die für diese DSFA durchgeführte technische Analyse des Netzwerkverkehrs weist darauf hin, dass Microsoft den Benutzernamen und/oder die E-Mail-Adresse eines Mitarbeiters zusammen mit dem Namen des Kunden (dem *Mandanten*) und dem Dateipfad mit dem vollständigen Namen des Dokuments erfassen kann. Microsoft erläuterte, warum dies in OneDrive notwendig sein könnte, beispielsweise wenn mehrere Benutzer gleichzeitig an demselben Dokument arbeiten. Microsoft erklärte auch, dass der Zugriff auf diese OneDrive-Diagnosedaten überwacht wird, auf die *Just-in-Time*-Sicherheitsgruppe beschränkt ist und auf Techniker beschränkt ist, die eine genehmigte geschäftliche Rechtfertigung haben. Darüber hinaus werden diese spezifischen Telemetriedaten nie länger als 30 Tage aufbewahrt.
5. Microsoft bietet **zwei verschiedene Analysedienste für Teams an**: *Teams Analytics & Reports* und *Viva Insights*. Das erste Tool (*Teams Analytics & Reports*) verschafft Administratoren detaillierte Einblicke in das individuelle Arbeitsverhalten. Während Microsoft die Möglichkeit bietet, Mitarbeiternamen zu pseudonymisieren, ist nicht klar, ob dies Auswirkungen auf die Rohdatenprotokolle von Microsoft haben wird. Erfahrene Administratoren von Universitäten und Regierungsorganisationen können dieses Risiko selbst mindern, indem sie diese Funktion deaktivieren. Microsoft ist nicht bereit, die Standardeinstellung zu ändern. Das andere Tool, *Viva Insights*, ist standardmäßig deaktiviert. Dieses Tool umfasst *MyAnalytics* und *Workplace Analytics*, Tools, die Mitarbeitern jeweils Informationen über ihre Produktivität und Managern Einblick in die Arbeitsmuster einzelner Mitarbeiter geben. Wenn ein Administrator den Dienst absichtlich aktiviert, hat der einzelne Benutzer immer noch die Möglichkeit, sich abzumelden.
6. Microsoft ist dabei**, Datenverkehr zu seiner Suchmaschine Bing strukturell von SharePoint zu entfernen,** wenn ein Enterprise- oder Education-Kunde die verbundenen Erfahrungen deaktiviert hat, für die Microsoft verantwortlich ist (sogenannte *zusätzliche optionale verbundene Erfahrungen*). Bei den ersten Tests für diese DSFA im Mai 2021 schickte SharePoint Bildsuchen aus dem Browser an Bing. Da Microsoft der Datenverantwortliche für die Datenverarbeitung von Bing ist, erlaubt sich Microsoft, personenbezogene Daten für alle 17 (kommerziellen) Zwecke aus seiner (Verbraucher-)Datenschutzerklärung zu verarbeiten. Der Datenverkehr zu Bing sollte bis Juli 2022 dauerhaft entfernt werden.

Hohes Risiko im Zusammenhang mit dem Zugriff auf unverschlüsselte besondere personenbezogene Daten

Es besteht ein hohes Datenschutzrisiko im Zusammenhang mit dem möglichen Zugriff von US-amerikanischen Strafverfolgungs- und Geheimdiensten auf hochsensible und spezielle personenbezogene Daten. Dieses Risiko besteht, obwohl Inhaltsdaten in Teams, OneDrive und SharePoint bereits ausschließlich in den europäischen Rechenzentren von Microsoft verarbeitet und gespeichert werden. Der Grund dafür ist, dass der Zugang zu diesen Daten durch US-Gesetze wie den US CLOUD Act gefordert werden kann. Unternehmen können dieses hohe Risiko für sensible personenbezogene Daten in Dateien auf OneDrive und SharePoint mindern, indem sie ihre eigenen Verschlüsselungsschlüssel mit Microsoft Double Key Encryption verwenden. Microsoft bietet noch keine Ende-zu-Ende-Verschlüsselung für Streaming-Kommunikation mit mehreren Teilnehmern in Teams an, sondern nur für ungeplante Eins-zu-Eins-Videoanrufe. Obwohl Microsoft in seiner Antwort auf diese DSFA bestätigt hat, dass es E2EE in Teams-Gruppenbesprechungen und für Chats ermöglichen wird, hat es noch keinen Termin genannt.

Für „normale" Arten personenbezogener Daten werden die Übermittlungsrisiken als sehr gering eingeschätzt, auch wenn die möglichen Folgen für die betroffenen Personen sehr hoch sein können. Die Wahrscheinlichkeit, dass Microsoft gezwungen wird, personenbezogene Daten von Kunden des öffentlichen Sektors in der EU bereitzustellen, ist sehr gering. Microsoft darf nicht offenlegen, ob es bestimmte Anträge erhalten hat, die der Vertraulichkeit unterliegen, aber Microsoft erklärt öffentlich, dass "Microsoft keine personenbezogenen Daten von Kunden des öffentlichen Sektors in der EU an eine Regierung weitergibt und dies auch nie getan hat". Diese historische Tatsache in Verbindung mit der von Microsoft verwendeten Verschlüsselung (mit eigenen Schlüsseln), seinen rechtlichen Garantien, dass es jede Anordnung anfechten wird, seiner nachgewiesenen Erfolgsbilanz und seinen Transparenzberichten reicht aus, um das Risiko eines unbefugten Zugriffs auf "gewöhnliche" personenbezogene Daten als geringes Datenschutzrisiko einzustufen. Organisationen sollten jedoch keine sehr sensiblen oder speziellen personenbezogenen Daten über Teams austauschen, es sei denn, die Daten sind von Natur aus öffentlich (z. B. Universitätsvorlesungen oder einige Gerichtsverfahren), da sie die Verschlüsselungsschlüssel nicht selbst kontrollieren.

Geltungsbereich: Inhalts-, Diagnose- und Kontodaten

In dieser DSFA geht es in erster Linie um die Datenschutzrisiken, wenn Microsoft Daten über die individuelle Nutzung von Teams, OneDrive und SharePoint in Kombination mit der Nutzung von Azure AD auf allen Plattformen speichert. Diese Metadaten (über die Nutzung der Dienste und Software) werden in der DSFA als Diagnosedaten bezeichnet.

Technisch gesehen sammelt Microsoft die Diagnosedaten auf unterschiedliche Weise: über vom System generierte Ereignisprotokolle auf seinen eigenen Cloud-Servern und über die Telemetrie-Clients in den verschiedenen Anwendungen und über den Browser. Ähnlich wie der Telemetrie-Client in Windows 10 und in Office 365 ProPlus hat Microsoft die mobilen Office-Apps und Office für das Web so programmiert, dass sie systematisch Telemetriedaten auf dem Gerät sammeln und in regelmäßigen Abständen an die Server von Microsoft in den USA senden. Darüber hinaus erstellt Microsoft detaillierte Analysen über die individuelle Nutzung von Teams.

Der Anwendungsbereich dieser DSFA umfasst auch die Verarbeitung der Inhaltsdaten und der Kontodaten im Hinblick auf die Risiken einer Übertragung in die USA.

Technische Analyse personenbezogener Daten

Die technische Untersuchung der Datenverarbeitung wurde durchgeführt, indem eine große Anzahl schriftlicher Szenarien durchgeführt und der ausgehende Netzwerkverkehr abgefangen und analysiert wurde. Darüber hinaus wurden Überprüfungsanfragen über das Überprüfungswerkzeug gestellt, das Microsoft den Administratoren zur Verfügung stellt, und Auditprotokolle über die individuelle Nutzung von Teams, SharePoint und OneDrive eingesehen.

Inhalt des Telemetrieverkehrs

Die Recherche zeigt, dass Microsoft über die Telemetrie-Ereignisse begrenzte Daten über die individuelle Nutzung von Teams, SharePoint und OneDrive erhebt. Obwohl die Telemetriedaten eindeutige Benutzer-IDs, Geräte-IDs und Korrelations-IDs enthalten, wurde der Inhalt unkenntlich gemacht. Die technische Analyse zeigt, dass Microsoft sein Versprechen, Benutzernamen niemals auf der (niedrigsten) Telemetrie-Ebene „keine/keine" einzufügen, nicht einhält. Einige Telemetrie-Ereignisse enthalten den Benutzernamen (lesbar) in SharePoint-URLs in den Ereignissen, die von Teams, OneDrive und SharePoint für das Web (Zugriff über einen Browser) und in OneDrive auf iOS generiert werden. Gemäß der Antwort von Microsoft auf diese DSFA ist die Erfassung dieser (direkt identifizierbaren) Inhaltsdaten in Verbindung mit der pseudonymen Benutzerkennung für die begrenzte Fehlererkennung in der Software unbedingt erforderlich.

Abgesehen von diesen direkt identifizierbaren Benutzernamen und OneDrive-Pfadnamen hat Privacy Company keine Inhaltsdaten in den abgefangenen Telemetrieereignissen beobachtet. Die Ereignisse enthalten auch keine Informationen über Dateinamen oder andere vom Benutzer bereitgestellte Daten wie Geräte- oder Profilnamen.

Inhalt der vom Dienst generierten Dienstprotokolle

Die Audit-Protokolle und die Ergebnisse der Zugriffsanfragen für die Diagnose zeigen, dass Microsoft in der Diagnose direkt identifizierbare personenbezogene Daten über die Nutzung von Teams, OneDrive und SharePoint in Kombination mit dem Azure AD verarbeitet. Die Logfiles über die Testnutzer zeigen, dass eine direkt identifizierbare Person zu einem bestimmten Zeitpunkt, mit welchem Browser und von welchem Betriebssystem aus eine Aktion in einer getesteten App durchgeführt hat. Microsoft zeichnet auch auf, ob ein Anmeldefehler aufgetreten ist, was ihn verursacht hat und wie der Benutzer authentifiziert wurde. Benutzer können direkt anhand der Felder Benutzername und E-Mail-Adresse identifiziert werden. Diese Zugriffsdateien enthalten auch die verwendete IP-Adresse.

Da jede Protokollzeile die Kombination aus Benutzer-ID und Organisations-ID enthält, handelt es sich bei jeder Protokollzeile um personenbezogene Daten. Darüber hinaus enthalten diese Protokolldateien Informationen über Aktionen auf den Servern und Inhaltsdaten in den Namen von Pfaden und Dateien.

Ziele, Rollen und Grundsätze

Die von SLM Rijk und SURF ausgehandelte Datenschutzänderung sieht vor, dass Microsoft die personenbezogenen Daten, die es von, über oder durch die Nutzung der Onlinedienste als Auftragsverarbeiter erhält, grundsätzlich nur für drei autorisierte Zwecke verarbeiten darf, aber nur wenn es verhältnismäßig ist. Diese drei Ziele sind:

1. den Dienst bereitzustellen und zu verbessern,
2. den Dienst aktuell zu halten und
3. den Dienst zu sichern.

Im Einklang mit dieser Datenschutzänderung verarbeitet Microsoft personenbezogene Daten im Zusammenhang mit der Nutzung von Teams, OneDrive, SharePoint und Azure AD als Auftragsverarbeiter.

Datenschutzrisiken und Minderungsmaßnahmen

Die folgende Tabelle listet die einen hohen und sechs niedrige Datenschutzrisiken für betroffene Personen sowie die Minderungsmaßnahmen auf, die Regierungsorganisationen, Universitäten und Microsoft ergreifen können.

Nr.	Hohes Risiko	Maßnahmen Regierungen und Universitäten	Maßnahmen Microsoft
1.	In der EU verarbeitete Inhaltsdaten sind zugänglich für Microsoft, wenn nicht E2EE	Tauschen Sie keine sensiblen oder speziellen persönlichen Daten über Team-Anrufe aus, die nicht Ende-zu-Ende-verschlüsselt sind.	Bekanntgabe eines klaren Termins, bis wann E2EE für Gruppentreffen und Chats unterstützt werden soll
		Verwenden Sie *Double Key Encryption* für Dateien mit sensiblen oder besonderen persönlichen Daten, die in SharePoint/OneDrive gespeichert sind. Dazu gehören auch Aufzeichnungen von Teamgesprächen. Verwenden Sie Customer Lockbox zum Schutz anderer gespeicherter persönlicher Daten.	Erfüllung der SCC-Anforderung, Kunden zu informieren, wenn Microsoft die Datenschutzgarantien in den SCC nicht mehr erfüllen kann.
		Aktivieren Sie E2EE standardmäßig für 1-zu-1-Unterhaltungen in Teams und weisen Sie die Endbenutzer an, E2EE ebenfalls zu aktivieren.	
		Erstellen Sie eine Teams- und OneDrive-Datenschutzrichtlinie für interne und Gastnutzer, legen Sie Regeln für die Datei- und Bildfreigabe fest. Bringen Sie Mitarbeiter und Gastbenutzer dazu, diese Regeln durch von Azure AD auferlegte Bedingungen zu akzeptieren	
Nr.	**Niedriges Risiko**	**Maßnahmen Regierungen und Universitäten**	**Maßnahmen Microsoft**
2.	Strukturelle *Übertragungen* von Telemetriedaten in die USA (bis Dezember 2022)	Akzeptieren Sie das vorübergehende Risiko der Übermittlung dieser pseudonymisierten Daten, während Microsoft die EU-Datengrenze entwickelt	Anwendung der EU-Datenschutz-Grenze auf alle personenbezogenen Daten (mit den bekannten Ausnahmen) bis Ende 2022
	Möglicher US-Zugriff auf Audit-Protokolle und Kontodaten in Azure AD und Telemetriedaten, die bereits in der EU oder nach 2022 verarbeitet und gespeichert werden	Nehmen Sie das Risiko des Zugriffs auf Namen und E-Mail-Adressen in Azure AD in Kauf oder erwägen Sie die Verwendung von Pseudonymen in Azure AD.	Information der Kunden über den aktuellen Stand der EU-Datengrenze pro Dienst/Applikation
		Verwenden Sie keine SMS zur Authentifizierung, um die Übermittlung unverschlüsselter Mobiltelefonnummern an Drittländer zu verhindern. Verwenden Sie stattdessen die Authenticator-App oder einen Hardware-Token	

		Verwenden Sie Pseudonyme bei der Verwendung von Azure AD für Single Sign-On mit externen Anbietern für Mitarbeiter, deren Arbeitsidentität vertraulich bleiben muss	
	Gelegentliche Übermittlung von pseudonymisierten Daten in die USA zu Sicherheitszwecken	Legen Sie bei der Verwendung von OneDrive und SharePoint Richtlinien fest, die verhindern, dass Dateinamen und Dateipfade persönliche Informationen enthalten.	
3.	Laufend anfallend Übertragung von Benutzernamen/ E-Mail-Adressen/ Pfadnamen auf OneDrive in die USA	Erwägen Sie die Verwendung von pseudonymen Konten für Mitarbeiter, deren berufliche Identität vertraulich bleiben muss	
		Legen Sie bei der Verwendung von OneDrive und SharePoint Richtlinien fest, die verhindern, dass Dateinamen und Dateipfade persönliche Daten enthalten.	
4.	Mangelnde Transparenz Telemetriedaten	Verwenden Sie regelmäßig das Data Viewer Tool, falls verfügbar, und vergleichen Sie die Ergebnisse mit der öffentlichen Dokumentation von Microsoft	Bietet ein funktionales Data Viewer Tool für die OneDrive Telemetriedaten auf Windows und MacOS
		Verwenden Sie das Microsoft-Tool Administrators View, um auf Diagnosedaten zuzugreifen und diese mit einer zufälligen Analyse des Netzwerkverkehrs zu vergleichen.	Überprüfen Sie die Einhaltung der Zweckbeschränkung, indem Sie spezifische Audit-Fragen zu Inhalt, Verwendungszwecken und Aufbewahrungsfristen der erforderlichen Servicedaten hinzufügen.
		Informieren Sie die Mitarbeiter über ihre Zugriffsmöglichkeiten über das Data Viewer Tool oder indem Sie einen DSAR an die Verwaltung der Organisation senden.	Bereitstellung weiterer Informationen über erforderliche Dienstdaten, einschließlich Telemetriedaten von Office for the Web

Nr.	hohem Risiko	Regierungs- und Universitätsmaßnahmen mit	Microsoft-Maßnahmen
5.	Beschränkungen des Umgangsrechts in die erforderlichen Leistungsdaten	Verwenden Sie das DSAR-Tool von Microsoft, um auf die Diagnosedaten zuzugreifen, und vergleichen Sie diese von Zeit zu Zeit mit der Analyse des Netzwerkverkehrs.	Verbesserung des Tools für den Zugang zu Diagnosedaten
		Unterstützung eines speziellen Audits von SLM Rijk über Microsofts Sammlung und Verwendung von Required Service Data	Stellen Sie eine klare und verständliche Erläuterung des Inhalts der erforderlichen Dienstdaten bereit
			Lassen Sie eine unabhängige Prüfung durchführen, um zu erklären, warum das Anzeigetool nur einen sehr eingeschränkten Zugang zu den erforderlichen Dienstdaten bietet: weil die Daten nur für eine sehr kurze Zeit aufbewahrt werden oder weil Microsoft keine persönlichen Daten sammeln würde.
6.	Mangelnde Kontrolle: Bereitstellung personenbezogener Daten an Microsoft und Dritte, die für die Datenverarbeitung verantwortlich sind	Deaktivieren Sie die zusätzlichen optionalen Connected Experiences	Sicherstellen, dass bis Ende Q2 2022 der gesamte Datenverkehr zu Bing von SharePoint Online entfernt wird
		Deaktivieren Sie den Zugriff auf Anwendungen von Drittanbietern im Teams-Appstore	
		Weisen Sie Endbenutzer an, keine Bing-Bildersuche in SharePoint Online zu verwenden (bis die Funktion entfernt wird)	Senden Sie keinen Datenverkehr zu Cloudflare auf Microsoft-Hilfeseiten, die in Hyperlinks im Einstellungsmenü von Teams plattformübergreifend empfohlen werden
7.	Personalüber-wachungssystem: Abschreckende Wirkung	Deaktivieren Sie die Teams Analytics & Reports-Funktionalität, verwenden Sie Pseudonymisierung: aktivieren Sie Viva Insights nicht	Erfüllen Sie Art. 25 DS-GVO (Datenschutz durch Design und Standardeinstellungen): Schalten Sie Teams Analytics & Reports standardmäßig aus
		Führen Sie vor dem Einsatz dieser Analysewerkzeuge eine DSFA durch, insbesondere wenn sie in Kombination mit anderen Analyse-Diensten von Microsoft Windows & Office verwendet werden.	Informieren Sie die Administratoren über die Folgen für die von Microsoft verwalteten Rohdaten, wenn sie sich für die Pseudonymisierung der Daten in Teams Analytics & Reports entscheiden.
		Erstellen Sie eine Richtlinie, um zu verhindern, dass Team Analytics & Reports als Werkzeug zur Mitarbeiterüberwachung verwendet wird.	

Schlussfolgerungen

Seit Juni 2019 hat Microsoft als Ergebnis der Verhandlungen mit SLM Rijk und SURF viele rechtliche, technische und organisatorische Maßnahmen ergriffen, um die Risiken zu mindern für die Beteiligten die Verarbeitung personenbezogener Daten durch den Einsatz von Teams, OneDrive, SharePoint und dem Azure AD einzuschränken. Als Reaktion auf die ersten Erkenntnisse dieser DSFA hat Microsoft eine Reihe von Mängeln behoben und seine Datenverarbeitung erläutert.

Angesichts des Schrems-II-Urteils und der technischen Erkenntnisse muss Microsoft weitere Anpassungen und Verbesserungen vornehmen, um das verbleibende hohe Risiko und die sechs niedrigen Risiken zu adressieren. Microsoft muss allen Teams-Gesprächen eine klare Frist für die Anwendung von E2EE mitteilen. Darüber hinaus muss Microsoft den Inhalt der Erforderlichen Dienstdaten transparenter machen und durch ein unabhängiges Audit verifizieren lassen, dass es die vereinbarten Zweckbeschränkungen und Aufbewahrungsfristen für diese spezifischen Telemetriedaten einhält. Microsoft muss es Administratoren ermöglichen, sich für alle neuen Analyse-Dienste zu entscheiden, basierend auf klaren Informationen über die Auswirkungen auf die Datenverarbeitung.

Wenn Regierungsorganisationen und Universitäten alle empfohlenen Maßnahmen umsetzen, sind keine hohen Risiken für die Datenverarbeitung bekannt.

Warnung

Es ist ungewiss, wie die nationalen Datenschutzbehörden bei ihrer gemeinsamen Untersuchung der Nutzung von Cloud-Diensten durch Organisationen des öffentlichen Sektors die Risiken des Pass-Through bewerten werden. Die Ergebnisse werden Ende 2022 erwartet. Für diese DSFA wurden die Übertragungsrisiken streng bewertet. Eine separate DTIA, eine Datentransfer-Folgenabschätzung, wurde ebenfalls durchgeführt. Bei Bedarf werden diese DSFA und DTIA im Jahr 2023 aktualisiert.