



Whitepaper

Microsoft 365 an Schulen
datenschutzkonform betreiben

Stefan Ritter | Christopher Löffel
22.01.2022

Inhaltsverzeichnis

1. Executive Summary.....	3
2. Ausgangslage.....	3
3. Aktuelle rechtliche Situation.....	4
3.1. Auslöser der DSGVO-Bedenken	4
3.2. Problemanalyse.....	4
3.3. Reaktion von Microsoft.....	5
3.4. Aktuelle Situation.....	5
4. Maßnahmen zur Verbesserung des Datenschutzes	5
4.1. Windows-Einstellung	5
4.2. Programm zur Verbesserung der Benutzerfreundlichkeit.....	6
4.3. Office-ProPlus-Version.....	6
4.3.1. Beschränkung der Diagnosedaten	6
4.3.2. Connected Experiences.....	6
4.3.3. Linked-In-Integration	6
4.3.4. Workplace Analytics, Activity Reports, Delve	7
4.3.5. Kunden-Lockbox.....	7
4.3.6. Office Online und Office Mobile	7
4.3.7. Durchführung einer Datenschutz-Folgenabschätzung	7
5. Betrieb und Evergreen	7
6. Zusammenfassung	8
7. Autor und Ansprechpartner.....	9

1. Executive Summary

Bei Microsoft 365 handelt es sich um eine cloudbasierte Office-Umgebung, die insbesondere durch Microsoft Teams in Zeiten von Covid-19 und Homeschooling immer mehr an Bedeutung gewinnt. Viele Schulen und öffentliche Einrichtungen haben sich deshalb in der Stunde der Not spontan für die Education Version von Microsoft 365 entschieden. Der Anbieter hat den öffentlichen Einrichtungen den Einstieg dabei vermeintlich einfach gemacht und Microsoft Teams kostenlos als Konferenztool angeboten.

Über die Möglichkeiten zur Kollaboration und dem Abhalten von Meetings von Microsoft Teams wurden dadurch viele grundlegende Anforderungen der Schulen an eine Lösung zur Fortführung des Unterrichts in den eigenen 4 Wänden erfüllt.

Nun gibt es jedoch immer massivere Bedenken bei den öffentlichen Einrichtern und den Datenschützern von Bund und Länder. Vieles deutet darauf hin, dass Daten unrechtmäßig abgezogen werden und es herrscht große Unsicherheit, um welche Daten es sich dabei handelt.

Dieses Whitepaper soll aufzeigen, wie unsere Einschätzung von Microsoft 365 ist und warum die Entscheidung der Datenschutzkonferenz aus unserer Sicht nicht mehr haltbar ist¹. Außerdem zeigen wir auf, wie Microsoft 365 an Schulen datenschutzkonform betrieben werden kann. Dabei wird ausschließlich auf Bordmittel von Microsoft 365, ohne zusätzliche Sicherheitssoftware, zugegriffen.

2. Ausgangslage

Als sich beim Treffen der Ministerpräsidenten der Länder am 13. März 2020 abzeichnete, dass neben Großveranstaltungen auch Kitas und Schulen im Betrieb ausgesetzt werden würden, sahen sich viele Schulen zum spontanen Handeln gezwungen. Das Homeschooling war bis zu diesem Zeitpunkt vielerorts nicht erprobt und kam für die meisten Schulen und öffentlichen Einrichtungen völlig überraschend.

Daher haben sich etliche Schulen neben dem bekannten Moodle auch für Microsoft 365, vor allem jedoch für Microsoft Teams als Austausch-Plattform entschieden. Diese Plattform ermöglicht es, Konferenzen auch mit größeren Gruppen abzuhalten. Beispielsweise war es dadurch möglich Klassen von 30 Schülern gemeinsam in einem virtuellen Klassenzimmer zu unterrichten. Das Teams-Meeting ermöglicht außerdem das Teilen des eigenen Arbeitsplatzes, bspw. um Arbeitsergebnisse zu teilen oder Unterrichtsunterlagen zu teilen. Die Kamerafunktion von Teams ermöglicht zumindest einen eingeschränkten Kontakt der Schüler:innen und Lehrkräfte untereinander.

Allerdings hat die Datenschutzkonferenz am 22. September 2020 mit knapper Mehrheit beschlossen, dass Microsoft 365 nicht den DSGVO Ansprüchen der Datenschützer genügt. Somit ergibt sich für viele Schulen und öffentliche Einrichtungen die Frage, wie nun mit dieser Entscheidung zu verfahren ist. Und tatsächlich gibt es vielerorts auch bereits erste Abschaltungen, während andere Schulen „im Stillen“ die Lösung weiterbetreiben. Eine vollständige Abschaltung der Microsoft 365 Lösung ist oftmals keine Alternative, da die Konkurrenzprodukte mit den gleichen oder ähnlichen Hürden bestückt sind². Oder es gibt schlicht noch keine Stellungnahme von der Datenschutzkonferenz dazu

¹ Dabei erhebt dieses Whitepaper jedoch keinen rechtlichen Anspruch auf Gültigkeit. Es handelt sich um die Meinung unserer Experten, nicht um eine Rechtsberatung.

² [Datenschutzbeauftragte: Einsatz von Cisco Webex an Universität rechtswidrig - Golem.de](#)

und man würde sich erneut ein potenzielles Problemkind ins Haus holen. Daher beschäftigt sich dieses Whitepaper mit der aktuellen Situation und klärt auf, wie die bestehenden Datenschutzbedenken ausgeräumt und das Microsoft 365 System für den Alltag gehärtet werden kann. Dabei ist jedoch zu beachten, dass ein permanenter Datenschutz nur durch regelmäßige Kontrolle und Nachbesserung gewährleistet wird. Ein Partner, der sich mit diesen Themen beschäftigt ist daher unerlässlich für den schulischen Alltag.

3. Aktuelle rechtliche Situation

3.1. Auslöser der DSGVO-Bedenken

Zunächst beginnen wir bei den Ursachen für die aktuell angespannte Situation zwischen Microsoft und dem Datenschutz. Die Datenschutzkonferenz hat am 22. September 2020 ein Dossier veröffentlicht, in dem folgende Punkte bei Microsoft 365 (damals noch unter dem Namen Microsoft Office 365) in Sachen Datenschutz kritisiert werden:

1. **Fehlende Details:**
Die Beschreibung der genauen Tätigkeiten ist nicht gut genug, um sagen zu können, ob Microsoft weiter genutzt werden kann.
2. **Telemetrie hat keine Rechtsgrundlage:**
Es fehlt die rechtliche Grundlage für die übermittelten Telemetrie-Diagnosedaten.
3. **Ungenauer Hinweis zu eventuellen Weitergaben:**
Es gibt gesetzlich vorgeschriebene Fälle, in denen die Datenweitergabe unter einem vertraglichen Vorbehalt steht, dieser Bereich ist zu abstrakt verfasst.

Diese Kritik wurde als Abschlussbekanntmachung der Datenschutzkonferenz verlautbart.

3.2. Problemanalyse

Die eigentlichen Probleme beim Einsatz von Microsoft 365 ergeben sich bei den verschiedenen Datenverarbeitungsvorgängen. Microsoft verarbeitet bei der Nutzung von Microsoft 365 eine Vielzahl von personenbezogenen Daten.

Zu diesen gehören auch die Funktionsdaten, die notwendig sind für die Bereitstellung des Service Microsoft 365, welche allerdings gleich nach der Bereitstellung wieder gelöscht werden. Dass Microsoft hierbei als Auftragsverarbeiter i. S. d. Art. 28 DSGVO tätig ist, wird aus dem Online Service Terms (OST) ersichtlich. Auftraggeber ist der jeweilige Nutzer von Microsoft 365.

Zudem werden Inhaltsdaten verarbeitet, d. h. also die tatsächlichen Dokumente, E-Mails, Präsentationen etc., die Nutzer mit Microsoft 365 erstellen. Laut den OST werden diese Daten aber wiederum nur für die Bereitstellung des Service und nicht zu anderen Zwecken verwendet.

Neben Funktions- und Inhaltsdaten werden eine große Anzahl an Diagnosedaten verarbeitet und an die Server von Microsoft geschickt. Nachdem für jeden Nutzer eine individuelle ID generiert wird, werden Daten erhoben wie die Nutzungsdauer eines Office-Dienstes – wie z. B. Outlook, Word, Power Point, Excel und den Cloudspeicher OneDrive – Größe der bearbeiteten Datei, User-, und Client ID und die verwendete Programmiersprache.

Laut Microsoft werden diese Daten nicht für Profiling, Marktforschung oder Werbung, sondern für das Bereitstellen, Verbessern und Aktualisieren des Dienstes und dessen Sicherheit verwendet.

3.3. Reaktion von Microsoft

Nachdem das erste Ergebnis der oben dargestellten Datenschutzfolgeabschätzung deutliche Defizite und die Unvereinbarkeit mit der DSGVO aufzeigte, hat Microsoft mittlerweile die Verarbeitungszwecke stärker eingeschränkt, da sie aufgrund der Verarbeitung zu anderen Zwecken nicht wie gewünscht „nur“ als Auftragsverarbeiter, sondern gleichzeitig mit dem Microsoft 365-Nutzer als Verantwortlicher (Joint-Controller Art. 26 DSGVO) im Sinne der DSGVO galten, inklusive der damit verbundenen Rechten und Pflichten.

Bei der Nutzung von Microsoft 365 muss den Nutzern klar sein, dass eine Übermittlung der oben genannten Daten an Microsoft nicht ausgeschlossen werden kann. Auch wenn Microsoft Privacy-Shield-zertifiziert ist und Standard-Vertragsklauseln anbietet, werden diese Absicherungen von Datenübermittlungen an Drittländer gerade vom Europäischen Gerichtshof (EuGH) überprüft.

3.4. Aktuelle Situation

Die Reaktionsgeschwindigkeit von Microsoft auf die erhobenen Datenschutzbedenken war beispielhaft und zeigt deutlich, dass große Interesse von Microsoft am Europäischen Markt und den damit verbundenen Auflagen und Vorschriften³. Auch hat Microsoft für den gesamten Bildungssektor einen eigenen Informationsprotal für M365 und Covid im Bildungsbereich eingerichtet⁴. Leider sind die Datenschutzkonferenz und die zuständigen Datenschützer bisher nicht dazu in der Lage gewesen, die neue Situation von Microsoft 365 erneut zu bewerten und das Ergebnis der Datenschutzkonferenz zu validieren.

Ausgehend von den Änderungen und der knappen Mehrheit für die Ablehnung von Microsoft 365 in der Datenschutzkonferenz ist nun allerdings anzunehmen, dass Microsoft 365 den aktuellen Standards und Anforderungen genügt. Unabhängig davon werden in den nächsten Abschnitten wichtige Maßnahmen und Einstellungen aufgezeigt, welche den Datenschutz in Microsoft 365 verbessern und verhindern, dass Daten unerwünscht abfließen.

4. Maßnahmen zur Verbesserung des Datenschutzes

Die nachfolgenden Maßnahmen sind nicht für alle Systeme gleichermaßen realisierbar. Beispielsweise werden nicht alle Anwender über Windows 10 Enterprise verfügen. Dennoch erhöht jede einzelne Maßnahme die Sicherheit und den Datenschutz und steht unabhängig von den anderen Maßnahmen. Daher sollten so viele Einstellungen wie möglich im Betrieb umgesetzt werden.

4.1. Windows-Einstellung

Das Level der Telemetrie- und Diagnosedatenübermittlung von Windows 10 Enterprise muss auf „Sicher“ eingestellt werden. Nutzer dürfen ihre Aktivitäten nicht mit der Zeitachsen-Funktion von Windows 10 synchronisieren⁵. Von Windows 11 Enterprise ist nach aktuellem Stand grundsätzlich abzuraten, da die Stabilität der Software zum Zeitpunkt der Erstellung des Whitepapers unzureichend ist. Doch auch hier verhält sich die Telemetrie- und Diagnosedatenübermittlung grundsätzlich identisch zu Windows 10 Enterprise.

³ [Neue Maßnahmen zum Schutz Ihrer Daten | News Center Microsoft](#)

⁴ [Alle Infos zu COVID-19 – so unterstützt Microsoft | News Center Microsoft](#)

⁵ [Windows 10 Telemetrie und Diagnosedaten richtig abschalten - Gruppenrichtlinien](#)

4.2. Programm zur Verbesserung der Benutzerfreundlichkeit

Die Funktion zur Datenübermittlung an das Microsoft-Programm zur Verbesserung der Benutzerfreundlichkeit von Anwendungen muss deaktiviert werden.⁶

4.3. Office-ProPlus-Version

Die in dieser Stellungnahme beschriebenen Einstellungen sind erst ab der Office-ProPlus-Version 1904 verfügbar. Es muss deshalb diese oder eine nachfolgende Version verwendet werden.

4.3.1. Beschränkung der Diagnosedaten

Die Übermittlung der Diagnosedaten muss auf die geringste Stufe, „Keine“, eingestellt werden.⁷

4.3.2. Connected Experiences

Folgende Connected Experiences sind zu deaktivieren⁸:

- 3D Maps
- Insert Online 3D Models
- Map Chart
- Office Store
- Insert Online Video
- Researcher
- Smart Lookup
- Insert Online Pictures
- LinkedIn Resume Assistant
- Weather Bar in Outlook
- PowerPoint QuickStarter
- Giving Feedback to Microsoft
- Suggest a Feature

4.3.3. LinkedIn-Integration

Eine Integration von LinkedIn-Accounts der Mitarbeiter:innen, Schüler:innen und Student:innen muss unterbunden werden.⁹

⁶ [Hilfe: Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren \(winfaq.de\)](#)

⁷ [Übersicht über die Datenschutzsteuerungen für Microsoft 365 Apps for Enterprise. - Deploy Office | Microsoft Docs](#)

⁸ [Microsoft Office 365 Admin optional verbundenen Erfahrungen deaktivieren | Düsiblog - Matthias Düsi \(duesiblog.de\)](#)

⁹ [Deaktivieren von LinkedIn-Informationen \(microsoft.com\)](#)

4.3.4. Workplace Analytics, Activity Reports, Delve

Diese Funktionalitäten sollten zunächst nicht genutzt werden. Eine Nutzung muss unbedingt im Einzelfall geprüft werden, da es sich um die Auswertung von Leistungsdaten handelt.¹⁰

4.3.5. Kunden-Lockbox

Werden sehr sensible Dokumente mit Microsoft 365 bearbeitet, sollte die Verwendung der Kunden-Lockbox-Funktion von Microsoft in Betracht gezogen werden. Diese stellt eine kundenseitige Verschlüsselung der Dokumente sicher.¹¹

4.3.6. Office Online und Office Mobile

Die Verwendung der Microsoft-365-Webanwendung und der Office-Apps muss bis auf weiteres als datenschutzrechtlich sehr kritisch angesehen werden, bis Microsoft weitere Schritte zur Verbesserung des Datenschutzniveaus innerhalb dieser Software unternimmt.

4.3.7. Durchführung einer Datenschutz-Folgenabschätzung

Je nach Art und Umfang der Daten, die mittels Microsoft 365 verarbeitet werden sollen, ist ggf. die Anfertigung einer eigenständigen Datenschutz-Folgenabschätzung notwendig.

Abschließend kann gesagt werden, dass Microsoft 365 aus datenschutzrechtlicher Sicht noch nicht mit der letzten Rechtssicherheit benutzt werden kann und eine Entwicklung und die ausstehende Rechtsprechung des EuGH abgewartet werden muss.

5. Betrieb und Evergreen

Wichtig bei den Maßnahmen zum Datenschutz und der richtigen Einstellung des Tenants ist es, dass Microsoft in jedem Quartal neue Features und Änderungen an der Microsoft 365 Plattform vornimmt. Eine regelmäßige und auf die Zyklen der Microsoft Releases angepasste Nachkontrolle der Datenschutzeinstellungen ist daher dringend anzuraten, um auch in Zukunft den Datenschutz für die Mitarbeiter:innen, Student:innen und Schüler:innen sicherzustellen. Hierzu sind von spezialisierten Firmen auch entsprechende Newsletter mit den wichtigsten Neuerungen zu finden.¹²

Um sicherzustellen, dass alle Funktionen richtig verstanden und eingestellt werden, empfiehlt Microsoft eine/n eigene/n Mitarbeiter:in, um sich auf den Stand der aktuellen Technik zu halten. Dieses Vorgehen ist für viele öffentliche Einrichtungen und Schulen jedoch zu kostenintensiv. Außerdem ist geeignetes Personal für diese Stelle oftmals nur schwer zu finden.

Aus diesem Grund bietet sich der Servicevertrag mit einem geeigneten Dienstleister an, der sich selbstständig immer auf dem Laufenden hält, und dieses Wissen als Dienstleistung oder Managed Service für die öffentlichen Auftraggeber bereitstellt.¹³

Über diesen Weg sind auch Schulungen der Mitarbeiter:innen, Student:innen und Schüler:innen möglich, um die Applikation möglichst effektiv zu nutzen und nicht unbeabsichtigt selbst Datenschutz-Löcher außerhalb der Microsoft 365 Plattform zu öffnen.

¹⁰ [Microsoft 365 DSGVO-freundlich gestalten \(haake.com\)](https://www.haake.com/microsoft-365-dsgvo-freundlich-gestalten)

¹¹ [Kunden-Lockbox-Anforderungen - Microsoft 365 Compliance | Microsoft Docs](#)

¹² [Evergreen Newsletter – Improve IT \(improve-it.gmbh\)](#)

¹³ [Evergreen Service Modell.pdf \(improve-it.gmbh\)](#)

Der Wechsel von stationärer Hard- und Software in die Cloud ist eine Herausforderung, die ganzheitlich betrachtet werden muss und sich sehr schnelllebig gestaltet. Ein/e Spezialist:in oder ein Partnerunternehmen auf dem Gebiet von Microsoft 365 und zukünftige oder weitere Cloud-Lösungen ist daher für die Zukunft dringend anzuraten.

6. Zusammenfassung

Microsoft hat auf die Bedenken der Datenschutzkonferenz und die gefunden Datenschutzverstöße erstaunlich schnell reagiert. Damit hat Microsoft seine Bereitschaft zur Einhaltung der DSGVO bekräftigt und es Schulen und öffentlichen Einrichtungen ermöglicht, auch zukünftig auf die Plattform Microsoft 365 zu setzen.

Dennoch ist zu beachten, dass ein datenschutzkonformes Microsoft 365-Tenant nicht standardmäßig und out-of-the-box für die europäische Union bereitgestellt wird. Vielmehr muss sich die/der Betreuer:in der eigenen Instanz durch viele einzelne Einstellungen durcharbeiten und die Anpassungen individuell vornehmen.

Außerdem ist zu beachten, dass durch die quartalsweisen Update-Zyklen der Software ein wesentlich höheres Tempo als in der Vergangenheit angeschlagen wird. Auch die Tatsache, dass Versionsupdates nicht mehr einfach ausgesetzt werden können, zwingt die öffentlichen Einrichtungen und Schulen immer mehr zum Handeln und zum schnellen Reagieren. Eine zuverlässige Administration ist daher unerlässlich, jedoch für öffentliche Einrichtungen oft nicht realisierbar.

Aus diesem Grund sollten sich Schulen und öffentliche Einrichtung zeitnah nach einem Partner umsehen, der diese Umgebung permanent analysiert und konkrete Datenschutzvorschläge aktiv an seine Kunden kommuniziert.

7. Autor und Ansprechpartner

Dieses Whitepaper wurde vom Competence Center Microsoft 365 – Modern Work der Improve IT erstellt. Das Competence Center versteht sich als Speerspitze des digitalen Wandels. Es analysiert und bewertet die Möglichkeiten und Auswirkungen von Microsoft 365 permanent und setzt diese Erkenntnisse bei unseren Kunden effektiv ein.



Stefan Ritter
Leiter IT und Prokurist
Tel: +49 172 260 3813
Mail: stefan.ritter@improve-it.gmbh



Wolfgang Fischer
Leiter Vertrieb und Partnermanagement
Tel: +49 172 954 9574
Mail: wolfgang.fischer@improve-it.gmbh

Besuchen Sie uns auf <https://improve-it.gmbh/evergreen>