PRODATIS®

The eBusiness Solution Company.

Office 365 unter Windows:
Datenschutz-Schwachstellen
und Lösungen

Office 365 unter Windows: Datenschutz-Schwachstellen und Lösungen

Office 365 ist derzeit stark in der Diskussion. Welche Variante lässt sich datenschutzkonform einsetzen, welche nicht? Und was muss ein Verantwortlicher dafür tun? Lesen Sie, welche Vor- und Nachteile die verschiedenen Office-Pakete haben.

Microsoft bietet derzeit drei Varianten von Office an:

- Office 365 (z.B. ProPlus/Business) besteht zunächst aus den Webversionen der Office-Programme. Im Weiteren bezeichnen wir diese Version als Office 365 Cloud.
- Dann gibt es die Desktop-Versionen der Office-Programme, im Weiteren Office 365 Desktop genannt.
- Schließlich haben wir noch die ebenfalls lokal installierten mobilen Versionen der Office-Programme für Android, iOS und Windows, hier Office 365 Mobile.

Office 365 Desktop ist im Wesentlichen identisch mit Office 2019, das nur aus den Desktop-Versionen besteht. Office 2019 erhält ausschließlich Sicherheitsupdates, Office 365 Desktop zusätzlich Funktionsupdates.

Grundlagen

Wer Office 365 Cloud nutzt, tut dies zwingend auf Servern von Microsoft. Er greift auf die Programme mit einem Browser zu.

Die Funktionen zur Datenspeicherung und Freigabe (OneDrive) sowie für Teamarbeit und Kommunikation (Teams und SharePoint) setzen ebenfalls ausnahmslos die Cloud-Nutzung voraus.

Rechtsgrundlagen

Jede Verarbeitung personenbezogener Daten unterliegt dem Prinzip des Verbots mit Erlaubnisvorbehalt, d.h. es muss eine Rechtsgrundlage vorhanden sein, die die jeweilige Datenverarbeitung rechtfertigt.

Office 365 ist ein Arbeitsmittel, das der Arbeitgeber zur Verfügung stellt. Für die Verarbeitung personenbezogener Daten, die dadurch erfolgt, ist zunächst der Arbeitgeber datenschutzrechtlich verantwortlich.
Die Haupt-Rechtsgrundlage für die Verarbeitung von per-

sonenbezogenen Beschäftigtendaten stellt Art. 88 Datenschutz-Grundverordnung (DSGVO) in Verbindung mit § 26 Bundesdatenschutzgesetz (BDSG) dar.

Er erlaubt dem Arbeitgeber – vereinfacht gesagt – die Datenverarbeitung, wenn sie erforderlich ist, um das Beschäftigungsverhältnis durchzuführen.

Hiervon ist auch die Verarbeitung personenbezogener Daten in den IT-Systemen bzw. durch die IT-Systeme des Arbeitgebers umfasst.

Ebenso gilt diese Rechtsgrundlage für die einzelnen Beschäftigten, die in Erfüllung ihrer arbeitsrechtlichen Vorgaben die erforderlichen Daten verarbeiten.

Zusätzlich kann die Rechtsgrundlage der Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO infrage kommen.

Das betrifft bei Office 365 die personenbezogenen Daten, die die Anwendung an Microsoft übermittelt und die anderen Zwecken als der Durchführung des Beschäftigungsverhältnisses dienen.

Technische & organisatorische Maßnahmen
Zu den Grundlagen gehören neben der rechtlichen Basis – ausgehend von der Sensibilität der Daten – angemessene technische und organisatorische Schutzmaßnahmen (Art. 32 DSGVO, § 22 BDSG).

Insbesondere wenn es um sogenannte besondere Kategorien personenbezogener Daten geht, sind die Anforderungen hoch.

Zu den besonderen Kategorien personenbezogener Daten gehören Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung, im Beitrag „sensible Daten" genannt.

Gemeinsame Verantwortung?
Sind an der Datenverarbeitung externe Unternehmen wie Microsoft beteiligt, sind je nach Konstellation zusätzlich Verträge nötig:

- Auftragsverarbeitung liegt vor, wenn der Externe die Daten im Auftrag der verantwortlichen Stelle verarbeitet. Der Auftragsverarbeiter darf die Daten dabei nicht zu eigenen Zwecken nutzen und muss sich an die Weisungen der verantwortlichen Stelle halten.
- Gemeinsame Verantwortung (Joint Controllership) liegt vor, wenn die verantwortliche Stelle gemeinsam mit dem Externen die Zwecke und Mittel einer Verarbeitung festlegt. Im Hinblick auf Office 365 scheint sich die herrschende Meinung auf eine gemeinsame Verantwortung festzulegen.

Findet bei der Verarbeitung ein Datentransfer in ein sogenanntes Drittland statt – Drittland ist jedes Land außerhalb der EU/des EWR –, dann sind die zusätzlichen rechtlichen Anforderungen der Art. 44 ff. DSGVO zu erfüllen.

Im Fall der USA liegt das EU-US-Abkommen „Privacy Shield" vor. Es garantiert für diejenigen Unternehmen, die sich danach zertifiziert haben, ein angemessenes Datenschutzniveau nach Art. 45 DSGVO. Die Microsoft Corporation ist derzeit nach Privacy Shield zertifiziert.

ACHTUNG: Formal ist der Privacy Shield, auf den sich die Datenübermittlung an Microsoft stützt, nach wie vor anwendbar.

Allerdings ist vor dem Europäischen Gerichtshof (EuGH) ein Verfahren zur Rechtmäßigkeit des Privacy Shield anhängig.

Insbesondere machen die Kläger geltend, dass nach wie vor anlassunabhängige Datenerhebungen aufgrund von US-Regelungen, wie etwa dem U.S. CLOUD Act (siehe Ehmann, Heft 09/2019, S. 13 ff.), möglich sind und keine effektiven Kontrollen existieren. Die Entscheidung des EuGH wird für Anfang 2020 erwartet.

Inhaltsdaten
Unabhängig davon, welche Version der Office-Programme – Cloud oder lokal installiert – ein Verantwortlicher nutzt, hat er immer die Wahl, Office-Dateien entweder in der Cloud oder lokal zu speichern.

Ist Office 365 Cloud im Einsatz, entsteht allerdings stets eine Kopie in der Cloud.

Nur wer ausschließlich die lokal installierte Office-365-Desktop-Version nutzt, kann auch die Inhalte der verarbeiteten Dateien lokal halten.

Microsoft bemüht sich zwar auch hier, in den Voreinstellungen die Anwender zu „überreden", die Daten in der Cloud, also in OneDrive oder SharePoint, zu speichern.

Die lokale Speicherung lässt sich jedoch voreinstellen. Hierzu einfach unter „Datei – Optionen – Speichen" die Option „Standardmäßig auf dem Computer speichern" aktivieren.

Diese Einstellung gilt dann für alle Anwendungen im Office-365-Desktop-Paket. Diese Einstellungen kann der Nutzer jedoch jederzeit ändern.

Office 365 Mobile speichert die Daten lokal auf dem Gerät. Je nach Betriebssystem des mobilen Geräts schlägt jedoch das Betriebssystem eine Speicherung in der Cloud des Betriebssystem-Herstellers vor.

Verschlüsselung
Arbeitsrelevante Inhalte in Dokumenten, E-Mails etc. sind von der Rechtsgrundlage von Art. 88 DSGVO in Verbindung mit § 26 BDSG erfasst.

Enthalten die Dokumente allerdings sensible Daten, wie z.B. Gesundheitsinformationen im Bereich der Personalverwaltung, so müssen die Mitarbeiter diese Daten nach herrschender Meinung verschlüsseln, bevor sie sie in der Cloud speichern. Das Gleiche gilt für Daten, die der Arbeitgeber für vertraulich erklärt hat.

Lässt sich eine verschlüsselte Speicherung nicht bewerkstelligen, muss es eine organisatorische Anweisung geben, solche Daten ausschließlich lokal zu speichern. Denn eine verschlüsselte Speicherung der Daten in der Cloud lässt sich nur mit Zusatzprogrammen erreichen.

Keine der Office-365-Varianten unterstützt standardmäßig eine verschlüsselte Speicherung der Dateien.

Lizenzkontrolle
Startet eine Office-365-Desktop-Anwendung zum ersten Mal am Tag, baut sie eine Verbindung mit einem Lizenzserver auf und führt dort ein Log-in durch.

Damit erhält Microsoft die IP-Adresse sowie den (dienstlichen) Nutzernamen und das Konto-Passwort des Office-365-Nutzers.

Das Office-365-Nutzerkonto ist personalisiert. Es lässt sich bestenfalls pseudonymisieren.

Für die Verarbeitung dieser Daten kommt als Rechtsgrundlage die Interessenabwägung in Betracht.

Dabei kann es sich sowohl um die berechtigten Interessen des Unternehmens als auch um das Interesse von Microsoft an einer ordnungsgemäßen Lizenzkontrolle handeln.

Die schutzwürdigen Interessen der betroffenen Personen am Ausschluss einer Übermittlung dürften in diesem Fall nicht überwiegen.

Zwar wäre es datenschutzrechtlich vorzuziehen, wenn eine Lizenzkontrolle nicht auf der Basis von Daten einzelner Personen, sondern anhand von Unternehmensdaten erfolgt.
Da es sich aber um dienstliche Nutzerdaten handelt und die Beschäftigten vernünftigerweise von dieser Art der Nutzung ausgehen müssen, erscheint diese Datenübertragung im Ergebnis gerechtfertigt.

Telemetriedaten

Microsoft erhebt sogenannte Telemetriedaten sowohl im Betriebssystem Windows 10 als auch im Office. Diese Daten werden an Microsoft transferiert und dort ausgewertet, z.B. um Funktionalitäten zu verbessern und Fehler zu suchen.

Die Telemetriedaten sind zumindest teilweise personenbezogen. Das Betriebssystem nutzt etwa 1.000 bis 1.200 unterschiedliche Ereignisarten, Office zwischen 23.000 und 25.000.

Bei der Übertragung der Telemetriedaten werden nach aktuellem Kenntnisstand keine Dateinamen und keine Dateiinhalte transferiert.

Während sich die Windows-Telemetriedaten-Übertragung reduzieren, aber nicht vollständig abstellen lässt, ist es möglich, die Office-365-Telemetriedaten-Übertragung ab der Version 1904 von Office 365 ProPlus komplett zu deaktivieren.

In anderen Versionen (z.B. Office für Mac) soll dies auch bald möglich sein (siehe https://ogy.de/overview-privacy-controls). Auch die Nutzung der sogenannten „verbundenen Dienste" und die Integration von LinkedIn sollten Verantwortliche über die Einstellungen unterbinden.

In Windows 10 Enterprise lässt sich die minimale Stufe „Sicherheit" wählen. Dann überträgt das Betriebssystem nur Daten, die zum Schutz von Windows und Windows Server erforderlich sind. Windows 10 Pro kennt diese Stufe nicht.

Allerdings dürften für die datenschutzrechtliche Legitimation ausschließlich die personenbezogenen Telemetriedaten übermittelt werden, die erforderlich sind, um die Services zu erbringen oder die Systeme zu schützen.

Nur dann liegen berechtigte Interessen vor, und nur dann überwiegen sie auch.

Fazit: Im Datenschutz schneidet Office 365 Desktop am besten ab

Wer die Variante Office 365 Desktop/2019 geeignet konfiguriert, kann sie rechtskonform einsetzen. „Geeignet" heißt:

- Telemetrie deaktivieren
- Speicherung in der Cloud nur eingeschränkt nutzen

Eine ausführliche Darstellung der datenschutzrechtlichen und technischen Fragen findet sich in zwei Analysen, die die Firma Privacy Company für das niederländische Ministerium für Recht und Sicherheit erstellt hat.

Die PDFs sind zu finden unter https://ogy.de/dpia-windows-10.

Der Bundesbeauftragte für den Datenschutz hat zur Frage, ob sich Office 365 in der Bundesverwaltung datenschutzkonform einsetzen lässt, ebenfalls eine Prüfung angestoßen. (Anmerkung: Den Verfassern ist nicht bekannt, auf welche der unterschiedlichen Einsatzvarianten sich diese Prüfung bezieht.)

Es gibt Hinweise darauf, dass das Ergebnis restriktiv ausfallen wird.

Die Office-365-Mobile-Varianten übertragen u.a. Nutzungsdaten an das Markforschungsunternehmen Braze (https://ogy.de/microsoft-telemetrie). Daher sind sie sehr kritisch zu sehen.

Die Office-365-Cloud-Variante lässt sich nur unter gewissen Voraussetzungen datenschutzkonform nutzen. Diese Voraussetzungen sind jedoch zum derzeitigen Zeitpunkt nicht in Gänze erfüllt.

Eine Zusammenfassung der Zulässigkeit der Nutzung der Office-Varianten zeigt die folgende Tabelle.

Office Variante	Nur lokale Speicherung	Speicherung in der Cloud
Office 365 Cloud	• nicht möglich, da immer eine Kopie in der Cloud existiert	• unverschlüsselte vertrauliche Daten • unverschlüsselte sensible personenbezogene Daten • normale personenbezogene Daten • verschlüsselte vertrauliche Daten • verschlüsselte sensible personenbezogene Daten • öffentliche Daten
Office 365 Desktop/2019	• vertrauliche Daten • normale und sensible personenbezogene Daten • öffentliche Daten	• unverschlüsselte vertrauliche Daten • unverschlüsselte sensible personenbezogene Daten • normale personenbezogene Daten • verschlüsselte vertrauliche Daten • verschlüsselte sensible personenbezogene Daten • öffentliche Daten
Office 365 Mobile	• vertrauliche Daten • normale und sensible personenbezogene Daten • öffentliche Daten	• unverschlüsselte vertrauliche Daten • unverschlüsselte sensible personenbezogene Daten • normale personenbezogene Daten • verschlüsselte vertrauliche Daten • verschlüsselte sensible personenbezogene Daten • öffentliche Daten

Die Übersicht zeigt die Zulässigkeit der Nutzung der Office-Varianten bei ausschließlich lokaler Speicherung bzw. bei Speicherung in der Cloud.

Rote Daten dürfen generell nicht gespeichert werden.

Gelbe Daten bedürfen einer Risikobewertung, ob sie in der Cloud unverschlüsselt gespeichert werden dürfen.

Grüne Daten dürfen lokal bzw. in der Cloud gespeichert werden.

Bei Office 365 Mobile ist zu prüfen, inwieweit die nativen Cloud-Dienste der mobilen Betriebssysteme (z.B. iCloud bei iOS) die Dateien in die Cloud synchronisieren.

Auf Dauer wäre der Betrieb der Office-365-Cloud-Software auf eigener Hardware („on premise“) sinnvoll.

Ob das möglich wird, hängt jedoch vom Druck der Datenschutzaufsicht sowie vom Druck der europäischen Kunden auf Microsoft ab.

Quelle:
www.datenschutz-praxis.de