BRANDI
RECHTSANWÄLTE

# DIE NUTZUNG VON MICROSOFT 365 IM UNTERNEHMEN

Informationen zum Datenschutz I Juni 2024

English version

## Einleitung

Microsoft 365 ist aus dem Arbeitsalltag vieler Unternehmen und Einrichtungen nicht mehr wegzudenken. Im Bereich der gängigen Office-Anwendungen (etwa Textverarbeitung und Tabellenkalkulation) verfügt Microsoft ohnehin über einen beherrschenden Marktanteil. Das Angebot für Microsoft 365 umfasst neben den Office-Anwendungen außerdem viele weitere Dienste und Funktionen, die den Unternehmensalltag bzw. die interne Organsation erheblich erleichtern und verbessern, beispielsweise durch die Einbeziehung der Kollaborationsprogramme Microsoft Teams oder Microsoft SharePoint.

Doch die Nutzung von Microsoft 365 wird, vor allem seitens der Aufsichtsbehörden, unter datenschutzrechtlichen Gesichtspunkten kritisch gesehen. Um bestehende Risiken zu minimieren, können verantwortliche Stellen aber zahlreiche Schutzvorkehrungen treffen.

## Nutzungs- und Vertragsmodell

Die Dienste werden in der Regel in Form von Abo-Modellen als Cloud-Lösung angeboten. Daten werden somit regelmäßig in der Cloud von Microsoft gespeichert. Angeboten werden aber weiter auch „on-premise"-Lösungen, in denen die Daten lokal auf den eigenen Systemen gespeichert werden. Diese Form der Zusammenarbeit ist aus datenschutzrechtlicher Sicht sicherlich zu begrüßen, aber für viele Unternehmen wohl nicht praktikabel.

Für die Nutzung von Microsoft 365 ist eine Lizenzvereinbarung mit dem Dienstleister abzuschließen. Da die Nutzung des Dienstes auch stets mit der Verarbeitung von personenbezogenen Daten verbunden ist, ist zur datenschutzrechtlichen Absicherung daneben auch eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO (bei Microsoft kurz „DPA") abzuschließen.

## Kritik an Microsoft

Die Nutzung von Microsoft 365 steht seitens von Aufsichtsbehörden unter stetiger Kritik. Die häufigsten Kritikpunkte beziehen sich dabei vor allem auf die intransparenten Datenverarbeitungsvorgänge durch Microsoft und Datenübermittlungen in die USA.

Darüber hinaus wird auch kritisiert, dass durch die Vertragsgestaltung erhebliche Abhängigkeiten für die Kunden entstehen. Durch das Abo-Modell ist es beispielsweise bei automatischen Updates teilweise nicht möglich, Updates auszulassen und ältere Versionen der Dienste zu nutzen. Aus dieser Problematik folgt jedenfalls, dass die neuesten Entwicklungen bei Microsoft stets sorgfältig beobachtet werden müssen, um bei etwaigen datenschutzwidrigen Praktiken bei Microsoft die Zusammenarbeit mit dem Dienstleister schnell umstellen oder im worst case gar beenden zu können.

Exemplarisch für die Kritik der Aufsichtsbehörden sei hier etwa die Festlegung der Datenschutzkonferenz aus dem November 2022 genannt. Diese kam zu dem Schluss, dass Verantwortlichen der Nachweis der datenschutzkonformen Nutzung auf Grundlage der Vertragsunterlagen und Informationen von Microsoft nicht erbracht werden kann.

Einige Kritikpunkte die hinsichtlich der Nutzung von Microsoft 365 üblicherweise erhoben werden, sollen nachfolgend näher dargestellt und eingeordnet werden.

**a) Transparenz bei Microsoft**

Ein Risikofaktor bei der Nutzung ist das Erfordernis zur Erfüllung der Rechenschaftspflicht. Nach Art. 5 Abs. 2 DSGVO müssen Unternehmen und Einrichtungen positiv nachweisen können, die datenschutzrechtlichen Bestimmungen einzuhalten.

Dies ist bei der Nutzung von Microsoft 365 angesichts der intransparenten Informationen von Microsoft zum Datenschutz nur schwer möglich. Interpretationsspielraum bietet die Rechenschaftspflicht dahingehend, wie umfassend der Nachweis der Datenschutzkonformität tatsächlich erbracht werden muss. Gerade das Modell der Auftragsverarbeitung, das im vorliegenden Fall einschlägig ist, geht davon aus, dass der Auftraggeber im Rahmen der Hinzuziehung von Dienstleistern nicht stets die volle Kontrolle über das Gesamtsystem hat. Dem Dienstleister stehen im Rahmen der durch die Weisung des Auftraggebers gesteckten Grenzen auch immer ein gewisser eigenständiger Handlungs- und Gestaltungsspielraum zu.

Microsoft argumentiert hinsichtlich der Abstraktheit der bereitgestellten Informationen auch mit dem Interesse am Schutz von Geschäftsgeheimnissen und der Sicherheit der technischen Systeme. Richtigerweise lässt sich kaum in Zweifel ziehen, dass je konkreter die technischen Systeme und Vorgänge beschrieben werden, desto einfacher es für potentielle Angreifer wird, technische Sicherungsmaßnahmen zu überwinden.

**b) Datenverarbeitung zu eigenen Zwecken**
Im Rahmen der Auftragsverarbeitung dürfen Daten nur nach Weisung des Auftraggebers verarbeitet werden. Microsoft verarbeitet nach eigenen Angaben Daten jedoch nicht ausschließlich auf Weisung des Auftraggebers, sondern bestimmte Daten (etwa Diagnose- und Telemetriedaten) auch zu eigenen Zwecken. Dies ist deutlich zu kritisieren.

Microsoft 365 sieht aber auch Möglichkeiten vor, die Verarbeitung von Diagnose- und Telemetriedaten zu unterbinden bzw. zu minimieren. Diese technischen Möglichkeiten sollten seitens nutzender Unternehmen und Einrichtungen auch wahrgenommen werden. Zusätzlich sollten Unternehmen Nutzer transparent über die Verwendung der Daten durch Microsoft informieren.

**c) Weitere Mängel bei der Vereinbarung zur Auftragsverarbeitung**
Bei der Ausgestaltung des DPA-Musters von Microsoft wird bemängelt, dass die verarbeiteten Datenarten und Kategorien betroffener Personen nicht hinreichend umrissen, sondern nur abstrakt benannt werden.

Hier muss man aber auch anmerken, dass Microsoft nur bedingt in der eigenen Hand hat, welche Daten konkret anfallen. Der konkrete Nutzungsumfang wird ja gerade vom nutzenden Unternehmen bestimmt und nicht von Microsoft als Dienstleister.

Weiterhin werden fehlende Weisungs- und Kontrollrechte bemängelt. Dies ist sicherlich zutreffend zu kritisieren, eingeschränkte Weisungs- und Kontrollrechte gehören bei den Big Playern aber wohl leider zur Natur der Sache. Die Kunden von Microsoft bleiben letztendlich aber stets die Herren der eigenen Daten und die Zusammenarbeit kann im worst case beendet werden. Somit kann man durchaus argumentieren, dass die Mindestanforderung an die Kontrolle von Auftraggebern im Bereich der Auftragsverarbeitung wohl gerade noch so eingehalten wird.

**d) Drittstaatenübermittlung in die USA**
Ein weiterer Kritikpunkt der Zusammenarbeit mit Microsoft ist die stattfindende Datenübermittlung in die USA und die damit verbundenen Zugriffsmöglichkeiten von US-Sicherheitsbehörden.

Dies wurde insbesondere nach dem Schrems II-Urteil aus dem Sommer 2020 relevant, in welchem der bis dahin anwendbare Angemessenheitsbeschluss „EU-US Privacy Shield“ für unwirksam erklärt wurde.

In der Zwischenzeit wurde ein neuer Angemessenheitsbeschluss der EU-Kommission erlassen, das EU-US Data Privacy Framework, unter dem Microsoft auch zertifiziert ist. Die Datenübermittlung in die USA kann somit momentan auf den Angemessenheitsbeschluss gestützt werden. Da an dem Regelwerk aber schon deutliche Kritik geäußert wurde und perspektivisch mit einer erneuten Überprüfung durch den EuGH zu rechnen ist, sollten die weiteren Entwicklungen genau beobachtet werden.

**e) Datenschutz-Folgenabschätzung**
Oftmals wird vertreten, dass vor der Nutzung des Dienstes stets eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen ist. Dies geht jedoch zu weit und nach richtiger Auffassung muss stattdessen im Rahmen einer Risikoabwägung im konkreten Fall ermittelt werden, ob eine erhöhte Gefährdung für die personenbezogenen Daten der betroffenen Personen besteht. Lediglich bei einem erhöhten Risiko für die Daten – etwa bei einer umfangreichen Verarbeitung von sensiblen personenbezogenen Daten nach Art. 9 DSGVO – sollte zwingend eine Datenschutz-Folgenabschätzung durchgeführt werden. Jedenfalls ist aber eine umfangreiche Dokumentation der Nutzung ratsam.

## Handlungsempfehlungen

Trotz der Kritik an Microsoft ist es möglich, bestehende Risiken zu minimieren, um so eine datenschutzkonforme Nutzung des Dienstes zu erreichen, auch wenn freilich stets bestimmte Restrisiken verbleiben.

Da die Standardvereinbarung von Microsoft stets aktualisiert wird, empfiehlt es sich, die aktuelle Fassung der Vereinbarung zur Auftragsverarbeitung mit dem Dienstleister abzuschließen.

Unternehmen und Einrichtungen sollten die Nutzung des Dienstes umfassend dokumentieren und technische Einstellungsmöglichkeiten möglichst datenschutzfreundlich nutzen, um etwa die Verarbeitung von Diagnose- und Telemetriedaten minimieren. Darüber hinaus sollten Daten bei Möglichkeit lediglich in verschlüsselter Form auf den Systemen von Microsoft gespeichert werden.

Daneben sollten organisatorische Maßnahmen ergriffen werden, beispielsweise dahingehend, dass den Mitarbeitern verbindliche Vorgaben zur Nutzung von Microsoft 365 gemacht werden. In diesem Zuge sollte auch die Remote-Tätigkeit durch technische Maßnahmen wie VPN-Verbindungen und Zwei-Faktor-Authentifizierungen technisch abgesichert werden.

Hendrik Verst

**Kontakt:**

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

**Hendrik Verst**
Wissenschaftlicher Mitarbeiter

T +49 521 96535 - 981
F +49 521 96535 - 113
M hendrik.verst@brandi.net