**Hinweise und Musterantworten**

**zur datenschutzkonformen Nutzung von Office/Microsoft 365**

*von Prof. Dr. Thomas Hoeren und Marten Tiessen*

# Hintergrund

Das Microsoft-Office-Paket gehört in vielen Unternehmen zur digitalen Grundausstattung. Die Büro-Suite enthält zahlreiche Dienste, die im Büroalltag eingesetzt werden, wie z.B. Word, PowerPoint, Excel, Outlook und Teams. Gegenüber früher gängigen Office-Paketen, deren Funktionen sich auf die lokale Anwendung beschränkten, bietet Microsoft 365, das ehemals Office 365 hieß, zusätzliche Onlinedienste. Dazu gehören unter anderem mehrere Cloud-Dienste, wie OneDrive und Exchange Online, bei denen die Daten statt im eigenen Unternehmen auf Servern von Microsoft gespeichert werden. Da sich unter den Daten, die an Microsoft weitergeleitet werden, auch personenbezogene Daten befinden, muss die Übertragung datenschutzrechtlichen Anforderungen entsprechen. Die Verantwortung dafür trifft nicht nur Microsoft, sondern in erster Linie die Unternehmen, die Microsoft 365 abonnieren und ihren Mitarbeitern zur Verfügung stellen. Sie sind datenschutzrechtlich Verantwortliche für die Verarbeitung personenbezogener Daten bei Nutzung der Dienste und haften für etwaige Datenschutzverstöße. Microsoft wird dagegen für die meisten Verarbeitungsvorgänge als Auftragsverarbeiter des Kunden angesehen. Nur in einigen Konstellationen sieht sich Microsoft selbst als Verantwortlicher der Datenverarbeitung.

Obwohl eine datenschutzkonforme Anwendung also sowohl im Interesse der Kunden als auch in Microsofts Interesse liegt, werden von den Datenschutzbehörden immer wieder Zweifel gestreut, ob sich Microsoft 365 zurzeit überhaupt im Einklang mit der Datenschutzgrundverordnung (DSGVO) anwenden lässt. Die bisherige Kritik stützt sich dabei hauptsächlich auf zwei Punkte: Zum einen wurde der zwischen Microsoft und seinen Kunden bestehende Auftragsverarbeitungsvertrag als zu unpräzise angesehen. Zum anderen besteht große Unsicherheit, ob die Datenübermittlung auf Microsoft-Server, die sich in den USA befinden, europäischen Datenschutzanforderungen gerecht wird. Diese Bedenken bestehen vor allem, seitdem der EuGH letztes Jahr in seinem Schrems-II-Urteil festgestellt hat, dass das sogenannte Privacy Shield keine wirksame Rechtsgrundlage für Datenübertragungen in die USA darstellt.

In einer Stellungnahme aus dem letzten Jahr kam die deutsche Datenschutzkonferenz, ein Zusammenschluss der Datenschutzbehörden des Bundes und der Länder, zum Ergebnis, dass das damalige Office 365 nicht datenschutzkonform verwendet werden kann. Ihre Bewertung beruhte dabei aber allein auf dem ersten der beiden zuvor genannten Kritikpunkte, der Formulierung des Auftragsverarbeitungsvertrags. Technische Begebenheiten wurden hingegen gar nicht berücksichtigt. Die Einschätzung der Datenschutzbehörden sollte jedoch kein Grund zur Beunruhigung sein, da die Bewertung schon zum Entscheidungszeitpunkt auf veralteten Vertragsbedingungen beruhte, die inzwischen mehrfach durch Microsoft überarbeitet wurden. Das Abstimmungsergebnis zeigt außerdem, dass zwischen den Datenschutzbehörden der Länder keinesfalls Einigkeit in der Sache bestand. Die Bewertung wurde nur von 9 der 17 Datenschutzbehörden mitgetragen. Insbesondere die Datenschutzbehörden von Bayern, Baden-Württemberg, Hessen und dem Saarland sowie das Bayerische Landesamt für Datenschutzaufsicht, das für Microsoft Deutschland zuständig ist, hielten die Bewertung für zu undifferenziert.

Auch in Hinblick auf die Datenübermittlung an Microsoft-Server besteht kein Grund zur Panik. Zwar verschärfen sich durch das Schrems-II-Urteil die Anforderungen an eine rechtskonforme Datenübertragung. Möglich ist eine solche aber weiterhin. Auch diesbezüglich stehen die Datenschutzbehörden zurzeit noch mit Microsoft im Dialog. Konkrete Sanktionen durch die Datenschutzbehörden sind daher zum jetzigen Zeitpunkt unwahrscheinlich. Allerdings haben die Datenschutzbehörden es sich in der Vergangenheit zur Gewohnheit gemacht, Fragebögen an Unternehmen zu schicken, um deren Datenumgang nachzuvollziehen. Auch wenn die Beantwortung solcher Fragebögen nicht immer verpflichtend ist, sollten Unternehmen proaktiv ihre eigene Verwendung von Microsoft 365 überprüfen und auf eine solche Befragung zumindest vorbereitet sein. Hierfür soll dieser Text eine Hilfestellung bieten, indem er mögliche Fragen zur datenschutzkonformen Nutzung von Microsoft 365 aufwirft und Hinweise und Beispiele zur Beantwortung darlegt. Bitte beachten Sie dabei zunächst die nachfolgenden Erläuterungen.

# Erläuterungen zu den Hinweisen und Antwortbeispielen

Die folgenden Hinweise wurden von Professor Dr. Thomas Hoeren und Marten Tiessen entwickelt. Die Hinweise und Antwortbeispiele sollen Ihnen bei der Beantwortung von Fragen der Datenschutzbehörden zur Drittstaatenübermittlung mittels Office/Microsoft 365 helfen. Es ist Ihnen gestattet, sich für diesen Zweck an den Formulierungen dieser Hinweise und Antwortbeispiele zu orientieren. Eine Nennung der Urheber ist für diesen Fall nicht erforderlich. Bitte beachten Sie jedoch, dass wir eine Gewährleistung und Haftung für die Rechtmäßigkeit und Richtigkeit des Inhalts ausdrücklich ausschließen und nachdrücklich vor einer unbedachten Übernahme der Antwortbeispiele, die auf die konkreten Bedürfnisse des Einzelfalls immer angepasst werden müssen, warnen.

# Beispielsfragen mit Hinweisen und Antwortbeispielen

## Wie nutzt Ihr Unternehmen Microsoft 365?

Hinweise: Microsoft 365 ist in verschiedenen Editionen erhältlich, die jeweils unterschiedliche Dienste und Funktionen beinhalten. Zu den wichtigsten Anwendungen gehören Word, Excel, PowerPoint, Outlook, OneNote, OneDrive, Skype for Business und Teams. Da die datenschutzrechtliche Einordnung zwischen den verschiedenen Anwendungen variieren kann, sollte bei der Beantwortung der Frage direkt aufgezeigt werden, welche Dienste genutzt werden. Dies gilt auch für die weiteren Anwendungen und Dienste, die oben nicht genannt wurden.

Antwortbeispiel: *Wir abonnieren als Unternehmen das Büropaket Microsoft 365 in der Edition E5*. *Von den im Paket enthaltenen Diensten nutzen wir ausschließlich Word, Excel, PowerPoint, Outlook und Exchange Online.*

## Welche personenbezogenen Daten werden dabei verarbeitet?

Hinweise: Bei der Nutzung der Microsoft-365-Dienste werden personenbezogene Daten durch den Kunden erhoben und vielfach an Microsoft weitergeleitet. Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu können Text-, Ton-, Video- oder Bilddateien, aber auch Diagnose- oder Metadaten gehören. Welche personenbezogenen Daten verarbeitet werden, hängt von den Diensten, die genutzt werden, sowie von der konkreten Art der Nutzung ab. Bei Microsoft Teams können beispielsweise Videoaufnahmen der Mitarbeiter verarbeitet werden, während in Outlook der Emailverkehr mit Geschäftspartnern gespeichert wird. Zu den betroffenen Personen können die Mitarbeiter, Kunden, Partner und Auftragnehmer des Abonnenten zählen.

Zur Beantwortung der Frage sollte sich das Unternehmen zunächst vergegenwärtigen, welche personenbezogenen Daten in den eigenen Prozessen bei der Nutzung eines Dienstes von Microsoft 365 verarbeitet werden. Wenn nicht bereits ein Verarbeitungsverzeichnis gem. Art. 30 DSGVO existiert, sollte diese Möglichkeit genutzt werden, um im Hinblick auf die Nutzung von Microsoft 365 ein solches zu entwerfen. Dabei sollte nicht nur berücksichtigt werden, welche Daten für eigene Zwecke verarbeitet werden, sondern auch, welche Daten Microsoft für deren Zwecke bereitgestellt werden.

Antwortbeispiel: *Folgende Kategorien personenbezogener Daten werden beim Einsatz von Microsoft 365 verarbeitet:*

*- E-Mailkommunikation*

*- Videokommunikation*

*- Daten der Termin- und Ressourcenverwaltung*

*- Dokumente, Präsentationen und Tabellen*

*- Kontaktinformationen*

*- Authentifizierungs- und Lizenzierungsdaten*

*- Personenbezogene Basisdaten*

*- Logfiles mit Zugriffen*

*- System-generierte Protokolldaten*

Ferner ist wichtig, welche Einstellungen das Unternehmen als Administrator vorgenommen hat. Microsoft 365 erlaubt es den Nutzern, bestimmte Dienste und die damit einhergehende Datenverarbeitung einzuschränken oder ganz auszuschalten. Dabei ist es aus datenschutzrechtlicher Sicht ratsam, eine Konfiguration vorzunehmen, bei der möglichst wenig personenbezogene Daten verarbeitet werden.

Antwortbeispiel: *Die Erhebung und Übertragung von Diagnosedaten wurde in den Konfigurationen ausgeschaltet. Die Synchronisierung von Telemetriedaten sowie die Anwendung von Microsoft Connected Experiences wurde deaktiviert. Microsoft Workplace Analytics wird nicht verwendet.*

## Zu welchen Zwecken und auf welcher Rechtsgrundlage erfolgt die Nutzung von Microsoft 365?

Hinweise: Die Zwecke der Verarbeitung sollten so konkret wie möglich formuliert sein. Als übergeordneter Zweck kann die Arbeit im Unternehmen sowie die Kommunikation zwischen Mitarbeitern, Kunden, Kooperationsunternehmen und Dienstleistern genannt werden.

Im Hinblick auf das ergangene Schrems-II-Urteil ist hier besonders die Verarbeitung personenbezogener Daten relevant, bei denen eine Übermittlung in die USA stattfindet. Wie unten noch dargelegt wird, kann dies auf sämtliche Daten zutreffen.

1. Erfüllung eines Vertrages

Der Großteil der personenbezogenen Daten wird von Unternehmen zur Erfüllung vertraglicher Verpflichtungen verarbeitet. Dabei gibt das Vertragsverhältnis oftmals den Zweck der Datenverarbeitung vor. Darunter fällt auch der vorvertragliche Bereich wie Bewerbungsgespräche oder Kostenvoranschläge.

So wird es zum Beispiel im Rahmen eines Versandhandelsgeschäfts notwendig, dass der Name und die Adresse des Kunden verarbeitet werden. Auch generell wird bei der Erstellung einer Rechnung die Adressierung an den Kunden erforderlich. Wird diese Rechnung mittels eines Programmes von Microsoft 365 erstellt, liegt eine Nutzung zu Zwecken einer Rechnungserstellung im Rahmen eines Vertrages vor. Die Verarbeitung kann in diesem Fall auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden.

Unter diesen Punkt können auch Verarbeitungen gefasst werden, die innerhalb eines Unternehmens auf Grundlage des Arbeitsvertrages notwendig werden. Eine innerbetriebliche Videokonferenz kann hier als Beispiel dienen. Die Verarbeitung von Mitarbeiterdaten richtet sich allerdings wegen der Öffnungsklausel in Art. 88 Abs. 1 DSGVO nach der Regelung aus § 26 Abs. 1 BDSG.

2. Erfüllung einer rechtlichen Verbindlichkeit

Art. 6 Abs. 1 lit. c DSGVO dient als Rechtsgrundlage, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verbindlichkeit notwendig ist. Der Zweck der Nutzung von Microsoft 365 liegt dann in der Erfüllung dieser rechtlichen Verbindlichkeit. Hier sollte genau beschrieben werden, welche rechtliche Verbindlichkeit erfüllt werden soll. Beispielsweise sind im Handels-, Gewerbe-, Steuer- und Sozialrecht gewisse Aufzeichnungs- und Aufbewahrungspflichten normiert, die zur Verschriftlichung die Nutzung eines Dienstes notwendig machen.

3. Berechtigte Interessen des Verantwortlichen

Als typischer Zweck kommen weiterhin berechtigte Interessen des Verantwortlichen in Betracht. In den Erwägungsgründen der DSGVO werden zum Beispiel der Datenaustausch innerhalb einer Unternehmensgruppe sowie die Gewährleistung der IT-Sicherheit genannt (ErG 47 ff.).

Verarbeitungen innerhalb dieser Kategorie können auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Jedoch ist mit diesem Erlaubnistatbestand eine gewisse Rechtsunsicherheit verbunden, da nicht zwingend davon ausgegangen werden kann, dass die Interessen des Verantwortlichen gegenüber denen der Betroffenen überwiegen.

Sind Daten zwingend für die Funktionalität eines Dienstes erforderlich, wie beispielsweise Authentifizierungs- oder Lizenzierungsdaten, können diese bereits auf die Erfüllung eines bestehenden Vertragsverhältnisses nach Art. 6 Abs. 1 lit. b DSGVO gestützt werden.

4. Verarbeitung zu anderen Zwecken:

Sollte die Verarbeitung zu anderen Zwecken als den hier beschriebenen Zwecken geschehen, sollte sich das Unternehmen vor der konkreten Verarbeitung um eine Einwilligung der betroffenen Person bemühen, sodass die Verarbeitung auf Art. 6 Abs. 1 lit. a DSGVO als Rechtsgrundlage gestützt werden kann. In der DSGVO bestehen zwar weitere Möglichkeiten rechtlicher Grundlagen. Diese betreffen privatrechtlich arbeitende Unternehmen jedoch im Regelfall nicht.

Antwortbeispiel: *Personenbezogene Daten, die bei der Nutzung von Outlook verarbeitet werden, dienen der Durchführung elektronischer Kommunikation, welche zur Erfüllung der Arbeitsverpflichtung notwendig ist und rechtlich auf Art. 88 Abs. 1 DSGVO iVm § 26 Abs. 1 BDSG fußt.*

Antwortbeispiel: *Werden Videokommunikationsinhalte unserer Kunden/unserer Mitarbeiter bei der Nutzung von Microsoft 365 verarbeitet, dient die Verarbeitung der Erfüllung des mit dem Kunden bestehenden Vertrags gemäß Art. 6 Abs. 1 lit. b DSGVO/dient dies der IT-gestützten Zusammenarbeit der Mitarbeiter mittels Teams auf Grundlage der Arbeitsverträge gemäß Art. 88 Abs. 1 DSGVO iVm § 26 Abs. 1 BDSG.*

## Werden die personenbezogenen Daten in die USA oder andere Staaten außerhalb des Europäischen Wirtschaftsraums übermittelt?

Hinweise: Datenübertragungen finden nur bei Bedarf oder mit Zustimmung statt, zum Beispiel, wenn eine E-Mail mit Fotoinhalten gesendet wird oder wenn Fotos oder Dokumente auf OneDrive geteilt werden. Soweit keine vorübergehende Datenübertragung in ein Drittland erforderlich ist, findet diese Datenübertragung innerhalb derselben geografischen Grenze statt. Wenn der Sitz des Unternehmens in Deutschland liegt, werden die allermeisten Datenverarbeitungsvorgänge innerhalb der Europäischen Union durchgeführt. Daraus ergibt sich, dass die Inhalte, die sich in Exchange-Online-Postfächern befinden, wie z.B. der E-Mail-Text, Kalendereinträge und E-Mail-Anhänge, bei deutschen Kunden ausschließlich in Deutschland gespeichert werden. Das gleiche gilt für SharePoint-Online-Website-Inhalte und Dateien, die auf OneDrive for Business hochgeladen wurden. Soweit jedoch eine vorübergehende Übertragung erforderlich ist, kann eine Übermittlung in Drittstaaten stattfinden, sodass gem. Art. 44 S. 1 DSGVO weitere Anforderungen an die Datenübertragung gestellt werden.

Etwas anderes gilt für die Dienste Sway und Workplace Analytics, bei denen die Kundendaten regulär in den USA gespeichert und verarbeitet werden. Aus datenschutzrechtlicher Sicht empfiehlt es sich daher, auf die Nutzung dieser Dienste zu verzichten.

Antwortbeispiel: *Personenbezogene Daten werden in der Regel innerhalb der EU verarbeitet. Soweit es erforderlich ist, kann es in Ausnahmefällen aber zu einer vorübergehenden Übertragung auf US-amerikanische Server kommen.*

## Auf welche Rechtsgrundlagen der DSGVO werden die Drittstaatenübermittlungen gestützt?

Hinweise: Die DSGVO stellt an Datenübermittlungen in ein Drittland erhöhte Anforderungen, da sichergestellt werden soll, dass nur dorthin Daten übertragen werden, wo ein angemessenes Datenschutzniveau besteht. Vor dem oben genannten Schrems-II-Urteil wurde die Übermittlung personenbezogener Daten in die USA auf das sogenannte Privacy-Shield-Abkommen zwischen der USA und der EU gestützt. Eine Übertragung war hiernach an Unternehmen möglich, die sich im Sinne des Privacy Shields zertifizieren ließen. Da der EuGH das Abkommen als unzureichende Rechtsgrundlage erachtet, müssen Unternehmen für Datentransfers in die USA nun auf sog. Standardvertragsklauseln (SCC) gem. Art. 46 Abs. 2 lit. c, Abs. 5 S. 2 DSGVO zurückgreifen. Diese Klauseln werden von der EU-Kommission für Datenübertragungen in Drittländer zur Verfügung gestellt und können in Verträge zwischen Datenexporteuren und Datenimporteuren eingebunden werden. Die Standardvertragsklauseln können außerdem von den Parteien durch weitere Klauseln ergänzt werden, sofern diese nicht im Widerspruch zu den Standardklauseln stehen.

Während Microsoft zugleich nach dem Privacy Shield zertifiziert ist, werden die SCC schon seit Jahren als Bestandteil der Standardverträge zwischen Microsoft und seinen Kunden eingebunden. Sie finden auf alle Übertragungen aus EU-Mitgliedstaaten Anwendung.

Antwortbeispiel: *Die Übertragung personenbezogener Daten in Drittländer erfolgt auf Grundlage von Standardvertragsklauseln zwischen unserem Unternehmen und Microsoft gem. Art. 46 Abs. 2 lit. c DSGVO.* *Sie befinden sich in der Anlage 2 des Data Protection Addendum (DPA).*

## Welche zusätzlichen Sicherheitsmaßnahmen wurden getroffen, um ein angemessenes Schutzniveau zu gewährleisten?

### Sicherheitsmaßnahmen durch Microsoft

Hinweise: Weitere Maßnahmen werden notwendig, sofern im Drittstaat trotz der SCC kein angemessenes Datenschutzniveau gewährleistet wird. Das bedeutet, dass gegebenenfalls über die SCC hinaus noch Maßnahmen getroffen werden müssen, um die Angemessenheit des Schutzniveaus im Empfängerland sicherzustellen. Welche zusätzlichen Maßnahmen erforderlich sind, hängt vom konkreten Übertragungsvorgang und den damit verbundenen Risiken ab. Wegen der Zugriffsmöglichkeiten der Sicherheitsbehörden ist die Übermittlung personenbezogener Daten in die USA nur zulässig, wenn solche weiteren Schutzmaßnahmen ergriffen werden. Insofern kommen per se vertragliche und technische Maßnahmen in Betracht. Von beiden Möglichkeiten hat Microsoft – wie im Folgenden erläutert – Gebrauch gemacht.

Um ein höheres Datenschutzniveau zu bieten, hat Microsoft die SCC um weitere Schutzvorschriften ergänzt. Darin verpflichtet sich Microsoft, Sicherheitsbehörden, die eine Offenlegung bestimmter Daten verlangen, zunächst an den Kunden zu verweisen, den Kunden so schnell wie möglich über die Aufforderung zu informieren und die Aufforderung gerichtlich anzufechten, sofern sie gegen die DSGVO verstößt. Zudem stellt Microsoft eine Entschädigung der betroffenen Person in Aussicht. Trotz dieser weiteren Zusicherungen sind die Datenschutzbehörden der Meinung, dass eine Erweiterung der Standardvertragsklauseln allein nicht genüge. Denn vertragliche Maßnahmen binden nur die Vertragspartner und sind deswegen nicht geeignet, den Zugriff von Überwachungsbehörden zu verhindern.

Ein wirksames Mittel bieten demnach nur zusätzliche technische Schutzmaßnahmen. Ein Beispiel für solche weitergehenden Maßnahmen ist die Ende-zu-Ende-Verschlüsselung aller Daten, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann. Mit einer solchen Verschlüsselung kann bspw. verhindert werden, dass ein mit europäischen Grundfreiheiten nicht zu vereinbarender Zugriff staatlicher Stellen erfolgt. Somit kann trotz der erhöhten Zugriffsmöglichkeit in den USA ein Datentransfer grundsätzlich legitimiert werden.

Soweit Daten in Drittstaaten übermittelt werden, verwendet Microsoft stets eine dem aktuellen Stand der Technik entsprechende Verschlüsselung und verspricht, dass die Daten unmittelbar nach der Verarbeitung wieder an den EU-internen Speicherort zurückgesendet werden. Auch Daten, die sich auf europäischen Servern oder im Transit befinden, werden von Microsoft verschlüsselt. Microsoft sichert zu, dass das Unternehmen – selbst wenn es zu einer Offenlegung der Daten gegenüber Sicherheitsbehörden gesetzlich verpflichtet ist – in keinem Fall den Verschlüsselungsschlüssel preisgibt oder die Umgehung der Verschlüsselung ermöglicht.

Antwortbeispiel: *Microsoft hat im Zuge des Schrems-II-Urteils die in seinen Verträgen eingebundenen Standardvertragsklauseln durch weitere Schutzbestimmungen erweitert. Demnach verpflichtet sich Microsoft, gegen jede Anfrage einer staatlichen Stelle vorzugehen und Nutzer im Falle eines staatlichen Zugriffs zu entschädigen. Soweit Daten in Drittstaaten übermittelt werden, verwendet Microsoft stets eine dem aktuellen Stand der Technik entsprechende Verschlüsselung und verspricht, dass die Daten unmittelbar nach der Verarbeitung wieder an den EU-internen Speicherort zurückgesendet werden.* *Microsoft sichert zu, dass das Unternehmen – selbst wenn es zu einer Offenlegung der Daten gegenüber Sicherheitsbehörden gesetzlich verpflichtet ist – nicht den Verschlüsselungsschlüssel preisgibt oder die Umgehung der Verschlüsselung ermöglicht.*

### Zusätzliche Sicherheitsmaßnahmen durch Kunden

Microsoft eröffnet den Nutzern zudem die Möglichkeit, die Art der Verschlüsselung selber einzustellen. Dabei wird den Kunden auch ermöglicht, den Schlüssel selbst zu verwalten (CMK – Customer Managed Keys). Auch ist eine doppelte Verschlüsselung der Inhalte möglich, bei der jeweils Microsoft und der Kunde über einen der zwei benötigten Schlüssel verfügen. Sofern es möglich ist, sollten Unternehmen von diesen zusätzlichen Sicherheitsmaßnahmen Gebrauch machen, besonders, wenn sensible Daten verarbeitet werden. Einen Weg, die Daten in der Cloud zu verschlüsseln, bietet beispielsweise die Software Boxcryptor.

Kunden können zudem zusätzliche Maßnahmen organisatorischer Art ergreifen. So dient die Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann, dem Zweck des beschränkten Zugriffs, jedoch ist diese Möglichkeit mit einem hohen Aufwand verbunden. Außerdem kann das Unternehmen seine Mitarbeiter anweisen, bestimmte Daten nicht über Onlinedienste zu verarbeiten. Personaldaten, Sozialdaten und andere sensible Daten sollten bestenfalls nicht über Teams oder Exchange Online kommuniziert oder auf OneDrive gespeichert werden.

## Erwägen Sie die Umstellung auf alternative Dienste?

Hinweise: Sofern nach einer Umstellung auf alternative Dienste gefragt ist, sollten zugleich die Gründe genannt werden, die einer Umstellung entgegenstehen.

Antwortbeispiel: *Zwar gibt es einige Alternativen zum Microsoft-Angebot, es ist aber zweifelhaft, ob diese Alternativen sowohl den gleichen Funktionsumfang als auch einen höheren Datenschutz bieten. Zudem müssen die Alternativen mit den Office-Formaten kompatibel sein, da diese weiterhin die verbreitetsten Formate darstellen. Ferner kommt der hohe Kostenaufwand hinzu, der mit einer Umstellung der gesamten digitalen Büroinfrastruktur einhergeht. Allein aus diesen Kostengründen ist eine Umstellung auf andere Systeme weder geplant noch durchführbar.*

## Können Sie uns die Stellen des Verarbeitungsverzeichnisses zusenden, die den Einsatz von Microsoft 365 in Ihrem Unternehmen betreffen?

Für jeden Verantwortlichen besteht gem. Art. 30 Abs. 1 DSGVO die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Die Datenschutzbehörden der Bundesländer halten hier teilweise Muster für diese Verzeichnisse bereit. Ein allgemein gehaltenes Muster befindet sich auf der [Seite der Landesbeauftragten für den Datenschutz NRW](https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf). Auch das Bayerische Landesamt für Datenschutzaufsicht verfügt über [verschiedene Muster](https://www.lda.bayern.de/de/thema_kleine_unternehmen.html) für unterschiedliche Arten von Unternehmen.