

Stellungnahmen zu Microsoft 365: eine Gegenüberstellung der wesentlichen Aussagen der Datenschutzkonferenz und von Microsoft – Update vom 27.01.2023

Eine Übersicht von Stefan Hessel, LL.M. und Christina Kiefer, LL.M
Stand: 27.01.2023

Einleitung

Am 25. November 2022 hat die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, eine [Stellungnahme zu Microsoft 365](#) veröffentlicht. Die Stellungnahme ist das Ergebnis einer Reihe von gemeinsamen Gesprächen zwischen der DSK und Microsoft, nachdem bereits im [September 2020 die DSK eine erste Bewertung von Microsoft Office 365](#) (jetzt: Microsoft 365) vorgenommen hatte. Nachdem die DSK im Jahr 2020 zu dem Ergebnis gekommen war, dass „*kein datenschutzrechtlicher Einsatz von Microsoft Office 365 möglich*“ sei, sollen nunmehr lediglich „*geringfügige Verbesserungen*“ zu erkennen sein. Grundlage der aktuellen Bewertung der DSK ist der „[Datenschutznachtrag zu den Produkten und Services von Microsoft](#)“ (auf Engl. „*Microsoft Products and Services Data Protection Addendum*“ („DPA“)) in der Version vom 15. September 2022. Die DSK betont, dass neben der Bewertung des Vertragswerkes keine technische Untersuchung der Verarbeitungsvorgänge und auch keine Evaluierung der Umsetzung der vertraglichen Vereinbarungen stattgefunden hat. Wesentliche Kritikpunkte sind unter anderem die aus Sicht der DSK intransparente Verarbeitung von Daten durch Microsoft zu eigenen Zwecken sowie die Datenübermittlung in die USA, wobei hier die [neue Executive Order des US-Präsidenten vom 07.10.2022](#) ausdrücklich noch keinen Eingang in die Bewertung gefunden hat.

Microsoft hat bereits am gleichen Tag auf die Bewertung der DSK reagiert und eine [eigene Stellungnahme](#) veröffentlicht. Darin erklärt das Unternehmen, dass die Microsoft-365-Produkte „*die strengen EU-Datenschutzgesetze nicht nur erfüllen, sondern oft sogar übertreffen*“. Die von der DSK geäußerten Bedenken berücksichtigen nach Ansicht des Unternehmens die bereits vorgenommenen Änderungen nicht angemessen und würden auf mehreren Missverständnissen hinsichtlich der Funktionsweise der Dienste beruhen.

Nachfolgend finden Sie unsere erste Einschätzung zu der Stellungnahme der DSK. Wir kommen darin zu dem Ergebnis, dass weiterhin ein datenschutzkonformer Einsatz von Microsoft 365 möglich ist. Die anschließende Gegenüberstellung der wesentlichen divergierenden Aussagen der beiden Stellungnahmen soll zudem eine Hilfestellung für die (rechtliche) Bewertung des Einsatzes von Microsoft 365 geben.

Update vom 27.01.2023: Nachdem die DSK zunächst lediglich eine Zusammenfassung ihrer Stellungnahme veröffentlicht hatte, wurde in der Folge auch der [Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“](#) veröffentlicht, der eine detaillierte Auseinandersetzung mit den einzelnen Kritikpunkten beinhaltet und eine ausführliche rechtliche Bewertung ermöglicht. Darüber hinaus haben einzelne deutsche Datenschutzaufsichtsbehörden angekündigt, nunmehr auf Verantwortliche in öffentlichen Stellen und Unternehmen zuzugehen, um die Einhaltung der datenschutzrechtlichen Vorgaben beim Einsatz von Microsoft 365 zu überprüfen. Außerdem hat auch Microsoft in der Zwischenzeit weitere Schritte unternommen und auf die Kritik der DSK reagiert. Was sich im Detail geändert hat und wie sich diese Änderungen auswirken, haben wir im Folgenden für Sie zusammengefasst.

Erste Einschätzung: Einsatz von Microsoft 365 trotz Bedenken der DSK weiterhin möglich

Die DSK hat bislang nur eine Zusammenfassung ihrer Stellungnahme veröffentlicht, sodass eine abschließende Bewertung der Aussagen zum jetzigen Zeitpunkt noch nicht möglich ist. Ausgehend von den bisher veröffentlichten Dokumenten stellt die Bewertung der DSK jedoch keine wesentliche datenschutzrechtliche Neuerung dar. Ausgehend davon halten wir einen datenschutzkonformen Einsatz von Microsoft 365 sowohl für öffentliche als auch für nichtöffentliche Stellen mit einer entsprechenden Argumentation und Dokumentation weiterhin für gut vertretbar. Dies folgt insbesondere daraus, dass die DSK in nahezu allen Punkten rechtliche Extrempositionen zu bisher ungeklärten Rechtsfragen vertritt und zugleich Anforderungen aufstellt, die in der Praxis durch moderne Clouddienste schwer bis kaum umzusetzen sind. Die Stellungnahme der DSK kann aufgrund ihrer strengen Auslegung in vielen Punkten sogar als technologiefeindlich angesehen werden und steht damit dem unionsweiten Ziel der Digitalisierung europäischer Unternehmen und öffentlicher Stellen entgegen. Nachdem bereits in der Vergangenheit [einige deutsche Aufsichtsbehörden für die Prüfung von Auftragsverarbeitungsverträgen in einer entsprechenden Checkliste](#) deutlich zu hohe Anforderungen an die Ausgestaltung von Auftragsverarbeitungsverträgen nach der Datenschutzgrundverordnung (DSGVO) gestellt haben, hat die DSK mit ihrer Stellungnahme diese nunmehr intensiviert und den Bezug zur Praxis weitgehend verloren. Wendet man die strengen Anforderungen der DSK allgemein auf sämtliche und damit auch rein europäische Anbieter an, dürfte der Einsatz von Cloud-Produkten aufgrund der schweren bis unmöglichen Umsetzbarkeit der Anforderungen in der Praxis zur Seltenheit werden. Zudem ist vor dem Hintergrund der Vollharmonisierung des europäischen Datenschutzrechts mehr als verwunderlich, dass die DSK die Aufsichtsbehörden der anderen EU-Länder, insbesondere die für die Microsoft Ireland Operations Ltd. zuständige irische Datenschutzaufsicht, nicht an ihrer Untersuchung beteiligt hat. Eine einheitliche Geltung des europäischen Datenschutzrechts wird durch die Datenschutzaufsichtsbehörden aktiv verhindert und an deutsche Verantwortliche werden offenkundig höhere Maßstäbe angelegt als an Verantwortliche in anderen EU-Mitgliedsstaaten.

Update vom 27.01.2023: Bereits in der Vergangenheit hat Microsoft die Kritik der Datenschutzaufsichtsbehörden immer wieder zum Anlass genommen, Verbesserungen vorzunehmen und das Datenschutzniveau zu erhöhen. Dies gilt auch für die jüngste Feststellung der DSK. Microsoft hat unter anderem zum 1. Januar 2023 ein [neues DPA](#) mit weiteren Regelungen zum Datenschutz sowie eine [aktualisierte Liste der eingesetzten Unterauftragsverarbeiter](#) veröffentlicht. Der Datenschutz beim Einsatz von Microsoft 365 wurde dadurch abermals erhöht. Gleichzeitig wurde mehr Transparenz und damit auch mehr Rechtssicherheit für die verantwortlichen Kunden geschaffen. Ob und wie die Datenschutzaufsichtsbehörden auf die Verbesserungen von Microsoft reagieren werden, bleibt vorerst abzuwarten. Konkrete Durchsetzungsmaßnahmen der Datenschutzaufsichtsbehörden scheinen bislang auszubleiben.

Gegenüberstellung der wesentlichen Aussagen

1. Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO

Was sagt die DSK?	Antwort von Microsoft
<p>„Verantwortliche müssen jederzeit in der Lage sein, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachzukommen. Beim Einsatz von Microsoft 365 lassen sich hierbei auf Grundlage des ‚Datenschutznachtrags‘ weiterhin Schwierigkeiten erwarten, da Microsoft nicht vollumfänglich offenlegt, welche Verarbeitungen im Einzelnen stattfinden. Zudem legt Microsoft weder vollständig dar, welche Verarbeitungen im Auftrag des Kunden, noch, welche zu eigenen Zwecken stattfinden. Die Vertragsunterlagen sind in der Hinsicht nicht präzise und erlauben im Ergebnis nicht abschließend bewertbare, ggf. sogar umfangreiche Verarbeitungen auch zu eigenen Zwecken.“</p>	<p>„(a) Ausufernde Erwartungen an die Rechenschaftspflicht</p> <ul style="list-style-type: none"> • An die Rechenschaftspflicht der Verantwortlichen dürfen keine übermäßigen Anforderungen gestellt werden: Kunden müssen die technische Funktionsweise von Microsoft 365 nicht vollständig verstehen. Die reine technische Umsetzung kann durch den Auftragsverarbeiter selbst in gewissem Rahmen bestimmt werden. • Eine ausufernde Erwartung an Verantwortliche ist praxisfern und blockiert technischen Fortschritt, selbst wenn dieser der Verbesserung der eingesetzten Technologie oder ihrer Sicherheit dient. • Microsoft 365 ist eine leistungsstarke Produktfamilie mit einer Vielzahl an Funktionalitäten (Microsoft Teams, Word, Excel, PowerPoint und mehr). Als Gesamtlösung ist Microsoft 365 notwendigerweise technisch komplexer als eine Teillösung (z.B. nur Videotelefonie). <p>(b) Detailgrad der von Microsoft bereitgestellten Dokumentation</p> <ul style="list-style-type: none"> • Microsoft stellt die nötige Transparenz über Verarbeitungstätigkeiten durch umfangreiche Dokumentation her. Diese ist teils für die Öffentlichkeit und teils nur für Kunden zugänglich. Noch mehr technische Details über die bereitgestellte Dokumentation hinaus schaffen keine größere Klarheit für Verantwortliche. • Die DSK hat nach unserem Eindruck im Rahmen ihrer Untersuchung den vollen Umfang dieser Kunden zur Verfügung stehenden Dokumentation nicht beachtet. Es bleibt unklar, in welchem Detailgrad Verantwortliche die technische Funktionsweise von Microsoft 365 nach Auffassung

	<p>der DSK verstehen müssen, um ihren Rechenschaftspflichten nachzukommen.“</p>
<p>Bewertung reuschlaw</p>	
<p>Die DSK stellt zu hohe Anforderungen an die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO. Ein Verantwortlicher muss nicht bis ins letzte Detail die Kontrolle über das von ihm eingesetzte System eines Anbieters innehaben. Gemäß der Leitlinie 07/2020 des Europäischen Datenschutzausschusses (EDSA) darf der Verantwortliche dem Auftragsverarbeiter vielmehr einen gewissen Handlungsspielraum bezüglich der nicht wesentlichen Mittel für die Verarbeitung einräumen. Setzt ein Verantwortlicher einen Auftragsverarbeiter mit höherem Fachwissen ein, darf ihm hieraus kein Nachteil entstehen. Er ist aufgrund der genannten Aussagen der Leitlinien 07/2020 nicht verpflichtet, sämtliche Verarbeitungsvorgänge bis ins kleinste Detail nachzuvollziehen und zu dokumentieren. Zu berücksichtigen ist zudem, dass die Rechenschaftspflicht allein den Verantwortlichen trifft, sodass die Anforderungen nicht gelten, wenn Microsoft selbst als Verantwortlicher (z.B. bezüglich der Verarbeitung von Daten für eigene Zwecke) agiert. Zuletzt ist zu berücksichtigen, dass trotz der Rechenschaftspflicht des Verantwortlichen weiterhin der Amtsermittlungsgrundsatz der Behörden gilt. Dieser ist in einen angemessenen Ausgleich mit der Rechenschaftspflicht zu bringen, sodass der Verantwortliche, insbesondere auch im Hinblick auf die unionsweit gültige Unschuldsvermutung, nicht sämtliche Nachweise, die eine Behörde zum Zwecke einer eigenen datenschutzrechtlichen Prüfung verlangt, vorlegen muss.</p>	
<p>Update vom 27.01.2023</p>	
<p>In Anlage 1 des neuen DPA verpflichtet sich Microsoft nunmehr ausdrücklich, den Kunden bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO während der gesamten Vertragslaufzeit zu unterstützen. Dem Kunden wird damit neben den gesetzlichen Ansprüchen nach der DSGVO ein vertraglicher Anspruch gegenüber Microsoft zur Bereitstellung der zur Erfüllung der Rechenschaftspflicht erforderlichen Informationen und Dokumente gewährt. Kunden können von dieser Möglichkeit Gebrauch machen und Microsoft bei Bedarf um Vorlage von Dokumenten bitten, die zur Erfüllung ihrer Rechenschaftspflicht erforderlich sind. Zu berücksichtigen ist außerdem, dass Microsoft den Anwendungsbereich seines DPA erweitert hat. Die Regelungen des DPA gelten jetzt für alle Kunden mit einem bestehenden Vertrag über Produkte und Services von Microsoft. Um Bedenken der Datenschutzaufsichtsbehörden bezüglich der Anwendbarkeit und Wirksamkeit der neuen vertraglichen Verpflichtung aus Anlage 1 vorwegzugreifen, hat Microsoft zudem eine zusätzliche Klausel zur Konkurrenz- und Hierarchieregelung in dem neuen DPA aufgenommen. Microsoft stellt in dem neuen DPA nun ausdrücklich klar, dass, soweit Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogene Daten, die der DSGVO unterfallen, verarbeitet, primär die DSGVO-Bestimmungen aus Anlage 1 gelten und die weiteren Regelungen zur Datenverarbeitung lediglich ergänzend Anwendung finden. Mit dieser Klarstellung garantiert Microsoft gegenüber seinen Kunden, die dem Anwendungsbereich der DSGVO unterliegen, vertraglich, die strengen Anforderungen aus Anlage 1 einzuhalten. Zur Gewährleistung von mehr Transparenz hat Microsoft zudem weitere Informationen zu den von Microsoft eingesetzten Unterauftragsverarbeitern sowie eine umfassende Dokumentation zu den Datenflüssen im Kontext des EU Data Boundary veröffentlicht. Auch diese Informationen sollten sich Verantwortliche zum Nachweis ihrer Datenschutz-Compliance zu eigen machen.</p>	

2. Festlegung von Art und Zweck der Verarbeitung sowie der Art der personenbezogenen Daten

Was sagt die DSK?	Antwort von Microsoft
<p>„Die Arbeitsgruppe konnte im Rahmen der Gespräche mit Microsoft keine signifikanten Nachbesserungen in der Vertragsgestaltung hinsichtlich der Festlegung von</p>	<ul style="list-style-type: none"> „Microsoft teilt diese Einschätzung der DSK nicht. Das DPA enthält Informationen gemäß Art. 28 Abs. 3 Satz 1 DS-GVO im Abschnitt

Arten und Zwecken der Verarbeitung sowie der Arten der verarbeiteten personenbezogenen Daten erreichen. Es bleiben Nachbesserungen erforderlich, die den Gegenstand der Auftragsverarbeitung nicht nur umfassend, sondern auch spezifisch und so detailliert als möglich beschreiben sollten. Dies könnte etwa durch eine kundenspezifische Konkretisierung nach dem Vorbild des Anhangs II der Standardvertragsklauseln der Kommission gemäß Art. 28 Abs. 7 DS-GVO erreicht werden. Möglich wäre auch, Verweise auf ein formgerecht in den Vertrag einzubeziehendes und hinreichend detailliertes Verzeichnis der Verarbeitungstätigkeiten (VVT) des Verantwortlichen vorzusehen.“

,Verarbeitungsdetails‘ (welcher auf das Verarbeitungsverzeichnis des Kunden gemäß Art. 30 DS-GVO verweist) und in Anhang B. Dies entspricht den Anforderungen des unabhängigen ISO/IEC-19944-Standards an die Darstellung von Datenerhebungskategorien und Nutzungszwecken im Kontext der Cloud.

- *Die Kontrolle über diese Verarbeitungsdetails liegt beim Kunden. Er bestimmt, welche Daten er wie lange für welchen Zweck in der Microsoft Cloud verarbeiten möchte.*
- *Das DPA und die standardisierte Leistungserbringung der Microsoft Cloud sind darauf ausgerichtet, alle legalen vertragsgemäßen Verarbeitungen durch Kunden zu ermöglichen. Deshalb würde eine weitere Konkretisierung der ,Verarbeitungsdetails‘ keine Änderung der Leistungserbringung durch Microsoft zur Folge haben. Microsoft erfüllt unabhängig von den Datenkategorien den gleichen hohen Standard an Sicherheit, Sicherheit und Funktionalität.*
- *Eine weitere Konkretisierung im DPA würde in der Praxis dazu führen, dass die gemachten Angaben regelmäßig veralten und somit unrichtig würden.“*

Bewertung reuschlaw

Die Anforderungen an eine datenschutzkonforme Auftragsverarbeitung richten sich nach Art. 28 DSGVO. Nach Art. 28 Abs. 9 DSGVO muss die Auftragsverarbeitung auf einer vertraglichen Regelung beruhen, deren gesetzliche Mindestanforderungen in Art. 28 Abs. 3 und Abs. 4 DSGVO festgelegt sind. Hiernach müssen sich insbesondere die Art und der Zweck der Verarbeitung sowie die Art der personenbezogenen Daten aus dem Vertrag selbst ergeben. Eine weitere Konkretisierung bzw. konkrete Anforderungen an die Ausgestaltung dieser Angaben sind in der Vorschrift jedoch nicht enthalten. Hierzu gibt es unterschiedliche Auffassung, insbesondere im Hinblick auf die Ausgestaltung von Auftragsverarbeitungsverträgen und deren Präzisionsgrad beim Einsatz von Clouddiensten. Zwar sollten gemäß der Leitlinien 07/2020 des EDSA grundsätzlich die Art und der Zweck der Verarbeitung sowie die Art der personenbezogenen Daten so detailliert wie möglich in dem Vertrag angegeben werden, doch kann gleichzeitig von den Vertragsparteien auch nichts Unmögliches verlangt werden. Entscheidend ist, dass sich die Anforderungen an die tatsächlichen Umstände und Möglichkeiten des Einzelfalles richten müssen. So kann gemäß den Leitlinien 07/2020 des EDSA im Einzelfall auch ein einseitig von einer Partei abgefasster Vertrag den Anforderungen des Art. 28 Abs. 3 DSGVO entsprechen. Microsoft 365 ist ein komplexer Cloud-Dienst, sodass eine weitere Präzisierung, wie sie von der DSK gefordert wird, im Hinblick auf die Vielzahl der Kunden und die Fülle von unterschiedlichen Einsatzszenarien in der Praxis unmöglich erscheint. Mit der Konkretisierung in dem neuen

DPA hat Microsoft u.E. nach hinreichende (allgemeine) Präzisierungen vorgenommen und damit ein zulässiges Standardvertragsregelwerk geschaffen, sodass es keiner weiteren Präzisierung im Einzelfall bedarf.

3. Eigene Verantwortlichkeit von Microsoft im Rahmen der „Verarbeitung für Geschäftstätigkeiten“

Was sagt die DSK?	Antwort von Microsoft
<p>„Zum Themenkomplex der eigenen Verantwortlichkeit Microsofts im Rahmen der Verarbeitungen ‚für legitime Geschäftszwecke‘ konnte die Arbeitsgruppe zwar Änderungen der vertraglichen Ausgestaltung erreichen. Ungeachtet unterschiedlicher Beurteilungen der datenschutzkonformen Ausgestaltung von Verarbeitungen vertragsgegenständlicher Daten zu eigenen Zwecken des Auftragsverarbeiters durch die europäischen Aufsichtsbehörden bewirken diese Vertragsänderungen jedoch aus Sicht der Arbeitsgruppe keine substantiellen Verbesserungen: Der ‚Datenschutznachtrag‘ vom September 2022 enthält als Konsequenz der Gespräche mit der Arbeitsgruppe einen begrifflich veränderten Abschnitt über Datenverarbeitungen, die Geschäftstätigkeiten Microsofts dienen sollen, der erste Ansätze zur Eingrenzung und Konkretisierung zeigt. Allerdings hat Microsoft nach eigener Aussage keine Anpassungen an den tatsächlichen Verarbeitungen vorgenommen. Eine genauere Untersuchung der vertraglichen Umgestaltung zeigt aus Sicht der Arbeitsgruppe, dass Microsoft die Grundansätze des bisherigen Regelungsmodells fortführt, sich für bestimmte Verarbeitungen unzureichend eingegrenzte Rechte zu wenig konkretisierten Verarbeitungen der verarbeiteten personenbezogenen Daten einräumen zu lassen. Es bleibt weiterhin unklar, welche personenbezogenen Daten im Rahmen der von Microsoft sogenannten ‚legitimen‘ Geschäftszwecke bzw. nun ‚Geschäftstätigkeiten‘ verarbeitet werden.</p> <p>Ebenso ist unklar, auf welcher Rechtsgrundlage die Überführung der im Auftrag verarbeiteten personenbezogenen Daten in die Verantwortlichkeit von Microsoft für die anschließende Verarbeitung zu Zwecken Microsofts samt der damit verbundenen umfassenden Nachweispflichten stattfindet. Ähnliches gilt für Daten wie Telemetrie- und Diagnosedaten, die Microsoft nach Kenntnis der Arbeitsgruppe in großem</p>	<p>„(a) Widersprüchliche Auslegung der DS-GVO seitens der Behörden in Europa</p> <ul style="list-style-type: none"> Wie die DSK anerkennt, beurteilen europäische Aufsichtsbehörden unterschiedlich, in welcher Position (Verantwortlicher oder Auftragsverarbeiter) Cloud-Anbieter im Zusammenhang mit der Dienstleistung personenbezogene Daten verarbeiten dürfen. Dieser unaufgelöste Dissens der nationalen Behörden stellt international agierende Unternehmen vor eine faktisch unüberwindbare Hürde. <p>(b) Rechtsgrundlage</p> <ul style="list-style-type: none"> Microsoft aggregiert lediglich pseudonymisierte, personenbezogene Daten und berechnet Statistiken bezogen auf Kundendaten. Dies resultiert in nichtpersonenbezogenen Daten, welche Microsoft dann für folgende Geschäftstätigkeiten nutzt: (i) Abrechnungs- und Kontoverwaltung, (ii) Vergütung, (iii) interne Berichterstattung und Geschäftsmodellierung und (iv) Finanzberichterstattung. Die Rechtsgrundlagen, die bereits den Einsatz von Microsoft 365 durch den Verantwortlichen (Kunden) rechtfertigen, decken auch diese Vorgänge ab. Microsoft wird seine Kunden durch geeignete Unterlagen und Dokumentation zu dieser Auffassung unterstützen. Die DSK übersieht auch, dass der Auftragsverarbeiter selbst Adressat der Verpflichtungen gemäß Art. 32 DS-GVO ist und für deren Durchführung nicht von einer Rechtsgrundlage des Verantwortlichen abhängig sein kann. Dies betrifft mindestens Aspekte der Weiterentwicklung, Produktstrategie und

Umfang und grundsätzlich für eigennützige Zwecke erhebt.

Besondere Schwierigkeiten bestehen dabei für öffentliche Stellen, da diese nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f) DSGVO zurückgreifen können.“

Kapazitätsplanung. Es ist daher widersprüchlich und nicht im Einklang mit der Systematik der DS-GVO, (i) Verantwortlichen Verarbeitungen und Maßnahmen zuzurechnen, zu deren Erbringung Auftragsverarbeiter verpflichtet und durch eine eigenständige Bußgeldnorm bedroht sind, und (ii) für diese falsch zugeordneten Verarbeitungen und Maßnahmen dann eine fehlende Rechtsgrundlage anzumahnen.

(c) Keine ‚eigenen Zwecke‘ losgelöst von Kundeninteressen

- *Von ‚eigenen Zwecken‘ Microsofts zu sprechen ist irreführend. Die Verarbeitung für Geschäftstätigkeiten ist durch die Bereitstellung der Produkte und Dienste an den Kunden veranlasst und erfolgt auch im Interesse der Kunden.*
- *Die vorgesehenen Geschäftstätigkeiten sind notwendiger Teil der Bereitstellung, Abrechnung und Planung jedes komplexen Cloud-Produktes, nicht nur bei Microsoft. Microsoft hebt sich durch seine Transparenz in dieser Frage hervor.*
- *Die DSK hat Bedenken geäußert, dass der Text des DPA (Stand 15.09.2021) Microsoft zu weitgehende Rechte einräume. Daraufhin hat Microsoft die Formulierungen im DPA (Stand 15.09.2022) eingeschränkt. Die genaueren Formulierungen entsprachen ohnehin der tatsächlichen, eingeschränkten Praxis Microsofts in Bezug auf diese Verarbeitungen.*

(d) Rein akademische Diskussion

- *Die datenschutzrechtliche Relevanz der Geschäftstätigkeiten ist minimal:*
- *Microsoft greift nicht auf Inhaltsdaten von Kunden zu.*
- *Wie oben dargestellt, ist zum Zeitpunkt der Nutzung der nichtpersonenbezogenen Daten für die Geschäftstätigkeiten von Microsoft der Anwendungsbereich der DSGVO bereits verlassen; und*

	<ul style="list-style-type: none"> • <i>Microsoft sagt Kunden im DPA zu, dass (i) die Datennutzung minimiert wird (etwa durch die Pseudonymisierung bereits bei der Erhebung) und (ii) keine Nutzung für sonstige (etwa Werbe- oder Profilierungszwecke) erfolgt.</i> • <i>Bei vernünftiger Betrachtung handelt es sich hier um eine rein akademische, den Interessen der Betroffenen und Kunden in keiner Weise dienende Diskussion um hoch standardisierte, industrietypische und datenschutzrechtlich neutrale Verarbeitungen.</i> • <i>Die Aussage, ein Anbieter für die öffentliche Hand dürfe keine eigenen Zwecke verfolgen, ist jedenfalls in Bezug auf Microsofts Geschäftstätigkeiten rechtlich nicht haltbar. Sie steht zumindest in dieser Pauschalität diametral im Gegensatz zur gesellschaftlich und politisch geforderten Digitalisierung der öffentlichen Hand.“</i>
--	--

Bewertung reuschlaw

Durch die Präzisierung der Beschreibung der Verarbeitungsvorgänge, die Microsoft für eigene Geschäftstätigkeiten vornimmt, hat Microsoft u.E. deutliche Verbesserungen in dem aktuellen DPA vorgenommen. Microsoft nennt ausdrücklich, in welchen Fällen Daten zu eigenen Zwecken verarbeitet werden, und legt die diesbezüglich einschlägigen Geschäftszwecke ausdrücklich und abschließend fest. Darüber hinaus sichert Microsoft verbindlich zu, dass das Unternehmen im Falle der Verarbeitung zu eigenen Zwecken den strengen Anforderungen der DSGVO sowie den unionsrechtlichen Datenschutzgrundsätzen vollumfänglich gerecht wird. Diese Vertragsregelungen stellen eine hinreichende Präzisierung der Verarbeitungen dar, die für den verantwortlichen Kunden auch leicht verständlich sind. Einzig bezüglich der Frage, welche Daten konkret zu eigenen Geschäftszwecken verarbeitet werden, ist der DSK zuzustimmen, dass dieser Punkt in dem DPA noch näher erläutert werden könnte. Der Anpassung der vertraglichen Regelungen steht jedoch nicht entgegen, dass die tatsächlichen Gegebenheiten nicht geändert wurden. Vielmehr zeigt dies, dass Microsoft der Bitte nach einer Präzisierung in dem DPA entsprechend den tatsächlichen Gegebenheiten nachgekommen ist.

Sofern Microsoft als Verantwortlicher Daten verarbeitet, ist zu berücksichtigen, dass den Kunden u.E. keine weiteren datenschutzrechtlichen Pflichten treffen. So liegt in dem bloßen Einsatz von Microsoft 365 und der damit einhergehenden Gelegenheit zur Verarbeitung von Daten durch Microsoft keine Übermittlung der Daten durch den Kunden an Microsoft vor. Der Kunde benötigt daher auch keine Rechtsgrundlage. Selbst wenn man eine Offenlegung der Daten durch den Kunden an Microsoft annehmen wollen würde, kann die einschlägige Rechtsgrundlage nicht pauschal für sämtliche Kunden ermittelt und in dem DPA festgeschrieben werden. Vielmehr richtet sich die Rechtsgrundlage nach den Umständen des Einzelfalls, sodass eine Aufnahme der Rechtsgrundlagen in dem DPA unmöglich erscheint. Zuletzt ist darauf hinzuweisen, dass öffentliche Stellen sich zwar nicht auf ein berechtigtes Interesse berufen können, jedoch sonstige Rechtsgrundlagen für eine etwaige Offenlegung der Daten gegenüber Microsoft (wie etwa § 25 Abs. 2 Nr. 2 Bundesdatenschutzgesetz oder ein Annex zur eigentlichen Rechtsgrundlage) einschlägig sein können.

Update vom 27.01.2023

Aus dem von der DSK veröffentlichten Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“ wird deutlich, dass die DSK insbesondere die Streichung der ehemals in dem DPA genannten Zwecke der „Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen“ kritisiert und es laut der DSK an einer Präzisierung der Verarbeitungsvorgänge und der Abgrenzung der Verantwortlichkeiten diesbezüglich fehle. Dieser Kritik ist jedoch bereits entgegenzuhalten, dass die DSK in ihrer Prüfung nicht die Besonderheiten des [Telekommunikation-Telemedien-Datenschutz-Gesetzes \(TTDSG\)](#) berücksichtigt hat. Nach den neuen Regelungen des TTDSG in Verbindung mit der neuen Definition von Telekommunikationsdiensten nach dem [Telekommunikationsgesetz \(TKG\)](#) unterliegt die Verarbeitung von Metadaten im Rahmen der Dienstleistung sowie die Verarbeitung von technischen Übertragungsdaten für den Transport von Inhaltsdaten den Regelungen des TTDSG. Es ist daher nur folgerichtig, dass Microsoft die ehemaligen Zwecke aus dem DPA gestrichen hat. Da dieses Vorgehen jedoch ebenfalls von der DSK bemängelt wurde, hat Microsoft erneut reagiert und in dem neuen DPA klarstellend eine Klausel zu der Verarbeitung von Telekommunikationsdaten aufgenommen.

4. Weisungsbindung und Offenlegung von Daten im Rahmen des CLOUD Act und FISA 702

Was sagt die DSK?	Antwort von Microsoft
<p>„Der aktuelle Datenschutznachtrag vom September 2022 enthält Veränderungen der bisherigen Bestimmungen, die die Offenlegung der von Microsoft als Auftragsverarbeiter bereitgestellten Daten im Rahmen eigener Geschäftszwecke ‚zur Erfüllung rechtlicher Verpflichtungen‘ regeln. Dabei enthalten die Änderungen zwar neue Formulierungen, im Ergebnis bleiben die Befugnisse aber ähnlich umfangreich. Mit der Regelung wird etwa das Weisungsrecht des Kunden in Bezug auf Offenlegungen der im Auftrag verarbeiteten Daten eingeschränkt. Der Datenschutznachtrag erlaubt die Offenlegung, wenn diese rechtlich vorgeschrieben oder im ‚Datenschutznachtrag‘ beschrieben ist. Solche Offenlegungen sind nicht auf Weisungen des Verantwortlichen beschränkt, sodass sie vor dem Hintergrund des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a DSGVO nur zulässig sind, wenn sie sich auf Verpflichtungen aus dem Unions- oder mitgliedstaatlichen Recht, dem Microsoft unterliegt, beschränken. Dies ist nicht der Fall. Damit genügt die Weisungsbindung Microsofts nicht den gesetzlichen Mindestanforderungen gemäß Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO.</p> <p>Aus den Untersuchungen der Arbeitsgruppe ergibt sich, dass sich Microsoft auch weitreichende Offenlegungen vertraglich vorbehält, die im Falle ihrer Umsetzung nicht den in</p>	<p>„(a) Weisungen an Auftragsverarbeiter bei Cloud-Diensten</p> <ul style="list-style-type: none"> • Das DPA wird zwischen Kunden und Microsoft vereinbart. Es enthält die allgemeinen Weisungen sowie Modalitäten für weitere Weisungen des Kunden an Microsoft. • Bei Cloud-Diensten ist es Industriestandard, dass (i) sich der Kunde die Erbringung der Dienste wie vertraglich und in der Produktdokumentation beschrieben als Weisung zu eigen macht; (ii) laufende Weisungen des Kunden über die Konfiguration und Nutzung des Dienstes durch den Kunden erfolgen; und (iii) darüber hinaus die Möglichkeit einer einvernehmlichen Vertragsanpassung besteht. • Diese Art, Weisungen zu erteilen, ist nötig, damit Kunden die gewünschten Vorteile der Cloud nutzen können: Kunden wollen Teile des Betriebs ihrer IT an einen Anbieter von Multi-Tenant-Lösungen auslagern, um an Skaleneffekten (Kostensparnis, Innovation etc.) teilzuhaben. <p>(b) CLOUD Act, FISA 702 etc.</p> <ul style="list-style-type: none"> • Es zeichnet sich bereits eine datenschutzrechtliche Lösung des gesamten Themenkomplexes nach Art. 45

Art. 48 DSGVO aufgestellten Anforderungen entsprechen würden.“

DS-GVO ab: Die Europäische Kommission arbeitet zurzeit an einem Angemessenheitsbeschluss, wonach das Datenschutzniveau in den USA als angemessen bewertet werden soll. Grundlage dafür ist, dass die USA mit Wirkung ab dem 7. Oktober 2022 bedeutende Änderungen an ihren Rechtsvorschriften vorgenommen haben und noch vornehmen werden, welche das Schrems-II-Urteil in vollem Umfang berücksichtigen.

- *Herausgabeverlangen von Behörden außerhalb der EU betreffen nicht nur Microsoft: Neben anderen amerikanischen Technologieanbietern können auch Anbieter mit Stammsitz innerhalb der EU (z.B. Unternehmen des DAX-Index) US-Überwachungsgesetzen unterliegen, etwa durch eine Präsenz in oder minimalen Kontakt mit den USA.“*

Bewertung von reuschlaw

Zur Weisungsbindung und deren konkreter Ausgestaltung im Vertrag zur Auftragsverarbeitung ist erneut auf Art. 28 Abs. 3 DSGVO hinzuweisen. Diese Vorschrift legt die gesetzlichen Mindestanforderungen an einen wirksamen Auftragsverarbeitungsvertrag und deren Ausgestaltung fest. Zwar darf eine Verarbeitung im Auftrag nur auf dokumentierte Weisung des Verantwortlichen erfolgen, die Detailtiefe der Weisungen unterliegt jedoch, ebenso wie die Form der Weisung, der Vertragsfreiheit der Parteien. Entscheidend ist lediglich, dass zwischen den Parteien vereinbart ist, dass eine Verarbeitung nur auf dokumentierte Weisung erfolgen darf. Die konkrete Ausgestaltung bleibt den Vertragsparteien im Einzelfall überlassen. Sofern eine Weisung besteht, die in ihren Grundzügen festgeschrieben und dokumentiert ist, genügt dies den Anforderungen des Art. 28 DSGVO. Die Leitlinien 07/2020 sehen diesbezüglich sogar ausdrücklich die Möglichkeit vor, dass der Auftragsverarbeiter Elemente vorschlagen darf, „*die, wenn sie von dem Verantwortlichen akzeptiert werden, Teil der erteilten Weisungen werden*“. Die gesetzlichen Mindestvoraussetzungen des Art 28 DSGVO sind daher durch das neue DPA erfüllt. Das neue DPA enthält ausdrücklich und an mehreren Stellen die Vereinbarung, dass Microsoft Daten nur nach den dokumentierten Weisungen des Kunden verarbeiten darf. In Bezug auf die Offenlegung von Daten gegenüber Dritten ist zu berücksichtigen, dass das DPA unmissverständlich klarstellt, dass Microsoft Daten nur dann offenlegen darf, „*wenn dies gesetzlich vorgeschrieben ist, vorausgesetzt, dass die Rechtsvorschriften und Gepflogenheiten den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um, soweit anwendbar, eines der in Artikel 23 Absatz 1 der DSGVO aufgeführten Ziele sicherzustellen*“. Diese Regelung stellt daher strenge Voraussetzungen insbesondere für eine Offenlegung gegenüber US-amerikanischen Behörden, die eine Auskunft im Rahmen des CLOUD Act und/oder FISA 702 ersuchen, dar und begründet u.E. hinreichende Schutzmaßnahmen.

5. Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO

Was sagt die DSK?	Antwort von Microsoft
<p>„Die ab 15. September 2022 geltende Version des ‚Datenschutznachtrags‘ enthält gegenüber der vom AK Verwaltung geprüften Version Ergänzungen zu den technisch-organisatorischen Maßnahmen. Für ausdrücklich beschränkte bestimmte Datenkategorien (nämlich Kundendaten in ‚Core-Onlinediensten‘ und nunmehr auch ‚Professional-Services-Daten‘) bestehen Garantie- und Datensicherheitsmaßnahmen. Zudem hat Microsoft dargelegt, dass es Interessierten nach einer Anmeldung Zugang zur Website servicetrust.microsoft.com (‚Service Trust Website‘), unter der Informationen über die durchgeführten technisch-organisatorischen Maßnahmen eingesehen werden können, bietet.</p> <p>Es bleiben Rechtsunsicherheiten, da die Garantien über ‚Sicherheitsmaßnahmen‘ formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten, nämlich Kundendaten in ‚Core-Onlinediensten‘ und ‚Professional-Services-Daten‘, erfassen.</p>	<ul style="list-style-type: none"> • Microsoft teilt diese Einschätzung der DSK nicht. Microsoft verpflichtet sich zur Einhaltung von TOMs für alle verarbeiteten Daten und dass die Maßnahmen den Anforderungen von ISO 27001, ISO 27002 und ISO 27018 entsprechen. Dies gilt für alle Services, insbesondere auch die sogenannten Non-Core Services, die im Übrigen in der Gesamtschau der vom DPA abgedeckten Leistungen eine sehr kleine Teilmenge bilden. Weitere Details dazu finden Kunden im Service Trust Portal. • Zusätzlich enthalten das DPA und die Dokumentation im Service Trust Portal weitergehende Verpflichtungen zu TOMs für die wesentlichen Leistungsgegenstände: Core Online Services und Professional Services. • Als Teil von Microsofts Bekenntnis dazu, die Vertragsbedingungen mit Hinblick auf Feedback von Aufsichtsbehörden und Kunden weiter zu verbessern, wird Microsoft untersuchen, ob weitere organisatorische Maßnahmen in die Vertragsbedingungen aufgenommen werden können, welche Microsoft in der Praxis bereits für personenbezogene Daten außerhalb von Kundendaten in Core Online Services und Professional Services anwendet.“
<p>Bewertung reuschlaw</p>	
<p>Neben den Angaben aus Anhang A des DPA von Microsoft sollten zur Beurteilung, ob hinreichende technische und organisatorische Maßnahmen gewährleistet werden, die Informationen von Microsoft in einer Gesamtschau herangezogen werden. So enthält bereits das DPA mehrfach an anderen Stellen die allgemeine Zusage, dass Microsoft Sicherheitsmaßnahmen implementiert, um nicht nur Kundendaten und Professional-Services-Daten, sondern auch personenbezogene Daten im Allgemeinen während der Verarbeitung zu schützen. Darüber hinaus ist zu berücksichtigen, dass Microsoft eine Vielzahl von Zertifizierungen entsprechend den gängigen Standards vorweisen kann und zudem weitreichende Informationen zu den ergriffenen Sicherheitsmaßnahmen beim Einsatz von Microsoft 365 zur Verfügung stellt. Diese Informationen hat die DSK in ihrer Bewertung offenbar (bislang) nicht berücksichtigt, sodass eine andere Ansicht diesbezüglich gut vertretbar erscheint.</p>	
<p>Update vom 27.01.2023</p>	
<p>Im neuen DPA hat Microsoft eine Klausel aufgenommen, die Microsoft vertraglich dazu verpflichtet, die technischen und organisatorischen Maßnahmen im Sinne des Annex II der Standardvertragsklauseln der EU-Kommission vom 4. Juni 2021 für sämtliche Dienste und Services zu implementieren. Microsoft gewährleistet ohnehin ein hohes Sicherheitsniveau.</p>	

Nun ist dies auch für sämtliche Dienste und Services formal geregelt. Diese Änderungen sollten die Verantwortlichen in ihrer Dokumentation zur Datenschutz-Compliance ebenfalls berücksichtigen.

6. Löschung und Rückgabe personenbezogener Daten

Was sagt die DSK?	Antwort von Microsoft
<p>„Microsoft hat der Arbeitsgruppe die einzelnen Löschrouten erläutert. Die Erläuterungen zeigen mit Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der ‚Cyberabwehr‘, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschrouten für personenbezogene Daten nicht verlängern sollten. Zudem haben sich im Zuge der Umgestaltung des ‚Datenschutznachtrags‘ auch Änderungen in Bezug auf Löschung ergeben, die allerdings auch Unklarheiten und Widersprüche mit sich bringen. Nach Bewertung der Arbeitsgruppe genügt die Ausgestaltung der Rückgabe- und Löschrouten nicht in jedem Fall den gesetzlichen Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO. Verantwortliche können wegen der Unklarheit der Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.“</p>	<p>„Das DPA ermöglicht dem Kunden sehr wohl in datenschutzkonformer Weise die Löschung sowie die Extraktion von Daten (die bei Cloud-Diensten die einzige einer Rückgabe entsprechende sinnvolle Option ist).“</p>
Bewertung reuschlaw	
<p>Die Frage der Ausgestaltung der vertraglichen Regelungen zur Löschung und Rückgabe der verarbeiteten Daten reiht sich in die klassischen Probleme der Ausgestaltung der gesetzlichen Mindestanforderungen des Art. 28 Abs. 3 DSGVO bei Clouddiensten ein. Nach Art. 28 Abs. 3 und Abs. 2 lit. g) DSGVO ist lediglich vorgesehen, dass nach Erbringung der Verarbeitungsleistungen alle Daten nach Wahl des Verantwortlichen grundsätzlich gelöscht oder zurückgegeben werden müssen. Weitere Anforderungen an die vertragliche Ausgestaltung dieser Regelung enthält Art. 28 DSGVO jedoch nicht. Die strenge Auslegung der DSK und die damit einhergehenden hohen Anforderungen dürften jedoch nicht von dem Unionsgesetzgeber intendiert gewesen sein, da diese in der Praxis zumindest in Bezug auf moderne Clouddienste unmöglich umzusetzen sind. Die Auslegung der DSK stellt damit eine Extremposition dar, die technologiefeindlich ist und im Widerspruch zu den Leitlinien 07/2020 des EDSA steht, wonach bezüglich der Ausgestaltung des Vertrages zur Auftragsverarbeitung jeweils die Umstände des Einzelfalles und damit das tatsächlich Mögliche und Machbare zu berücksichtigen sind.</p>	

7. Information über Unterauftragsverarbeiter

Was sagt die DSK?	Antwort von Microsoft
<p>„Die Arbeitsgruppe hat mehrfach, teils kontrovers mit Microsoft die Ausgestaltung der Kontrollrechte des Verantwortlichen bei Veränderungen der Unterauftragsverarbeitungsverhältnisse diskutiert. Microsoft konnte trotz anfänglicher Vorbehalte gegen</p>	<ul style="list-style-type: none"> • „Microsoft teilt diese Einschätzung der DSK nicht. Microsoft stellt Kunden jederzeit eine Übersicht der von Microsoft eingesetzten Unterauftragsverarbeiter zur Verfügung.“

eine Umstellung des bisher als Holschuld des Verantwortlichen ausgestalteten Verfahrens zu organisatorischen und vertraglichen Anpassungen bewogen werden. Dies hat zu einer bereits Ende März eingeführten **Neugestaltung des Unterrichtsverfahrens** geführt, die im aktuellen ‚Datenschutznachtrag‘ vom September 2022 zu einer Streichung des bisherigen ‚Holschuld‘-Verfahrens geführt hat.

Die Arbeitsgruppe versteht Art. 28 Abs. 2 DSGVO dahingehend, dass die Information des Verantwortlichen ‚über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter‘ die konkret beabsichtigte Änderung enthalten muss und nicht nur den allgemeinen Hinweis, dass Änderungen geplant sind.

Das von Microsoft bereitgestellte Muster einer Benachrichtigungs-E-Mail enthält nur eine Information über geplante Änderungen, aber nicht die konkret geplanten Änderungen. Die der Arbeitsgruppe vorgestellte Liste über Unterauftragsverhältnisse unterscheidet zudem bislang im Wesentlichen danach, für welchen Dienst bzw. welche Funktionalität Unterauftragnehmer eingesetzt sind, und benennt deren Sitz und die ihnen zugänglichen Datenkategorien. Im Vergleich dazu sehen die von der EU-Kommission bereitgestellten Standardvertragsklauseln deutlich detailliertere Angaben über Name, Anschrift und Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der jeweiligen Verarbeitung vor, die eine klare Abgrenzung der Verantwortlichkeiten mehrerer eingesetzter Unterauftragsverarbeiter erlauben sollen.“

- Bereits in der Vergangenheit konnten Kunden Updates per E-Mail abonnieren.
- Darüber hinaus ist Microsoft dem Wunsch der DSK nachgekommen, ein Benachrichtigungsverfahren per E-Mail einzuführen, welches alle Kunden von Microsoft 365 aktiv über Aktualisierungen informiert. Diese Benachrichtigung verweist auf die online verfügbare Liste der Unterauftragsverarbeiter, welche Änderungen konkret und leicht nachvollziehbar benennt.
- Microsoft arbeitet bereits an einer detaillierteren Liste von Unterauftragsverarbeitern.“

Bewertung reuschlaw

Bezüglich der Information über Unterauftragsverarbeiter intensiviert die DSK die hohen Anforderungen der Checkliste einiger deutscher Datenschutzaufsichtsbehörden zur Prüfung von Auftragsverarbeitungsverträgen und verlangt mehr, als gesetzlich nach Art. 28 Abs. 3 DSGVO vorgeschrieben ist. Die Informationen von Microsoft sollten auch hier in einer Gesamtschau gesehen werden, sodass nicht allein der Inhalt der Nachricht im Rahmen des Unterrichtsverfahrens ausschlaggebend sein sollte. Vielmehr sollten sämtliche Informationen, die Microsoft im Zusammenhang mit dem Einsatz von Unterauftragsverarbeitern den Kunden zur Verfügung stellt, berücksichtigt werden. Beispielsweise verweist Microsoft richtigerweise neben den E-Mails auch auf die allgemeine Liste der Unterauftragsverarbeiter, die fortlaufend überarbeitet wird. Nach der Checkliste der deutschen Aufsichtsbehörden soll gerade ein Verweis auf eine solche Liste ausreichen, sodass die Stellungnahme der DSK nunmehr eine gewisse Rechtsunsicherheit für die Verantwortlichen, die sich bislang auf die Checkliste berufen haben, hervorruft.

Update vom 27.01.2023

Microsoft hat auf die Kritik der DSK reagiert und die [Liste der von Microsoft eingesetzten Unterauftragsverarbeiter](#) überarbeitet. Mit der aktualisierten Liste nennt Microsoft nicht nur

die einzelnen Unterauftragsverarbeiter, sondern stellt den Kunden weitere Informationen zur Verfügung. Microsoft gibt nunmehr Auskunft über die folgenden Punkte: den Namen des jeweiligen Unterauftragsverarbeiters, den Online-Service oder das Produkt, zu deren Bereitstellung die Dienste des Unterauftragsverarbeiters genutzt werden, die konkrete Verarbeitungstätigkeit, die Verarbeitungsorte, die registrierte Anschrift, den Hauptsitz sowie die registrierte Nummer und die Muttergesellschaft des Unterauftragsverarbeiters. Microsoft liefert damit umfassende Informationen zu den eingesetzten Unterauftragsverarbeitern. Diese Informationen sollten die Verantwortlichen in ihre Dokumentation zur Datenschutz-Compliance einfließen lassen.

8. Datenübermittlungen in Drittstaaten

Was sagt die DSK?	Antwort von Microsoft
<p>„Der ‚Datenschutznachtrag‘ vom September 2022 enthält die Regelung, dass der Kunde Microsoft ,beauftragt (...), (...) personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind‘. Für sämtliche Übermittlungen von insbesondere personenbezogenen Daten gelten danach die von Microsoft implementierten Standardvertragsklauseln der EU-Kommission von 2021.</p> <p>Die Gespräche der Arbeitsgruppe mit Microsoft bestätigten entsprechend den vertraglichen Regelungen, dass bei der Nutzung von Microsoft 365 personenbezogene Daten jedenfalls in die USA übermittelt werden. Eine Nutzung von Microsoft 365 ohne Übermittlungen personenbezogener Daten in die USA sei nicht möglich. Ab Dezember 2022 plane Microsoft, allen Kunden im EU-Raum anzubieten, Kundendaten, Supportdaten und sonstige personenbezogene Daten der Kunden grundsätzlich – d.h. nicht ausnahmslos, nicht etwa für bestimmte IT-Sicherheitsmaßnahmen – im EU-Raum zu speichern und zu verarbeiten (‚EU Data Boundary‘).</p> <p>Für die USA hat der EuGH in ‚Schrems II‘ festgestellt, dass FISA 702 und E.O. 12333 unverhältnismäßige Zugriffsrechte für US-Geheimdienste vorsehen und für EU-Bürger kein gerichtlicher Rechtsschutz gegeben ist. Um die vom EuGH identifizierten am EU-Maßstab gemessenen grundrechtlichen Unzulänglichkeiten von FISA 702 auszugleichen, wäre es erforderlich, Maßnahmen zu ergreifen, die den Zugriff der US-Behörden – und damit von Microsoft – auf personenbezogene Daten verhindern oder ineffektiv machen. Viele der in Microsoft 365 enthaltenen Dienste erfordern einen Zugriff von</p>	<ul style="list-style-type: none"> • „Microsoft teilt diese Einschätzung der DSK nicht. Es ist rechtlich nicht geboten, jedes theoretische Restrisiko, etwa eines behördlichen Zugriffs im Drittstaat, im Zusammenhang mit einer internationalen Datenübermittlung auszuschließen. • Microsofts EU-Datengrenze wird das aktuell bestehende Restrisiko durch maßgeblich reduzierte Datenflüsse (von Kundendaten und personenbezogenen Daten) nach außerhalb der EU weiter mindern. • Der erwartete Angemessenheitsbeschluss der EU-Kommission wird die Notwendigkeit von zusätzlichen Schutzmaßnahmen für Datentransfers in die USA komplett entfallen lassen. Microsoft setzt gemäß Art. 32 DS-GVO und dem aktuellen Stand der Technik umfangreiche, differenzierte und wirkungsvolle technische und organisatorische Maßnahmen ein. • Mit den vertraglichen Zusagen im DPA (vgl. insbesondere Anhang C) geht Microsoft über die rechtlichen Anforderungen hinaus, um die Daten seiner Kunden zu schützen.“

Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten. Die naheliegende Möglichkeit der **Verschlüsselung der verarbeiteten Daten ist regelmäßig nicht möglich**, beispielsweise wenn die Daten im Browser angezeigt werden müssen. Microsoft hat somit regelmäßig und letztlich schon zur Erfüllung vertraglicher Leistungspflichten die Möglichkeit, Daten im Klartext zu lesen. Es handelt sich mithin um eine klassische Ausprägung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. **Für diesen Anwendungsfall ist es den Aufsichtsbehörden bislang nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten.**

Die von Microsoft derzeit im Abschnitt ‚Ort der ruhenden Daten‘ vorgesehenen Maßnahmen für die Speicherung der Daten (data at rest) führen weder zum Ausschluss einer Übermittlung noch begründen sie hinreichende Schutzmaßnahmen. Für die weiteren Verarbeitungen (abseits der Speicherung) enthält der Abschnitt ‚Datenübermittlung und Ort‘ (‚Data Transfers and Location‘) keine Aussagen zur Datenlokalisierung. Auch die von Microsoft im ‚Nachtrag zu zusätzlichen Schutzmaßnahmen‘ zugesagten Maßnahmen sind nicht geeignet, die am Maßstab des EU-Rechts gemessenen grundrechtlichen Unzulänglichkeiten des US-amerikanischen Rechts auszugleichen. Zudem behält sich Microsoft vertraglich auch weitreichende Offenlegungen vor, die im Falle ihrer Umsetzung nicht den in Art. 48 DSGVO aufgestellten Anforderungen entsprechen würden.

Für Übermittlungen personenbezogener Daten **in andere Drittländer als die USA** fehlt es bereits an einer Bewertungsgrundlage.

Die von Microsoft bereits avisierte künftige verstärkte **Verlagerung der Datenverarbeitung in die EU erscheint vor diesem Hintergrund hilfreich**, ist in der Umsetzung aber auch vor dem Hintergrund etwaiger extraterritorial wirkender Rechtsvorschriften zu beobachten und zu bewerten.

Ob und in welchem Umfang durch die am 7. Oktober 2022 von US-Präsident Biden und Generalstaatsanwalt Garland vorgestellte Executive Order ‚Enhancing Safeguards for United States Signals Intelligence Activities‘ und begleitende Rechtsverordnungen des

US-Justizministeriums Änderungen der für die Bewertung von Drittstaatentransfers maßgeblichen Bedingungen des US-Rechts eingetreten sind, bleibt angesichts noch ausstehender Vollzugsschritte zur Implementierung dieser Regelungen im Rahmen dieses Berichts unberücksichtigt.“

Bewertung reuschlaw

Mit dem aktualisierten DPA hat Microsoft eine Reihe von wesentlichen Neuerungen für eine datenschutzkonforme Datenübermittlung in die USA ergriffen. So verpflichtet sich Microsoft nun ausdrücklich zur Vereinbarung und Einhaltung der neuen Standardvertragsklauseln (auf Engl. „Standard Contractual Clauses“ („SCC“)) der EU-Kommission in der aktuellen Version von 2021. Zu Transparenzzwecken und zur weiteren Prüfung hat Microsoft kürzlich zudem die unterzeichnete Version der SCC zwischen der Microsoft Ireland Operations Ltd. (Microsoft Irland) und der Microsoft Corporation (Microsoft USA) veröffentlicht. Diese dienen als geeignete Garantie für die Drittlandsübermittlung von Daten in die USA. Darüber hinaus verpflichtet sich Microsoft Irland mit dem neuen DPA sowie mit Unterzeichnung der SCC zur Durchführung eines sog. „Transfer Impact Assessment“, welches jedoch bislang nicht veröffentlicht wurde. Daneben sollten zudem die weiteren Erklärungen und Informationen von Microsoft zu etwaigen Drittlandsübermittlungen für eine umfassende Prüfung herangezogen werden, sodass aus einer Gesamtschau der Informationen gut vertretbar ist, dass bereits jetzt eine datenschutzkonforme Drittlandsübermittlung sichergestellt werden kann. Jedenfalls im Hinblick auf das von Microsoft angekündigte EU Data Boundary als europäische Cloudlösung und den angekündigten neuen Angemessenheitsbeschluss der EU-Kommission für Datenübermittlung in die USA dürfte sich die Problematik der Drittlandsübermittlungen eher kurz- als mittelfristig erübrigen.

Weitere Informationen zu einzelnen Kritikpunkten der DSK

- [Datenschutz bei MS 365 – neues DPA für 2023 veröffentlicht!](#)
- [FAQ zu Telemetrie- und Diagnosedaten in Microsoft 365](#)
- [US-Datentransfers bei Microsoft 365](#)
- [Neue Rechtslage in den USA](#)
- [Microsoft 365: mehr Datenschutz durch das EU Data Boundary!](#)
- [Einsatz von Microsoft 365 durch öffentliche Stellen](#)
- [5 Tipps für den datenschutzkonformen Einsatz von Microsoft 365 durch öffentliche Stellen](#)
- [Der Einsatz von Microsoft 365 durch kirchliche Stellen](#)

Next Step: Kontaktaufnahme

Melden Sie sich jederzeit gerne, wenn Sie unsere Unterstützung beim datenschutzkonformen Einsatz von Microsoft 365 benötigen oder Fragen haben. Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch und stimmen anschließend einen Kick-off-Workshop mit Ihnen ab.

T + 49 681 / 859 160 0

E info@reuschlaw.de

www.reuschlaw.de