Stand: 2. November 2022/endg.*

AG DSK „Microsoft-Onlinedienste“

Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung Stand 2. November 2022

* Das Dokument gibt den von der 104. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Kenntnis genommenen Ergebnisbericht wieder. Von der Veröffentlichung seiner Anlagen wurde mit Rücksicht auf den von Microsoft insoweit geltend gemachten Schutz von Geschäftsgeheimnissen zunächst abgesehen.

1. Untersuchungsauftrag

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Sitzung vom 22. September 2020 eine Bewertung des Arbeitskreises Verwaltung zu den dem Einsatz des Produkts Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die Bewertung kommt zum Ergebnis, *„dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“* sei. Die DSK hat eine Arbeitsgruppe unter Federführung Brandenburgs und des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gebeten, Gespräche mit dem Hersteller aufzunehmen, *„um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentliche und nicht öffentlicher Stellen zu erreichen*[1]*.“*

Der vorliegende Bericht behandelt die Ergebnisse der hierauf bis April 2022 geführten Gespräche (vgl. Anhang) und leitet daraus erste Vorschläge zum weiteren Vorgehen ab. Der Bericht folgt in seiner Struktur der Bewertung des AK Verwaltung[2], schreibt diese – ohne Anspruch auf Vollständigkeit – fort und ergänzt sie entsprechend dem Untersuchungsauftrag der DSK durch eine nicht abschließende Untersuchung grundlegender Fragestellungen an Datenübermittlungen in die USA bei der Nutzung von Microsoft 365. Es erfolgte ausdrücklich keine umfassende Prüfung des gesamten einschlägigen Vertragswerks von Microsoft, die vielmehr unter Berücksichtigung seiner jeweiligen konkreten Verarbeitungstätigkeiten nach Art. 5 Abs. 2 DSGVO dem einzelnen Verantwortlichen vorbehalten bleibt.[3]

2. Verfahren, Untersuchungsgegenstand und maßgeblicher Beurteilungszeitpunkt

In den Gesprächen der Arbeitsgruppe mit Microsoft haben neben Brandenburg und BayLDA (beide Leitung) Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie der Datenschutzaufsichtsbehörden Baden-Württembergs, Berlins, Hessens, Mecklenburg-Vorpommern, Sachsens, des Saarlandes und Schleswig-Holsteins teilgenommen. Microsoft hat die Gespräche federführend durch leitende Vertreter der Microsoft Deutschland GmbH sowie je nach Schwerpunkt Ansprechpartner der Microsoft Corporation wahrgenommen.

---

[1] Vgl. TOP 9 („TOP 9 – Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365“), S. 5, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf.

[2] Anlage 1, S. 10ff. („Bewertung der AK Verwaltung vom 15.07.2020“) ebd.

[3] Etwa anhand der Checkliste zur Prüfung von Auftragsverarbeitungsverträgen, abrufbar unter: https://www.datenschutz-berlin.de/themen/unternehmen/auftragsverarbeitung.

Die folgenden Untersuchungen berücksichtigen die von Microsoft im Fortgang der Gespräche bis 10. Juni 2022 übermittelten Informationen, die, soweit für das Bewertungsergebnis unmittelbar maßgeblich, entweder wiedergegeben oder als Anlage beigefügt sind. Maßgeblicher Prüfungsgegenstand ist der der Arbeitsgruppe zunächst vorab im Entwurf in englischer Fassung zur Verfügung gestellte „Datenschutznachtrag zu den Produkten und Services von Microsoft – letzte Aktualisierung: 15. September 2022“ [4] (im Folgenden: „Datenschutznachtrag“), in den die von Microsoft in den Gesprächen mit der Arbeitsgruppe entwickelten Vorschläge aufgenommen wurden.

Der vorliegende Bericht enthält weder eigenständige technische Untersuchungen durch die Arbeitsgruppe noch abschließende Bewertungen der konkreten Umsetzung der vertraglich festgelegten Verarbeitungen, noch behandelt der Bericht für Einzelkomponenten oder -funktionen des Produktpakets Microsoft 365 ggf. nunmehr maßgebliche datenschutzrechtliche Anforderungen des TTDSG. Weitere Fragestellungen, die über die sechs vom AK Verwaltung im oben genannten Bericht aufgeführten hinausgehen, wurden nicht vertieft untersucht. Daneben existieren von einzelnen Aufsichtsbehörden durchgeführte weitere Untersuchungen. [5] Microsoft hat mit einem Antwortschreiben vom 10. Oktober 2022 von der Gelegenheit Gebrauch gemacht, sich vorab zu dem Entwurf dieses Berichts zu äußern. Die Stellungnahme wurde durch die Arbeitsgruppe geprüft und zusammen mit ihren abschließenden Bericht zur Berücksichtigung im Zuge der weiteren Beratungen der DSK vorgelegt.

Der Bericht beschränkt sich auf eine Bewertung der zum Abschluss dieses Beteiligungsverfahrens am 10. Oktober 2022 bestehenden Sach- und Rechtslage. 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 des für die Bewertung von Drittstaatentransfers maßgeblichen Bedingungen des US-Rechts eingetreten sind, bleibt daher angesichts noch ausstehender Vollzugsschritte zur Implementierung dieser Regelungen im Rahmen dieses Berichts unberücksichtigt.

---

[4] Abrufbar unter https://aka.ms/dpa bzw. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. Da eine durch Microsoft freigegebene deutsche Übersetzung des Dokuments erst im Laufe der abschließenden Abstimmungen des Berichts bereitgestellt wurde, sind punktuelle, inhaltlich nicht relevante Abweichungen zwischen der im nachfolgenden wiedergegebenen Übersetzung durch die Arbeitsgruppe und der mittlerweile veröffentlichten Textfassung nicht auszuschließen (s. auch Fn. 27).

[5] Vgl. z.B. seitens der deutschen Aufsichtsbehörden: Ausführlich LfDI BW, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen/#zusammenfassung; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, Version 2.0 vom 18. Februar 2021, S. 20 ff., https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf.

3. Wesentliche Ergebnisse

3.1. Allgemeines

Da datenschutzrechtliche Anforderungen der DSGVO grundsätzlich an Verarbeitungstätigkeiten, nicht an Produkten oder Dienstleistungen anknüpfen, bleibt zur Eingrenzung des Prüfungsgegenstandes zunächst der Umfang von Diensten und Funktionen zu betrachten, den Microsoft mit dem Angebot

Abbildung 1

„Microsoft 365“ in an verschiedenen Zielgruppen ausgerichteten „Plänen“ zusammenfasst.

So umfasst beispielsweise alleine das Produktpaket „Microsoft 365 Business Premium“ [6] 15 unterschiedliche Anwendungen, die gängige Büro-Software zur Textverarbeitung oder Tabellenkalkulation, Cloudspeicher, Video-Konferenzsysteme mit Social Media-Elementen oder Sicherheits-Funktionen bereitstellen. Die Arbeitsgruppe hat keine Untersuchung der einzelnen Produkte vorgenommen und die Funktionalitäten sowie datenschutzrechtlichen Fragen der einzelnen Produkte im Rahmen der Gespräche nicht bzw. nur sehr rudimentär angesprochen.

Der durch die Arbeitsgruppe geprüfte „Datenschutznachtrag“ umfasst u.a. als Vereinbarung zur Auftragsverarbeitung sämtliche mit diesen Anwendungen verbundenen Verarbeitungsvorgänge (soweit diese vom „Datenschutznachtrag“ umfasst werden), [7] allerdings ohne diese genauer zu

[6] https://www.microsoft.com/de-de/microsoft-365/business/microsoft-365-business-premium?market=de&activetab=pivot%3aoverviewtab.

[7] Vgl. hierzu den „Datenschutznachtrag“ etwa unter „Scope“ oder in der Definition von „DPA Terms“.

spezifizieren. Ebenso gilt der Vertragstext aber ohne jede weitere Unterscheidung auch für im Umfang erweiterte „Microsoft 365“-Pakete oder andere Microsoft-Dienste wie den Cloud-Service „Azure.[8]. Eine umfassende Information über alle Verarbeitungsvorgänge – sowohl solche die Microsoft im Auftrag des Verantwortlichen als auch als eigenständiger Verantwortlicher durchführt – wurde weder der Arbeitsgruppe vorgelegt noch haben Verantwortliche die Möglichkeit, eine solche einzusehen.

Der Vereinheitlichungsanspruch des Vertragstextes gilt im Übrigen nicht nur sachlich, sondern auch territorial. Unabhängig davon, ob das Rechtsverhältnis zwischen Microsoft und seinem Kunden der DSGVO oder anderen Rechtsordnungen unterliegt, ergeben sich die datenschutzrechtlichen Regelungen stets aus dem derzeit 20-seitigen „Datenschutznachtrag“. Gegenüber weiteren vertraglichen Regelungen zwischen Microsoft und dem jeweiligen Kunden – mit Ausnahme der produktspezifischen Regelungen, die wiederum dem „Datenschutznachtrag“ vorgehen [9] – beansprucht der „Datenschutznachtrag“ Vorrang[10], wobei die Arbeitsgruppe nicht prüfen konnte, ob dies auch in den anderen Vertragsdokumenten so vereinbart ist.

Für Microsoft-Kunden, die der DSGVO unterliegen, sieht das Vertragswerk einen in der aktuellsten Version als Anhang gekennzeichneten Abschnitt „Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union“ vor, der aber keine abschließende Bestimmung darstellt, sondern die Bestimmungen des Unterabschnitts „Verarbeitung personenbezogener Daten; DSGVO“ gelten ausdrücklich ebenfalls und ohne Normenhierarchie.[11]

Nicht abschließend thematisiert hat die Arbeitsgruppe, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als (eigenständiger oder gemeinsam) Verantwortlicher. Dies ist nicht in allen Fällen geklärt.[12] Die Arbeitsgruppe setzt vielmehr für ihre Bewertungen teilweise die Anwendbarkeit der Vorschriften des „Datenschutznachtrags“ voraus.

Die allgemeine datenschutzrechtliche Bewertung des „Datenschutznachtrags“ als Vereinbarung zur Auftragsverarbeitung kann im Übrigen für die individuelle Bewertung einzelner Verantwortlicher nur als Anhaltspunkt herangezogen werden, da sie nur die zum Abschluss dieser Untersuchung vorliegende Version betrifft. Ob die ursprünglich bei Begründung eines Service-Bezugs oder eine teils auch mehrfach aktualisierte Folgeversion gilt, bleibt einzelfallbezogen nach Maßgabe der Bestimmungen

---

[8] Vgl. hierzu auch https://www.microsoft.com/licensing/terms/de-DE/product/PrivacyandSecurityTerms/.

[9] Vgl. Definition „DPA Terms“.

[10] So der Abschnitt „Einleitung“, Absatz 2.

[11] So ausdrücklich der Abschnitt „Verarbeitung personenbezogener Daten, DSGVO“, Absatz 2. Dass der Anhang 1 als in seinem Anwendungsbereich speziellere Regelung Vorrang beanspruchen soll, ist dem Text nicht zu entnehmen

[12] Vgl. zu Problemen bereits den Anwendungsbereichs der Regelungen des „Datenschutznachtrags“ zur Auftragsverarbeitung im Detail Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, Version 2.0 vom 18. Februar 2021, S. 23 f., https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf.

über „Anwendbare DPA-Bestimmungen und –Aktualisierungen“[13] zu beurteilen.[14] Unabhängig davon hat Microsoft gegenüber der Arbeitsgruppe mitgeteilt, dass die von der Arbeitsgruppe geforderten oder vorgeschlagenen Änderungen des „Datenschutznachtrags“ stets allen Kunden zugutekommen würden und sich Microsoft insoweit nicht darauf berufen würde, dass noch eine Vorfassung des DPA in Kraft ist.

3.2. Zusammenfassung der Gesprächsergebnisse

Im Rahmen der Gespräche mit Microsoft wurden insbesondere die einzelnen Gründe für die Bewertung des AK Verwaltung aus dem Jahr 2020 erörtert. Die folgende Darstellung greift die sechs Gründe und die Gesprächsergebnisse dazu auf.

3.2.1. Festlegung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten

3.2.1.1. Feststellungen des AK Verwaltung

Die Untersuchung des AK Verwaltung vom 15. Juli 2020 rügt die fehlende Möglichkeit des Verantwortlichen, personenbezogene Daten und deren Verarbeitungszweck näher zu beschreiben und gegebenenfalls zu konkretisieren, insbesondere bei mit besonderen Anforderungen verbundenen Daten nach Art. 9 DS-GVO. Microsoft wurde empfohlen, den Abstraktionsgrad der Auftragsverarbeitungsvereinbarung zu verringern und Freifelder mit Anpassungsmöglichkeiten einzufügen.

3.2.1.2. Aktueller Prüfungsgegenstand

Gegenüber der durch den AK Verwaltung bewerteten Fassung der Vereinbarung vom Januar 2020 enthält der aktuelle „Datenschutznachtrag“ keine strukturellen Veränderungen:

Zwar wurden bereits mit der im Untersuchungszeitraum veröffentlichten Vorgängerversion vom 15. September 2021 die als Anknüpfungspunkt für verschiedene Regelungen relevanten zentralen Begrifflichkeiten der „Kundendaten“ und „Professional-Services-Daten“ modifiziert. Inhaltliche Änderungen, insbesondere Konkretisierungen dieser generischen Definitionen, wurden damit jedoch nicht erreicht.

Gleiches gilt für letztlich rein sprachliche Anpassungen im neu gefassten Anhang B des „Datenschutznachtrags“, die inhaltlich der den Standardvertragsklauseln 2010 entnommenen Fassung

[13] „Microsoft Produkt an d Services DPA“, S. 3.

[14] Unbeschadet dessen sollen nach Aussage von Microsoft die DSGVO-spezifischen Zusicherungen des Abschnitts „Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union“ im Wege einer einseitigen Verpflichtung durch Microsoft für sämtliche Kundenbeziehungen mit Microsoft als Auftrags- oder Unterauftragsverarbeiter unabhängig von ihrer Vertragssituation unmittelbar ab 25. Mai 2018 gelten.

des Anhangs 1 vom Januar 2020 entspricht. Seine Anwendbarkeit für der DSGVO unterliegende Kunden von Microsoft ergibt sich aus seiner Inbezugnahme im Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“ des Vertragswerks. Die 19 Einzelkategorien umfassende Liste soll, wie die Kategorie der „alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten“ verdeutlicht, den möglichen Vertragsgegenstand umfassend beschreiben.

3.2.1.3. Gesprächsergebnisse

Microsoft hat der Rüge mangelnder Eingrenzung des Vertragsgegenstandes im Verlauf der Gespräche nicht abgeholfen. Microsoft leitet seine Bewertung, dass weitere Konkretisierungen „keinen substanziell anderen datenschutzrechtlichen Effekt erzielen“ würden, im Wesentlichen daraus ab, dass der Umfang der zur Beschreibung von Datenarten und Verarbeitungszwecken bereitgestellten Angaben sich aus Aussagen der WP-29-Stellungnahme 03/2013 zum Grundsatz der Zweckbindung ergebe und dass die Darstellung der Datenerhebungskategorien und Nutzungszwecke mit der ISO/IEC 19944 einem anerkannten Standard folge, der eine logisch vollständige Beschreibung aller Datenkategorien gewährleiste, für die Microsoft gleiche Datensicherheitsstandards gewährleiste.

Zu berücksichtigen bleibt, dass die „DSGVO-Bestimmungen“ (Anlage 1) zur Bestimmung des Vertragsgegenstandes zusätzlich eine Verweisung auf den Lizenzvertrag enthalten, zugleich aber eine Rückverweisung auf die „DSGVO-Bestimmungen“ des Datenschutznachtrags:

„2. (…) Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen sowie Pflichten und Rechte des Kunden werden im Lizenzvertrag des Kunden festgelegt, der die DSGVO-Bestimmungen einschließt.“[Hervorhebung durch Verf.][15]

Ob Microsoft-Kunden im Rahmen spezifischer Lizenzverträge für unterschiedliche Sektoren oder Vergütungsmodelle z.B. über Freifeldeintragungen Möglichkeiten zur Konkretisierung des von der Auftragsverarbeitung betroffenen Personenkreises und der damit verbundenen Datenkategorien eingeräumt sind, wurde weder von Microsoft selbst näher dargelegt noch war dies anderweitig abschließend zu klären. Die allgemeine Version des „Microsoft-Kundenvertrages“ [16] lässt solche Möglichkeiten jedenfalls nicht erkennen.
Vorbehaltlich anderweitiger Optionen im Rahmen des jeweiligen Lizenzvertrages über Microsoft 365 sind damit einzelfallbezogene Konkretisierungsmöglichkeiten des Gegenstands der Auftragsverarbeitung auch weiterhin nicht erkennbar.

[15] „Datenschutznachtrag“, S. 19

[16] Abgerufen unter https://www.microsoft.com/licensing/docs/customeragreement, letztes Update 18. Oktober 2019.

3.2.1.4. Bewertung

a) Prüfungsmaßstab

Art. 28 Abs. 3 Satz 1 DSGVO fordert, dass in dem Vertrag oder sonstigen Rechtsinstrument zur Regelung der Auftragsverarbeitung „Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind".

In den mit Durchführungsbeschluss 2012/915 der EU-Kommission vom 4. Juni 2021 bereitgestellten Standardvertragsklauseln nach Art. 28 Abs. 7 DS-GVO sehen Klausel 6 und Anhang II eine individualisierende, konkrete Beschreibung der Verarbeitung nach Kategorien betroffener Personen, Kategorien personenbezogener Daten, Art der Verarbeitung, Zwecken und Dauer der Verarbeitung vor.

Die Leitlinien des Europäischen Datenschutzausschusses 07/2020 zum Konzept der Auftragsverarbeitung und gemeinsam Verantwortung schließen zwar die Nutzung standardisierter Dienstleistungsverträge als Grundlage der Auftragsverarbeitung nicht aus,[17] verlangen gleichzeitig aber zur nachvollziehbaren Festlegung von Rechten und Pflichten der Vertragsparteien zumindest eine Abfassung des Vertrages, bei der die konkrete Datenverarbeitung berücksichtigt wird.[18]

b) Detailbewertung

Auch wenn die Aufzählung des Anhangs B über „Betroffene Personen und Kategorien personenbezogener Daten" begrifflich und systematisch eine formale Eingrenzung der wesentlichen Vertragsmerkmale erreichen mag, begründet der Regelungsansatz, „im Zweifel alle und alles" in den Geltungsbereich des Vertrages einzuschließen, die Gefahr, wesentliche Vertragsziele zu verfehlen. Beim Vergleich der Vertragsversionen wird deutlich, dass Anhang B letztlich nach wie vor auf Regelungsmodellen aufbaut, die auf die Standvertragsvertragsklauseln 2010 zurückgehen. Wie schon der Anhang 1 zu den Standardvertragsklauseln in der Version 01/2020 des „Datenschutznachtrags" beschreibt Anhang B nicht etwa zwischen den Vertragsparteien für den Einzelfall festgelegte Verarbeitungen, sondern vertraglich zugesicherte Verarbeitungsmöglichkeiten, über deren Inanspruchnahme der Kunde einseitig entscheidet:

„Microsoft bestätigt, dass sich der Kunde je nach Nutzung der Produkte und Services dafür entscheiden kann, personenbezogene Daten von einer der folgenden Arten von betroffenen Personen in die personenbezogenen Daten aufzunehmen:"

[17] EDSA, Leitlinien 07/2020, Rn. 84.

[18] EDSA, Leitlinien 07/2020, Rn. 113.

„Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte und Services die Möglichkeit hat, personenbezogene Daten aus einer der folgenden Kategorien in die personenbezogenen Daten aufzunehmen:“ [Hervorhebungen durch Verf.]

Dem steht gegenüber, dass mit Geltungsbeginn der DSGVO Verantwortliche und Auftragsverarbeiter in höherem Maße Kooperationspflichten zur Gewährleistung datenschutzrechtlicher Anforderungen unterworfen sind. So verlangt z.B. Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe f DSGVO im Rahmen der Gewährleistung der Anforderungen von Art. 32 bis 36 DSGVO, dass der Auftragsverarbeiter den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt. Das Erfordernis spezifischer Informationen über den Kreis der betroffenen Personen und der Kategorien betroffener Personen wird auch bei der im „Datenschutznachtrag“[19] vorgesehenen Anwendung der Standardvertragsklauseln 2021 deutlich, die in ihrem Anhang I B[20] zur Beschreibung der Datenübermittlung hierzu genauere Angaben vorsehen.

Die gesetzlichen Pflichtangaben zur Beschreibung der Auftragsverarbeitung dienen auch dazu, die Rollen der Vertragsparteien abzugrenzen und ihnen die Erfüllung ihrer Verpflichtungen – etwa im Hinblick auf Art. 32 DSGVO – zu ermöglichen. Im Hinblick auf Art. 32 DSGVO mag das Fehlen von Konkretisierungsmöglichkeiten bei gleichzeitiger Einbeziehung beliebig schutzbedürftiger personenbezogener Daten letztlich zu Lasten des Auftragsverarbeiters gehen, der dadurch die höchsten denkbaren Anforderungen erfüllen muss. Hinsichtlich der Frage, für welche Verarbeitungen sich der Auftragnehmer den Verpflichtungen als Auftragsverarbeiter unterwirft, könnte man eine „Alles“-Klausel zwar grundsätzlich als zulässig ansehen, wenn auch sich daraus mittelbar große Herausforderungen für den Verantwortlichen zur Erfüllung seiner Transparenzpflichten ergeben würden, sei es bei der genauen Erfüllung seiner Informationspflichten oder bei der Beschreibung von Verarbeitungstätigkeiten, zu deren Durchführung Microsoft 365 eingesetzt wird. Allerdings scheint es naheliegender, davon auszugehen, dass der Gesetzgeber die Angaben zur Konkretisierung der Auftragsverarbeitung nicht als reine Formalia ansieht, sondern auch als Mittel zur Selbstkontrolle der Parteien, welche Verarbeitungen ausgelagert werden sollen und welche Risiken damit ggf. verbunden sind. Dies würde dem von Microsoft verfolgten Ansatz, keine konkrete Festlegung der Auftragsverarbeitung zuzulassen, entgegenstehen.

3.2.1.5. Schlussfolgerungen

Ungeachtet des Zeitabstands und weiterer Besonderheiten entsprechen die dargestellten Befunde hinsichtlich der Erforderlichkeit grundlegender Präzisierungen des Vertragsgegenstandes zur jüngsten Fassung des „Datenschutznachtrags“ noch den im Juli 2020 veröffentlichten Untersuchungsergebnissen [21] des Europäischen Datenschutzbeauftragten zu den vertraglichen

[19] „Datenschutznachtrag“, Abschnitt „Datenübermittlungen und Speicherstelle – Datenübermittlungen“.

[20] Abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj#d1e32-58-1.

[21] Abrufbar unter: https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf#page=14.

Grundlagen des Einsatzes von Microsoft-Produkten bei den EU-Institutionen. An Stelle des jetzigen „im Zweifel alle und alles“-Ansatzes bleiben wie schon bei den Prüfungen und Handlungsempfehlungen des EDPS zur Beschreibung des Gegenstands der Auftragsverarbeitung gem. Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO Nachbesserungen erforderlich, die diesen nicht nur umfassend, sondern auch spezifisch und so detailliert als möglich beschreiben sollten. Durch solche Nachbesserungen würde dann auch der Microsoft 365 einsetzende Kunde (Verantwortliche) eher in die Lage versetzt, seinen datenschutzrechtlichen Verpflichtungen wie der Erfüllung der Transparenzpflichten nachkommen zu können.

Microsoft wird daher weiterhin empfohlen, zu überprüfen, wie eine kundenspezifische Konkretisierung nach dem Vorbild des Anhangs II der Standardvertragsklauseln der Kommission gemäß Art. 28 Abs. 7 DS-GVO[22] erreicht werden kann. Gemeinsam mit den Verantwortlichen könnte auch erwogen werden, entsprechend den Handlungsoptionen in der von verschiedenen Aufsichtsbehörden genutzten „Checkliste zur Prüfung von Auftragsverarbeitungsverträgen“ z.B. Verweise auf ein formgerecht in den Vertrag einzubeziehendes und hinreichend detailliertes Verzeichnis der Verarbeitungstätigkeiten (VVT) des Verantwortlichen vorzusehen [23] . Die bisher im Abschnitt „Verarbeitung personenbezogener Daten; DSGVO — Verarbeitungsdetails“ aufgenommene Erwähnung des Kunden-VVT[24] setzt ein solches Modell noch nicht hinreichend um, da die Bestimmung rein deskriptiv auf das VVT verweist, aber keinen Prozess etabliert, in dem dieses für beiden Seiten einseh- und nutzbar sowie formgerecht zum Vertragsgegenstand erhoben wird.

3.2.2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime Geschäftszwecke“

3.2.2.1. Feststellungen des AK Verwaltung

Die Untersuchung des AK Verwaltung vom 15. Juli 2020 hat sich eingehendmit den vertraglichen Bestimmungen zu von Microsoft zunächst als „legitime Geschäftszwecke“ bezeichneten Verarbeitungen befasst, die im Gesamtgefüge des Vertrages mit der Rolle Microsofts als „unabhängiger Datenverantwortlicher“ [25] neben die Auftragsverarbeitung treten. Diese Verarbeitungstätigkeiten sind auch im Kontext der Löschung und Rückgabe personenbezogener Daten von Bedeutung (siehe unten 2.2.5).

---

[22] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE.

[23] Vgl. als Handlungsoption die Checkliste der Berliner Aufsichtsbehörde zur Prüfung von Auftragsverarbeitungsverträgen abrufbar unter: https://www.datenschutz-berlin.de/themen/unternehmen/auftragsverarbeitung.

[24] Ausdrücklich [Hervorhebung durch Verf.]: „Bei den Arten von personenbezogenen Daten, die der Kunde in die Kundendaten und Professional Services-Daten aufnehmen möchte, kann es sich um alle Kategorien von personenbezogenen Daten handeln, die in Aufzeichnungen genannt werden, die vom Kunden als Verantwortlicher gemäß Artikel 30 DSGVO handelnd gepflegt werden, einschließlich der in Anhang B aufgeführten Kategorien personenbezogener Daten.“

[25] Vgl. etwa „Datenschutznachtrag“ 09/21, Abschnitt „Auftragsverarbeiter und Verantwortlicher“, Absatz 2.

Im Kern rügt der AK Verwaltung, dass die vertraglichen Bestimmungen nicht hinreichend erkennen ließen, welche weiteren personenbezogenen Daten im Rahmen dieser Bestimmungen verarbeitet werden sollen. Zudem bestehe „für die Übermittlung weiterer personenbezogener Daten vom Verantwortlichen an Microsoft, z.B. im Rahmen der Telemetrie, neben dem Auftragsverarbeitungsvertrag keine weitere Rechtsgrundlage“.

Soweit nicht-öffentliche Stellen sich für die Übermittlung an Microsoft als eigenständigen Verantwortlichen u.U. auf ein berechtigtes Interesse nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO berufen könnten, gelte dies gemäß Art. 6 Absatz 1 Satz 2 DSGVO nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Es bedürfe daher einer eigenen Rechtsgrundlage, die es der öffentlichen Verwaltung erlaube, Daten von Beschäftigten oder Bürgerinnen und Bürgern für diese Zwecke zur Verfügung zu stellen.

3.2.2.2. Aktueller Prüfungsgegenstand

Gegenüber der Fassung vom Januar 2020 findet sich im „Datenschutznachtrag“ vom 15. September 2022 eine begrifflich wie inhaltlich deutlich geänderte Bestimmung über die „Verarbeitung für Geschäftstätigkeiten“.

Noch in der Version 09/2021 des „Datenschutznachtrags“ umfasste die Microsoft im Rahmen einer eigenständigen Verantwortlichkeit unterschiedslos für sämtliche Kategorien personenbezogener Daten[26] eingeräumte Verarbeitungsbefugnis

„(1) Abrechnungs- und Kontoverwaltung;
(2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives);
(3) interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie);
(4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten;
(5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und
(6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im Folgenden beschriebenen Beschränkungen für die Offenlegung verarbeiteter Daten).“

Unbeschadet weiterer Anpassungen gilt ab 15. September 2022 eine in Struktur und Systematik deutlich veränderte Umgrenzung von Verarbeitungen, deren Zuordnung als Teil der Auftragsverarbeitung oder eigenständige Verantwortlichkeit Microsofts unter der Überschrift [27]

[26] So ausdrücklich Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse“, Satz 1.

[27] Da zum Zeitpunkt der Erstellung dieses Berichts noch keine von Microsoft freigegebene deutsche Sprachfassung des „Datenschutznachtrags“ 09/2022 vorlag, sind bei allen Zitaten Abweichungen gegenüber der hiesigen Übersetzung nicht auszuschließen.

„Verarbeitung für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Dienstleistungen für den Kunden“ offen bleibt:

„Für die Zwecke dieses DPA bezeichnet der Begriff „Geschäftstätigkeiten“ die vom Kunden in diesem Abschnitt genehmigten Verarbeitungsvorgänge.

Der Kunde ermächtigt Microsoft:
(i) aggregierte statistische, nicht personenbezogene Daten aus Daten, die pseudonymisierte Identifikatoren enthalten (z. B. Nutzungsprotokolle, die eindeutige, pseudonymisierte Identifikatoren enthalten), zu erstellen; und

(ii) zur Berechnung von Statistiken in Bezug auf Kundendaten oder Professional Services-Daten

in jedem Fall ohne Zugriff auf oder Analyse des Inhalts von Kundendaten oder Professional Services-Daten und beschränkt auf die Erreichung der unten aufgeführten Zwecke, jeweils im Zusammenhang mit der Bereitstellung der Produkte und Dienstleistungen für den Kunden.

Diese Zwecke sind:
- *Abrechnung und Kontoverwaltung;*
- *Vergütungen wie die Berechnung von Mitarbeiterprovisionen und Partneranreizen;*
- *internes Berichtswesen und Geschäftsmodellierung, wie z. B. Prognosen, Umsatz- und Kapazitätsplanung und Produktstrategie; und*
- *Finanzberichterstattung.“*

3.2.2.3. Gesprächsergebnisse

Die tatsächliche und rechtliche Analyse der von Microsoft zur „Verarbeitung für Geschäftstätigkeiten“ durchgeführten Prozesse bildete insgesamt einen Schwerpunkt der Gespräche zwischen Microsoft und der DSK-Arbeitsgruppe.

Auf Grundlage einer von Microsoft einer detaillierten Betrachtung der derzeitigen Geschäftsprozesse, die in einer Matrix zusammengefasst wurden (Anlage 1 zu diesem Bericht) und einer in den Gesprächen präsentierten Grafik über Datenflüsse (Anlage 2), konnten zwar grundlegende Fragen zur rechtlichen Strukturierung dieser Verarbeitungsvorgänge letztlich auch mit Rücksicht auf abweichende Beurteilungsmaßstäbe anderer europäischer Datenschutzaufsichtsbehörden nicht abschließend geklärt und konnte keine Einigkeit über die rechtliche Einordnung erzielt werden. Gleichwohl haben die Analysen den Impuls für eine geänderte und konkrete Grenzen[28] enthaltende Beschreibung der

[28] nämlich ”in jedem Fall ohne Zugriff auf oder Analyse des Inhalts von Kundendaten oder Professional Services-Daten und beschränkt auf die Erreichung der unten aufgeführten Zwecke, jeweils im Zusammenhang mit der Bereitstellung der Produkte und Dienstleistungen für den Kunden.“

deutlich überschießenden Erlaubnisse zur Nutzung der vertragsgegenständlichen Daten durch Microsoft gesetzt.

Nach Darstellung Microsofts nutzen die ursprünglich sechs eigenen Verarbeitungszwecke die von Microsoft generisch definierten Kategorien der

(1) Kundendaten,
(2) Diagnosedaten,
(3) Dienstgenerierten Daten,
(4) „Professional Service"-Daten (i.S.v. Microsoft-spezifischen Beratungs- und Supportleistungen),
(5) sonstigen Support-Daten.

Die vertragliche Bezeichnung der jeweiligen Kategorien ist nicht selbsterklärend und hat sich über die Versionen hinweg immer wieder geändert, sodass eine rechtssichere Abgrenzung, welche Verarbeitung personenbezogener Daten welche Datenkategorien betrifft, nicht immer gewährleistet ist.

In der Vorstellung der tatsächlich verfolgten Geschäftszwecke gab Microsoft an (siehe Anlage 1), dass mit Ausnahme der Verarbeitungszwecke „Betrugsabwehr und Cybersicherheit" sowie der „Erfüllung rechtlicher Verpflichtungen" für sämtliche übrigen Geschäftszwecke

- nur statistisch aggregierte Datensätze,
- nur mengenbezogene Kundendaten,
- keine Inhaltsdaten aus Kundendaten und „Professional Service Daten"

weiterverwendet werden würden. Für deren Generierung würden jedoch personenbezogene Daten sämtlicher Kategorien verarbeitet.

Für den in der Fassung des „Datenschutznachtrags" 09/2022 entfallenen Verarbeitungszweck „Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz" wurden durch Microsoft in den gesamten Gesprächen keine aktuellen Anwendungsfälle genannt, die auf einer Nutzung personenbezogener Daten beruhten.

Ungeachtet einzelner Beispiele vermitteln die Darstellungen Microsofts keine abschließende Übersicht der Datenarten, die im Rahmen der jeweiligen generischen Datenkategorien für die beschriebenen Prozesse verarbeitet werden und umfasst sein können. In den Gesprächen wurden alleine von Microsoft ausgewählte, nicht abschließende Beispiele für Anwendungsfälle, ohne vollständige Einsichtsmöglichkeit in tatsächlich erfolgte Datenverarbeitungen, präsentiert. Intern, so Microsoft, würden Prozesse existieren, die Genehmigungsanforderungen für einzelne Anwendungsfälle voraussetzen würden. Auch würde auf die Einhaltung der Erforderlichkeit bei der Nutzung von Daten geachtet. Eine vollständige Übersicht der verarbeiteten Daten und der Verarbeitungen wurde aber

weder der Arbeitsgruppe vorgelegt noch haben Verantwortliche die Möglichkeit, eine solche einzusehen.

Die Erläuterungen Microsofts zeigen jedenfalls auf, dass die Nutzung von „Kundendaten“ (also zum Beispiel Dokumente und Bilder der Kunden) zu eigenen Geschäftszwecken grundsätzlich nicht durch die Erzeugung eines zweiten, diesen Zwecken vorbehaltenen Bestandes der „Kundendaten“ sondern durch eigenständige Zugriffsprozesse auf in Microsoft-Systemen gespeicherte Datenbestände der einzelnen Verantwortliche erfolgen. Damit würden, so die Erläuterungen, etwa „Kundendaten“, die im Rahmen der Nutzung des Produkts gelöscht werden, nach Durchführung der Löschprozesse auch nicht für später eingeleitete Verarbeitungen zu eigenen Geschäftszwecken herangezogen. Die vertraglichen Regelungen spiegeln diese Aussage allerdings nicht wider.

Die in den letzten Jahren erfolgten vertraglichen Änderungen haben nach Aussage Microsofts keine Änderungen an den tatsächlich durchgeführten Verarbeitungen zur Folge. Auf Nachfrage wurden in den Gesprächen auch keine Änderungen der tatsächlichen Datenverarbeitungsprozesse angekündigt. Bis auf Weiteres ist daher davon auszugehen, dass die in der Version des „Datenschutznachtrags“ vom 15. September 2022 vorgenommenen Änderungen der vertraglichen Bestimmungen über Verarbeitungen für Microsofts Geschäftstätigkeiten zunächst keine technischen Änderungen bzw. Änderungen an den tatsächlich durchgeführten Verarbeitungen nach sich ziehen, d.h. dass nicht mehr als „Geschäftstätigkeiten“ umfasste Verarbeitungen nunmehr nicht entfallen, sondern anderweitig, z.B. in der Rolle Microsofts als Auftragsverarbeiter, legitimiert werden sollen. Nicht abschließend geklärt werden konnte, welchen Bereichen die Verarbeitung von Telemetrie- und Diagnosedaten sowie anders genannten ähnlichen Daten (z.B. „Wesentliche Dienste“) zugeordnet werden und auf welcher Rechtsgrundlage die Verarbeitung dieser Daten erfolgt.

3.2.2.4. Bewertung

a) <u>Prüfungsmaßstab</u>

Die Arbeitsgruppe geht in Übereinstimmung mit dem Bericht des AK Verwaltung davon aus, dass Verantwortliche für die vertragliche Einräumung der Erlaubnis an Microsoft, personenbezogene Daten auch zu eigenen Geschäftstätigkeiten zu verarbeiten, in vollem Umfang für die Einhaltung datenschutzrechtlicher Anforderungen nachweispflichtig sind (Art. 5 Abs. 2 DSGVO), d.h. insbesondere eine Rechtsgrundlage nach Art. 6 und 9 DSGVO nachweisen können müssen und alle Verarbeitungen in einer für die betroffenen Personen transparenten Art stattfinden (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz). Ebenso müssen sie nachweisen können, dass für ihren Verantwortungsbereich die Grundsätze der Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, sowie Integrität und Vertraulichkeit eingehalten werden. Dieses Erfordernis besteht auch, wenn diese Verarbeitung personenbezogener Daten im Ergebnis nur dazu führt, dass Microsoft aus Daten, die pseudonymisierte Identifikatoren enthalten, aggregierte statistische, nicht personenbezogene Daten ableitet.

Bei Verantwortlichen des öffentlichen Bereichs bleibt zu berücksichtigen, dass eine Rechtfertigung der Datenverarbeitung durch berechtigte Interessen Microsofts als Dritter durch Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DSGVO wegen Art. 6 Abs. 1 UAbs. 2 DSGVO ausgeschlossen ist, sodass die Gestattung einer Nutzung behördlicher Daten durch Microsoft für eigene Geschäftstätigkeiten letztlich nur im Rahmen von Art. 6 Abs. 1 UAbs. 1 Buchstabe e) DSGVO begründet werden könnte.

Ähnlich scheint auch die Untersuchung des EDPS – der letztlich sogar die datenschutzrechtliche Begründbarkeit eines Outsourcings von Cloud-Diensten jedenfalls im Bereich der EU-Institutionen insgesamt in Frage stellt [29] – das Vorliegen einer Rechtsgrundlage für die Einräumung solcher Verarbeitungsbefugnisse des Auftragsverarbeiters im öffentlichen Bereich, zusätzlich aber auch die Zweckkompatabilität zu verneinen.[30]

Dem steht gegenüber, dass Microsoft die Ausgestaltung der ursprünglich sechs Gruppen von Verarbeitungen für eigene Geschäftstätigkeiten auf Grund detaillierter Untersuchungen einschließlich technischer Prüfungen der Datenflüsse und Forderungen der durch das dortige Justizministerium vertretenen niederländischen Verwaltung erst im Herbst 2019 angekündigt und im Januar 2020 in sein Vertragswerk aufgenommen hat.[31] Die Beteiligung der niederländischen Aufsichtsbehörde in diesen Verfahren konnte nicht abschließend nachvollzogen werden, genauso wenig sind aber auch aus zahlreichen Folgeuntersuchungen der niederländischen Regierung zu Microsoft-Produkten Anhaltspunkte für eine grundsätzliche Kritik der niederländischen Aufsichtsbehörde an diesem Regelungsmodell erkennbar geworden. Insgesamt legt der Diskussionsprozess der niederländischen Regierung daher eine Einordnung der vorliegenden Fragestellungen nahe, die im grundsätzlichen Widerspruch sowohl zu den hiesigen Prüfungsmaßstäben als auch der Bewertung des EDPS steht.

Einen weiteren möglichen Prüfungsmaßstab zur Beurteilung der Verarbeitungs- bzw. „Geschäftstätigkeiten“, die im „Datenschutznachtrag“ Microsoft als Verantwortlicher zugewiesen werden, ergibt sich aus einer Veröffentlichung der französischen Aufsichtsbehörde CNIL vom 12. Januar 2022 unter dem Titel „Auftragsverarbeiter: die Weiterverwendung von Daten, die von einem Verantwortlichen anvertraut werden“: [32] Sie fordert dabei zusammengefasst, dass ein Auftragsverarbeiter im Auftrag verarbeitete personenbezogene Daten nur dann zu seinen eigenen Zwecken weiterverarbeiten darf, wenn eine solche Weiterverwendung mit der ursprünglichen

[29] EDPS, a.a.O., Rn. 58: “In its investigation, the EDPS found a risk that protections designed for the public interest context in which personal data was entrusted to EU institutions would be circumvented by means of the outsourcing process.”

[30] EDPS, a.a.O., Rn. 51 und vertieft 57: „However, the GDPR does not permit processing on grounds of a controller’s legitimate interests to be carried out by public authorities in the performance of their tasks. Nor are there any legitimate interests grounds for processing by EU institutions under Regulation (EU) 2018/1725. Recital 25 and Article 6 of Regulation (EU) 2018/1725 [see also recital 50 and Article 6(4) of the GDPR] suggest that when EU institutions use IT products and services to carry out tasks in the public interest entrusted to them by EU law, any processing for other tasks and purposes should be compatible with the tasks and roles of the EU institutions. When EU institutions act as controllers, they must ascertain whether the purposes for which other or further processing is undertaken is compatible under Article 6 of Regulation (EU) 2018/1725 [see also Article 6(4) of the GDPR].“

[31] https://blogs.microsoft.com/eupolicy/2019/11/18/introducing-privacy-transparency-commercial-cloud-customers/.

[32] https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement.

Verarbeitung vereinbar ist und der Verantwortliche ihm eine schriftliche Genehmigung dazu erteilt hat.

Im Mittelpunkt der von der CNIL beschriebenen Anforderungen an die Weiterverwendung von Daten durch den Auftragsverarbeiter stehen damit Fragen der Zweckkompatibilität, nicht einer Rechtsgrundlage, die offenbar alleine auf Seiten des „Ex-Auftragsverarbeiters“ gefordert wird. Für den in der hiesigen Untersuchung im Mittelpunkt stehenden Verantwortlichen stellt, so die CNIL, eine Weiterverwendung der Daten durch einen Auftragnehmer für eigene Zwecke eine Weiterverarbeitung dar, d.h. eine Verarbeitung, die dem Erhebungsvorgang folgt und einen anderen Zweck hat als den, der die ursprüngliche Erhebung rechtfertigt. Diese „Kompatibilitätsprüfung“ müsse für eine bestimmte Verarbeitung unter Berücksichtigung der Zwecke und Merkmale jeder Verarbeitung, für die der Auftragsverarbeiter die Daten weiterverarbeiten möchte, durchgeführt werden.

Das CNIL-Papier enthält keine dogmatische Begründung. In jedem Fall hält die CNIL fest, dass eine vorherige und allgemeine Genehmigung zur Weiterverwendung der Daten nicht rechtmäßig sei, sondern der erforderliche Kompatibilitätstest müsse für eine im Detail zu bewertende Verarbeitung durchgeführt werden. Auch bei erfolgreichem Kompatibilitätstest stehe es zudem dem Verantwortlichen frei, die Genehmigung zur Weiterverarbeitung zu erteilen oder zu verweigern. Auch wenn nicht völlig klar ist, ob die CNIL eine die Weisungsbindung des Auftragsverarbeiters auflösende Billigung der Weiterverarbeitung im Auftrag verarbeiteter personenbezogener Daten durch vertragliche Regelung akzeptieren würde oder ob insoweit nur eine spezifische Genehmigung im Einzelfall als zulässig erachtet wird, sprechen doch die Betonung der Prüfung im Einzelfall und vor allem der Entscheidungsfreiheit des Verantwortlichen auch bei positivem Kompatibilitätstest gegen die Möglichkeit einer vorab erteilten vertraglichen Erlaubnis.

b) <u>Detailbewertung</u>

Mit der Fassung des „Datenschutznachtrags“ vom 15. September 2022 verteilen sich die bisher im Hinblick auf Verarbeitungen für Microsofts Geschäftstätigkeiten aufgeworfenen Fragestellungen zunächst auf zwei Ebenen: Die ursprünglichen Microsoft-Verarbeitungszwecke

- „Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz“; „Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen können“ und
- „Erfüllung rechtlicher Verpflichtungen“

wurden nicht in die Liste der Verarbeitungen für Microsofts Geschäftstätigkeiten übernommen.

Dabei ist zu berücksichtigen, dass Microsoft im Rahmen der Gespräche erläutert hat, dass jegliche Verarbeitung zur Verbesserung der Kernfunktionen in Bezug auf Zugänglichkeit, Datenschutz oder Energieeffizienz nur im Rahmen der Tätigkeit von Microsoft als Auftragsverarbeiter im Auftrag der Kunden erfolgen würden. Die Verarbeitung zur Sicherung der Dienste erfolge ebenfalls im Rahmen

der Tätigkeit von Microsoft als Auftragsverarbeiter. Im Zuge der Abstimmungen und Untersuchungen habe man außerdem analysiert, dass jegliche Verarbeitung zur Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen ebenfalls im Rahmen der Tätigkeiten von Microsoft als Auftragsverarbeiter erfolgte.

Die genannten eigenen Geschäftszwecke seien durch Microsoft nach eingehender Diskussion entfernt worden, um dem von der Arbeitsgruppe gesetzten Ziel einer klareren Regelungsstruktur näher zu kommen.

Vor diesem Hintergrund bleibt indessen zunächst davon auszugehen, dass diese Verarbeitungstätigkeiten weiter durchgeführt werden und daher nach den gesetzlichen und ggf. sonstigen vertraglichen Regelungen beurteilt werden müssen.

Dagegen muss jedenfalls nach den Prüfungsmaßstäben der Arbeitsgruppe die Einräumung der Nutzung auftragsgegenständlicher personenbezogener Daten zu Zwecken von

- „Abrechnungs- und Kontoverwaltung“,
- „Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives)“,
- „interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie)“,
- „Finanzberichterstattung“

unbeschadet weiterer Voraussetzungen von einer Rechtsgrundlage gedeckt sein, die bei nicht-öffentlichen Stellen regelmäßig mangels anderer Ansätze nur aus Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DSGVO und bei öffentlichen Stellen nur aus Art. 6 Abs. 1 UAbs. 1 Buchstabe e) DSGVO abgeleitet werden könnte. Zu prüfen bleibt zudem, ob Daten verarbeitet werden, die nach Art. 9 DSGVO besonderen Schutzanforderungen unterliegen.

Die Arbeitsgruppe geht dabei davon aus, dass die im Abschnitt über eigene „Geschäftstätigkeiten“ ausgesprochene „Ermächtigung[33]“ des Auftragsverarbeiters zu bestimmten Datenverarbeitungen ihn nicht im Sinne einer Weisung zu bestimmten Datenverarbeitungen verpflichtet. Sie räumt Microsoft vielmehr eine Entscheidungsbefugnis jedenfalls über die Mittel der Datenverarbeitung im Rahmen einvernehmlicher[34] vertraglicher Zwecksetzung ein. Daraus ergibt sich aus Sicht der Arbeitsgruppe, dass Microsoft in diesem Bereich als Verantwortlicher und nicht als Auftragsverarbeiter tätig wird.[35] Diese Einordnung wird auch durch die Formulierung von Abs. 2 Satz 1 des Abschnitts „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ des

[33] In der englischen Fassung im Absatz „Processing for Business Operations Incident to Providing the Products and Services to Customer“ ausgedrückt mit „authorize“.

[34] Die sich daraus ergebende Frage einer gemeinsamen Verantwortlichkeit wird in der weiteren Untersuchung ausgeklammert.

[35] Vgl. EDSA, Leitlinien 07/2020, Rn. 15 ff.

„Datenschutznachtrags“ vom 15. September 2022 gestützt, da dort vereinbart wird, dass Microsoft sich an die Pflichten eines unabhängigen Verantwortlichen halten wird.

Für beiden „Rollen“ Microsofts sieht der „Datenschutznachtrag“ bestimmte Ausschlusstatbestände vor, die die Verarbeitung bestimmter Datenkategorien und Verarbeitungen zu bestimmten Zwecken ausschließen:

- *„Bei der Bereitstellung von Produkten und Services wird Microsoft Kundendaten, Professional Services-Daten oder personenbezogene Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) Marktforschung zur Entwicklung neuer Funktionen, Dienstleistungen oder Produkte oder zu anderen Zwecken; es sei denn, eine solche Verwendung oder Verarbeitung erfolgt nach den dokumentierten Anweisungen des Kunden.“*[36]
- *„Bei der Verarbeitung für diese Geschäftstätigkeiten wendet Microsoft die Grundsätze der Datenminimierung an und verwendet oder verarbeitet keine Kundendaten, Professional Services-Daten oder personenbezogenen Daten für: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke.“*[37]
- *Bei der Verarbeitung für Geschäftstätigkeiten von Microsoft darf nicht auf den Inhalt von Kundendaten und „Professional Service Daten“ zugegriffen oder dieser analysiert werden, und teilweise darf nur auf Daten mit pseudonymisierten Identifiern zugegriffen werden und dürfen die Ergebnisse keine personenbezogenen Daten enthalten.*[38]

Im Einzelnen ergibt sich daraus folgendes Bild:

i) Betrugs- und insbesondere Cyberabwehr als vormalige Teile weisungsgebundener Auftragsverarbeitung

Während in der Version vom September 2021 des „Datenschutznachtrags“ noch „Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten“ als eigene Geschäftstätigkeit deklariert wurde,[39] sind diese Verarbeitungszwecke in der Fassung vom 15. September 2022 gestrichen worden. Nunmehr wird lediglich der Verarbeitungszweck „Steigerung der (...) Sicherheit“ im Abschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ benannt.

Art. 32 DSGVO begründet einerseits die unmittelbare Verpflichtung des Auftragsverarbeiters, geeignete technische und organisatorische Maßnahmen zu treffen, andererseits hat er nach

[36] „Datenschutznachtrag“, Abschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“.

[37] „Datenschutznachtrag“, Abschnitt „Verarbeitung für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Dienstleistungen für den Kunden“.

[38] „Datenschutznachtrag“, Abschnitt „Verarbeitung für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Dienstleistungen für den Kunden“.

[39] „Datenschutznachtrag“, Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse — Verarbeitung für legitime Geschäftstätigkeiten von Microsoft“.

Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe f) DSGVO die gesondert zu betrachtende[40] Verpflichtung, den Verantwortlichen bei dem von diesen zu treffenden technischen und organisatorischen Maßnahmen zu unterstützen, und die gesetzliche Verpflichtung aus Art. 32 DSGVO ist dem Auftragsverarbeiter nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe c) DSGVO zudem vertraglich aufzuerlegen.

Beide Bestimmungen begründen aber für sich betrachtet keine Befugnis zur Verarbeitung von personenbezogenen Daten.

Mögliche Verarbeitungsbefugnisse im nicht-öffentlichen Bereich

Eine Verarbeitung personenbezogener Daten wird in den Erwägungsgründen 47 und 49 der DSGVO zur in dem zur Gewährleistung der Netz- und Informationssicherheit, zur Verhinderung der Verbreitung schädlicher Programmcodes oder der Schädigung von Computer- und elektronischen Kommunikationsnetzen unbedingt erforderlichen Umfang als berechtigtes Interesse des Verantwortlichen und damit zumindest als eine Verarbeitungsbefugnis nicht-öffentlicher Stellen explizit anerkannt.

Jedenfalls im nicht-öffentlichen Bereich können vor diesem Hintergrund berechtigte Interessen des Verantwortlichen zur Rechtfertigung von Verarbeitungen auftragsgegenständlicher Daten zu Zwecken der IT-Sicherheit im hierzu unbedingt erforderlichen Umfang in Betracht kommen. Insoweit es um anwendungsübergreifende Schutzmaßnahmen geht, die die Sicherheit der Plattform insgesamt erhöhen, können auch Interessen anderer Microsoft-Kunden als Dritter i.S.v. Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DSGVO herangezogen werden.

Um eine solche Begründung für nicht-öffentliche Verantwortliche zu ermöglichen, müssen diesen freilich Zusatzinformationen bereit gestellt werden, da alleine die Vertragsbestimmungen zur Verarbeitung personenbezogener Daten um „Produkte auf dem neuesten Stand und leistungsfähig zu halten und die Produktivität, Zuverlässigkeit, Wirksamkeit, Qualität und Sicherheit der Benutzer zu verbessern“ keine hinreichenden Hinweise auf das Ziel und den Umfang von Maßnahmen zur Gewährleistung von IT-Sicherheit vermitteln.

Mögliche Verarbeitungsbefugnisse im öffentlichen Bereich

Für die Begründung von Weisungen zur Datenverarbeitung für IT-Sicherheitszwecke durch Verantwortliche des öffentlichen Bereichs ist Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DSGVO keine nutzbare Rechtsgrundlage. Für öffentliche Stellen als Verantwortliche ist auf das jeweilige Fachrecht des Bundes und der Länder abzustellen.

[40] EDSA, Leitlinien 07/2020, Rn. 135.

Bereichsspezifische Konkretisierungen wie etwa § 75c SGB V hinsichtlich der IT-Sicherheit von Krankenhäusern[41] spiegeln das Gebot der Gewährleistung der Funktionsfähigkeit der öffentlichen Verwaltung wieder, aus dem unter den Bedingungen fortschreitender Digitalisierung öffentlicher Aufgabenerfüllung die Verpflichtung abzuleiten ist, interne IT-Systeme genauso wie eGovernment-Angebote für Bürgerinnen und Bürger mit risikoangemessenen Maßnahmen gegen manipulative Nutzung und Angriffe auf ihre Funktionsfähigkeit oder auf die mit ihnen verarbeiteten Daten zu schützen.

Außerhalb dieser Begründungsansätze liegen allerdings etwaige Verarbeitungen, die keinen Bezug zu der jeweiligen vertragsgegenständlichen Verarbeitung haben oder die sich von dem in Art. 6 Abs. 1 UAbs. 1 Buchstabe e) genauso wie in Buchstaben f) DSGVO enthaltenen Erforderlichkeitsmaßstab abkoppeln.

Nicht anders als für Verantwortliche des nicht-öffentlichen Bereichs erfordert eine abschließende Bewertung dieser möglichen Rechtsgrundlagen ebenso wie die Erfüllung daran anknüpfender Transparenzpflichten auch für Verantwortliche des öffentlichen Bereichs deutlich über die Vertragsbestimmungen hinausgehende Einblicke in genaue Zwecksetzungen und den Umfang der von Microsoft zur Gewährleistung der IT-Sicherheit vorgenommenen Verarbeitungen auftragsgegenständlicher Daten.

Bereichsübergreifende Fragestellungen

Anders als im Rahmen der Verarbeitungen zu Microsofts Geschäftstätigkeiten und über die von Microsoft im Rahmen der Gespräche erläuterten tatsächlichen Verarbeitungsprozesse[42] hinaus, fehlen im Datenschutznachtrag 09/2022 Ausschlusstatbestände, die den Umfang der für Verarbeitungen zu Zwecken der „Verbesserung der Sicherheit“[43] genutzten Daten begrenzen: Soweit diese als Teil der weisungsgebundenen Auftragsverarbeitung stattfinden, gestattet der Abschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ auch die Einbeziehung von Inhalten der Kundendaten und schließt Nutzungen von Verhaltensdaten der Kunden zur Beobachtung des Nutzerverhaltens oder hierzu Inhaltsdaten zu verwenden bzw. heranzuziehen oder neue Daten zu erzeugen nicht aus.

Soweit nicht aus spezialgesetzlichen Aufgabenzuweisungen wie § 75c SGB V weitergehende Verarbeitungsbefugnisse abgeleitet werden können, ergibt sich hieraus potentiell eine Verarbeitung, für die jedenfalls im öffentlichen Bereich oder bei nach Art. 9 DSGVO besonders geschützten Daten keine hinreichende Verarbeitungsbefugnis des Verantwortlichen begründet werden kann.

---

[41] Allgemein zur Gewährleistung der Sicherheit informationstechnischer Systeme von Staat und Kommunen etwa Art. 3 Abs. 2 und 3 des Bayerischen Digitalgesetzes, abrufbar unter: https://www.gesetze-bayern.de/Content/Document/BayDiG/true.

[42] Vgl. Anhang 1, Folie 8.

[43] In der englischen Fassung des „Datenschutznachtrags“ 09/22: „enhancing ... security“

Hinzu kommt für den öffentlichen und nicht öffentlichen Bereich:

Allenfalls durch die gesondert festgelegten technischen und organisatorischen Maßnahmen könnte für den Verantwortlichen deutlicher werden, in welchem Umfang Microsoft als Auftragsverarbeiter zu Zwecken von (vormals) Betrugs- und Cyberabwehr bzw. heute „Verbesserung der Sicherheit“ Maßnahmen ergreift, für die die Verarbeitung personenbezogener Daten erforderlich sein kann. Da Microsoft diese Maßnahmen in weitem Umfang einseitig ausgestalten kann, ergibt sich aber auch hieraus für den Verantwortlichen keine hinreichend genauere Erkenntnis über die tatsächlich durchgeführten Verarbeitungen.

Ob die „Bekämpfung von Betrug“ eigenständige, nicht alleine durch die Zwecke der Bekämpfung von Cyberkriminalität oder von Cyberangriffen gerechtfertigte Datenverarbeitungen auslöst, ist auch unter Berücksichtigung der von Microsoft im Rahmen der Gespräche vorgestellten Prozesse für die Arbeitsgruppe nicht abschließend zu beurteilen. Sie bleibt daher bei der Untersuchung möglicher Rechtsgrundlagen außer Betracht.

ii) Erfüllung rechtlicher Verpflichtungen als Teil weisungsgebundener Auftragsverarbeitung

Die Erfüllung rechtlicher Verpflichtungen ist zwar nicht mehr ausdrücklich als Verarbeitung zu Microsofts legitimen Geschäftszwecken beschrieben. Allerdings lässt sich aus dem Abschnitt „Offenlegung verarbeiteter Daten“ ableiten, dass diese weiterhin als Verarbeitung in eigener Verantwortlichkeit Microsofts gesehen wird (auch wenn Microsoft das im Vertrag offen lässt). Dies ist folgerichtig, da der Verantwortliche seinen eigenen rechtlichen Pflichten selbst oder durch Weisung an Microsoft nachzukommen hat. Soweit Microsoft verpflichtet ist, kann der Kunde die Erfüllung dieser Pflichten weder anweisen noch verhindern., dass diese weiterhin als Verarbeitung in eigener Verantwortlichkeit Microsofts gesehen wird (auch wenn Microsoft das im Vertrag offen lässt). Dies ist folgerichtig, da der Verantwortliche seinen eigenen rechtlichen Pflichten selbst oder durch Weisung an Microsoft nachzukommen hat. Soweit Microsoft verpflichtet ist, kann der Kunde die Erfüllung dieser Pflichten weder anweisen noch verhindern.

Problematisch ist allerdings, dass der Kunde Microsoft mindestens implizit vertraglich entsprechende Verarbeitungsbefugnisse einräumt, die den nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstaben a, g DSGVO zulässigen Rahmen verlassen, da sie nicht auf Verarbeitungen auf Grund europäischen oder mitgliedsstaatlichen Rechts begrenzt bleiben.

Zur Vermeidung von Überschneidungen werden die insoweit aufgeworfenen Fragen aus Gründen des Sachzusammenhangs im unmittelbar nachfolgenden Abschnitt 2.2.3 näher untersucht.

Zu (2): Verarbeitungsbefugnis Verantwortlicher für die Einräumung der Nutzung personenbezogener Daten für „Geschäftstätigkeiten“[44]

Die Arbeitsgruppe hat in ihren Gesprächen mit Microsoft intensiv die Möglichkeiten einer datenschutzgerechten Ausgestaltung des Vertragsabschnitts über die Nutzung personenbezogener Daten zu Abrechnungs-, Vergütungs-, Unternehmensplanungs- und Finanzberichterstattungszwecken (im Folgenden zusammengefasst als „Geschäftstätigkeiten“) erörtert.

Als datenschutzrechtlich grundsätzlich begründbar wurden dabei Ausgestaltungen angesehen, in den denen der Kunde Microsoft die Weisung erteilt, spezifische statistische Auswertungen im Auftrag des Kunden zu erstellen und die (nicht personenbezogenen) Ergebnisse an Microsoft zu übermitteln. Für diese dann im Auftrag des Kunden erfolgenden Verarbeitungen personenbezogener Daten benötigt dieser natürlich eine Rechtsgrundlage, die je nach Einzelfall etwa im Beschäftigungsverhältnis aus § 26 BDSG, im Kundenverhältnis Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DSGVO oder bei öffentlichen Stellen aus Art. 6 Abs. 1 UAbs. 1 Buchstabe e) DSGVO in Verbindung mit den jeweiligen fachrechtlichen Aufgabenzuweisungsnormen folgen könnte. Dies betrifft allerdings nur solche Daten, die bereits für Zwecke der Kunden selbst vorhanden sind und verarbeitet werden, nicht jedoch solche Daten, die zusätzlich erhoben und anderweitig verarbeitet werden.

Vor dem Hintergrund der Diskussion Microsofts mit dem niederländischen Justizministerium und der abweichenden Einordnung der CNIL zu Verarbeitungen, mit denen eigene Zwecke des Auftragnehmers verfolgt werden, hat die Arbeitsgruppe jedoch davon abgesehen, Microsoft ein derartiges Weisungsmodell als einzige datenschutzgerechte Ausgestaltungsmöglichkeit von Verarbeitungen für „Geschäftstätigkeiten“ zu Vertragsdurchführungszwecken vorzugeben.

Der „Datenschutznachtrag“ 09/2022 greift diese Diskussionen zwar mit einer grundlegenden Umgestaltung des Abschnitts über Verarbeitungen personenbezogener Daten für Microsofts „Geschäftstätigkeiten“ auf, vollzieht aber im Ergebnis keinen grundlegende dogmatische Neuausrichtung zur Rolle bzw. datenschutzrechtlichen Verantwortlichkeit Microsofts für diese Verarbeitungen: Die nunmehr vorgesehene Klausel ist mit ihrer zentralen, aber auch mehrdeutigen Formulierung „authorize“ nach Auffassung der Arbeitsgruppe nicht geeignet (und nach den Festlegungen im Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ auch ersichtlich nicht dazu gedacht),[45] eine Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen zu regeln. Denn sie enthält keine Weisung des

[44] Formulierung im „Datenschutznachtrag“ vom 15. September 2022: „Processing for Business Operations Incident to Providing the Products and Services to Customer“.

[45] Siehe DPA vom Sep. 2022, Abschnitt “Processing of Personal Data, GDPR”, Unterabschnitt “Processor and Controller Roles and Responsibilities” Zitat: “To the extend Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an indepedent data cotroller under GDPR for such use”. Der Terminus “business operations incident to providing the Products and Services to Customer” verweist dabei auf ein gleichnamigen Unterabschnitt im Abschnitt “Nature of Data Processing, Ownership” des “Datenschutznachtrags”

Verantwortlichen an Microsoft, die dargestellten Datenverarbeitungen vorzunehmen, sondern ermächtigt Microsoft, die Verarbeitungen für „Geschäftstätigkeiten“ nach eigenem Ermessen vorzunehmen. Zwar kann im Rahmen der Auftragsverarbeitung unter der DSGVO dem Auftragsverarbeiter auch eine relativ weite Entscheidungshoheit bezüglich der nicht wesentlichen Mittel der Verarbeitung zugebilligt werden, ohne dass dies den Charakter einer Auftragsverarbeitung ausschließen würde.[46] Vorliegend erhält Microsoft aber bereits eine Entscheidungsbefugnis über die Zwecke, nämlich durch die Entscheidungsbefugnis, ob zu den jeweiligen Zwecken überhaupt personenbezogene Daten verarbeitet werden oder nicht. Darüber hinaus ist Microsoft laut dem Vertrag weitgehend frei in der Entscheidung über die wesentlichen Mittel der Verarbeitung, etwa welche Daten wie lange verarbeitet werden. Entscheidungen über Zwecke und wesentliche Mittel sind aber jedoch stets dem Verantwortlichen vorbehalten.[47] Dementsprechend ist die Regelung schon im Ansatz ungeeignet, die in Rede stehenden Verarbeitungen als im Auftrag des Kunden erfolgend zu qualifizieren.

Die Arbeitsgruppe weist darauf hin, dass die Formulierung „authorize“ dahingehend missverstanden werden könnte, dass (alleine) dadurch die Verarbeitungen von Microsoft für seine Geschäftstätigkeiten eine Rechtsgrundlage erhalten würden. Vielmehr ist vom Verantwortlichen – wie oben dargestellt – zu klären, ob er eine Rechtsgrundlage hat, die eine Überführung der personenbezogenen Daten in die Verantwortlichkeit von Microsoft zu eigenen „Geschäftstätigkeiten“ gestattet. Gelingt dies nicht, verletzt der Verantwortliche den Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 Buchstabe a) DSGVO).

Darüber hinaus gilt:

Die Untersuchungen der Arbeitsgruppe zur Ausgestaltung von Verarbeitungen für bestimmte Geschäftszwecke des Auftragsverarbeiters als Vorgang in dessen eigener Verantwortlichkeit stellen die Frage der Rechtsgrundlage für den Verantwortlichen in den Mittelpunkt. Weitere Fragestellungen wurden dagegen nur kursorisch behandelt. Unberücksichtigt und damit weiterhin im Einzelfall untersuchungsbedürftig bleibt etwa, ob die Verarbeitungen Microsofts für eigene „Geschäftstätigkeiten“ für den jeweiligen Verantwortlichen mit den allgemeinen Zweckbindungsanforderungen des Art. 6 Abs. 4 DSGVO und erst recht bereichsspezifischen Begrenzungen wie § 78 SGB X vereinbar ist. Entsprechendes gilt für die Frage einer gemeinsamen Verantwortlichkeit des Kunden mit Microsoft für Microsofts eigene „Geschäftstätigkeiten“.

Anders als im vorstehend beschriebenen Modell (vgl. Zeile 639 ff.) eng weisungsgebundener Verarbeitungen zu Vertragsdurchführungszwecken werden Verantwortliche in der nun vorliegenden Ausgestaltung der Einräumung einer Verarbeitungsbefugnis des Auftragnehmers zumindest an bestimmten Daten betroffener Personen jedenfalls den Nachweis der Erforderlichkeit der

[46] ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, Rn. 39

[47] Siehe Art. 4 Nr. 7 DS-GVO i.V.m. “Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, Rn. 19 - 27

Verarbeitung, wie Rechtsgrundlagen wie § 26 Abs. 1 und 3 BDSG oder Art. 6 Abs. 1 UAbs. 1 Buchstabe b) oder e) DSGVO ihn vorsehen, regelmäßig nicht erbringen können.

3.2.2.5. Schlussfolgerungen

Der im „Datenschutznachtrag“ 09/2022 fortgeführte Regelungsmodell, sich für bestimmte Verarbeitungen weit reichende Rechte zur Verarbeitung der im Auftrag verarbeiteten personenbezogenen Daten einräumen zu lassen, ist bereits im Ansatz nicht geeignet, eine Auftragsverarbeitung zu begründen. Damit bleibt die Problematik der Erforderlichkeit einer Rechtsgrundlage für die Überführung der im Auftrag verarbeiteten personenbezogenen Daten in die Verantwortlichkeit von Microsoft samt der damit verbundenen umfassenden Nachweispflichten bestehen. Microsoft könnte zwar konkrete Verarbeitungen definieren und für diese Verarbeitungen Weisungen der Verantwortlichen einholen. In den Gesprächen mit der Arbeitsgruppe hat Microsoft diesen Ansatz allerdings nicht aufgegriffen, um die Flexibilität eines großen Cloud-Anbieters zu wahren. Entscheidungsmöglichkeiten über Zwecke und Mittel sind allerdings mit einer Funktion als Auftragsverarbeiter unvereinbar. Zudem müsste in jedem Fall sichergestellt sein, dass die Verantwortlichen konkrete Weisungen zur Ausführung der von Microsoft gewünschten Auswertungen tatsächlich erteilen, was derzeit im Vertrag nicht erfolgt – und dass sie auch die Möglichkeit haben, die Weisungen zu ändern oder zu widerrufen. Voraussetzung wäre zudem, dass die Verantwortlichen eine detaillierte Kenntnis über die tatsächlichen Verarbeitungen haben.

Dementsprechend geht Microsoft auch für seine „Geschäftstätigkeiten“ nicht von einer Auftragsverarbeitung aus, was jedoch das Problem mit sich bringt, dass für diese Überführung in die Verantwortlichkeit von Microsoft eine Rechtsgrundlage für den Verantwortlichen erforderlich ist.

Für Verantwortliche, die Microsoft 365 zur Durchführung ihrer Verarbeitungstätigkeiten einsetzen, verbleiben unabhängig von diesen grundsätzlichen Schwierigkeiten auch nach den mit dem „Datenschutznachtrag“ 09/2022 auf Grundlage der Gespräche mit der DSK-Arbeitsgruppe erreichten Fortschritten große Herausforderungen, um insbesondere ihren Verpflichtungen hinsichtlich Rechtmäßigkeit, Erforderlichkeit sowie Transparenz und Nachweisführung nachzukommen. Nicht anders als in den vorangehenden Versionen des „Datenschutznachtrags“ beruhen auch aktuell sämtliche bisher als Verarbeitungen im Rahmen eigener Geschäftstätigkeiten Microsofts eingeordneten Prozesse weiterhin nach dem von der Arbeitsgruppe für geboten erachteten Prüfungsmaßstab der Art. 6 Abs. 1 UAbs. 1 Buchstaben e) bzw. f) DSGVO. Sie sind damit weiterhin mit vertieften Informationspflichten verknüpft. Gleichwohl bleibt anzuerkennen, dass die jetzt für Verarbeitungen zu eigenen Geschäftstätigkeiten aufgenommenen Ausschlusstatbestände und Maßgaben für einen positiven Abschluss der Interessenabwägung des Verantwortlichen Erleichterungen bedeuten. Für Telemetrie- und Diagnosedaten bleibt im Detail sowohl zu klären, in wessen Verantwortlichkeit sie verarbeitet werden als auch der Umfang der Verarbeitungen, die Erforderlichkeit und die Rechtsgrundlagen.

Microsoft wird empfohlen, den eingeleiteten Nachbesserungsprozess fortzusetzen. Dabei sollte Microsoft vertraglich klarstellen, dass auch Verarbeitungen wie zur „Verbesserung der Sicherheit“ dem datenschutzrechtlichen Erforderlichkeitsgrundsatz unterliegen und dass auf den Zugriff auf Inhaltsdaten weitestmöglich verzichtet wird. Darüber hinaus sollte geprüft werden, wie die der Arbeitsgruppe zur Verfügung gestellten Informationen über Verarbeitungen für eigene „Geschäftstätigkeiten“ in geeigneter Form Verantwortlichen zur Verfügung gestellt werden können, um diese bei der Erfüllung datenschutzrechtlicher Anforderungen etwa an Informationspflichten zu unterstützen.

Darüber hinaus hält es die Arbeitsgruppe für erforderlich, die in ihrer Untersuchung erkennbar gewordenen Differenzen zwischen den Aufsichtsbehörden bei der Beurteilung von Datenverarbeitungen des Auftragsverarbeiters zu eigenen Zwecken in geeigneter Form weiter in den Gremien des Europäischen Datenschutzausschusses zu erörtern, um für diese nicht auf Microsoft beschränkten Fragestellungen zu gemeinsamen, rechtssicheren Bewertungsmaßstäben der Aufsichtsbehörden zu gelangen.

3.2.3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, CLOUD Act, FISA 702

3.2.3.1. Feststellungen des AK Verwaltung

Der AK Verwaltung stellte fest, dass in den Datenschutzbestimmungen für Microsoft-Onlinedienste darauf verwiesen worden sei, dass verarbeitete Daten außerhalb der Weisung des Kunden auch offengelegt werden können, wenn die Datenschutzbestimmungen es vorsehen oder dies gesetzlich vorgeschrieben wird. Diese Beschreibung sei nicht hinreichend konkret und bestimme nicht die durch den Auftraggeber vertraglich zu definierendem Rechten. Die Ausnahme dürfe sich zudem ausschließlich auf das Recht der Union oder eines Mitgliedsstaates beziehen, wobei nicht ausgeschlossen sei, dass zu diesem Recht auch Rechtshilfeabkommen mit Drittländern gehörten. Die konkrete Umsetzung und die Auswirkungen des CLOUD Acts, dem Microsoft als US-amerikanischer Hersteller unterliege, seien nicht abschließend geklärt.

3.2.3.2. Aktueller Prüfungsgegenstand

Der „Datenschutznachtrag“ September 2022 regelt unter „Offenlegung verarbeiteter Daten“, dass Microsoft verarbeitete Daten nicht offenlegen oder Zugriff auf diese geben wird, außer wie vom Kunden angewiesen, wie im „Datenschutznachtrag“ beschrieben oder durch Gesetz verlangt.

Anfragen von Strafverfolgungsbehörden werde Microsoft versuchen an den Kunden umzuleiten. Im Fall einer Verpflichtung zur Offenlegung oder Zugangsgewährung an Strafverfolgungsbehörden regelt der „Datenschutznachtrag“ unter „Offenlegung verarbeiteter Daten“, dass Microsoft den Kunden unverzüglich benachrichtigt, sofern dies nicht gesetzlich verboten ist. Neu in den „Datenschutznachtrag“ September 2022 aufgenommen hat Microsoft eine Regelung, nach der

Microsoft verarbeitete Daten nur dann offenlegen oder Zugang zu ihnen gewähren werde, wenn dies gesetzlich vorgeschrieben ist, vorausgesetzt, dass die Gesetze und Praktiken den Kern der Grundrechte und -freiheiten respektieren und nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, und gegebenenfalls, um eines der in Art. 23 Absatz 1 DSGVO aufgeführten Ziele zu schützen.

Für andere Anfragen Dritter (also insbesondere auch von Geheimdiensten) hinsichtlich verarbeiteter Daten regelt der „Datenschutznachtrag“ unter „Offenlegung verarbeiteter Daten“, dass Microsoft den Kunden unverzüglich benachrichtigt, sofern dies nicht gesetzlich verboten ist, und die Anfrage zurückweist, soweit nicht Microsoft gesetzlich zur Befolgung verpflichtet ist. Wenn die Anfrage rechtsgültig ist, werde Microsoft versuchen, den Dritten an den Kunden zu verweisen.

Microsoft vertritt die Auffassung, die neu aufgenommene Regelung zur Notwendigkeit und Verhältnismäßigkeit beziehe sich auf sämtliche Offenlegungen, also auch gegenüber Geheimdiensten.

Der Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“ des „Datenschutznachtrags“ erklärt zudem, dass, soweit Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter ist, die DSGVO-Bestimmungen in Anlage 1 und „zudem“ die Bestimmungen in diesem Abschnitt gelten. Dieser Abschnitt regelt unter anderem, dass der Kunde abschließend Weisungen etwa durch den Vertrag und die Nutzung der Dienstleistungen erteilt, weitergehende Weisungen allerdings einer Einigung nach Maßgabe des Verfahrens zur Änderung des Vertrages des Kunden bedürfen.

Für die Verarbeitung personenbezogener Daten, die der DSGVO unterliegen, zu eigenen Geschäftstätigkeiten von Microsoft im Zusammenhang mit der Leistungserbringung[48] verpflichtet sich Microsoft als datenschutzrechtlich Verantwortlicher zudem zu weiteren Schutzmaßnahmen.[49] Diese weiteren Schutzmaßnahmen im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ umfassen Verpflichtungen zur Verweisung anfragender Dritter an den Kunden, zur Benachrichtigung unter bestimmten Bedingungen, zur Anfechtung von Aufforderungen zur Offenlegung unter bestimmten Bedingungen (im Wesentlichen unter der Voraussetzung der Rechtswidrigkeit der Anfrage nach dem Recht der anfragenden Stelle) und zur Leistung von Entschädigungen unter bestimmten Bedingungen.[50]

[48] „Geschäftstätigkeiten“, hierzu Abschnitt 2.2.2

[49] „Datenschutznachtrag“, Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“, am Ende, verweist für Verarbeitungen „in Bezug auf die Verarbeitung personenbezogener Daten gemäß diesem Absatz“ — also „soweit Microsoft personenbezogene Daten, die der DSGVO unterliegen, für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Services an den Kunden nutzt oder anderweitig verarbeitet“, im Gegensatz zu der im vorangehenden Absatz geregelten Situation „wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt“ — insoweit auf Anhang C – „Nachtrag zu zusätzlichen Schutzmaßnahmen“.

[50] Im Detail „Datenschutznachtrag“, Anhang C – „Nachtrag zu zusätzlichen Schutzmaßnahmen“.

Die „Anlage 1 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union“ des Datenschutznachtrags enthält unter Ziff. 2 Verpflichtungen, die Art. 28 Abs. 3 DSGVO entsprechen.

3.2.3.3. Gesprächsergebnisse

Im Rahmen der Gespräche der Arbeitsgruppe mit Microsoft kam zur Sprache, dass die Standardvertragsklauseln der EU-Kommission für Datenexporte in Klausel 14 a) das Verständnis festhalten, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Art. 23 Abs. 1 DSGVO aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu den Standardvertragsklauseln stehen. Diese Regelung steht dort im Zusammenhang mit der Zusicherung der Parteien, keinen Grund zu der Annahme zu haben, dass Rechtslage und -praxis im Drittland den Datenimporteur an der Erfüllung seiner Pflichten gemäß den Standardvertragsklauseln hindern. Die Weisungsbindung des Auftragsverarbeiters in Klausel 8.1 a) Modul Zwei bzw. Klausel 8.1 b) Modul Drei der Standardvertragsklauseln für Datenexporte dagegen ist nicht beschränkt. Klausel 7.1 a) der Standardvertragsklauseln für Auftragsverarbeitungsverträge sieht diejenigen Einschränkungen der Weisungsbindung vor, die Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a) DSGVO gestattet. Es wurde diskutiert, ob Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstaben a) und g) DSGVO – jedenfalls im Kontext von Datenexporten in Drittländer – teleologisch so reduziert werden können, dass Rechtsvorschriften und Gepflogenheiten von Drittländern, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Art. 23 Abs. 1 DSGVO aufgeführten Ziele sicherzustellen, trotz des Widerspruchs zum Wortlaut der DSGVO als zulässig betrachtet werden können. Dies wurde jedenfalls als ein denkbarer Lösungsansatz für die Beurteilung extraterritorialer Zugriffsbefugnisse auf Auftragsverarbeiter in der EU angesehen. Wohl auf dieser Diskussion fußt die Einfügung der im Abschnitt 2.2.3.2 beschriebenen Klausel im „Datenschutznachtrag“ 09/2022.

Im Rahmen der Gespräche über den US-amerikanischen CLOUD Act und der Vorstellung des „EU Data Boundary“-Projekts wies Microsoft unter Verweis auf das US-Justizministerium darauf hin, dass der CLOUD Act nur klarstelle, dass US-Behörden Daten anfordern können, die sich im Besitz (possession), im Gewahrsam (custody) oder unter der Kontrolle (control) einer der US-Gerichtsbarkeit unterliegenden Einrichtung befinden, auch wenn diese Daten nicht in den USA gespeichert sind. Es handle sich dabei nicht um eine Ausweitung der Befugnisse, sondern um eine Kodifizierung des bereits bestehenden Rechts.[51] Aus den Erläuterungen Microsofts kann entnommen werden, dass diese rechtliche Konstruktion auch nach Auffassung des US-Justizministeriums im Rahmen der Anwendung

[51] Präsentation zum Gespräch am 29. April 2022, Anlage 4, Seite 2, 5.

aller US-Überwachungsgesetze, sowohl der strafrechtlichen als auch derjenigen für die nationale Sicherheit gilt.[52]

Microsoft erläuterte außerdem die auf Grund US-Gewohnheitsrechts anerkannte Klagebefugnis von Providern, die sog. Comity-Anforderungen geltend zu machen, wenn die Befolgung einer US-amerikanischen Rechtsvorschrift mit den Gesetzen einer anderen Rechtsordnung kollidieren kann. Diese Klagebefugnis werde durch den CLOUD Act vorbehalten. Der Kongress stelle ausdrücklich fest, dass der CLOUD Act nicht dahingehend ausgelegt werden sollte, dass er die gewohnheitsrechtlichen Standards für die Verfügbarkeit oder Anwendung der Comity-Analyse auf Gerichtsverfahren nach dem Stored Communications Act ändert oder anderweitig beeinträchtigt.

3.2.3.4. Bewertung

a) Prüfungsmaßstab

Nach Art. 28 Abs. 1 DSGVO dürfen Verantwortliche nur solche Auftragsverarbeiter einsetzen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Nach Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO muss der zwischen dem Verantwortlichen und dem Auftragsverarbeiter zu schließende Vertrag bzw. das andere Rechtsinstrument insbesondere vorsehen, dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten in[53] ein Drittland oder an eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe g DSGVO verlangt eine Regelung, dass der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht; weitere Fragestellungen hierzu werden im Abschnitt „Löschung“ behandelt.

Art. 48 DSGVO hält fest, dass unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V, Entscheidungen von Gerichten und Behörden von Drittländern zur Offenlegung personenbezogener

[52] Präsentation zum Gespräch am 29. April 2022, Anlage 4, Seite 5.

[53] So die korrekte Übersetzung anstatt des in der deutschen Sprachfassung verwendeten „an“, vgl. die englische Fassung von Art. 44: „to a third country“, die den Sinn etwa klarer macht; eindeutig die französische Fassung: „vers un pays tiers“.

Daten nur auf der Grundlage einschlägiger internationaler Übereinkommen wie etwa einem Rechtshilfeabkommen beachtlich sind.

b) Detailbewertung

i. Vertragliche Weisungsbindung, Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO

Anlage 1 des „Datenschutznachtrags“ enthält für sich genommen eine den Anforderungen des Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO entsprechende Weisungsbindung von Microsoft. Allerdings wird diese Weisungsbindung an anderen Stellen des „Datenschutznachtrags“ eingeschränkt, ohne dass erkennbar wäre, welche der Regelungen vorgehen soll.

Der Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“ des „Datenschutznachtrags“ könnte so interpretiert werden, dass er grundsätzlich gegenüber anderen Regelungen des „Datenschutznachtrags“ vorrangige Klauseln enthält.[54] Allerdings enthalten schon die gleichrangigen Wortlaute dieses Abschnitts und der Anlage 1 Regelungen, die sich widersprechen. So wird in diesem Abschnitt etwa das Weisungsrecht des Kunden im Wesentlichen unter den Vorbehalt einer Einigung mit Microsoft im Vertragsänderungsverfahren gestellt. Bereits diese Unklarheit führt dazu, dass Verantwortliche nicht ihrer Rechenschaftspflicht nachkommen können und die Anforderungen des Art. 28 DSGVO als nicht erfüllt zu bewerten sind. Die Auslegung der ihrem Wortlaut nach widersprüchlichen Klauseln führt zudem dazu, dass nach allgemeinen Auslegungsregeln wohl die speziellere Vorschrift gelten soll, also die gesetzeswidrige Einschränkung des Weisungsrechts durch Unterstellung unter das Vertragsänderungsverfahren.

Hinsichtlich der Frage einer Verarbeitung durch Microsoft auf Basis von Drittlands-Recht außerhalb der Weisungen des Kunden enthält zwar der Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“ des „Datenschutznachtrags“ eine Regelung, die eine strikte Weisungsbindung für Microsoft vorsieht, die sogar noch über die Weisungsbindung in Anlage 1 Ziff. 2 a) des „Datenschutznachtrags“ hinausgeht, weil sie keine Einschränkungen vorsieht (vom bereits angesprochenen weitgehenden Unterstellen unter das Vertragsänderungsverfahren abgesehen). Allerdings enthält der Abschnitt „Offenlegung verarbeiteter Daten“ für spezifische Verarbeitungen, namentlich Offenlegungen, spezifischere Regelungen, die ersichtlich auch unter Anwendbarkeit der DSGVO gelten sollen, wie die im „Datenschutznachtrag“ September 2022 erfolgte Einfügung, die auf Art. 23 DSGVO Bezug nimmt, zeigt. In Ermangelung einer klaren Konkurrenz- bzw. Hierarchieregelung bleibt daher auch hier unauflösbar, welche der drei unterschiedlichen Regelungen Geltung beansprucht, was im Hinblick auf die Rechenschaftspflicht der Verantwortlichen (Art. 5 Abs. 2 DSGVO) zu der Bewertung führt, dass Art. 28 DSGVO nicht erfüllt ist.[55]

[54] Zur Problematik der Anwendbarkeit vgl. bereits oben Abschnitt 3.1.

[55] Art. 5 Abs. 2 DSGVO enthält nach der Rechtsprechung des BVerwG (Urt. v. 2.3.2022 – 6 C 7.20, Rn. 50) auch eine Beweislastregel, und zwar sowohl im Verhältnis zu betroffenen Personen als auch im Verhältnis zur Aufsichtsbehörde.

Offenlegungen der im Auftrag verarbeiteten Daten gestattet der Abschnitt „Offenlegung verarbeiteter Daten“ bereits, wenn diese rechtlich vorgeschrieben oder im „Datenschutznachtrag“ beschrieben sind. 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. Selbst wenn man eine teleologische Reduktion der erforderlichen Weisungsbindung in Anlehnung an Art. 23 Abs. 1 DSGVO vornehmen würde – anders aber die EU-Kommission in den Standardvertragsklauseln für Auftragsverarbeitungsverträge und auch in den Standardvertragsklauseln für Datenexporte nur hinsichtlich der Zusicherungen in Klausel 14 –, würde die von Microsoft eingefügte Klausel, die auf Art. 23 DSGVO Bezug nimmt, aufgrund ihrer systematischen Stellung und der Abgrenzung im folgenden Wortlaut [56] einerseits nur für Offenlegungen gegenüber Strafverfolgungsbehörden gelten (und nicht etwa für die vom EuGH in „Schrems II“ als problematisch bewerteten Befugnisse von US-Geheimdiensten nach FISA 702). Der von Microsoft vertretenen Auffassung, die neu aufgenommene Regelung zur Notwendigkeit und Verhältnismäßigkeit beziehe sich auf sämtliche Offenlegungen, also auch gegenüber Geheimdiensten, vermag die Arbeitsgruppe vor dem Hintergrund der systematischen Stellung und des eindeutig abgrenzenden Wortlauts „sonstige Anfragen von Dritten“ nicht zu folgen. Andererseits betrifft die Klausel nur die Frage von Verarbeitungen auf der Basis von Drittlands-Recht, nicht aber die Erlaubnis für alle weiteren im Datenschutz-Nachtrag beschriebenen Offenlegungen. Der „Datenschutznachtrag“ beschreibt im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ ausdrücklich Offenlegungen personenbezogener Daten „unter Verletzung der Verpflichtungen von Microsoft gemäß Kapitel V der DSGVO“. Die Abweichung vom Wortlaut der Klausel 14 der Standardvertragsklauseln für Datenexporte durch Einfügung eines „gegebenenfalls“[57] wirft ebenfalls Fragen auf, ob hierdurch eine inhaltliche Abweichung vom Maßstab der Standardvertragsklauseln beabsichtigt ist.

ii. Drittlands-Recht, Art. 48 DSGVO

Aus den vorstehenden Feststellungen ergibt sich, dass Microsoft sich vertraglich auch weit reichende Offenlegungen vorbehält, die im Falle ihrer Umsetzung nicht den in Art. 48 DSGVO aufgestellten Anforderungen entsprechen würden.

iii. FISA 702 und CLOUD Act

Die Microsoft Corporation ist ein US-amerikanisches Unternehmen, das „electronic communication service provider” im Sinne von 50 U.S.C. § 1881(b)(4) ist. Unter diesen Begriff fallen Telekommunikationsunternehmen, Anbieter von elektronischen Kommunikationsdiensten („ECS“), Anbieter von „remote computing services“ („RCS“), also Computerspeicher- oder -verarbeitungsdiensten für die Öffentlichkeit mittels elektronischer Kommunikationssysteme,[58] andere

[56] „Bei Erhalt einer sonstigen Anfrage von Dritten“ in Abgrenzung zu „gegenüber Strafverfolgungsbehörden“.

[57] Im Englischen „as applicable“.

[58] 18 U.S.C. § 2711(2).

Kommunikationsdienstleister, die Zugang zu drahtgebundener oder elektronischer Kommunikation entweder bei der Übermittlung oder während der Speicherung solcher Kommunikationen haben, und deren Mitarbeiter und Beauftragte/Vertreter.[59] Microsoft bietet zumindest elektronische Kommunikationsdienste und „remote computing services“ an.

Ob alle in Microsoft 365 enthaltenen Leistungen unter diese Begriffe zu subsumieren sind, ist dabei nach dem von der DSK eingeholten Gutachten von Prof. Vladeck, an dem zu zweifeln die Arbeitsgruppe keinen Grund sieht, irrelevant, denn bereits die Einordnung als ECS oder RCS für einen geringen Teil der Tätigkeiten eines Unternehmens führt danach dazu, das es als Ganzes den in Rede stehenden Überwachungsvorschriften unterliegt.[60]

Von besonderer Bedeutung ist hier Section 702 des Foreign Intelligence Surveillance Act (FISA 702 = 50 U.S.C. § 1881a), da der EuGH diese Norm im Urteil „Schrems II“[61] im Detail bewertet und für nicht mit den europäischen Grundrechten vereinbar erklärt hat. Diese Bewertung ist weiterhin entscheidend, da hinsichtlich der Kritikpunkte des EuGH bis zum für diesen Bericht maßgeblichen Zeitpunkt keine Änderungen der Rechtslage festzustellen sind. Was die in der Executive Order[62] vorgesehenen Änderungen angeht, so sind diese erst noch umzusetzen, unbeschadet der Frage, ob sie den Anforderungen des europäischen Datenschutzrechts überhaupt hinreichend Rechnung tragen. FISA 702 ermöglicht es US-Behörden, von jedem „electronic communication service provider” im Sinne von 50 U.S.C. § 1881(b)(4) unter den gesetzlichen Voraussetzungen die Herausgabe von Informationen wie personenbezogenen Daten zu verlangen.[63] Die Arbeitsgruppe entnimmt den Erläuterungen von Microsoft[64], dass jedenfalls das US-Justizministerium davon auszugehen scheint, dass FISA 702 extraterritorial anwendbar sei, also auch, wenn Daten durch ein FISA 702 unterfallendes Unternehmen oder eine Tochtergesellschaft dieses Unternehmens etwa in der EU verarbeitet werden.[65] Betroffen von Herausgabeverlangen können dabei auch Daten sein, die Unternehmen, die selbst nicht FISA 702

---

[59] „officer, employee, or agent“.

[60] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.5.b, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

61 EuGH, Urt. v. EuGH, 16.7.2020 – C-311/18.

62 Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities - https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

63 Vgl. Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.1, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[64] Siehe die Darstellung im Abschnitt 3.2.3.2

[65] Vgl. auch Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.6, II.3.k, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf; Wissenschaftliche Dienste des Deutschen Bundestages, Dokumentation „US-Datenrecht - Zugriff US-amerikanischer Behörden auf Daten“. 3. August 2020, WD 3 - 3000 - 181/20, sowie die dort aufgeführte Literatur.

[65] Vgl. auch Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.6, II.3.k, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf; Wissenschaftliche Dienste des Deutschen Bundestages, Dokumentation „US-Datenrecht - Zugriff US-amerikanischer Behörden auf Daten“. 3. August 2020, WD 3 - 3000 - 181/20, sowie die dort aufgeführte Literatur.

unterfallen, durch ein Unternehmen verarbeiten lassen, das FISA 702 unterfällt.[66] Anordnungen auf der Basis von FISA 702 können zwangsweise durchgesetzt werden.[67]

Auch der CLOUD Act ist in diesem Zusammenhang als extraterritoriale Zugriffsmöglichkeit für US-Behörden auf in der EU verarbeitete Daten zu nennen, wird hier nicht untersucht, da der Arbeitsgruppe keine Bewertung dieses strafrechtlichen Regelwerks und ggf. weiterer in diesem Zusammenhang zu bewertender Gesetze im Hinblick auf europäische Grundrechte vorliegt.[68]

[66] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.5.f, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[67] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.2, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[68] Zu Fragen der extraterritorialen Anwendbarkeit des CLOUD Act siehe Gretchen Ramos, Andrea Maciejewski, Herald Jongen (Greenberg Traurig LLP), Memorandum to Dutch Ministry of Justice and Security - NCSC RE: Application of the CLOUD Act to EU Entities, 26. Juli 2022, https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/augustus/16/cloud-act-memo/Cloud+Act+Memo+Final.pdf.

iv. Anwendbarkeit des Kapitels V DSGVO auf Datenverarbeitungen in der EU

Aus einer extraterritorialen Anwendbarkeit des US-Rechts wird teilweise gefolgert, dass bereits in der Offenlegung an ein diesem Recht unterliegendes Unternehmen – etwa einen Auftragsverarbeiter – eine Übermittlung in ein Drittland liege.[69]

Die Arbeitsgruppe folgt — vorbehaltlich einer Meinungsbildung auf europäischer Ebene — dieser Ansicht nicht. Die reine Gefahr, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die US-Muttergesellschaft anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln, genügt nach Ansicht der Arbeitsgruppe noch nicht, um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO anzunehmen.

Allerdings liegen bei der Nutzung von Microsoft 365 tatsächlich Übermittlungen in Drittländer vor; sie werden abschließend unter Abschnitt 3.2.7 betrachtet. Im vorliegenden Abschnitt werden nur die extraterritorialen Wirkungen des US-Rechts betrachtet.

v. Zuverlässigkeit des Auftragsverarbeiters, Art. 28 Abs. 1 DSGVO

Auch wenn gemäß der soeben erfolgten Herleitung bei rein auf die EU beschränkten Verarbeitungen personenbezogener Daten durch Microsoft nach Ansicht der Arbeitsgruppe keine Übermittlungen in Drittländer vorliegen, ist eine extraterritoriale Anwendbarkeit von Drittlands-Recht auf einen Auftragsverarbeiter bzw. ein solches Risiko doch von erheblicher rechtlicher Bedeutung.

Nach Art. 28 Abs. 1 und ErwG 81 DSGVO dürfen Verantwortliche nur solche Auftragsverarbeiter einschalten, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen der DSGVO genügen. Die Darlegungs- und Beweislast hierfür liegt, wie bereits die eine Ausnahme regelnde Formulierung „nur“ zeigt, beim Verantwortlichen. Ebenfalls betrifft die Frage, ob der Auftragsverarbeiter hinreichende Garantien bietet, die Rechtmäßigkeit der Verarbeitung und damit einen Umstand, für den den Verantwortlichen die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO trifft. Die Rechenschaftspflicht stellt nicht nur eine Pflicht des Verantwortlichen dar, sondern auch eine Beweislastregelung.[70]

Bei einem Auftragsverarbeiter, der Regelungen wie dem CLOUD Act oder ggf. FISA 702 unterliegt, besteht ein näher zu betrachtendes Risiko, dass er im Fall eines Konflikts der Rechtsordnungen seinem Heimatrecht folgt und nicht der DSGVO, insbesondere, wenn dieses – wie im vorliegenden Fall – unter hohen Sanktionsdrohungen durchsetzbar ist, während der verlangte Verstoß gegen die DSGVO in der

[69] So wohl Vergabekammer Baden-Württemberg, Beschl. v. 13.07.2022 – 1 VK 23/22, Landesrecht BW Bürgerservice Rn. 88 ff., auch wenn im konkreten Fall vermutlich auch „echte“ Übermittlungen in die USA vorgelegen haben dürften und die Vergabekammer zunächst den auch von der Arbeitsgruppe geteilten Maßstab darstellt.

[70] EuGH, Urt. v. 24.2.2022 — C-175/20, Rn. 77, 81; BVerwG, Urt. v. 2.3.2022 – 6 C 7.20, Rn. 50.

Regel nicht einmal von den betroffenen Personen oder den europäischen Aufsichtsbehörden entdeckt werden kann.

Wie oben unter Abschnitt iii) ausgeführt, besteht das Risiko, dass FISA 702 auch auf EU-Tochtergesellschaften von US-Unternehmen, die FISA 702 unterliegen, anwendbar ist. Die Verarbeitung durch eine EU-Tochtergesellschaft als Auftragsverarbeiter genügt mithin – unabhängig von der Frage, ob die Muttergesellschaft möglicherweise als Unterauftragsverarbeiter einbezogen ist – für sich genommen nicht, um eine Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO zu erreichen.

Aus den vorliegenden Erläuterungen und Analysen etwa von Microsoft,[71] Prof. Vladeck[72] und des Wissenschaftlichen Dienstes des Bundestages[73] sowie der dort zitierten Autoren ergeben sich starke Hinweise dafür, dass FISA 702 extraterritorial anwendbar ist. Unabhängig davon, ob die extraterritoriale Anwendbarkeit von FISA 702 als nachgewiesen angesehen wird oder von einem dahingehenden Risiko ausgegangen wird, liegt, wie bereits ausgeführt, die Darlegungs- und Beweislast für das Vorliegen der Voraussetzungen des Art. 28 Abs. 1 DSGVO beim Verantwortlichen. Ob die extraterritoriale Anwendbarkeit von FISA 702 als nachgewiesen anzusehen ist oder nur nicht hinreichend sicher ausgeschlossen werden kann, ist daher für die Bewertung der Zuverlässigkeit des Auftragsverarbeiters im Sinne von Art. 28 Abs. 1 DSGVO nicht ausschlaggebend.

Mithin sind in solchen Fällen weitere technische und organisatorische Maßnahmen zu ergreifen, die die Einhaltung der DSGVO hinreichend garantieren. Um hinreichende Garantien im Sinne des Art. 28 Abs. 1 DSGVO darzustellen, müssen die Maßnahmen genau diejenigen Defizite der Rechtslage oder -praxis des drittstaatlichen Rechts ausgleichen, die zu der mangelnden Zuverlässigkeit des Auftragsverarbeiters geführt haben, d.h. genau die identifizierten Rechtsschutzlücken schließen.[74] Konkret bedeutet dies, dass die Maßnahmen sicher verhindern, dass potentielle Herausgabeanordnungen nach FISA 702 erfüllt werden.

Aufgrund der bestehenden gesellschaftsrechtlichen Befugnisse der Muttergesellschaft – und sei es nur zur Auswechslung einer lokalen Geschäftsführung, die sich unter Verweis auf die DSGVO weigert, Daten herauszugeben – und aufgrund des Umstandes, dass auch die Geschäftsführer der Tochtergesellschaft persönlich Verpflichtete nach FISA 702 sind,[75] denen im Weigerungsfall persönlich Sanktionen drohen, ist die datenschutzrechtliche Zuverlässigkeit einer EU-Tochtergesellschaft im Sinne des Art. 28 Abs. 1 DSGVO im Hinblick auf FISA 702 nach Ansicht der Arbeitsgruppe zunächst nicht

---

[71] Präsentation zum Gespräch am 29. April 2022, Anlage 4, Seite 2, 5.[72] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.6, II.3.k, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[72] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.6, II.3.k, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[73] Wissenschaftliche Dienste des Deutschen Bundestages, Dokumentation „US-Datenrecht - Zugriff US-amerikanischer Behörden auf Daten“. 3. August 2020, WD 3 - 3000 - 181/20.

[74] Zu Datenexporten vgl. EDSA, Empfehlungen 01/2020, Version 2.0, Rn. 75.

[75] 50 U.S.C. § 1881(b)(4)(E)

anders zu bewerten als die der US-Muttergesellschaft. Eine besondere Schwierigkeit ergibt sich, wenn die Muttergesellschaft die verwendete Software liefert und sich faktisch darüber den gewünschten Zugriff verschaffen kann. Ist die Muttergesellschaft über Administration und Support in die Leistungserbringung eingebunden, hat sie die Zugriffsmöglichkeiten ohnehin regelmäßig.

Welche Maßstäbe an technische oder organisatorische Maßnahmen zur Gewährleistung der nach Art. 28 Abs. 1 DSGVO erforderlichen Zuverlässigkeit zu stellen sind, ist bislang weder durch die europäischen Datenschutzaufsichtsbehörden noch durch die Rechtsprechung abschließend geklärt. Vereinzelt wird ein Rückgriff Verantwortlicher auf die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses für sachgerecht angesehen.[76] Dabei ist allerdings zu beachten, dass diese für den Kontext von Datenübermittlungen in Drittländer konzipiert worden sind. Die Empfehlungen 01/2020 bilden mit der Analyse des einschlägigen Drittlands-Rechts (und, soweit dieses nicht schon problematisch ist, der Praxis), der Identifikation der eine Datenschutz-Compliance verhindernden Umstände und der Suche nach ergänzenden Maßnahmen, die genau die identifizierten Unzulänglichkeiten ausgleichen, diejenigen Schritte ab, die zur Erfüllung von Art. 28 Abs. 1 DSGVO erforderlich sind.

Die als Microsoft 365 angebotenen Dienste erfordern in vielen Anwendungsfällen den Zugriff von Microsoft auf Klardaten.[77] Insbesondere die naheliegende Verschlüsselung verarbeiteter Daten, die einen Zugriff von Microsoft und damit der US-Behörden verhindern würde, ist regelmäßig nicht möglich, wenn die Daten beispielsweise im Browser angezeigt werden müssen. Die vorliegend gegebene Gestaltung, dass der Empfänger der Daten diese im Klartext verarbeiten muss, hat der Europäische Datenschutzausschuss als Anwendungsfall 6 des Anhangs 2 der Empfehlungen 01/2020 beschrieben. Für diesen Anwendungsfall ist es den Aufsichtsbehörden – im Hinblick auf Datenübermittlungen – nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten. In der entsprechenden Anwendung im Rahmen der Auftragsverarbeitung bedeutet dies, dass besonders kritisch zu prüfen ist, wie den Anforderungen des Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann. Ausreichende zusätzliche Schutzmaßnahmen konnte der Europäische Datenschutzausschuss nur in bestimmten, begrenzten Anwendungsfällen identifizieren. Konkret anzuführen wären die Anwendungsfälle 1 (Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern), 2 (Übermittlung pseudonymisierter Daten) und 5 (Aufgeteilte Verarbeitung oder Verarbeitung durch mehrere Beteiligte, Multi-party Processing) des Anhangs 2 der Empfehlungen

[76] Vgl. die Entscheidungen des Conseil d'État (Frankreich) in den zwei Eilverfahren „Health Data Hub" und „Doctolib", Entscheidung v. 13.10.2020 – 444937, Az.: ECLI:FR:CEORD:2020:444937.20201013, und v. 12.3.2021 – 450163, Az.: ECLI:FR:CEORD:2021:450163.20210312

[77] Von Dritten angebotene Dienste, die zu einer Umformung bzw. Verschlüsselung der bei Microsoft verarbeiteten Daten führen, sind nicht Gegenstand dieser Untersuchung. Die Arbeitsgruppe weist allerdings darauf hin, dass jedenfalls in bestimmten Konstellationen wie der E-Mail-Nutzung die Schutzmaßnahmen als unzureichend erscheinen. Auch von einzelnen Cloud-Anbietern für bestimmte Anwendungsfälle selbst angebotene Funktionen zu einer abgeschotteten Verarbeitung müssten sicherstellen und nachweisen können, dass hinreichende Garantien bestehen, dass der Anbieter sich keinen Zugriff auf die Daten verschaffen kann. Dies stellt im Cloud-Umfeld zumindest eine Herausforderung dar, für die keinem der Mitglieder der Arbeitsgruppe bisher eine geeignete Lösung bekannt ist.

01/2020 des Europäischen Datenschutzausschusses, soweit die dort aufgestellten Bedingungen eingehalten werden.

Die von Microsoft im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ zugesagten Maßnahmen sind nicht geeignet, die nach der Rechtsprechung des EuGH gemessen an den EU-Grundrechten bestehenden Unzulänglichkeiten des US-amerikanischen Rechts auszugleichen. Am ehesten mag noch die Verpflichtung zur Anfechtung von Herausgabeanordnungen als ergänzende Schutzmaßnahme in Betracht kommen. Doch besteht diese Verpflichtung zur Anfechtung nur, wenn die Herausgabeanordnung nach demjenigen Recht unzulässig ist, dem die Behörde bzw. das Gericht unterliegt, die bzw. das die Herausgabe anordnet, wozu auch relevante Konflikte mit dem anwendbaren EU- oder mitgliedsstaatlichen Recht gehören. Da aber FISA 702, wie der EuGH festgestellt hat,[78] keine inhaltliche Begrenzung der Überwachungsbefugnisse vorsieht und FISA 702 unterliegende Unternehmen die Anwendung dieser Norm nicht mit dem Argument abwenden können, dadurch würde EU- oder mitgliedsstaatliches Recht verletzt[79], ist nicht erkennbar, wie eine Verletzung des in Art. 52 EU-Grundrechtecharta geregelten Grundsatzes der Verhältnismäßigkeit durch eine solche Herausgabeanordnung auf diesem Wege erfolgreich geltend gemacht werden könnte. Dementsprechend sehen die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses derartige Maßnahmen auch nur als Ergänzung anderer Maßnahmen vor.[80] Darüber hinaus gelten die Verpflichtungen im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ gemäß der Einbeziehungsklausel im Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ nur für Verarbeitungen im Rahmen der „Geschäftstätigkeiten“ von Microsoft, die dort im zweiten Absatz geregelt sind, auf den sich der Verweis beschränkt. Die eigentliche Auftragsverarbeitung ist mithin nicht abgedeckt. Auch die von Microsoft vorgesehenen Maßnahmen für die Speicherung der Daten (data at rest) genügen nicht, da die weitergehende Verarbeitung bei vielen der in Microsoft 365 enthaltenen Dienste technisch zwingend im Klartext erfolgen muss.

Die Arbeitsgruppe weist darauf hin, dass nach der Rechtsprechung des Bundesverwaltungsgerichts aus der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auch eine Beweislastverteilung folgt,[81] so dass Verantwortliche bereits unabhängig von der implizit durch die Regel-Ausnahme-Formulierung des Art. 28 Abs. 1 DSGVO die Erfüllung der Anforderungen des Art. 28 Abs. 1 DSGVO zweifelsfrei nachweisen können müssen.

Insofern ergeben sich relevante Abweichungen von den Beurteilungsmaßstäben des Vergaberechts. Der öffentliche Auftraggeber darf im Vergabeverfahren grundsätzlich davon ausgehen, dass ein Bieter

[78] EuGH, Urt. v. 16.7.2020 – C-311/18, Rn. 180 ff.

[79] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.7, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[80] EDSA, Empfehlungen 01/2020, Rn. 119.

[81] BVerwG, Urt. v. 2.3.2022 – 6 C 7.20, Rn. 50.

seine vertraglichen Zusagen erfüllen wird.[82] Er muss seine (Auftragsverarbeitungs-)Verträge mit Unterauftragnehmern so ausgestalten, dass diese die gestellten (datenschutzrechtlichen) Anforderungen erfüllen.[83] Nach einer OLG-Ansicht erst, nach anderer OLG-Ansicht jedenfalls wenn sich konkrete Anhaltspunkte dafür ergeben, dass die Erfüllung der vertraglichen Zusagen zweifelhaft ist, ist der öffentliche Auftraggeber gehalten, durch Einholung ergänzender Informationen die Erfüllbarkeit des Leistungsversprechens beziehungsweise die hinreichende Leistungsfähigkeit des Bieters zu prüfen.[84] Das OLG Karlsruhe vertritt in einem Vergabenachprüfungsverfahren ohne Begründung die Ansicht, dass der öffentliche Auftraggeber nicht allein aufgrund der Tatsache, dass ein Unterauftragsverarbeiter (hier: AWS) ein Tochterunternehmen eines US-amerikanischen Konzerns ist, an der Erfüllbarkeit des Leistungsversprechens zweifeln müsse.[85] Auch wenn der Unterauftragsverarbeiter üblicherweise unzureichende Auftragsverarbeitungsverträge abschließe, stelle dies keine konkreten Anhaltspunkte dafür dar, dass dies entgegen den Zusagen des Bieters auch im konkreten Fall so geschehen werde.[86] Dies lässt sich wegen der vollständig abweichenden Maßstäbe – vollständige Nachweispflicht im Datenschutzrecht im Vergleich zum Erfordernis konkreter Anhaltspunkte für Zweifel an der Erfüllbarkeit des vertraglichen Leistungsversprechens als Voraussetzung einer vergaberechtlichen Verpflichtung (nicht eines Rechts) zur Überprüfung – nicht mit den datenschutzrechtlichen Anforderungen vergleichen. Zwar ist der öffentliche Auftraggeber vergaberechtlich nicht verpflichtet, die schriftlichen Angaben der Bieter anlasslos zu verifizieren. Dennoch darf er von seinem Recht zur Überprüfung auch ohne besonderen Anlass Gebrauch machen.[87] Vor dem Hintergrund ihrer datenschutzrechtlichen Verpflichtungen sollten Verantwortliche von ihrem Recht zur Überprüfung nach Ansicht der Arbeitsgruppe auch Gebrauch machen.

3.2.3.5. Schlussfolgerungen

Die Weisungsbindung Microsofts genügt nicht den gesetzlichen Mindestanforderungen gemäß Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO. Dies gilt selbst dann, wenn man die Vorschrift teleologisch analog Art. 23 Abs. 1 DSGVO reduziert. Microsoft sollte auch hier den Datenschutznachtrag grundlegend strukturell überarbeiten und eine eindeutige, umfassende und widerspruchsfreie Regelung treffen, die die gesetzlichen Anforderungen erfüllt. Insbesondere wäre es empfehlenswert, den offenbar auf Basis der Kritik der deutschen Aufsichtsbehörden bereits durch Microsoft eingeschlagenen Weg konsequent zu Ende zu gehen und Durchbrechungen der Weisungsbindung nur noch dann vorzusehen, wenn die DSGVO diese auch gestattet, nicht aber etwa bereits, wenn der Datenschutznachtrag eine Verarbeitung „beschreibt“, wie der aktuelle Wortlaut es vorsieht.

---

[82] OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22, Rn. 29; OLG Düsseldorf, Beschl. v. 19.9.2018 – Verg 17/18, NRWE Rn. 177.

[83] OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22, Rn. 34.

[84] OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22, Rn. 29; OLG Frankfurt, Beschl. v. 16.6.2015 – 11 Verg 3/15, unter II.4.b; OLG Düsseldorf, Beschl. v. 19.9.2018 – Verg 17/18, NRWE Rn. 177.

[85] OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22, Rn. 36.

[86] OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22, Rn. 34.

[87] OLG Düsseldorf, Beschl. v. 19.9.2018 – Verg 17/18, NRWE Rn. 177.

Nach Einschätzung der Arbeitsgruppe - und vorbehaltlich einer Meinungsbildung auf europäischer Ebene - führt die extraterritoriale Anwendbarkeit von US-Recht, insbesondere des CLOUD Acts sowie ggf. von FISA 702, für sich genommen (also das bloß bestehende Zugriffsrisiko) noch nicht zu einer Übermittlung personenbezogener Daten in ein Drittland, mithin noch nicht zur Anwendbarkeit des Kapitels V DSGVO. Allerdings kann sie dazu führen, dass solchen Rechtsvorschriften unterliegenden Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, soweit er – oder auch der Verantwortliche – nicht technische und/oder organisatorische Maßnahmen ergriffen hat, die hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen angeht, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.

Die zu ergreifenden technischen und organisatorischen Maßnahmen müssen dabei die konkreten Risiken aufgrund des extraterritorial geltenden Rechts ausgleichen. Im konkreten Fall müssen die Maßnahmen also verhindern, dass Microsoft Herausgabeverlangen nach extraterritorial geltendem US-amerikanischem Recht, deren Erfüllung nach EU-Recht nicht nachweisbar zulässig ist, nachkommen kann. Um diese Anforderungen zu erfüllen, können Verantwortliche die Maßstäbe der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses heranziehen. Dabei ist allerdings zu beachten, dass diese für den Kontext von Datenübermittlungen an Drittländer konzipiert worden sind.

Die Nutzung von Microsoft 365 erfordert allerdings in vielen Anwendungsfällen den Zugriff von Microsoft auf Klardaten. Dies entspricht dem Anwendungsfall 6 des Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. Für diesen Anwendungsfall ist es den Aufsichtsbehörden im Hinblick auf Datenübermittlungen nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten. Entsprechend ist auch beim Einsatz von Microsoft 365 besonders kritisch zu prüfen, wie den Anforderungen des Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann.

Die Arbeitsgruppe regt an, die Entwicklung von Modellen zu unterstützen, in denen Dritte als Betreiber bzw. Treuhänder eingesetzt werden, bei denen rechtssicher extraterritoriale Offenlegungsverpflichtungen ausgeschlossen werden können.

Unabhängig davon empfiehlt die Arbeitsgruppe den Mitgliedern der DSK auf eine einheitliche Auslegung der DS-GVO hinsichtlich der Auswirkungen extraterritorial wirkender behördlicher Zugriffsbefugnisse in drittstaatlichem Recht hinzuwirken. Hierzu sollte das Thema in die zuständigen Gremien auf nationaler und europäischer Ebene eingebracht werden.

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

3.2.4.1. Feststellungen des AK Verwaltung

Der AK Verwaltung kritisiert, dass die zum Zeitpunkt seiner Untersuchung geltenden Vertragstexte zur Auftragsverarbeitung vor Vertragsschluss keine hinreichende Prüfung der für die beabsichtigte Tätigkeit bereitgestellten technischen und organisatorischen Maßnahmen durch den Verantwortlichen erlauben. Alleine die damalige Darstellung zu den technischen und organisatorischen Maßnahmen in den Vertragsunterlagen reiche für den Verantwortlichen nicht aus, um eine objektive Einschätzung zu treffen, ob die Maßnahmen dem Risiko angemessen sind und sei zudem nicht prüffähig.

3.2.4.2. Aktueller Prüfungsgegenstand

Gegenüber der Fassung des „Datenschutznachtrags“, die der Untersuchung des AK Verwaltung zu Grunde lag, enthält die ab 15. September 2022 geltende Version eine Ergänzung (Hervorhebung durch Verf.):

„Darüber hinaus müssen diese Maßnahmen den Anforderungen der ISO 27001, ISO 27002 und ISO 27018 entsprechen. Eine Beschreibung der Sicherheitskontrollen für diese Anforderungen steht Kunden zur Verfügung.“

Im Übrigen enthält der „Datenschutznachtrag“ in Anhang A auch in seiner Fassung vom 15. September 2022 eine auf bestimmte Datenkategorien, nämlich Kundendaten in „Core-Onlinediensten“ und nunmehr auch „Professional Services-Daten“ [88] ausdrücklich beschränkte Garantie- von Datensicherheitsmaßnahmen:

„Anhang A – Sicherheitsmaßnahmen

Microsoft hat für Kundendaten in den Core-Onlinediensten und für Professional Services-Daten die folgenden Sicherheitsmaßnahmen getroffen, die in Verbindung mit den Sicherheitsverpflichtungen in diesem DPA (einschließlich der DSGVO-Bestimmungen) die einzige Verantwortung von Microsoft in Bezug auf die Sicherheit dieser Daten darstellen, und wird diese Maßnahmen aufrechterhalten.“

[88] Der Begriff „Core-Online Service“ wird mehrfach im „Datenschutznachtrag“ genutzt, ohne dass dabei wie „Professional-Service –Daten“ eine eigenständige Definition oder aus dem Kontext zu erschließende Konkretisierung ersichtlich wird. Die Arbeitsgruppe mutmaßt, dass es sich um einen im Lizenzvertrag definierten Begriff handelt und weist darauf hin, dass über eine solche Einbeziehung auch der Lizenzvertrag formbedürftig nach Art. 28 Abs. 9 DSGVO wird, was möglicherweise von den Vertragsparteien nicht gewollt ist.

3.2.4.3. Gesprächsergebnisse

Microsoft hat in seiner Stellungnahme vom 11. Dezember 2020 und in ergänzenden Gesprächen darauf hingewiesen, dass die Microsoft-Website servicetrust.microsoft.com („Servicetrust Website“) umfassende Informationen zur Dokumentation und Überprüfung der von Microsoft umgesetzten technischen und organisatorischen Maßnahmen vermittele. Insgesamt gesehen ermögliche dieses Informationsangebot Kunden sowohl die Durchführung einer Due-Diligence-Prüfung der in den Diensten umgesetzten Datenschutzmaßnahmen vor dem Einsatz als auch die Überwachung und Sicherstellung der laufenden Durchführung dieser Maßnahmen durch Microsoft im Betrieb. Wegen der geheimhaltungsbedürftigen Inhalte sei eine Authentisierung (Anmeldung mittels Logins) erforderlich, die ein Interessent über ein kostenloses Testkonto erlangen könne. Alle Nutzer, die mit einem bestehenden Kunden verbunden sind, hätten, so Microsoft, Zugang zu diesen Unterlagen.

3.2.4.4. Bewertung

a) Prüfungsmaßstab

In Konkretisierung der Anforderungen von Art. 28 Abs. 1 und Abs. 3 UAbs. 1 Satz 2 Buchstaben c) und f) DSGVO sollten Verantwortliche entsprechend den Leitlinien des Europäischen Datenschutzausschusses 07/2020 im Auftragsverarbeitungsvertrag eine Reihe grundlegender Anforderungen festlegen oder auf diese verweisen, nämlich [redaktionell durch Verf. angepasst][89]

- *„die zu ergreifenden Sicherheitsmaßnahmen,*
- *eine Verpflichtung des Auftragsverarbeiters, die Zustimmung des Verantwortlichen einzuholen, bevor er Änderungen vornimmt, und*
- *eine regelmäßige Überprüfung der Sicherheitsmaßnahmen, um deren Angemessenheit im Hinblick auf Risiken, die sich im Laufe der Zeit entwickeln können, zu gewährleisten.*

Die Informationen über die in den Vertrag aufzunehmenden Sicherheitsmaßnahmen müssen so detailliert sein, dass der Verantwortliche die Angemessenheit der Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO beurteilen kann. Darüber hinaus ist die Beschreibung auch erforderlich, damit der Verantwortliche seiner Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO in Bezug auf die dem Auftragsverarbeiter auferlegten Sicherheitsmaßnahmen nachkommen kann.“

Selbst wenn nach Art. 28 Abs. 3 UAbs. 1 S. 2 Buchst. c) DSGVO auch eine pauschale Verpflichtung des Auftragsverarbeiters zur Einhaltung der Anforderungen des Art. 32 DSGVO genügen sollte, muss der Verantwortliche doch jederzeit in der Lage sein nachzuweisen, dass die Anforderungen des Art. 32 DSGVO vollumfänglich und für sämtliche verarbeiteten personenbezogenen Daten eingehalten werden.

b) Detailbewertung

[89] EDSA, Leitlinien 07/2020, Rn. 126

Mit der Bereitstellung eines Gastzugangs eröffnet Microsoft für Verantwortliche des nichtöffentlichen und öffentlichen Bereichs den Zugang zu einer[90] umfangreichen, freilich auch komplexen und vertiefte Auseinandersetzung erfordernden Datenbank über die von Microsoft vorgesehenen technischen und organisatorischen Datenschutzmaßnahmen. Auch wenn insoweit die Gesprächsergebnisse die Kritik des AK Verwaltung teilweise entkräften, bleiben Rechtsunsicherheiten, da die einseitigen Änderungen entzogenen Garantien Microsofts über „Sicherheitsmaßnahmen" formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten, nämlich „Kundendaten in „Core-Onlinediensten" und „Professional-Service-Daten", erfassen. Microsoft 365 zählt nach der Erläuterung durch Microsoft jedenfalls zu den hiervon umfassten Angeboten.[91]

Da die Verpflichtungen Microsofts im Hinblick auf technische und organisatorische Maßnahmen zudem abschließend beschrieben sind, wäre zudem durch die Verantwortlichen in jedem Einzelfall zu prüfen und nachzuweisen, dass die vereinbarten Maßnahmen die Anforderungen des Art. 32 DSGVO erfüllen.

3.2.4.5. Schlussfolgerungen

Microsoft wird empfohlen, den Geltungsbereich der „Sicherheitsmaßnahmen" in Anhang A des „Datenschutznachtrags" auf sämtliche im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten zu erstrecken, um Verkürzungen der gebotenen Datenschutzmaßnahmen auszuschließen.

Verantwortliche sollten vor Begründung eines Auftragsverarbeitungsverhältnisses mit Microsoft die durch das Unternehmen angebotenen Möglichkeiten der Überprüfung von Datenschutzmaßnahmen gemäß Art. 28 Abs. 1 DSGVO nutzen und das Ergebnis dokumentieren und deren Einhaltung und Angemessenheit nach Vertragsschluss kontinuierlich und in dokumentierter Form überwachen.

3.2.5. Löschung und Rückgabe personenbezogener Daten

3.2.5.1. Feststellungen des AK Verwaltung

Microsoft differenziert, so der Ausgangsbefund des AK Verwaltung, im Rahmen der Verarbeitung zwischen den Kundendaten, die sich aus dem Auftragsverhältnis ergeben, und Daten, die zur Erbringung „professioneller Dienstleistungen" und der Verarbeitung für „legitime Geschäftszwecke" eigenverantwortlich verarbeitet werden. Der AK Verwaltung ging daher davon aus, dass Microsoft entsprechend der Rolle als Verantwortlicher Daten, die zu eigenen Zwecken verarbeitet werden, nicht löscht. Es sei zwar nachzuvollziehen, dass diese Daten nicht Teil der Auftragsverarbeitung sind und

[90] AV-Prüfschema (vgl. FN 3) , Nr. 14

[91] Vgl. die Definition und der Außnahmen der Core-Onlinedienste in den Lizenzbestimmungen - Datenschutz- und Sicherheitsbestimmungen, https://www.microsoft.com/licensing/terms/de-DE/product/PrivacyandSecurityTerms.

demnach aufgrund einer anderen Rechtsgrundlage verarbeitet werden, dennoch sei zu hinterfragen, wie lange die Daten für eigene Zweck vorgehalten werden. Hierzu äußere sich Microsoft nicht.

3.2.5.2. Aktueller Prüfungsgegenstand

Abweichend vom Prüfungsgegenstand des AK Verwaltung erstreckt der aktuelle „Datenschutznachtrag" 09/2022 die vertragliche Vereinbarung zur Speicherdauer und Löschung von Daten auch auf „Professional-Service"-Daten, während die dem AK Verwaltung vorliegende Version 01/2020 nur die „in jedem Online-Dienst gespeicherten Kundendaten" umfasste:

„Speicherung und Löschung von Daten
Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu löschen." [Hervorhebung durch Verf.]

Hinsichtlich der Verpflichtung des Auftragsverarbeiters zur Löschung nach Erbringung der Verarbeitungsleistungen ergeben sich in der hierfür maßgeblichen Anlage über die „Bestimmungen der Datenschutz-Grundverordnung der Europäischen Union" keine Abweichungen. Diese enthält weiterhin die Zusicherung, *„nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Kunden sämtliche personenbezogenen Daten zu löschen oder dem Kunden zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.*[92]*"*

Der Abschnitt „Speicherung und Löschung von Daten" enthält eine abweichende Regelung, wonach Microsoft die Daten nach Vertragsende 90 Tage mit einer Zugriffsmöglichkeit für den Kunden aufbewahrt und danach grundsätzlich innerhalb weiterer 90 Tage löscht, es sei denn, der „Datenschutznachtrag" erlaubt Microsoft die weitere Speicherung, hierbei gelten abweichende Regelungen für Testversionen.

3.2.5.3. Gesprächsergebnisse

Microsoft hat Einzelheiten der Löschprozesse, insbesondere die Auswirkungen einer Verarbeitung von Daten für eigene Geschäftstätigkeiten im Rahmen eines Gesprächs am 17. Februar 2022 erläutert (vgl. Anlage 3, Seiten 2 bis 8)[93]. Im Einzelnen wird dabei dargestellt:

- Soweit diese in den „Kundendaten" enthalten sind, bestimme der Kunde über Löschung und Aufbewahrung von Daten. Stellt Microsoft Protokolle zur Verfügung (über Verwaltungstools oder

[92] „Datenschutznachtrag" 09/2022, Anhang, Ziff. 2 g)

[93] Siehe auch "Data retention, deletion, and destruction in Microsoft 365" - https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview

APIs), würden diese für die Zwecke der Aufbewahrung und Löschung zu Kundendaten, sobald der Kunde eine Kopie dieser Protokolle erstellt und sie in einem kundenbezogenen Speicher ablegt.

- Bei „Servicegenerierte Daten/Diagnosedaten“ (personenbezogene Daten, die nicht in den Kundendaten enthalten sind) sei zu differenzieren:
  - sog. aktive Löschung: Der Kunde könne die Löschung des Benutzerkontos veranlassen, was zur Löschung der personenbezogenen Daten, die mit dem Benutzer verbunden sind, führe.
  - sog. passive Löschung: Wenn die Benutzeridentitäten des Kunden aufgrund des Endes des Abonnements gelöscht werden, führe dies zur Löschung der personenbezogenen Daten innerhalb von 180 Tagen, ohne dass der Kunde etwas unternimmt.
- Aufbewahrungsfrist:
  Wenn personenbezogene Daten in den vom Dienst generierten Daten enthalten sind, die durch Benutzeraktionen in den Online-Diensten (z.B. Mailbox-Zugriffsprotokolle) oder in Diagnosedaten enthalten sind, richte sich die Aufbewahrung nach dem Zweck, für den die Daten gesammelt wurden, und der Notwendigkeit, die Daten zur Erfüllung dieses Zwecks aufzubewahren.
- Für die Nutzung personenbezogener Daten für Geschäftstätigkeiten (ehemals „legitime Geschäftszwecke“) gebe es keine separaten Speicher, daher habe die Nutzung keine Auswirkungen auf Löschung oder Aufbewahrung. Microsoft nutze für die Geschäftstätigkeiten aggregierte Daten, die jeweils auf dem aktuellen „Datenpool“ beruhen würden. Die genutzten Daten seien höchstens pseudonymisierte Daten. Auf Grundlage aggregierter Daten könnten Einzelpersonen nicht herausgegriffen werden können. Die aggregierten Daten seien, so Microsoft, nichtpersonenbezogen.
- Sonderfälle mit besonderem Verlauf:
  - Microsoft könne Kundendaten oder personenbezogene Daten aufbewahren, wenn es gesetzlich verpflichtet sei, diese Daten aufzubewahren und diese Verpflichtung entstehe, bevor der Kunde die Daten gelöscht hat.
  - Microsoft könne vom Dienst generierte Daten, die personenbezogene Daten enthalten, aufbewahren, wenn dies für Zwecke der Cybersicherheit erforderlich sei.

Die Arbeitsgruppe hatte diese Angaben nicht zu überprüfen und hat auch weitergehende Fragen — etwa ob Microsoft tatsächlich Protokolle löscht, sobald der Kunde sie aus seinem kundenbezogenen Speicher löscht, nachdem er sie dorthin kopiert hat — nicht weiterverfolgt.

3.2.5.4. Bewertung

a) Prüfungsmaßstab

Die Kritik des AK Verwaltung zielt im Kern auf die Frage weisungsgemäßer Verarbeitung durch den Auftragsverarbeiter (Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a DSGVO), wirft aber auch Detailfragen auf, die nochmals die Ausgestaltung der Verarbeitungen Microsofts für eigene Geschäftstätigkeiten betreffen.

b) Detailbewertung

Unbeschadet einer technischen Überprüfung und Bestätigung der von Microsoft erläuterten Speicher-, Verarbeitungs- und Löschprozesse scheinen diese zunächst die Kritik des AK Verwaltung, es erfolge eine dauerhafte Speicherung durch Microsoft, nicht zu rechtfertigen. Die Erläuterungen zeigen mit Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der Cyberabwehr, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschfristen für personenbezogene Daten nicht verlängern sollten.

Allerdings genügt die Ausgestaltung der Rückgabe- und Löschverpflichtung dann nicht den gesetzlichen Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO, wenn man die spezielle Regelung im Abschnitt „Speicherung und Löschung von Daten“ zu Grunde legt, die dem Kunden nicht die Wahl lässt, ob Microsoft die Daten zurückgibt oder löscht, sondern ihm nur eine Möglichkeit zur Extraktion lässt, und Microsoft nur stark verzögert und zudem nur eingeschränkt zur Löschung verpflichtet. Es ließe sich argumentieren, dass die (den Anforderungen des Art. 28 Abs. 3 UAbs. 1 Buchstabe g DSGVO entsprechenden) Regelungen der Anlage 1 Vorrang gegenüber den (unzureichenden) Regelungen im Abschnitt „Speicherung und Löschung von Daten“ genießen sollen. Allerdings ergibt sich dies nicht aus dem Wortlaut und würde zudem bedeuten, dass eine sehr allgemein gehaltene Klausel sehr spezifische Regelungen verdrängen würde. In jedem Fall können Verantwortliche wegen der Unklarheit dieser Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.

Hinsichtlich des vormaligen „eigenen“ Geschäftszwecks“ der Bekämpfung von „Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte“ betreffen können, ergeben sich noch näher zu klärende Folgefragen:

Zum Zeitpunkt der Erläuterung der technischen Abläufe durch Microsoft sollten diese Prozesse noch durch vertragliche Regelungen der vorangehenden Fassungen des „Datenschutznachtrags“ legitimiert werden, die für diese Verarbeitungstätigkeiten eine – seitens des Verantwortlichen freilich zu rechtfertigende – Ermächtigung zur Nutzung durch Microsoft und damit ggf. auch zur selbstständigen Speicherung und allen sonstigen Verarbeitungsmodalitäten umfasst hätten. Dagegen unterliegen diese Verarbeitungstätigkeiten zur Gewährleistung von IT-Sicherheit bzw. Cyberabwehr in der aktuellen Struktur des Datenschutznachtrags 09/2022 nunmehr [94] den allgemeinen Regelungen weisungsgebundener Auftragsverarbeitung.

Da diese Maßstäbe aber die von Microsoft beschriebene, von sonstigen Löscherfordernissen abgekoppelte längerfristige Speicherung „dienstgenerierter Daten“ nicht rechtfertigen können, verbleibt ohne Anpassung der tatsächlichen Verarbeitung – die Microsoft ausdrücklich ausgeschlossen hat – ein Konflikt: Die für die Durchführung des Vertrages gewährleisteten Löschungsrechte des Kunden wie auch die Verpflichtung, nach Vertragsbeendigung Kundendaten zu löschen oder

[94] Verweis auf Abschnitt 3.2.2.

zurückzugeben, enthalten keinerlei Sonderbestimmungen zu Zwecken der IT-Sicherheit. Sie lassen daher keine über die Auftragsverarbeitung hinausgehenden oder nachwirkenden Verarbeitungen zu. Ob nationales oder europäisches Recht je nach Fallkonstellation eine längerfristige Verarbeitung rechtfertigen könnte, kann nur einzelfallbezogen bewertet werden.

3.2.5.5. Schlussfolgerungen

Die Gesprächsergebnisse zur Löschung von Kunden- und „Professional-Service-Daten“ klären zwar die grundlegenden vom AK Verwaltung aufgeworfenen Fragestellungen zur Gewährleistung weisungsgerechter Verarbeitung auf, zeigen zugleich aber eine Detailfrage zur Verarbeitungstätigkeit Microsofts zur Bekämpfung von „Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten.“ Für diese in der aktuellen Fassung nicht mehr in eigener Verantwortung, sondern — jedenfalls nach der Grundsystematik — vertrags- und weisungsgebunden durchzuführenden Verarbeitungen sind z.B. im Hinblick auf die Löschung personenbezogener Daten weitere Untersuchungen ratsam.

Microsoft sollte zudem die Unklarheiten und Widersprüche des Datenschutznachtrags beheben und sicherstellen, dass die Kunden die nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g) DSGVO erforderlichen Wahlrechte und Microsoft die entsprechenden Pflichten zur Rückgabe bzw. Löschung haben.

Auch wenn im Übrigen dem Wortlaut nach keine Differenzen zwischen den erläuterten Verarbeitungsprozessen und den vertraglich festgelegten Verarbeitungstätigkeiten erkennbar geworden sind, sollte durch Microsoft geprüft werden, wie klargestellt werden kann, dass auch bei Verarbeitungen für eigene Geschäftstätigkeiten die vertraglichen Löschrechte des Verantwortlichen vorgehen.[95] Neben der Erfüllung von Transparenzpflichten des Verantwortlichen etwa im Hinblick auf Art. 13 Abs. 2 Buchstabe a DSGVO würden damit auch die bereits erörterten Abwägungen berechtigter Interessen und Prüfungen der Zweckkompatibilität hinsichtlich der mit diesen Verarbeitungen verbundenen Speicherdauer einen wünschenswerten belastbaren Anknüpfungspunkt erhalten.

3.2.6. Information über Unterauftragsverarbeiter

3.2.6.1. Feststellungen des AK Verwaltung

In Bezug auf die Weitergabe personenbezogener Daten an Unterauftragnehmer ist nach der Analyse des AK Verwaltung die vorherige schriftliche Zustimmung des Kunden zur Weitervergabe der Verarbeitung von Kundendaten und personenbezogenen Daten durch Microsoft nur dann ausreichend, „wenn eine Übersicht der zum Zeitpunkt der Unterzeichnung des Auftragsverarbeitungsvertrages vom Verantwortlichen (Kunden/Auftraggeber) genehmigten

[95] Z.B. durch eine Einfügung „Dies gilt auch für Daten, auf deren Grundlage Verarbeitungen für Geschäftstätigkeiten durchgeführt werden“ im Abschnitt „Speicherung und Löschung von Daten“ sowie im Anhang der „DSGVO-Bedingungen“.

Unterauftragnehmer aufgenommen wird (siehe dazu auch 3.2.7 der Opinion 14/2019 des Europäischen Datenschutzausschusses).“

Der zur Information über Hinzuziehung oder Ersetzung von Unterauftragnehmern vorgesehene „Mechanismus zur Benachrichtigung des Kunden über dieses Update“ durch das Abonnement von Push-Benachrichtigungen ist, so der AK Verwaltung, dementsprechend proaktiv durch Microsoft einzusetzen.

3.2.6.2. Aktueller Prüfungsgegenstand

Die mehrfache, teils kontroverse Erörterung der Ausgestaltung der Kontrollrechte des Verantwortlichen bei Veränderungen der Unterauftragsverarbeitungsverhältnisse hat zu einer bereits Ende März eingeführten Neugestaltung des Unterrichtungsverfahrens geführt, die im aktuellen „Datenschutznachtrag“ 09/2022 zu einer Streichung des bisherigen „Hol-Schuld“-Verfahrens geführt hat.

Die maßgebliche Bestimmung des Abschnitts „*Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern*“ lautet nunmehr [Hervorhebung zur Kennzeichnung der Abweichungen von vorangehenden Fassungen durch Verf.]:

„Microsoft beauftragt gelegentlich möglicherweise neue Unterauftragsverarbeiter. Microsoft informiert den Kunden und aktualisiert die Webseite mindestens 6 Monate, bevor dieser Zugriff auf Kundendaten erhält über jeden neuen Unterauftragsverarbeiter ~~(durch Aktualisierung der Website und Bereitstellung eines Mechanismus zur~~

~~Benachrichtigung des Kunden über diese Aktualisierung).~~ Darüber hinaus informiert

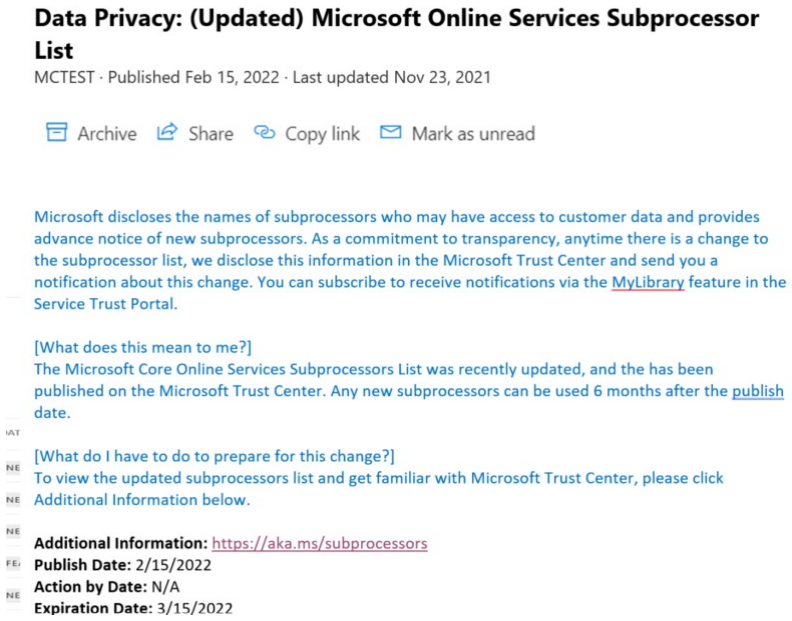
Microsoft den Kunden über und aktualisiert die Webseite im Hinblick auf jeden neuen Unterauftragsverarbeiter mindestens 30 Tage bevor er Zugriff auf andere Professional Services-Daten oder personenbezogene Daten erhält, die nicht in den Kundendaten enthalten sind. Wenn Microsoft einen neuen Unterauftragsverarbeiter für ein neues Produkt oder einen Professional Service beauftragt, der Kundendaten, Professional Services-Daten oder personenbezogene Daten verarbeitet, wird Microsoft den Kunden vor der Verfügbarkeit dieses Produkts oder Professional Services benachrichtigen.“

3.2.6.3. Gesprächsergebnisse

In den Gesprächen mit der Arbeitsgruppe konnte Microsoft trotz anfänglicher Vorbehalte zur rechtlichen Erforderlichkeit und Praktikabilität zu einer Umstellung des bisher als Hol-Schuld des Verantwortlichen ausgestalteten Verfahrens zu organisatorischen und vertraglichen Anpassungen bewogen werden. Hierzu wurden im Wesentlichen folgende Eckpunkte vorgetragen (vgl. Anhang 3, Seiten 10 bis 15):

- Nutzung des bestehenden Microsoft Service Messaging Center (SMC) als bestehende proaktive Benachrichtigungsmethode, die für die Servicekommunikation für Microsoft-365-Kunden verwendet wird.
- Push-Benachrichtigung per E-Mail (Versand an zwingend benannten „Global Admin“ und (sofern zugewiesen) „Privacy Reader“ des Kunden), um diese über das Update zu informieren, ohne dass kundenseitiges Handeln erforderlich ist. Der Kunde kann diese Benachrichtigung allerdings abbestellen.
- Die Benachrichtigung über Änderungen an der Liste der Online-Dienste-Unterauftragsverarbeiter wird mit dem zusätzlichen Hinweis „Datenschutz“ versehen. Diese Benachrichtigungen können von den Rollen Global Admin und Privacy Reader gelesen werden. Alle Dienstbenachrichtigungen sind standardmäßig zunächst für den Global Admin aktiviert.
- Wenn die Liste der Online-Dienste-Unterauftragsverarbeiter aktualisiert wird, löst dies automatisch eine SMC-Benachrichtigung an den Global Admin und den Privacy Reader (falls Letzterer zugewiesen ist) aus. Eine E-Mail-Benachrichtigung wird auch an den Global Admin und den Privacy Reader (falls zugewiesen) gesendet, die sie über die Aktualisierung informieren, ohne dass weitere Maßnahmen erforderlich sind.

Nachfolgendes Schaubild zeigt ein Umsetzungsbeispiel der SMC-Benachrichtigungs-Mail über Veränderungen von Unterauftragsverhältnissen:



Data Privacy: (Updated) Microsoft Online Services Subprocessor List

MCTEST · Published Feb 15, 2022 · Last updated Nov 23, 2021

Archive Share Copy link Mark as unread

Microsoft discloses the names of subprocessors who may have access to customer data and provides advance notice of new subprocessors. As a commitment to transparency, anytime there is a change to the subprocessor list, we disclose this information in the Microsoft Trust Center and send you a notification about this change. You can subscribe to receive notifications via the MyLibrary feature in the Service Trust Portal.

[What does this mean to me?]
The Microsoft Core Online Services Subprocessors List was recently updated, and the has been published on the Microsoft Trust Center. Any new subprocessors can be used 6 months after the publish date.

[What do I have to do to prepare for this change?]
To view the updated subprocessors list and get familiar with Microsoft Trust Center, please click Additional Information below.

Additional Information: https://aka.ms/subprocessors
Publish Date: 2/15/2022
Action by Date: N/A
Expiration Date: 3/15/2022

Abbildung

3.2.6.4. Bewertung

a) Prüfungsmaßstab

Art. 28 Abs. 2 Satz 2 DSGVO sieht vor, dass der Auftragsverarbeiter im Falle einer allgemeinen schriftlichen Genehmigung von Unterauftragsverhältnissen den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Diese Informationspflicht wird in den Leitlinien des Europäischen Datenschutzausschusses 07/2020 ausdrücklich als „Bring-Schuld“ des durch eine solche generelle Genehmigung begünstigten Auftragsverarbeiters klargestellt:

„Es sei darauf hingewiesen, dass die Pflicht des Auftragsverarbeiters, den Verantwortlichen über jede Änderung bei den Unterauftragsverarbeitern zu informieren, impliziert, dass der Auftragsverarbeiter solche Änderungen gegenüber dem Verantwortlichen aktiv anzeigt oder kennzeichnet.“[96]

[96] EDSA, a.a.O, Rn. 128, die außerdem in ihrer Fußnote 54 ein Verfahren wie es Microsoft zuvor praktiziert hatte, ausdrücklich als unzureichend einordnet.

b) Detailbewertung

Mit der Anpassung und vertragsrechtlichen Verankerung des Unterrichtungsverfahrens trägt Microsoft der Kritik des AK Verwaltung und den Anforderungen der Leitlinien des Europäischen Datenschutzausschusses Rechnung, soweit es um die Ausgestaltung als „Push"-Verfahren geht. Die oben abgebildete E-Mail verweist allerdings für den tatsächlichen Inhalt der Benachrichtigung auf eine WWW-Seite von Microsoft. 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.

3.2.6.5. Schlussfolgerungen

Für den Verantwortlichen als Vertragspartner des „Datenschutznachtrags" 09/2022 erfordert die rechtlich gebotene Anpassung des Unterrichtungsverfahrens durch Microsoft, nunmehr innerorganisatorisch einen Informationsfluss sicherzustellen, der die Weiterleitung einer Änderungsmitteilung über Unterauftragsverhältnisse an die zur datenschutzrechtlichen Bewertung dieses Sachverhalts berufenen Funktionsträger gewährleistet oder aber deren unmittelbare Nutzung des Benachrichtigungsdienstes sicherstellt.

Um eine zielgenaue Bewertung z.B. im Hinblick auf die Anforderungen an Drittstaatentransfers zu ermöglichen und auch selbst inhaltlich die Anforderungen des Art. 28 zu erfüllen, bleibt freilich weiterhin auch Microsoft gefordert, die Informationen zu Unterauftragsverarbeitern zu präzisieren: 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. Microsoft wird empfohlen, die den Verantwortlichen bereitgestellten Informationen über Unterauftragsverhältnisse an diese in Anhang IV der Standardvertragsklauseln zusammengefassten Anforderungen anzupassen.

Auch wenn dies — die gesetzliche Verpflichtung zur Information liegt beim Auftragsverarbeiter — außerhalb der Zuständigkeit der deutschen Aufsichtsbehörden liegt, sei der Vollständigkeit halber angemerkt, dass Microsoft auch den tatsächlichen Versand der Benachrichtigungen sicherstellen muss, insbesondere also die Möglichkeit zur Abbestellung deaktivieren sollte.

3.2.7. Datenübermittlungen in Drittstaaten

3.2.7.1. Feststellungen des AK Verwaltung, Untersuchungsauftrag

Der AK Verwaltung hat sich in seiner Bewertung vom 15. Juli 2020 nicht zu Fragen der Übermittlung personenbezogener Daten in Drittländer geäußert. Die DSK hat in ihrem Beschluss vom 29. September 2020 aber die Arbeitsgruppe beauftragt, zeitnah Anpassungen an die durch die Schrems-II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen.

3.2.7.2. Aktueller Prüfungsgegenstand

Der „Datenschutznachtrag" September 2022 enthält unter „Datenübermittlungen und Speicherstelle – Datenübermittlungen" die Regelung, dass der Kunde – unter Würdigung der in diesem Abschnitt geregelten und für verbindlich erklärten Sicherheitsmaßnahmen – 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 aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Produkte und Services gelten danach die von Microsoft implementierten Standardvertragsklauseln der EU-Kommission von 2021. Microsoft halte sich an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung, Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz. Alle Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation unterlägen geeigneten Garantien, wie sie in Art. 46 DSGVO beschrieben sind, und solche Übermittlungen und Garantien würden nach Art. 30 Abs. 2 DSGVO dokumentiert.

Im Abschnitt „Datenübermittlungen und Speicherstelle – Ort der ruhenden Kundendaten" findet sich zudem eine Regelung, wo bestimmte Daten gespeichert werden.

3.2.7.3. Gesprächsergebnisse

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, für alle gewerblichen und Kunden des öffentlichen Sektors, die im EU-Raum ansässig sind, anzubieten, Kundendaten, Supportdaten und sonstige personenbezogene Daten der Kunden grundsätzlich – d.h. nicht ausnahmslos, nicht etwa für bestimme IT-Sicherheitsmaßnahmen – im EU-Raum zu speichern und zu verarbeiten.

Nach Aufbau des Konzepts der „EU Data Boundary“ sollen u.a.

- Supportleistungen „für erste Lösungen“ innerhalb der EU durch Aufstockung des Personals in der Region erbracht werden,
- Unterauftragsverhältnisse vermindert werden, um den Zugang zu personenbezogenen Daten von EU-Kunden zu begrenzen,
- Technologien wie eine virtuellen Desktop-Infrastruktur (VDI) eingerichtet werden, um den Schutz bei erforderlichen Support-Fernzugriffen auf personenbezogene Daten von EU-Kunden zu erhöhen und die physische Übertragung von Daten zu verhindern (vgl. im Einzelnen Anlage 4, Seiten 10 bis 15).

Ergänzend ist auf die nicht spezifisch für Datenexporte geltenden Regelungen über weitere Schutzmaßnahmen für Verarbeitungen zu eigenen Geschäftstätigkeiten von Microsoft im Zusammenhang mit der Leistungserbringung zu verweisen, die in Abschnitt 3.2.2 behandelt werden.

3.2.7.4. Bewertung

a) Prüfungsmaßstab

Nach Art. 44 DSGVO ist jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in[97] ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter (einschließlich aller eventuellen Unterauftragsverarbeiter) die in Kapitel V der DSGVO niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen der DSGVO eingehalten werden. Die Anforderungen sind auch bei Weiterübermittlungen aus einem Drittland an ein anderes Drittland einzuhalten.

Zur Rechtfertigung der Übermittlung zieht Microsoft die Standardvertragsklauseln für Datenexporte 2021[98] heran. Entsprechend der Rechtsprechung des EuGHs in „Schrems II“ verlangen diese Standardvertragsklauseln in Klausel 14 eine Untersuchung und Bewertung der Rechtslage und -praxis in dem jeweiligen Zielland jeglicher Übermittlungen personenbezogener Daten. Hierfür enthalten die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses eine detaillierte Schritt-für-Schritt-Anleitung. Hindern die Rechtslage oder -praxis im Bestimmungsdrittland den Datenimporteur an der Erfüllung seiner Pflichten aus den Standardvertragsklauseln, sind ergänzende Schutzmaßnahmen zu treffen, die diejenigen Rechtsvorschriften oder Gepflogenheiten des Drittlandes ausgleichen, die den Datenexporteur an der Erfüllung seiner Verpflichtungen aus den Standardvertragsklauseln hindern, d.h. genau die identifizierten Rechtsschutzlücken schließe.[99] Ist es nicht möglich, diejenigen Rechtsvorschriften oder Gepflogenheiten des Drittlandes, die den Datenexporteur an der Erfüllung

[97] So die korrekte Übersetzung anstatt des in der deutschen Sprachfassung verwendeten „an“, vgl. die englische Fassung von Art. 44: „to a third country“, die den Sinn etwa klarer macht; eindeutig die französische Fassung: „vers un pays tiers“.

[99] EDSA, Empfehlungen 01/2020, Version 2.0, Rn. 75.

seiner Verpflichtungen aus den Standardvertragsklauseln hindern, vollständig auszugleichen, darf eine Übermittlung in das jeweilige Drittland nicht erfolgen.[100] Primär kommt es dabei auf eine Bewertung der geltenden Gesetze im Drittland an. Nur wenn insoweit Unklarheiten bestehen, besteht Raum für eine ergänzende Betrachtung der Praxis im Drittland.[101]

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. Während gegen Überwachung auf der Basis von E.O. 12333 technische Maßnahmen – insbesondere Verschlüsselung – unter bestimmten Bedingungen als möglich erachtet werden,[102] können Diensteanbieter und ihre Mitarbeiter, die FISA 702 unterfallen, zur Herausgabe der gewünschten Daten gezwungen werden. Der Einwand, dass die Herausgabe nach der DSGVO unzulässig ist, ist – nach der von Microsoft bestrittenen Expertenbewertung - nach US-Recht irrelevant.[103]

b) Detailbewertung

Um die vom EuGH identifizierten am EU-Maßstab gemessenen grundrechtlichen Unzulänglichkeiten von FISA 702 auszugleichen, wäre es mithin erforderlich, Maßnahmen zu ergreifen, die den Zugriff der US-Behörden – und damit von Microsoft – auf personenbezogene Daten verhindern oder ineffektiv machen. Dies kann in bestimmten, begrenzten Anwendungsfällen möglich sein. Konkret anzuführen wären die Anwendungsfälle 1 (Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern), 2 (Übermittlung pseudonymisierter Daten) und 5 (Aufgeteilte Verarbeitung oder Verarbeitung durch mehrere Beteiligte, Multi-party Processing) des Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses, soweit die dort aufgestellten Bedingungen eingehalten werden.

Viele der in Microsoft 365 enthaltenen Dienste erfordern allerdings einen Zugriff von Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten.[104] Insbesondere die naheliegende Verschlüsselung verarbeiteter Daten, die einen Zugriff von Microsoft und damit der US-Behörden verhindern würde, ist regelmäßig nicht möglich, wenn die Daten beispielsweise im Browser angezeigt werden müssen. 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

---

[100] Vgl. EDSA, Empfehlungen 01/2020, Version 2.0, Rn. 75.

[101] Vgl. EDSA, Empfehlungen 01/2020, Version 2.0, Rn. 43.3.

[102] Vgl. den Anwendungsfall 3 des Anhangs 2 von EDSA, Empfehlungen 01/2020, Version 2.0, Rn. 90.

[103] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.7, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[104] Von Dritten angebotene Dienste, die zu einer Umformung bzw. Verschlüsselung der bei Microsoft verarbeiteten Daten führen, sind nicht Gegenstand dieser Untersuchung. Die Arbeitsgruppe weist allerdings darauf hin, dass jedenfalls in bestimmten Konstellationen wie der E-Mail-Nutzung die Schutzmaßnahmen als unzureichend erscheinen. Auch von einzelnen Cloud-Anbietern für bestimmte Anwendungsfälle selbst angebotene Funktionen zu einer abgeschotteten Verarbeitung müssten sicherstellen und nachweisen können, dass hinreichende Garantien bestehen, dass der Anbieter sich keinen Zugriff auf die Daten verschaffen kann. Dies stellt im Cloud-Umfeld zumindest eine Herausforderung dar, für die keinem der Mitglieder der Arbeitsgruppe bisher eine geeignete Lösung bekannt ist.

den Aufsichtsbehörden 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, da die weitergehende Verarbeitung bei den meisten der in Microsoft 365 enthaltenen Dienste technisch zwingend im Klartext erfolgen muss und die örtliche Beschränkung sich nur auf den Ort der Speicherung der Daten bezieht. Für die weiteren Verarbeitungen (abseits der Speicherung) enthält der Abschnitt „Datenübermittlung und Ort“ („Data Transfers and Location“) keine Aussagen zur Datenlokalisierung.[105]

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. Am ehesten mag noch die Verpflichtung zur Anfechtung von Herausgabeanordnungen als ergänzende Schutzmaßnahme in Betracht kommen. Doch besteht diese Verpflichtung zur Anfechtung nur, wenn die Herausgabeanordnung nach demjenigen Recht unzulässig ist, dem die Behörde bzw. das Gericht unterliegt, die bzw. dass die Herausgabe anordnet, wozu auch relevante Konflikte mit dem anwendbaren EU- oder mitgliedsstaatlichen Recht gehören. Da aber FISA 702, wie der EuGH festgestellt hat, [106] keine inhaltliche Begrenzung der Überwachungsbefugnisse vorsieht und FISA 702 unterliegende Unternehmen die Anwendung dieser Norm nicht mit dem Argument abwenden können, dadurch würde EU- oder mitgliedsstaatliches Recht verletzt,[107] ist nicht erkennbar, wie eine Verletzung des in Art. 52 EU-Grundrechtecharta geregelten Grundsatzes der Verhältnismäßigkeit durch eine solche Herausgabeanordnung auf diesem Wege erfolgreich geltend gemacht werden könnte. Dementsprechend sehen die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses derartige Maßnahmen auch nur als Ergänzung anderer Maßnahmen vor.[108]

Zu der Frage, inwieweit Microsoft sich vertraglich Offenlegungen vorbehält, die Art. 48 DSGVO widersprechen, wird auf Abschnitt 3.2.3. verwiesen.

Für Übermittlungen personenbezogener Daten in andere Länder als die USA fehlt es bereits an einer Bewertungsgrundlage. Auch im Dokument „Compliance with EU transfer requirements for personal

---

[105] Siehe „Datenschutznachtrag“ 09/2022: Abschnitt „Data transfer and location“, Unterabschnitt „Location of Customer Data at Rest“ enthält Ausführungen zum Speicherort. Der vorhergehende Abschnitt „Data Transfer“ umfasst weitere Teile der Verarbeitung, wie z.B. „collection, use, transfer, retention, and other processing of Personal Data“, die nicht zwangsläufig am Speicherort ausgeführt werden und daher dem Transfer in ein Drittland unterliegen können.

[106] EuGH, Urt. v. 16.7.2020 – C-311/18, Rn. 180 ff.

[107] Stephen Vladeck, Memo on Current State of U.S. Surveillance Law and Authorities, 15. November 2021, Kapitel I.7, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

[108] EDSA, Empfehlungen 01/2020, Rn. 119.

data in the Microsoft cloud“[109] beschränkt sich Microsoft auf die Aussage, anzunehmen, dass die drittstaatlichen Gesetze und Gewohnheiten Microsoft in der Praxis nicht daran hindern würden, die Verpflichtungen aus den Standardvertragsklauseln einzuhalten. Insoweit ist im Übrigen darauf hinzuweisen, dass für die von Microsoft im genannten Dokument entscheidend vorgenommene Bewertung der Praxis kein Raum ist, wenn die Rechtslage bereits als problematisch identifiziert ist, wie dies in den USA der Fall ist.

Zusätzliche Fragen wirft die im „Datenschutznachtrag“ vorgesehene Weisung („beauftragt (…), (…) personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind“) auf, die für den Kunden regelmäßig nicht bestimmbare weitere Datenübermittlungen in Drittländer vorsieht. Selbst wenn Microsoft dem Kunden vor Vertragsschluss entsprechende Informationen bereitstellen würde, müssten auch die Informationen über neue Unterauftragsverarbeiter entsprechend ergänzt werden. Darüber hinaus müsste auch eine Information vorgesehen werden, wenn sich die Länder, in denen Microsoft selbst oder bestehende Unterauftragsverarbeiter tätig sind (und zwar unabhängig davon, ob diese Tätigkeit einen Bezug zur Auftragsverarbeitung hat), ändern.

Die Arbeitsgruppe weist darauf hin, dass nach der Rechtsprechung des Bundesverwaltungsgerichts aus der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auch eine Beweislastverteilung folgt,[110] sodass Verantwortliche bereits unabhängig von der implizit durch die Regel-Ausnahme-Formulierung der Art. 44, 45 Abs. 1 DSGVO erfolgten Beweislastregelung die Erfüllung der Anforderungen des Kapitels V DSGVO zweifelsfrei nachweisen können müssen.

3.2.7.5. Schlussfolgerungen

Die Nutzung von Microsoft 365 unter Geltung des „Datenschutznachtrags“ 09/2022 verlangt zwingend Weisungen des Verantwortlichen zu Übermittlungen personenbezogener Daten in Drittländer, namentlich die USA und alle anderen Länder, in denen Microsoft oder ihre Unterauftragsverarbeiter tätig sind. Jedenfalls Datenübermittlungen in die USA lassen sich auch technisch nicht verhindern.

Insbesondere das US-amerikanische nationale Sicherheitsrecht in Form von FISA 702 kann die Erfüllung der Verpflichtungen aus den Standardvertragsklauseln in Frage stellen. Damit wären also ergänzende Schutzmaßnahmen zu treffen, die jeden Zugriff von US-Behörden und auch von Microsoft und seinen Mitarbeitern unmöglich oder ineffektiv machen, um so zu verhindern, dass Microsoft Herausgabeverlangen nach FISA 702 nachkommen kann.

Die Nutzung der Dienste von Microsoft 365 als klassische Cloud-Dienste erfordert allerdings in vielen Anwendungsfällen den Zugriff von Microsoft auf Klardaten. Dies entspricht dem Anwendungsfall 6 des

[109] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1?culture=en-us&country=US.

[110] BVerwG, Urt. v. 2.3.2022 – 6 C 7.20, Rn. 50.

Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. Für diesen Anwendungsfall ist es den Aufsichtsbehörden nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten. Die von Microsoft vorgesehenen Maßnahmen sind unzureichend, da sie nicht die bestehenden Schutzlücken – insbesondere exzessive Zugriffsrechte und fehlender gerichtlicher Rechtsschutz – beheben.

Nur in besonderen Ausnahmefällen kommen ergänzende Schutzmaßnahmen in Betracht, die für die erforderliche Gewährleistung eines vergleichbaren Schutzniveaus für die übermittelten Daten effektiv sind, etwa die Speicherung sicher verschlüsselter Backups in der Microsoft-Cloud, wenn der Schlüssel beim Kunden verbleibt.

Die von Microsoft bereits avisierte künftige verstärkte Verlagerung der Datenverarbeitung in die EU erscheint vor diesem Hintergrund hilfreich, ist in der Umsetzung aber vor dem Hintergrund etwaiger extraterritorial wirkender Rechtsvorschriften zu beobachten und zu bewerten. Microsoft sollte auch die derzeit unbestimmte Weisung zu Datenexporten beschränken und klar bestimmt fassen.

4. Gesamtbewertung, weiteres Vorgehen

Auf Grundlage ihrer Gespräche mit Microsoft von Dezember 2020 bis April 2022 und Berücksichtigung des am 15. September 2022 von Microsoft veröffentlichten „Datenschutznachtrags“ unterbreitet die Arbeitsgruppe der DSK Vorschläge für eine zusammenfassende Bewertung, die gesondert zu diesem Bericht zur abschließenden Beratung vorgelegt werden.

4.1.1.1. Anhang: Übersicht über die Arbeitsgespräche der Arbeitsgruppe mit Microsoft

18.12.2020	Auftaktgespräch der Arbeitsgruppe mit MS
12.02.2021	2. Gespräch Arbeitsgruppe mit MS
25.03.2021	3. Gespräch Arbeitsgruppe mit MS
23.04.2021	4. Gespräch Arbeitsgruppe mit MS
14.06.2021	„EU Data Boundary-Projekt“ – Sondertermin Arbeitsgruppe mit MS
28.06.2021	5. Gespräch Arbeitsgruppe mit MS
29.10.2021	6. Gespräch Arbeitsgruppe mit MS
05.11.2021	7. Gespräch Arbeitsgruppe mit MS
09.12.2021	8. Gespräch Arbeitsgruppe mit MS
21.01.2022	9. Gespräch Arbeitsgruppe mit MS
17.02.2022	10. Gespräch Arbeitsgruppe mit MS
16.03.2022	11. Gespräch Arbeitsgruppe mit MS
29.04.2022	12. Gespräch Arbeitsgruppe mit MS
19.09.2022	Abschlussgespräch der Arbeitsgruppe mit MS