

2 AG DSK „Microsoft-Onlinedienste“

3 **Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung,** 4 **Stand 2. November 2022**

5	1.	Untersuchungsauftrag.....	3
6	2.	Verfahren, Untersuchungsgegenstand und maßgeblicher Beurteilungszeitpunkt	3
7	3.	Wesentliche Ergebnisse.....	5
8	3.1.	Allgemeines	5
9	3.2.	Zusammenfassung der Gesprächsergebnisse	7
10	3.2.1.	Festlegung von Art und Zweck der Verarbeitung, Art der personen- bezogenen Daten.....	7
11	3.2.1.1.	Feststellungen des AK Verwaltung	7
12	3.2.1.2.	Aktueller Prüfungsgegenstand	7
13	3.2.1.3.	Gesprächsergebnisse.....	8
14	3.2.1.4.	Bewertung	9
15	3.2.1.5.	Schlussfolgerungen.....	10
16	3.2.2.	Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime 17 Geschäftszwecke“	11
18	3.2.2.1.	Feststellungen des AK Verwaltung.....	11
19	3.2.2.2.	Aktueller Prüfungsgegenstand	12
20	3.2.2.3.	Gesprächsergebnisse.....	13
21	3.2.2.4.	Bewertung	15
22	3.2.2.5.	Schlussfolgerungen	25
23	3.2.3.	Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, 24 CLOUD Act, FISA 702	26
25	3.2.3.1.	Feststellungen des AK Verwaltung.....	26
26	3.2.3.2.	Aktueller Prüfungsgegenstand	26
27	3.2.3.3.	Gesprächsergebnisse.....	28
28	3.2.3.4.	Bewertung	29
29	3.2.3.5.	Schlussfolgerungen.....	38
30	3.2.4.	Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO.....	39
31	3.2.4.1.	Feststellungen des AK Verwaltung.....	39

* 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.

32	3.2.4.2. Aktueller Prüfungsgegenstand	40
33	3.2.4.3. Gesprächsergebnisse.....	40
34	3.2.4.4. Bewertung	41
35	3.2.4.5. Schlussfolgerungen.....	42
36	3.2.5. Löschung und Rückgabe personenbezogener Daten	42
37	3.2.5.1. Feststellungen des AK Verwaltung	42
38	3.2.5.2. Aktueller Prüfungsgegenstand	42
39	3.2.5.3. Gesprächsergebnisse.....	43
40	3.2.5.4. Bewertung	44
41	3.2.5.5. Schlussfolgerungen	45
42	3.2.6. Information über Unterauftragsverarbeiter	46
43	3.2.6.1. Feststellungen des AK Verwaltung.....	46
44	3.2.6.2. Aktueller Prüfungsgegenstand	46
45	3.2.6.3. Gesprächsergebnisse.....	47
46	3.2.6.4. Bewertung	48
47	3.2.6.5. Schlussfolgerungen	49
48	3.2.7. Datenübermittlungen in Drittstaaten	50
49	3.2.7.1. Feststellungen des AK Verwaltung, Untersuchungsauftrag	50
50	3.2.7.2. Aktueller Prüfungsgegenstand	50
51	3.2.7.3. Gesprächsergebnisse.....	50
52	3.2.7.4. Bewertung	51
53	3.2.7.5. Schlussfolgerungen	54
54	4. Gesamtbewertung, weiteres Vorgehen	55
55	Anhang: Übersicht über alle Termine mit Microsoft	56
56		
57	Anlagen.....	entfallen*
58		

59 1. Untersuchungsauftrag

60 Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat
61 in ihrer Sitzung vom 22. September 2020 eine Bewertung des Arbeitskreises Verwaltung zu den dem
62 Einsatz des Produkts Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service
63 Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing
64 Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von
65 Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die Bewertung
66 kommt zum Ergebnis, „dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von
67 Microsoft Office 365 möglich“ sei. Die DSK hat eine Arbeitsgruppe unter Federführung Brandenburgs
68 und des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gebeten, Gespräche mit dem
69 Hersteller aufzunehmen, „um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an
70 die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für
71 die Anwendungspraxis öffentliche und nicht öffentlicher Stellen zu erreichen¹.“

72 Der vorliegende Bericht behandelt die Ergebnisse der hierauf bis April 2022 geführten Gespräche (vgl.
73 Anhang) und leitet daraus erste Vorschläge zum weiteren Vorgehen ab. Der Bericht folgt in seiner
74 Struktur der Bewertung des AK Verwaltung², schreibt diese – ohne Anspruch auf Vollständigkeit – fort
75 und ergänzt sie entsprechend dem Untersuchungsauftrag der DSK durch eine nicht abschließende
76 Untersuchung grundlegender Fragestellungen an Datenübermittlungen in die USA bei der Nutzung von
77 Microsoft 365. Es erfolgte ausdrücklich keine umfassende Prüfung des gesamten einschlägigen
78 Vertragswerks von Microsoft, die vielmehr unter Berücksichtigung seiner jeweiligen konkreten
79 Verarbeitungstätigkeiten nach Art. 5 Abs. 2 DSGVO dem einzelnen Verantwortlichen vorbehalten
80 bleibt.³

81 2. Verfahren, Untersuchungsgegenstand und maßgeblicher Beurteilungs- 82 zeitpunkt

83

84 In den Gesprächen der Arbeitsgruppe mit Microsoft haben neben Brandenburg und BayLDA (beide
85 Leitung) Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie
86 der Datenschutzaufsichtsbehörden Baden-Württembergs, Berlins, Hessens, Mecklenburg-
87 Vorpommern, Sachsens, des Saarlandes und Schleswig-Holsteins teilgenommen. Microsoft hat die
88 Gespräche federführend durch leitende Vertreter der Microsoft Deutschland GmbH sowie je nach
89 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>.

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

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

108 Der Bericht beschränkt sich auf eine Bewertung der zum Abschluss dieses Beteiligungsverfahrens am
109 10. Oktober 2022 bestehenden Sach- und Rechtslage. Ob und in welchem Umfang durch die am 7.
110 Oktober 2022 von US-Präsident Biden und Generalstaatsanwalt Garland vorgestellte Executive Order
111 „Enhancing Safeguards for United States Signals Intelligence Activities“ und begleitende
112 Rechtsverordnungen des US-Justizministeriums Änderungen des für die Bewertung von
113 Drittstaatentransfers maßgeblichen Bedingungen des US-Rechts eingetreten sind, bleibt daher
114 angesichts noch ausstehender Vollzugsschritte zur Implementierung dieser Regelungen im Rahmen
115 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.

116 3. Wesentliche Ergebnisse

117 3.1. Allgemeines

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



Abbildung 1

121 „Microsoft 365“ in an verschiedenen Zielgruppen ausgerichteten „Plänen“ zusammenfasst.
122

123 So umfasst beispielsweise alleine das Produktpaket „Microsoft 365 Business Premium“⁶
124 15 unterschiedliche Anwendungen, die gängige Büro-Software zur Textverarbeitung oder
125 Tabellenkalkulation, Cloudspeicher, Video-Konferenzsysteme mit Social Media-Elementen oder
126 Sicherheits-Funktionen bereitstellen. Die Arbeitsgruppe hat keine Untersuchung der einzelnen
127 Produkte vorgenommen und die Funktionalitäten sowie datenschutzrechtlichen Fragen der einzelnen
128 Produkte im Rahmen der Gespräche nicht bzw. nur sehr rudimentär angesprochen.

129 Der durch die Arbeitsgruppe geprüfte „Datenschutznachtrag“ umfasst u.a. als Vereinbarung zur
130 Auftragsverarbeitung sämtliche mit diesen Anwendungen verbundenen Verarbeitungsvorgänge
131 (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“.

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

137 Der Vereinheitlichungsanspruch des Vertragstextes gilt im Übrigen nicht nur sachlich, sondern auch
138 territorial. Unabhängig davon, ob das Rechtsverhältnis zwischen Microsoft und seinem Kunden der
139 DSGVO oder anderen Rechtsordnungen unterliegt, ergeben sich die datenschutzrechtlichen
140 Regelungen stets aus dem derzeit 20-seitigen „Datenschutznachtrag“. Gegenüber weiteren
141 vertraglichen Regelungen zwischen Microsoft und dem jeweiligen Kunden – mit Ausnahme der
142 produktspezifischen Regelungen, die wiederum dem „Datenschutznachtrag“ vorgehen⁹ –
143 beansprucht der „Datenschutznachtrag“ Vorrang¹⁰, wobei die Arbeitsgruppe nicht prüfen konnte, ob
144 dies auch in den anderen Vertragsdokumenten so vereinbart ist.

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

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

154 Die allgemeine datenschutzrechtliche Bewertung des „Datenschutznachtrags“ als Vereinbarung zur
155 Auftragsverarbeitung kann im Übrigen für die individuelle Bewertung einzelner Verantwortlicher nur
156 als Anhaltspunkt herangezogen werden, da sie nur die zum Abschluss dieser Untersuchung vorliegende
157 Version betrifft. Ob die ursprünglich bei Begründung eines Service-Bezugs oder eine teils auch
158 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 Anwendungsbereich 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.

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

164 3.2. Zusammenfassung der Gesprächsergebnisse

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

168 3.2.1. Festlegung von Art und Zweck der Verarbeitung, Art der personen- 169 bezogenen Daten

170 3.2.1.1. Feststellungen des AK Verwaltung

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

177 3.2.1.2. Aktueller Prüfungsgegenstand

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

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

185 Gleiches gilt für letztlich rein sprachliche Anpassungen im neu gefassten Anhang B des
186 „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.

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

192 3.2.1.3. Gesprächsergebnisse

193 Microsoft hat der Rüge mangelnder Eingrenzung des Vertragsgegenstandes im Verlauf der Gespräche
194 nicht abgeholfen. Microsoft leitet seine Bewertung, dass weitere Konkretisierungen „keinen
195 substantiell anderen datenschutzrechtlichen Effekt erzielen“ würden, im Wesentlichen daraus ab, dass
196 der Umfang der zur Beschreibung von Datenarten und Verarbeitungszwecken bereitgestellten
197 Angaben sich aus Aussagen der WP-29-Stellungnahme 03/2013 zum Grundsatz der Zweckbindung
198 ergebe und dass die Darstellung der Datenerhebungskategorien und Nutzungszwecke mit der ISO/IEC
199 19944 einem anerkannten Standard folge, der eine logisch vollständige Beschreibung aller
200 Datenkategorien gewährleiste, für die Microsoft gleiche Datensicherheitsstandards gewährleiste.

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

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

208

209

210 Ob Microsoft-Kunden im Rahmen spezifischer Lizenzverträge für unterschiedliche Sektoren oder
211 Vergütungsmodelle z.B. über Freifeldeintragungen Möglichkeiten zur Konkretisierung des von der
212 Auftragsverarbeitung betroffenen Personenkreises und der damit verbundenen Datenkategorien
213 eingeräumt sind, wurde weder von Microsoft selbst näher dargelegt noch war dies anderweitig
214 abschließend zu klären. Die allgemeine Version des „Microsoft-Kundenvertrages“¹⁶ lässt solche
215 Möglichkeiten jedenfalls nicht erkennen.

216 Vorbehaltlich anderweitiger Optionen im Rahmen des jeweiligen Lizenzvertrages über Microsoft 365
217 sind damit einzelfallbezogene Konkretisierungsmöglichkeiten des Gegenstands der
218 Auftragsverarbeitung auch weiterhin nicht erkennbar.

¹⁵ „Datenschutznachtrag“, S. 19

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

219 3.2.1.4. Bewertung

220 a) Prüfungsmaßstab

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

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

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

235 b) Detailbewertung

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

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

¹⁷ EDSA, Leitlinien 07/2020, Rn. 84.

¹⁸ EDSA, Leitlinien 07/2020, Rn. 113.

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

252 Dem steht gegenüber, dass mit Geltungsbeginn der DSGVO Verantwortliche und Auftragsverarbeiter
253 in höherem Maße Kooperationspflichten zur Gewährleistung datenschutzrechtlicher Anforderungen
254 unterworfen sind. So verlangt z.B. Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe f DSGVO im Rahmen der
255 Gewährleistung der Anforderungen von Art. 32 bis 36 DSGVO, dass der Auftragsverarbeiter den
256 Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung
257 stehenden Informationen unterstützt. Das Erfordernis spezifischer Informationen über den Kreis der
258 betroffenen Personen und der Kategorien betroffener Personen wird auch bei der im
259 „Datenschutznachtrag“¹⁹ vorgesehenen Anwendung der Standardvertragsklauseln 2021 deutlich, die
260 in ihrem Anhang I B²⁰ zur Beschreibung der Datenübermittlung hierzu genauere Angaben vorsehen.

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

277 3.2.1.5. Schlussfolgerungen

278 Ungeachtet des Zeitabstands und weiterer Besonderheiten entsprechen die dargestellten Befunde
279 hinsichtlich der Erforderlichkeit grundlegender Präzisierungen des Vertragsgegenstandes zur jüngsten
280 Fassung des „Datenschutznachtrags“ noch den im Juli 2020 veröffentlichten
281 Untersuchungsergebnissen²¹ 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.

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

290 Microsoft wird daher weiterhin empfohlen, zu überprüfen, wie eine kundenspezifische
291 Konkretisierung nach dem Vorbild des Anhangs II der Standardvertragsklauseln der Kommission gemäß
292 Art. 28 Abs. 7 DS-GVO²² erreicht werden kann. Gemeinsam mit den Verantwortlichen könnte auch
293 erwogen werden, entsprechend den Handlungsoptionen in der von verschiedenen Aufsichtsbehörden
294 genutzten „Checkliste zur Prüfung von Auftragsverarbeitungsverträgen“ z.B. Verweise auf ein
295 formgerecht in den Vertrag einzubeziehendes und hinreichend detailliertes Verzeichnis der
296 Verarbeitungstätigkeiten (VVT) des Verantwortlichen vorzusehen²³. Die bisher im Abschnitt
297 „Verarbeitung personenbezogener Daten; DSGVO — Verarbeitungsdetails“ aufgenommene
298 Erwähnung des Kunden-VVT²⁴ setzt ein solches Modell noch nicht hinreichend um, da die Bestimmung
299 rein deskriptiv auf das VVT verweist, aber keinen Prozess etabliert, in dem dieses für beiden Seiten
300 einseh- und nutzbar sowie formgerecht zum Vertragsgegenstand erhoben wird.

301 3.2.2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für 302 legitime Geschäftszwecke“

303 3.2.2.1. Feststellungen des AK Verwaltung

304 Die Untersuchung des AK Verwaltung vom 15. Juli 2020 hat sich eingehend mit den vertraglichen
305 Bestimmungen zu von Microsoft zunächst als „legitime Geschäftszwecke“ bezeichneten
306 Verarbeitungen befasst, die im Gesamtgefüge des Vertrages mit der Rolle Microsofts als
307 „unabhängiger Datenverantwortlicher“²⁵ neben die Auftragsverarbeitung treten. Diese
308 Verarbeitungstätigkeiten sind auch im Kontext der Löschung und Rückgabe personenbezogener Daten
309 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.

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

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

321 3.2.2.2. Aktueller Prüfungsgegenstand

322 Gegenüber der Fassung vom Januar 2020 findet sich im „Datenschutznachtrag“ vom 15. September
323 2022 eine begrifflich wie inhaltlich deutlich geänderte Bestimmung über die „Verarbeitung für
324 Geschäftstätigkeiten“.

325 Noch in der Version 09/2021 des „Datenschutznachtrags“ umfasste die Microsoft im Rahmen einer
326 eigenständigen Verantwortlichkeit unterschiedslos für sämtliche Kategorien personenbezogener
327 Daten²⁶ eingeräumte Verarbeitungsbefugnis

328 *„(1) Abrechnungs- und Kontoverwaltung;*

329 *(2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives);*

330 *(3) interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung,*
331 *Produktstrategie);*

332 *(4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-*
333 *Produkte betreffen könnten;*

334 *(5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder*
335 *Energieeffizienz; und*

336 *(6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im*
337 *Folgenden beschriebenen Beschränkungen für die Offenlegung verarbeiteter Daten).“*

338 Unbeschadet weiterer Anpassungen gilt ab 15. September 2022 eine in Struktur und Systematik
339 deutlich veränderte Umgrenzung von Verarbeitungen, deren Zuordnung als Teil der
340 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.

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

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

345 Der Kunde ermächtigt Microsoft:

346 (i) aggregierte statistische, nicht personenbezogene Daten aus Daten, die pseudonymisierte
347 Identifikatoren enthalten (z. B. Nutzungsprotokolle, die eindeutige, pseudonymisierte Identifikatoren
348 enthalten), zu erstellen; und

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

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

353 Diese Zwecke sind:

- 354 - Abrechnung und Kontoverwaltung;
- 355 - Vergütungen wie die Berechnung von Mitarbeiterprovisionen und Partneranreizen;
- 356 - internes Berichtswesen und Geschäftsmodellierung, wie z. B. Prognosen, Umsatz- und
357 Kapazitätsplanung und Produktstrategie; und
- 358 - Finanzberichterstattung.“

359 3.2.2.3. Gesprächsergebnisse

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

363 Auf Grundlage einer von Microsoft einer detaillierten Betrachtung der derzeitigen Geschäftsprozesse,
364 die in einer Matrix zusammengefasst wurden (Anlage 1 zu diesem Bericht) und einer in den Gesprächen
365 präsentierten Grafik über Datenflüsse (Anlage 2), konnten zwar grundlegende Fragen zur rechtlichen
366 Strukturierung dieser Verarbeitungsvorgänge letztlich auch mit Rücksicht auf abweichende
367 Beurteilungsmaßstäbe anderer europäischer Datenschutzaufsichtsbehörden nicht abschließend
368 geklärt und konnte keine Einigkeit über die rechtliche Einordnung erzielt werden. Gleichwohl haben
369 die Analysen den Impuls für eine geänderte und konkrete Grenzen²⁸ 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."

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

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

374 (1) Kundendaten,

375 (2) Diagnosedaten,

376 (3) Dienstgenerierten Daten,

377 (4) „Professional Service“-Daten (i.S.v. Microsoft-spezifischen Beratungs- und Supportleistungen),

378 (5) sonstigen Support-Daten.

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

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

386 • nur statistisch aggregierte Datensätze,

387 • nur mengenbezogene Kundendaten,

388 • keine Inhaltsdaten aus Kundendaten und „Professional Service Daten“

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

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

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

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

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

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

425 3.2.2.4. Bewertung

426 a) Prüfungsmaßstab

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

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

444 Ähnlich scheint auch die Untersuchung des EDPS – der letztlich sogar die datenschutzrechtliche
445 Begründbarkeit eines Outsourcings von Cloud-Diensten jedenfalls im Bereich der EU-Institutionen
446 insgesamt in Frage stellt²⁹ – das Vorliegen einer Rechtsgrundlage für die Einräumung solcher
447 Verarbeitungsbefugnisse des Auftragsverarbeiters im öffentlichen Bereich, zusätzlich aber auch die
448 Zweckkompatibilität zu verneinen.³⁰

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

460 Einen weiteren möglichen Prüfungsmaßstab zur Beurteilung der Verarbeitungs- bzw.
461 „Geschäftstätigkeiten“, die im „Datenschutznachtrag“ Microsoft als Verantwortlicher zugewiesen
462 werden, ergibt sich aus einer Veröffentlichung der französischen Aufsichtsbehörde CNIL vom
463 12. Januar 2022 unter dem Titel „Auftragsverarbeiter: die Weiterverwendung von Daten, die von
464 einem Verantwortlichen anvertraut werden“:³² Sie fordert dabei zusammengefasst, dass ein
465 Auftragsverarbeiter im Auftrag verarbeitete personenbezogene Daten nur dann zu seinen eigenen
466 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>.

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

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

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

489 b) Detailbewertung

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

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

497 wurden nicht in die Liste der Verarbeitungen für Microsofts Geschäftstätigkeiten übernommen.
498

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

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

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

510

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

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

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

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

526 Die Arbeitsgruppe geht dabei davon aus, dass die im Abschnitt über eigene „Geschäftstätigkeiten“
527 ausgesprochene „Ermächtigung³³“ des Auftragsverarbeiters zu bestimmten Datenverarbeitungen ihn
528 nicht im Sinne einer Weisung zu bestimmten Datenverarbeitungen verpflichtet. Sie räumt Microsoft
529 vielmehr eine Entscheidungsbefugnis jedenfalls über die Mittel der Datenverarbeitung im Rahmen
530 einvernehmlicher³⁴ vertraglicher Zwecksetzung ein. Daraus ergibt sich aus Sicht der Arbeitsgruppe,
531 dass Microsoft in diesem Bereich als Verantwortlicher und nicht als Auftragsverarbeiter tätig wird.³⁵
532 Diese Einordnung wird auch durch die Formulierung von Abs.2 Satz 1 des Abschnitts
533 „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.

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

536

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

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

555 Im Einzelnen ergibt sich daraus folgendes Bild:

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

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

564 Art. 32 DSGVO begründet einerseits die unmittelbare Verpflichtung des Auftragsverarbeiters,
565 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“.

566 Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe f) DSGVO die gesondert zu betrachtende⁴⁰ Verpflichtung, den
567 Verantwortlichen bei dem von diesen zu treffenden technischen und organisatorischen Maßnahmen
568 zu unterstützen, und die gesetzliche Verpflichtung aus Art. 32 DSGVO ist dem Auftragsverarbeiter nach
569 Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe c) DSGVO zudem vertraglich aufzuerlegen.

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

572 Mögliche Verarbeitungsbefugnisse im nicht-öffentlichen Bereich

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

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

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

591 Mögliche Verarbeitungsbefugnisse im öffentlichen Bereich

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

⁴⁰ EDSA, Leitlinien 07/2020, Rn. 135.

596 Bereichsspezifische Konkretisierungen wie etwa § 75c SGB V hinsichtlich der IT-Sicherheit von
597 Krankenhäusern⁴¹ spiegeln das Gebot der Gewährleistung der Funktionsfähigkeit der öffentlichen
598 Verwaltung wieder, aus dem unter den Bedingungen fortschreitender Digitalisierung öffentlicher
599 Aufgabenerfüllung die Verpflichtung abzuleiten ist, interne IT-Systeme genauso wie eGovernment-
600 Angebote für Bürgerinnen und Bürger mit risikoangemessenen Maßnahmen gegen manipulative
601 Nutzung und Angriffe auf ihre Funktionsfähigkeit oder auf die mit ihnen verarbeiteten Daten zu
602 schützen.

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

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

613 Bereichsübergreifende Fragestellungen

614 Anders als im Rahmen der Verarbeitungen zu Microsofts Geschäftstätigkeiten und über die von
615 Microsoft im Rahmen der Gespräche erläuterten tatsächlichen Verarbeitungsprozesse⁴² hinaus, fehlen
616 im Datenschutznachtrag 09/2022 Ausschlussstatbestände, die den Umfang der für Verarbeitungen zu
617 Zwecken der „Verbesserung der Sicherheit“⁴³ genutzten Daten begrenzen: Soweit diese als Teil der
618 weisungsgebundenen Auftragsverarbeitung stattfinden, gestattet der Abschnitt „Verarbeitung zur
619 Bereitstellung der Produkte und Services für Kunden“ auch die Einbeziehung von Inhalten der
620 Kundendaten und schließt Nutzungen von Verhaltensdaten der Kunden zur Beobachtung des
621 Nutzerverhaltens oder hierzu Inhaltsdaten zu verwenden bzw. heranzuziehen oder neue Daten zu
622 erzeugen nicht aus.

623 Soweit nicht aus spezialgesetzlichen Aufgabenzuweisungen wie § 75c SGB V weitergehende
624 Verarbeitungsbefugnisse abgeleitet werden können, ergibt sich hieraus potentiell eine Verarbeitung,
625 für die jedenfalls im öffentlichen Bereich oder bei nach Art. 9 DSGVO besonders geschützten Daten
626 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“

627 Hinzu kommt für den öffentlichen und nicht öffentlichen Bereich:

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

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

640 ii) Erfüllung rechtlicher Verpflichtungen als Teil weisungsgebundener Auftragsverarbeitung

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

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

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

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

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

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

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

679 Der „Datenschutznachtrag“ 09/2022 greift diese Diskussionen zwar mit einer grundlegenden
680 Umgestaltung des Abschnitts über Verarbeitungen personenbezogener Daten für Microsofts
681 „Geschäftstätigkeiten“ auf, vollzieht aber im Ergebnis keinen grundlegende dogmatische
682 Neuausrichtung zur Rolle bzw. datenschutzrechtlichen Verantwortlichkeit Microsofts für diese
683 Verarbeitungen: Die nunmehr vorgesehene Klausel ist mit ihrer zentralen, aber auch mehrdeutigen
684 Formulierung „authorize“ nach Auffassung der Arbeitsgruppe nicht geeignet (und nach den
685 Festlegungen im Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und
686 Verantwortlichkeiten“ auch ersichtlich nicht dazu gedacht),⁴⁵ eine Verarbeitung personenbezogener
687 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 independent data controller 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“

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

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

708 Darüber hinaus gilt:

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

718 Anders als im vorstehend beschriebenen Modell (vgl. Zeile 639 ff.) eng weisungsgebundener
719 Verarbeitungen zu Vertragsdurchführungszwecken werden Verantwortliche in der nun vorliegenden
720 Ausgestaltung der Einräumung einer Verarbeitungsbefugnis des Auftragnehmers zumindest an
721 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

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

724 3.2.2.5. Schlussfolgerungen

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

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

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

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

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

772 3.2.3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher 773 Verpflichtungen, CLOUD Act, FISA 702

774 3.2.3.1. Feststellungen des AK Verwaltung

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

784 3.2.3.2. Aktueller Prüfungsgegenstand

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

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

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

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

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

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

811 Für die Verarbeitung personenbezogener Daten, die der DSGVO unterliegen, zu eigenen
812 Geschäftstätigkeiten von Microsoft im Zusammenhang mit der Leistungserbringung⁴⁸ verpflichtet sich
813 Microsoft als datenschutzrechtlich Verantwortlicher zudem zu weiteren Schutzmaßnahmen.⁴⁹ Diese
814 weiteren Schutzmaßnahmen im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ umfassen
815 Verpflichtungen zur Verweisung anfragender Dritter an den Kunden, zur Benachrichtigung unter
816 bestimmten Bedingungen, zur Anfechtung von Aufforderungen zur Offenlegung unter bestimmten
817 Bedingungen (im Wesentlichen unter der Voraussetzung der Rechtswidrigkeit der Anfrage nach dem
818 Recht der anfragenden Stelle) und zur Leistung von Entschädigungen unter bestimmten
819 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“.

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

822 3.2.3.3. Gesprächsergebnisse

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

845 Im Rahmen der Gespräche über den US-amerikanischen CLOUD Act und der Vorstellung des „EU Data
846 Boundary“-Projekts wies Microsoft unter Verweis auf das US-Justizministerium darauf hin, dass der
847 CLOUD Act nur klarstelle, dass US-Behörden Daten anfordern können, die sich im Besitz (possession),
848 im Gewahrsam (custody) oder unter der Kontrolle (control) einer der US-Gerichtsbarkeit
849 unterliegenden Einrichtung befinden, auch wenn diese Daten nicht in den USA gespeichert sind. Es
850 handle sich dabei nicht um eine Ausweitung der Befugnisse, sondern um eine Kodifizierung des bereits
851 bestehenden Rechts.⁵¹ Aus den Erläuterungen Microsofts kann entnommen werden, dass diese
852 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.

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

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

862 3.2.3.4. Bewertung

863 a) Prüfungsmaßstab

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

868 Nach Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO muss der zwischen dem Verantwortlichen und
869 dem Auftragsverarbeiter zu schließende Vertrag bzw. das andere Rechtsinstrument insbesondere
870 vorsehen, dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung
871 des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten in⁵³ ein
872 Drittland oder an eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der
873 Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in
874 einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen
875 Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht
876 wegen eines wichtigen öffentlichen Interesses verbietet. Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe g
877 DSGVO verlangt eine Regelung, dass der Auftragsverarbeiter nach Abschluss der Erbringung der
878 Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder
879 löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder
880 dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten
881 besteht; weitere Fragestellungen hierzu werden im Abschnitt „Löschung“ behandelt.

882 Art. 48 DSGVO hält fest, dass unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V,
883 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“.

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

886 b) Detailbewertung

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

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

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

903 Hinsichtlich der Frage einer Verarbeitung durch Microsoft auf Basis von Drittlands-Recht außerhalb der
904 Weisungen des Kunden enthält zwar der Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“
905 des „Datenschutznachtrags“ eine Regelung, die eine strikte Weisungsbindung für Microsoft vorsieht,
906 die sogar noch über die Weisungsbindung in Anlage 1 Ziff. 2 a) des „Datenschutznachtrags“
907 hinausgeht, weil sie keine Einschränkungen vorsieht (vom bereits angesprochenen weitgehenden
908 Unterstellen unter das Vertragsänderungsverfahren abgesehen). Allerdings enthält der Abschnitt
909 „Offenlegung verarbeiteter Daten“ für spezifische Verarbeitungen, namentlich Offenlegungen,
910 spezifischere Regelungen, die ersichtlich auch unter Anwendbarkeit der DSGVO gelten sollen, wie die
911 im „Datenschutznachtrag“ September 2022 erfolgte Einfügung, die auf Art. 23 DSGVO Bezug nimmt,
912 zeigt. In Ermangelung einer klaren Konkurrenz- bzw. Hierarchieregelung bleibt daher auch hier
913 unauflösbar, welche der drei unterschiedlichen Regelungen Geltung beansprucht, was im Hinblick auf
914 die Rechenschaftspflicht der Verantwortlichen (Art. 5 Abs. 2 DSGVO) zu der Bewertung führt, dass
915 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.

916 Offenlegungen der im Auftrag verarbeiteten Daten gestattet der Abschnitt „Offenlegung verarbeiteter
917 Daten“ bereits, wenn diese rechtlich vorgeschrieben oder im „Datenschutznachtrag“ beschrieben sind.
918 Solche Offenlegungen sind nicht auf Weisungen des Verantwortlichen beschränkt, sodass sie vor dem
919 Hintergrund des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a) DSGVO nur zulässig sind, wenn sie sich auf
920 Verpflichtungen aus dem Unions- oder mitgliedstaatlichen Recht, dem Microsoft unterliegt,
921 beschränken. Dies ist nicht der Fall. Selbst wenn man eine teleologische Reduktion der erforderlichen
922 Weisungsbindung in Anlehnung an Art. 23 Abs. 1 DSGVO vornehmen würde – anders aber die EU-
923 Kommission in den Standardvertragsklauseln für Auftragsverarbeitungsverträge und auch in den
924 Standardvertragsklauseln für Datenexporte nur hinsichtlich der Zusicherungen in Klausel 14 –, würde
925 die von Microsoft eingefügte Klausel, die auf Art. 23 DSGVO Bezug nimmt, aufgrund ihrer
926 systematischen Stellung und der Abgrenzung im folgenden Wortlaut⁵⁶ einerseits nur für
927 Offenlegungen gegenüber Strafverfolgungsbehörden gelten (und nicht etwa für die vom EuGH in
928 „Schrems II“ als problematisch bewerteten Befugnisse von US-Geheimdiensten nach FISA 702). Der
929 von Microsoft vertretenen Auffassung, die neu aufgenommene Regelung zur Notwendigkeit und
930 Verhältnismäßigkeit beziehe sich auf sämtliche Offenlegungen, also auch gegenüber Geheimdiensten,
931 vermag die Arbeitsgruppe vor dem Hintergrund der systematischen Stellung und des eindeutig
932 abgrenzenden Wortlauts „sonstige Anfragen von Dritten“ nicht zu folgen. Andererseits betrifft die
933 Klausel nur die Frage von Verarbeitungen auf der Basis von Drittlands-Recht, nicht aber die Erlaubnis
934 für alle weiteren im Datenschutz-Nachtrag beschriebenen Offenlegungen. Der „Datenschutznachtrag“
935 beschreibt im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ ausdrücklich Offenlegungen
936 personenbezogener Daten „unter Verletzung der Verpflichtungen von Microsoft gemäß Kapitel V der
937 DSGVO“. Die Abweichung vom Wortlaut der Klausel 14 der Standardvertragsklauseln für Datenexporte
938 durch Einfügung eines „gegebenenfalls“⁵⁷ wirft ebenfalls Fragen auf, ob hierdurch eine inhaltliche
939 Abweichung vom Maßstab der Standardvertragsklauseln beabsichtigt ist.

940 ii. Drittlands-Recht, Art. 48 DSGVO

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

944 iii. FISA 702 und CLOUD Act

945 Die Microsoft Corporation ist ein US-amerikanisches Unternehmen, das „electronic communication
946 service provider“ im Sinne von 50 U.S.C. § 1881(b)(4) ist. Unter diesen Begriff fallen
947 Telekommunikationsunternehmen, Anbieter von elektronischen Kommunikationsdiensten („ECS“),
948 Anbieter von „remote computing services“ („RCS“), also Computerspeicher- oder -
949 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).

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

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

959 Von besonderer Bedeutung ist hier Section 702 des Foreign Intelligence Surveillance Act (FISA 702 =
960 50 U.S.C. § 1881a), da der EuGH diese Norm im Urteil „Schrems II“⁶¹ im Detail bewertet und für nicht
961 mit den europäischen Grundrechten vereinbar erklärt hat. Diese Bewertung ist weiterhin
962 entscheidend, da hinsichtlich der Kritikpunkte des EuGH bis zum für diesen Bericht maßgeblichen
963 Zeitpunkt keine Änderungen der Rechtslage festzustellen sind. Was die in der Executive Order⁶²
964 vorgesehenen Änderungen angeht, so sind diese erst noch umzusetzen, unbeschadet der Frage, ob sie
965 den Anforderungen des europäischen Datenschutzrechts überhaupt hinreichend Rechnung tragen.
966 FISA 702 ermöglicht es US-Behörden, von jedem „electronic communication service provider“ im Sinne
967 von 50 U.S.C. § 1881(b)(4) unter den gesetzlichen Voraussetzungen die Herausgabe von Informationen
968 wie personenbezogenen Daten zu verlangen.⁶³ Die Arbeitsgruppe entnimmt den Erläuterungen von
969 Microsoft⁶⁴, dass jedenfalls das US-Justizministerium davon auszugehen scheint, dass FISA 702
970 extraterritorial anwendbar sei, also auch, wenn Daten durch ein FISA 702 unterfallendes Unternehmen
971 oder eine Tochtergesellschaft dieses Unternehmens etwa in der EU verarbeitet werden.⁶⁵ Betroffen
972 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/Vladeck_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/Vladeck_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/Vladeck_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/Vladeck_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.

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

975 Auch der CLOUD Act ist in diesem Zusammenhang als extraterritoriale Zugriffsmöglichkeit für US-
976 Behörden auf in der EU verarbeitete Daten zu nennen, wird hier nicht untersucht, da der Arbeitsgruppe
977 keine Bewertung dieses strafrechtlichen Regelwerks und ggf. weiterer in diesem Zusammenhang zu
978 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 1.5.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 1.2,
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>.

979 iv. Anwendbarkeit des Kapitels V DSGVO auf Datenverarbeitungen in der EU
980 Aus einer extraterritorialen Anwendbarkeit des US-Rechts wird teilweise gefolgert, dass bereits in der
981 Offenlegung an ein diesem Recht unterliegendes Unternehmen – etwa einen Auftragsverarbeiter –
982 eine Übermittlung in ein Drittland liege.⁶⁹

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

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

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

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

996 Nach Art. 28 Abs. 1 und ErWG 81 DSGVO dürfen Verantwortliche nur solche Auftragsverarbeiter
997 einschalten, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen –
998 hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die
999 Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen der DSGVO genügen. Die
1000 Darlegungs- und Beweislast hierfür liegt, wie bereits die eine Ausnahme regelnde Formulierung „nur“
1001 zeigt, beim Verantwortlichen. Ebenfalls betrifft die Frage, ob der Auftragsverarbeiter hinreichende
1002 Garantien bietet, die Rechtmäßigkeit der Verarbeitung und damit einen Umstand, für den den
1003 Verantwortlichen die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO trifft. Die Rechenschaftspflicht
1004 stellt nicht nur eine Pflicht des Verantwortlichen dar, sondern auch eine Beweislastregelung.⁷⁰

1005 Bei einem Auftragsverarbeiter, der Regelungen wie dem CLOUD Act oder ggf. FISA 702 unterliegt,
1006 besteht ein näher zu betrachtendes Risiko, dass er im Fall eines Konflikts der Rechtsordnungen seinem
1007 Heimatrecht folgt und nicht der DSGVO, insbesondere, wenn dieses – wie im vorliegenden Fall – unter
1008 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.

1009 Regel nicht einmal von den betroffenen Personen oder den europäischen Aufsichtsbehörden entdeckt
1010 werden kann.

1011 Wie oben unter Abschnitt iii) ausgeführt, besteht das Risiko, dass FISA 702 auch auf EU-
1012 Tochtergesellschaften von US-Unternehmen, die FISA 702 unterliegen, anwendbar ist. Die
1013 Verarbeitung durch eine EU-Tochtergesellschaft als Auftragsverarbeiter genügt mithin – unabhängig
1014 von der Frage, ob die Muttergesellschaft möglicherweise als Unterauftragsverarbeiter einbezogen ist
1015 – für sich genommen nicht, um eine Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO zu erreichen.

1016 Aus den vorliegenden Erläuterungen und Analysen etwa von Microsoft,⁷¹ Prof. Vladeck⁷² und des
1017 Wissenschaftlichen Dienstes des Bundestages⁷³ sowie der dort zitierten Autoren ergeben sich starke
1018 Hinweise dafür, dass FISA 702 extraterritorial anwendbar ist. Unabhängig davon, ob die
1019 extraterritoriale Anwendbarkeit von FISA 702 als nachgewiesen angesehen wird oder von einem
1020 dahingehenden Risiko ausgegangen wird, liegt, wie bereits ausgeführt, die Darlegungs- und Beweislast
1021 für das Vorliegen der Voraussetzungen des Art. 28 Abs. 1 DSGVO beim Verantwortlichen. Ob die
1022 extraterritoriale Anwendbarkeit von FISA 702 als nachgewiesen anzusehen ist oder nur nicht
1023 hinreichend sicher ausgeschlossen werden kann, ist daher für die Bewertung der Zuverlässigkeit des
1024 Auftragsverarbeiters im Sinne von Art. 28 Abs. 1 DSGVO nicht ausschlaggebend.

1025 Mithin sind in solchen Fällen weitere technische und organisatorische Maßnahmen zu ergreifen, die
1026 die Einhaltung der DSGVO hinreichend garantieren. Um hinreichende Garantien im Sinne des Art. 28
1027 Abs. 1 DSGVO darzustellen, müssen die Maßnahmen genau diejenigen Defizite der Rechtslage oder -
1028 praxis des drittstaatlichen Rechts ausgleichen, die zu der mangelnden Zuverlässigkeit des
1029 Auftragsverarbeiters geführt haben, d.h. genau die identifizierten Rechtsschutzlücken schließen.⁷⁴
1030 Konkret bedeutet dies, dass die Maßnahmen sicher verhindern, dass potentielle
1031 Herausgabeanordnungen nach FISA 702 erfüllt werden.

1032 Aufgrund der bestehenden gesellschaftsrechtlichen Befugnisse der Muttergesellschaft – und sei es nur
1033 zur Auswechslung einer lokalen Geschäftsführung, die sich unter Verweis auf die DSGVO weigert,
1034 Daten herauszugeben – und aufgrund des Umstandes, dass auch die Geschäftsführer der
1035 Tochtergesellschaft persönlich Verpflichtete nach FISA 702 sind,⁷⁵ denen im Weigerungsfall persönlich
1036 Sanktionen drohen, ist die datenschutzrechtliche Zuverlässigkeit einer EU-Tochtergesellschaft im Sinne
1037 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)

1038 anders zu bewerten als die der US-Muttergesellschaft. Eine besondere Schwierigkeit ergibt sich, wenn
1039 die Muttergesellschaft die verwendete Software liefert und sich faktisch darüber den gewünschten
1040 Zugriff verschaffen kann. Ist die Muttergesellschaft über Administration und Support in die
1041 Leistungserbringung eingebunden, hat sie die Zugriffsmöglichkeiten ohnehin regelmäßig.

1042 Welche Maßstäbe an technische oder organisatorische Maßnahmen zur Gewährleistung der nach
1043 Art. 28 Abs. 1 DSGVO erforderlichen Zuverlässigkeit zu stellen sind, ist bislang weder durch die
1044 europäischen Datenschutzaufsichtsbehörden noch durch die Rechtsprechung abschließend geklärt.
1045 Vereinzelt wird ein Rückgriff Verantwortlicher auf die Empfehlungen 01/2020 des Europäischen
1046 Datenschutzausschusses für sachgerecht angesehen.⁷⁶ Dabei ist allerdings zu beachten, dass diese für
1047 den Kontext von Datenübermittlungen in Drittländer konzipiert worden sind. Die Empfehlungen
1048 01/2020 bilden mit der Analyse des einschlägigen Drittlands-Rechts (und, soweit dieses nicht schon
1049 problematisch ist, der Praxis), der Identifikation der eine Datenschutz-Compliance verhindernden
1050 Umstände und der Suche nach ergänzenden Maßnahmen, die genau die identifizierten
1051 Unzulänglichkeiten ausgleichen, diejenigen Schritte ab, die zur Erfüllung von Art. 28 Abs. 1 DSGVO
1052 erforderlich sind.

1053 Die als Microsoft 365 angebotenen Dienste erfordern in vielen Anwendungsfällen den Zugriff von
1054 Microsoft auf Klardaten.⁷⁷ Insbesondere die naheliegende Verschlüsselung verarbeiteter Daten, die
1055 einen Zugriff von Microsoft und damit der US-Behörden verhindern würde, ist regelmäßig nicht
1056 möglich, wenn die Daten beispielsweise im Browser angezeigt werden müssen. Die vorliegend
1057 gegebene Gestaltung, dass der Empfänger der Daten diese im Klartext verarbeiten muss, hat der
1058 Europäische Datenschutzausschuss als Anwendungsfall 6 des Anhangs 2 der Empfehlungen 01/2020
1059 beschrieben. Für diesen Anwendungsfall ist es den Aufsichtsbehörden – im Hinblick auf
1060 Datenübermittlungen – nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer
1061 Rechtmäßigkeit des Datenexports führen könnten. In der entsprechenden Anwendung im Rahmen der
1062 Auftragsverarbeitung bedeutet dies, dass besonders kritisch zu prüfen ist, wie den Anforderungen des
1063 Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann. Ausreichende zusätzliche
1064 Schutzmaßnahmen konnte der Europäische Datenschutzausschuss nur in bestimmten, begrenzten
1065 Anwendungsfällen identifizieren. Konkret anzuführen wären die Anwendungsfälle 1
1066 (Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten
1067 erfordern), 2 (Übermittlung pseudonymisierter Daten) und 5 (Aufgeteilte Verarbeitung oder
1068 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.

1069 01/2020 des Europäischen Datenschutzausschusses, soweit die dort aufgestellten Bedingungen
1070 eingehalten werden.

1071 Die von Microsoft im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ zugesagten Maßnahmen sind
1072 nicht geeignet, die nach der Rechtsprechung des EuGH gemessen an den EU-Grundrechten
1073 bestehenden Unzulänglichkeiten des US-amerikanischen Rechts auszugleichen. Am ehesten mag noch
1074 die Verpflichtung zur Anfechtung von Herausgabeanordnungen als ergänzende Schutzmaßnahme in
1075 Betracht kommen. Doch besteht diese Verpflichtung zur Anfechtung nur, wenn die
1076 Herausgabeanordnung nach demjenigen Recht unzulässig ist, dem die Behörde bzw. das Gericht
1077 unterliegt, die bzw. das die Herausgabe anordnet, wozu auch relevante Konflikte mit dem
1078 anwendbaren EU- oder mitgliedstaatlichen Recht gehören. Da aber FISA 702, wie der EuGH
1079 festgestellt hat,⁷⁸ keine inhaltliche Begrenzung der Überwachungsbefugnisse vorsieht und FISA 702
1080 unterliegende Unternehmen die Anwendung dieser Norm nicht mit dem Argument abwenden können,
1081 dadurch würde EU- oder mitgliedstaatliches Recht verletzt⁷⁹, ist nicht erkennbar, wie eine Verletzung
1082 des in Art. 52 EU-Grundrechtecharta geregelten Grundsatzes der Verhältnismäßigkeit durch eine
1083 solche Herausgabeanordnung auf diesem Wege erfolgreich geltend gemacht werden könnte.
1084 Dementsprechend sehen die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses
1085 derartige Maßnahmen auch nur als Ergänzung anderer Maßnahmen vor.⁸⁰ Darüber hinaus gelten die
1086 Verpflichtungen im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ gemäß der Einbeziehungsklausel im
1087 Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ nur für
1088 Verarbeitungen im Rahmen der „Geschäftstätigkeiten“ von Microsoft, die dort im zweiten Absatz
1089 geregelt sind, auf den sich der Verweis beschränkt. Die eigentliche Auftragsverarbeitung ist mithin
1090 nicht abgedeckt. Auch die von Microsoft vorgesehenen Maßnahmen für die Speicherung der Daten
1091 (data at rest) genügen nicht, da die weitergehende Verarbeitung bei vielen der in Microsoft 365
1092 enthaltenen Dienste technisch zwingend im Klartext erfolgen muss.

1093 Die Arbeitsgruppe weist darauf hin, dass nach der Rechtsprechung des Bundesverwaltungsgerichts aus
1094 der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auch eine Beweislastverteilung folgt,⁸¹ so dass
1095 Verantwortliche bereits unabhängig von der implizit durch die Regel-Ausnahme-Formulierung des
1096 Art. 28 Abs. 1 DSGVO die Erfüllung der Anforderungen des Art. 28 Abs. 1 DSGVO zweifelsfrei
1097 nachweisen können müssen.

1098 Insofern ergeben sich relevante Abweichungen von den Beurteilungsmaßstäben des Vergaberechts.
1099 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/Vladeck_Rechtsgutachten_DSK_en.pdf.

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

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

1100 seine vertraglichen Zusagen erfüllen wird.⁸² Er muss seine (Auftragsverarbeitungs-)Verträge mit
1101 Unterauftragnehmern so ausgestalten, dass diese die gestellten (datenschutzrechtlichen)
1102 Anforderungen erfüllen.⁸³ Nach einer OLG-Ansicht erst, nach anderer OLG-Ansicht jedenfalls wenn sich
1103 konkrete Anhaltspunkte dafür ergeben, dass die Erfüllung der vertraglichen Zusagen zweifelhaft ist, ist
1104 der öffentliche Auftraggeber gehalten, durch Einholung ergänzender Informationen die Erfüllbarkeit
1105 des Leistungsversprechens beziehungsweise die hinreichende Leistungsfähigkeit des Bieters zu
1106 prüfen.⁸⁴ Das OLG Karlsruhe vertritt in einem Vergabenaachprüfungsverfahren ohne Begründung die
1107 Ansicht, dass der öffentliche Auftraggeber nicht allein aufgrund der Tatsache, dass ein
1108 Unterauftragsverarbeiter (hier: AWS) ein Tochterunternehmen eines US-amerikanischen Konzerns ist,
1109 an der Erfüllbarkeit des Leistungsversprechens zweifeln müsse.⁸⁵ Auch wenn der
1110 Unterauftragsverarbeiter üblicherweise unzureichende Auftragsverarbeitungsverträge abschließe,
1111 stelle dies keine konkreten Anhaltspunkte dafür dar, dass dies entgegen den Zusagen des Bieters auch
1112 im konkreten Fall so geschehen werde.⁸⁶ Dies lässt sich wegen der vollständig abweichenden
1113 Maßstäbe – vollständige Nachweispflicht im Datenschutzrecht im Vergleich zum Erfordernis konkreter
1114 Anhaltspunkte für Zweifel an der Erfüllbarkeit des vertraglichen Leistungsversprechens als
1115 Voraussetzung einer vergaberechtlichen Verpflichtung (nicht eines Rechts) zur Überprüfung – nicht mit
1116 den datenschutzrechtlichen Anforderungen vergleichen. Zwar ist der öffentliche Auftraggeber
1117 vergaberechtlich nicht verpflichtet, die schriftlichen Angaben der Bieter anlasslos zu verifizieren.
1118 Dennoch darf er von seinem Recht zur Überprüfung auch ohne besonderen Anlass Gebrauch
1119 machen.⁸⁷ Vor dem Hintergrund ihrer datenschutzrechtlichen Verpflichtungen sollten Verantwortliche
1120 von ihrem Recht zur Überprüfung nach Ansicht der Arbeitsgruppe auch Gebrauch machen.

1121 3.2.3.5. Schlussfolgerungen

1122 Die Weisungsbindung Microsofts genügt nicht den gesetzlichen Mindestanforderungen gemäß Art. 28
1123 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO. Dies gilt selbst dann, wenn man die Vorschrift teleologisch
1124 analog Art. 23 Abs. 1 DSGVO reduziert. Microsoft sollte auch hier den Datenschutznachtrag
1125 grundlegend strukturell überarbeiten und eine eindeutige, umfassende und widerspruchsfreie
1126 Regelung treffen, die die gesetzlichen Anforderungen erfüllt. Insbesondere wäre es empfehlenswert,
1127 den offenbar auf Basis der Kritik der deutschen Aufsichtsbehörden bereits durch Microsoft
1128 eingeschlagenen Weg konsequent zu Ende zu gehen und Durchbrechungen der Weisungsbindung nur
1129 noch dann vorzusehen, wenn die DSGVO diese auch gestattet, nicht aber etwa bereits, wenn der
1130 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.

1131 Nach Einschätzung der Arbeitsgruppe - und vorbehaltlich einer Meinungsbildung auf europäischer
1132 Ebene - führt die extraterritoriale Anwendbarkeit von US-Recht, insbesondere des CLOUD Acts sowie
1133 ggf. von FISA 702, für sich genommen (also das bloß bestehende Zugriffsrisiko) noch nicht zu einer
1134 Übermittlung personenbezogener Daten in ein Drittland, mithin noch nicht zur Anwendbarkeit des
1135 Kapitels V DSGVO. Allerdings kann sie dazu führen, dass solchen Rechtsvorschriften unterliegenden
1136 Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, soweit er – oder auch
1137 der Verantwortliche – nicht technische und/oder organisatorische Maßnahmen ergriffen hat, die
1138 hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt,
1139 insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen
1140 die Weisung des Verantwortlichen angeht, im Speziellen auf der Grundlage von Verpflichtungen aus
1141 drittstaatlichem Recht.

1142 Die zu ergreifenden technischen und organisatorischen Maßnahmen müssen dabei die konkreten
1143 Risiken aufgrund des extraterritorial geltenden Rechts ausgleichen. Im konkreten Fall müssen die
1144 Maßnahmen also verhindern, dass Microsoft Herausgabeverlangen nach extraterritorial geltendem
1145 US-amerikanischem Recht, deren Erfüllung nach EU-Recht nicht nachweisbar zulässig ist, nachkommen
1146 kann. Um diese Anforderungen zu erfüllen, können Verantwortliche die Maßstäbe der Empfehlungen
1147 01/2020 des Europäischen Datenschutzausschusses heranziehen. Dabei ist allerdings zu beachten,
1148 dass diese für den Kontext von Datenübermittlungen an Drittländer konzipiert worden sind.

1149 Die Nutzung von Microsoft 365 erfordert allerdings in vielen Anwendungsfällen den Zugriff von
1150 Microsoft auf Klardaten. Dies entspricht dem Anwendungsfall 6 des Anhangs 2 der Empfehlungen
1151 01/2020 des Europäischen Datenschutzausschusses. Für diesen Anwendungsfall ist es den
1152 Aufsichtsbehörden im Hinblick auf Datenübermittlungen nicht gelungen, ergänzende
1153 Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten.
1154 Entsprechend ist auch beim Einsatz von Microsoft 365 besonders kritisch zu prüfen, wie den
1155 Anforderungen des Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann.

1156 Die Arbeitsgruppe regt an, die Entwicklung von Modellen zu unterstützen, in denen Dritte als Betreiber
1157 bzw. Treuhänder eingesetzt werden, bei denen rechtssicher extraterritoriale
1158 Offenlegungsverpflichtungen ausgeschlossen werden können.

1159 Unabhängig davon empfiehlt die Arbeitsgruppe den Mitgliedern der DSK auf eine einheitliche
1160 Auslegung der DS-GVO hinsichtlich der Auswirkungen extraterritorial wirkender behördlicher
1161 Zugriffsbefugnisse in drittstaatlichem Recht hinzuwirken. Hierzu sollte das Thema in die zuständigen
1162 Gremien auf nationaler und europäischer Ebene eingebracht werden.

1163 3.2.4. Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32
1164 DSGVO

1165 3.2.4.1. Feststellungen des AK Verwaltung

1166 Der AK Verwaltung kritisiert, dass die zum Zeitpunkt seiner Untersuchung geltenden Vertragstexte zur
1167 Auftragsverarbeitung vor Vertragsschluss keine hinreichende Prüfung der für die beabsichtigte
1168 Tätigkeit bereitgestellten technischen und organisatorischen Maßnahmen durch den
1169 Verantwortlichen erlauben. Alleine die damalige Darstellung zu den technischen und
1170 organisatorischen Maßnahmen in den Vertragsunterlagen reiche für den Verantwortlichen nicht aus,
1171 um eine objektive Einschätzung zu treffen, ob die Maßnahmen dem Risiko angemessen sind und sei
1172 zudem nicht prüffähig.

1173 3.2.4.2. Aktueller Prüfungsgegenstand

1174 Gegenüber der Fassung des „Datenschutznachtrags“, die der Untersuchung des AK Verwaltung zu
1175 Grunde lag, enthält die ab 15. September 2022 geltende Version eine Ergänzung (Hervorhebung durch
1176 Verf.):

1177 *„Darüber hinaus müssen diese Maßnahmen den Anforderungen der ISO 27001, ISO 27002 und ISO
1178 27018 entsprechen. Eine Beschreibung der Sicherheitskontrollen für diese Anforderungen steht Kunden
1179 zur Verfügung.“*

1180 Im Übrigen enthält der „Datenschutznachtrag“ in Anhang A auch in seiner Fassung vom 15. September
1181 2022 eine auf bestimmte Datenkategorien, nämlich Kundendaten in „Core-Onlinediensten“ und
1182 nunmehr auch „Professional Services-Daten“⁸⁸ ausdrücklich beschränkte Garantie- von
1183 Datensicherheitsmaßnahmen:

1184 *„Anhang A – Sicherheitsmaßnahmen*

1185 *Microsoft hat für Kundendaten in den Core-Onlinediensten und für Professional Services-Daten die
1186 folgenden Sicherheitsmaßnahmen getroffen, die in Verbindung mit den Sicherheitsverpflichtungen in
1187 diesem DPA (einschließlich der DSGVO-Bestimmungen) die einzige Verantwortung von Microsoft in
1188 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.

1189 3.2.4.3. Gesprächsergebnisse

1190 Microsoft hat in seiner Stellungnahme vom 11. Dezember 2020 und in ergänzenden Gesprächen
1191 darauf hingewiesen, dass die Microsoft-Website servicetrust.microsoft.com („Servicetrust Website“)
1192 umfassende Informationen zur Dokumentation und Überprüfung der von Microsoft umgesetzten
1193 technischen und organisatorischen Maßnahmen vermittele. Insgesamt gesehen ermögliche dieses
1194 Informationsangebot Kunden sowohl die Durchführung einer Due-Diligence-Prüfung der in den
1195 Diensten umgesetzten Datenschutzmaßnahmen vor dem Einsatz als auch die Überwachung und
1196 Sicherstellung der laufenden Durchführung dieser Maßnahmen durch Microsoft im Betrieb. Wegen
1197 der geheimhaltungsbedürftigen Inhalte sei eine Authentisierung (Anmeldung mittels Logins)
1198 erforderlich, die ein Interessent über ein kostenloses Testkonto erlangen könne. Alle Nutzer, die mit
1199 einem bestehenden Kunden verbunden sind, hätten, so Microsoft, Zugang zu diesen Unterlagen.

1200 3.2.4.4. Bewertung

1201 a) Prüfungsmaßstab

1202 In Konkretisierung der Anforderungen von Art. 28 Abs. 1 und Abs. 3 UAbs. 1 Satz 2 Buchstaben c) und
1203 f) DSGVO sollten Verantwortliche entsprechend den Leitlinien des Europäischen
1204 Datenschutzausschusses 07/2020 im Auftragsverarbeitungsvertrag eine Reihe grundlegender
1205 Anforderungen festlegen oder auf diese verweisen, nämlich [redaktionell durch Verf. angepasst]⁸⁹

- 1206 • *„die zu ergreifenden Sicherheitsmaßnahmen,*
1207 • *eine Verpflichtung des Auftragsverarbeiters, die Zustimmung des Verantwortlichen einzuholen,*
1208 • *bevor er Änderungen vornimmt, und*
1209 • *eine regelmäßige Überprüfung der Sicherheitsmaßnahmen, um deren Angemessenheit im Hinblick*
1210 • *auf Risiken, die sich im Laufe der Zeit entwickeln können, zu gewährleisten.*

1211 *Die Informationen über die in den Vertrag aufzunehmenden Sicherheitsmaßnahmen müssen so*
1212 *detailliert sein, dass der Verantwortliche die Angemessenheit der Maßnahmen gemäß Artikel 32*
1213 *Absatz 1 DSGVO beurteilen kann. Darüber hinaus ist die Beschreibung auch erforderlich, damit der*
1214 *Verantwortliche seiner Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO in Bezug*
1215 *auf die dem Auftragsverarbeiter auferlegten Sicherheitsmaßnahmen nachkommen kann.“*

1216 Selbst wenn nach Art. 28 Abs. 3 UAbs. 1 S. 2 Buchst. c) DSGVO auch eine pauschale Verpflichtung des
1217 Auftragsverarbeiters zur Einhaltung der Anforderungen des Art. 32 DSGVO genügen sollte, muss der
1218 Verantwortliche doch jederzeit in der Lage sein nachzuweisen, dass die Anforderungen des Art. 32
1219 DSGVO vollumfänglich und für sämtliche verarbeiteten personenbezogenen Daten eingehalten
1220 werden.

1221 b) Detailbewertung

⁸⁹ EDSA, Leitlinien 07/2020, Rn. 126

1222 Mit der Bereitstellung eines Gastzugangs eröffnet Microsoft für Verantwortliche des nichtöffentlichen
1223 und öffentlichen Bereichs den Zugang zu einer⁹⁰ umfangreichen, freilich auch komplexen und vertiefte
1224 Auseinandersetzung erfordernden Datenbank über die von Microsoft vorgesehenen technischen und
1225 organisatorischen Datenschutzmaßnahmen. Auch wenn insoweit die Gesprächsergebnisse die Kritik
1226 des AK Verwaltung teilweise entkräften, bleiben Rechtsunsicherheiten, da die einseitigen Änderungen
1227 entzogenen Garantien Microsofts über „Sicherheitsmaßnahmen“ formal nur eine Teilmenge der
1228 vertragsgegenständlichen personenbezogenen Daten, nämlich „Kundendaten in „Core-
1229 Onlinediensten“ und „Professional-Service-Daten“, erfassen. Microsoft 365 zählt nach der Erläuterung
1230 durch Microsoft jedenfalls zu den hiervon umfassten Angeboten.⁹¹

1231 Da die Verpflichtungen Microsofts im Hinblick auf technische und organisatorische Maßnahmen
1232 zudem abschließend beschrieben sind, wäre zudem durch die Verantwortlichen in jedem Einzelfall zu
1233 prüfen und nachzuweisen, dass die vereinbarten Maßnahmen die Anforderungen des Art. 32 DSGVO
1234 erfüllen.

1235 3.2.4.5. Schlussfolgerungen

1236 Microsoft wird empfohlen, den Geltungsbereich der „Sicherheitsmaßnahmen“ in Anhang A des
1237 „Datenschutznachtrags“ auf sämtliche im Rahmen der Auftragsverarbeitung verarbeiteten
1238 personenbezogenen Daten zu erstrecken, um Verkürzungen der gebotenen Datenschutzmaßnahmen
1239 auszuschließen.

1240 Verantwortliche sollten vor Begründung eines Auftragsverhältnisses mit Microsoft die
1241 durch das Unternehmen angebotenen Möglichkeiten der Überprüfung von Datenschutzmaßnahmen
1242 gemäß Art. 28 Abs. 1 DSGVO nutzen und das Ergebnis dokumentieren und deren Einhaltung und
1243 Angemessenheit nach Vertragsschluss kontinuierlich und in dokumentierter Form überwachen.

1244 3.2.5. Löschung und Rückgabe personenbezogener Daten

1245 3.2.5.1. Feststellungen des AK Verwaltung

1246 Microsoft differenziert, so der Ausgangsbefund des AK Verwaltung, im Rahmen der Verarbeitung
1247 zwischen den Kundendaten, die sich aus dem Auftragsverhältnis ergeben, und Daten, die zur
1248 Erbringung „professioneller Dienstleistungen“ und der Verarbeitung für „legitime Geschäftszwecke“
1249 eigenverantwortlich verarbeitet werden. Der AK Verwaltung ging daher davon aus, dass Microsoft
1250 entsprechend der Rolle als Verantwortlicher Daten, die zu eigenen Zwecken verarbeitet werden, nicht
1251 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 Ausnahmen der Core-Onlinedienste in den Lizenzbestimmungen - Datenschutz- und Sicherheitsbestimmungen, <https://www.microsoft.com/licensing/terms/de-DE/product/PrivacyandSecurityTerms>.

1252 demnach aufgrund einer anderen Rechtsgrundlage verarbeitet werden, dennoch sei zu hinterfragen,
1253 wie lange die Daten für eigene Zweck vorgehalten werden. Hierzu äußere sich Microsoft nicht.

1254 3.2.5.2. Aktueller Prüfungsgegenstand

1255 Abweichend vom Prüfungsgegenstand des AK Verwaltung erstreckt der aktuelle
1256 „Datenschutznachtrag“ 09/2022 die vertragliche Vereinbarung zur Speicherdauer und Löschung von
1257 Daten auch auf „Professional-Service“-Daten, während die dem AK Verwaltung vorliegende Version
1258 01/2020 nur die „in jedem Online-Dienst gespeicherten Kundendaten“ umfasste:

1259 *„Speicherung und Löschung von Daten*

1260 *Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional*
1261 *Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst*
1262 *gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu*
1263 *löschen.“ [Hervorhebung durch Verf.]*

1264

1265 Hinsichtlich der Verpflichtung des Auftragsverarbeiters zur Löschung nach Erbringung der
1266 Verarbeitungsleistungen ergeben sich in der hierfür maßgeblichen Anlage über die „Bestimmungen
1267 der Datenschutz-Grundverordnung der Europäischen Union“ keine Abweichungen. Diese enthält
1268 weiterhin die Zusicherung, *„nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des*
1269 *Kunden sämtliche personenbezogenen Daten zu löschen oder dem Kunden zurückzugeben, sofern nicht*
1270 *nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der*
1271 *personenbezogenen Daten besteht.“⁹²*

1272

1273 Der Abschnitt „Speicherung und Löschung von Daten“ enthält eine abweichende Regelung, wonach
1274 Microsoft die Daten nach Vertragsende 90 Tage mit einer Zugriffsmöglichkeit für den Kunden
1275 aufbewahrt und danach grundsätzlich innerhalb weiterer 90 Tage löscht, es sei denn, der
1276 „Datenschutznachtrag“ erlaubt Microsoft die weitere Speicherung, hierbei gelten abweichende
1277 Regelungen für Testversionen.

1278 3.2.5.3. Gesprächsergebnisse

1279 Microsoft hat Einzelheiten der Löschprozesse, insbesondere die Auswirkungen einer Verarbeitung von
1280 Daten für eigene Geschäftstätigkeiten im Rahmen eines Gesprächs am 17. Februar 2022 erläutert (vgl.
1281 Anlage 3, Seiten 2 bis 8)⁹³. Im Einzelnen wird dabei dargestellt:

- 1282 • Soweit diese in den „Kundendaten“ enthalten sind, bestimme der Kunde über Löschung und
1283 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>

1284 APIs), würden diese für die Zwecke der Aufbewahrung und Löschung zu Kundendaten, sobald der
1285 Kunde eine Kopie dieser Protokolle erstellt und sie in einem kundenbezogenen Speicher ablegt.
1286 • Bei „Servicegenerierte Daten/Diagnosedaten“ (personenbezogene Daten, die nicht in den
1287 Kundendaten enthalten sind) sei zu differenzieren:
1288 • sog. aktive Löschung: Der Kunde könne die Löschung des Benutzerkontos veranlassen, was
1289 zur Löschung der personenbezogenen Daten, die mit dem Benutzer verbunden sind, führe.
1290 • sog. passive Löschung: Wenn die Benutzeridentitäten des Kunden aufgrund des Endes des
1291 Abonnements gelöscht werden, führe dies zur Löschung der personenbezogenen Daten
1292 innerhalb von 180 Tagen, ohne dass der Kunde etwas unternimmt.
1293 • Aufbewahrungsfrist:
1294 Wenn personenbezogene Daten in den vom Dienst generierten Daten enthalten sind, die durch
1295 Benutzeraktionen in den Online-Diensten (z.B. Mailbox-Zugriffsprotokolle) oder in Diagnosedaten
1296 enthalten sind, richte sich die Aufbewahrung nach dem Zweck, für den die Daten gesammelt
1297 wurden, und der Notwendigkeit, die Daten zur Erfüllung dieses Zwecks aufzubewahren.
1298 • Für die Nutzung personenbezogener Daten für Geschäftstätigkeiten (ehemals „legitime
1299 Geschäftszwecke“) gebe es keine separaten Speicher, daher habe die Nutzung keine
1300 Auswirkungen auf Löschung oder Aufbewahrung. Microsoft nutze für die Geschäftstätigkeiten
1301 aggregierte Daten, die jeweils auf dem aktuellen „Datenpool“ beruhen würden. Die genutzten
1302 Daten seien höchstens pseudonymisierte Daten. Auf Grundlage aggregierter Daten könnten
1303 Einzelpersonen nicht herausgegriffen werden können. Die aggregierten Daten seien, so Microsoft,
1304 nichtpersonenbezogen.
1305 • Sonderfälle mit besonderem Verlauf:
1306 • Microsoft könne Kundendaten oder personenbezogene Daten aufbewahren, wenn es
1307 gesetzlich verpflichtet sei, diese Daten aufzubewahren und diese Verpflichtung entstehe,
1308 bevor der Kunde die Daten gelöscht hat.
1309 • Microsoft könne vom Dienst generierte Daten, die personenbezogene Daten enthalten,
1310 aufbewahren, wenn dies für Zwecke der Cybersicherheit erforderlich sei.
1311 Die Arbeitsgruppe hatte diese Angaben nicht zu überprüfen und hat auch weitergehende Fragen —
1312 etwa ob Microsoft tatsächlich Protokolle löscht, sobald der Kunde sie aus seinem kundenbezogenen
1313 Speicher löscht, nachdem er sie dorthin kopiert hat — nicht weiterverfolgt.

1314 3.2.5.4. Bewertung

1315 a) Prüfungsmaßstab

1316 Die Kritik des AK Verwaltung zielt im Kern auf die Frage weisungsgemäßer Verarbeitung durch den
1317 Auftragsverarbeiter (Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a DSGVO), wirft aber auch Detailfragen
1318 auf, die nochmals die Ausgestaltung der Verarbeitungen Microsofts für eigene Geschäftstätigkeiten
1319 betreffen.

1320 b) Detailbewertung

1321 Unbeschadet einer technischen Überprüfung und Bestätigung der von Microsoft erläuterten Speicher-
1322 , Verarbeitungs- und Löschprozesse scheinen diese zunächst die Kritik des AK Verwaltung, es erfolge
1323 eine dauerhafte Speicherung durch Microsoft, nicht zu rechtfertigen. Die Erläuterungen zeigen mit
1324 Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der
1325 Cyberabwehr, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschfristen für
1326 personenbezogene Daten nicht verlängern sollten.

1327 Allerdings genügt die Ausgestaltung der Rückgabe- und Löschverpflichtung dann nicht den
1328 gesetzlichen Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO, wenn man die
1329 spezielle Regelung im Abschnitt „Speicherung und Löschung von Daten“ zu Grunde legt, die dem
1330 Kunden nicht die Wahl lässt, ob Microsoft die Daten zurückgibt oder löscht, sondern ihm nur eine
1331 Möglichkeit zur Extraktion lässt, und Microsoft nur stark verzögert und zudem nur eingeschränkt zur
1332 Löschung verpflichtet. Es ließe sich argumentieren, dass die (den Anforderungen des Art. 28 Abs. 3
1333 UAbs. 1 Buchstabe g DSGVO entsprechenden) Regelungen der Anlage 1 Vorrang gegenüber den
1334 (unzureichenden) Regelungen im Abschnitt „Speicherung und Löschung von Daten“ genießen sollen.
1335 Allerdings ergibt sich dies nicht aus dem Wortlaut und würde zudem bedeuten, dass eine sehr
1336 allgemein gehaltene Klausel sehr spezifische Regelungen verdrängen würde. In jedem Fall können
1337 Verantwortliche wegen der Unklarheit dieser Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2
1338 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.

1339 Hinsichtlich des vormaligen „eigenen“ Geschäftszwecks“ der Bekämpfung von „Cyberkriminalität oder
1340 Cyberangriffen, die Microsoft oder Microsoft-Produkte“ betreffen können, ergeben sich noch näher
1341 zu klärende Folgefragen:

1342 Zum Zeitpunkt der Erläuterung der technischen Abläufe durch Microsoft sollten diese Prozesse noch
1343 durch vertragliche Regelungen der vorangehenden Fassungen des „Datenschutznachtrags“ legitimiert
1344 werden, die für diese Verarbeitungstätigkeiten eine – seitens des Verantwortlichen freilich zu
1345 rechtfertigende – Ermächtigung zur Nutzung durch Microsoft und damit ggf. auch zur selbstständigen
1346 Speicherung und allen sonstigen Verarbeitungsmodalitäten umfasst hätten. Dagegen unterliegen
1347 diese Verarbeitungstätigkeiten zur Gewährleistung von IT-Sicherheit bzw. Cyberabwehr in der
1348 aktuellen Struktur des Datenschutznachtrags 09/2022 nunmehr⁹⁴ den allgemeinen Regelungen
1349 weisungsgebundener Auftragsverarbeitung.

1350 Da diese Maßstäbe aber die von Microsoft beschriebene, von sonstigen Löscherfordernissen
1351 abgekoppelte längerfristige Speicherung „dienstgenerierter Daten“ nicht rechtfertigen können,
1352 verbleibt ohne Anpassung der tatsächlichen Verarbeitung – die Microsoft ausdrücklich ausgeschlossen
1353 hat – ein Konflikt: Die für die Durchführung des Vertrages gewährleisteten Löschrechte des
1354 Kunden wie auch die Verpflichtung, nach Vertragsbeendigung Kundendaten zu löschen oder

⁹⁴ Verweis auf Abschnitt 3.2.2.

1355 zurückzugeben, enthalten keinerlei Sonderbestimmungen zu Zwecken der IT-Sicherheit. Sie lassen
1356 daher keine über die Auftragsverarbeitung hinausgehenden oder nachwirkenden Verarbeitungen zu.
1357 Ob nationales oder europäisches Recht je nach Fallkonstellation eine längerfristige Verarbeitung
1358 rechtfertigen könnte, kann nur einzelfallbezogen bewertet werden.

1359 3.2.5.5. Schlussfolgerungen

1360 Die Gesprächsergebnisse zur Löschung von Kunden- und „Professional-Service-Daten“ klären zwar die
1361 grundlegenden vom AK Verwaltung aufgeworfenen Fragestellungen zur Gewährleistung
1362 weisungsgerechter Verarbeitung auf, zeigen zugleich aber eine Detailfrage zur Verarbeitungstätigkeit
1363 Microsofts zur Bekämpfung von „Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-
1364 Produkte betreffen könnten.“ Für diese in der aktuellen Fassung nicht mehr in eigener Verantwortung,
1365 sondern — jedenfalls nach der Grundsystematik — vertrags- und weisungsgebunden
1366 durchzuführenden Verarbeitungen sind z.B. im Hinblick auf die Löschung personenbezogener Daten
1367 weitere Untersuchungen ratsam.

1368 Microsoft sollte zudem die Unklarheiten und Widersprüche des Datenschutznachtrags beheben und
1369 sicherstellen, dass die Kunden die nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g) DSGVO
1370 erforderlichen Wahlrechte und Microsoft die entsprechenden Pflichten zur Rückgabe bzw. Löschung
1371 haben.

1372 Auch wenn im Übrigen dem Wortlaut nach keine Differenzen zwischen den erläuterten
1373 Verarbeitungsprozessen und den vertraglich festgelegten Verarbeitungstätigkeiten erkennbar
1374 geworden sind, sollte durch Microsoft geprüft werden, wie klargestellt werden kann, dass auch bei
1375 Verarbeitungen für eigene Geschäftstätigkeiten die vertraglichen Löschrrechte des Verantwortlichen
1376 vorgehen.⁹⁵ Neben der Erfüllung von Transparenzpflichten des Verantwortlichen etwa im Hinblick auf
1377 Art. 13 Abs. 2 Buchstabe a DSGVO würden damit auch die bereits erörterten Abwägungen berechtigter
1378 Interessen und Prüfungen der Zweckkompatibilität hinsichtlich der mit diesen Verarbeitungen
1379 verbundenen Speicherdauer einen wünschenswerten belastbaren Anknüpfungspunkt erhalten.

1380 3.2.6. Information über Unterauftragsverarbeiter

1381 3.2.6.1. Feststellungen des AK Verwaltung

1382 In Bezug auf die Weitergabe personenbezogener Daten an Unterauftragnehmer ist nach der Analyse
1383 des AK Verwaltung die vorherige schriftliche Zustimmung des Kunden zur Weitervergabe der
1384 Verarbeitung von Kundendaten und personenbezogenen Daten durch Microsoft nur dann
1385 ausreichend, „wenn eine Übersicht der zum Zeitpunkt der Unterzeichnung des
1386 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“.

1387 Unterauftragnehmer aufgenommen wird (siehe dazu auch 3.2.7 der Opinion 14/2019 des
1388 Europäischen Datenschutzausschusses).“

1389 Der zur Information über Hinzuziehung oder Ersetzung von Unterauftragnehmern vorgesehene
1390 „Mechanismus zur Benachrichtigung des Kunden über dieses Update“ durch das Abonnement von
1391 Push-Benachrichtigungen ist, so der AK Verwaltung, dementsprechend proaktiv durch Microsoft
1392 einzusetzen.

1393 3.2.6.2. Aktueller Prüfungsgegenstand

1394 Die mehrfache, teils kontroverse Erörterung der Ausgestaltung der Kontrollrechte des
1395 Verantwortlichen bei Veränderungen der Unterauftragsverarbeitungsverhältnisse hat zu einer bereits
1396 Ende März eingeführten Neugestaltung des Unterrichtsverfahrens geführt, die im aktuellen
1397 „Datenschutznachtrag“ 09/2022 zu einer Streichung des bisherigen „Hol-Schuld“-Verfahrens geführt
1398 hat.

1399 Die maßgebliche Bestimmung des Abschnitts *„Hinweise und Kontrollen beim Einsatz von*
1400 *Unterauftragsverarbeitern“* lautet nunmehr [Hervorhebung zur Kennzeichnung der Abweichungen von
1401 vorangehenden Fassungen durch Verf.]:

1402 *„Microsoft beauftragt gelegentlich möglicherweise neue Unterauftragsverarbeiter. Microsoft*
1403 *informiert den Kunden und aktualisiert die Webseite mindestens 6 Monate, bevor dieser Zugriff auf*
1404 *Kundendaten erhält über jeden neuen Unterauftragsverarbeiter ~~(durch Aktualisierung der Website und~~*
1405 *~~Bereitstellung eines Mechanismus zur~~*

1406 *~~Benachrichtigung des Kunden über diese Aktualisierung)~~. Darüber hinaus informiert*

1407 *Microsoft den Kunden über und aktualisiert die Webseite im Hinblick auf jeden neuen*
1408 *Unterauftragsverarbeiter mindestens 30 Tage bevor er Zugriff auf andere Professional Services-Daten*
1409 *oder personenbezogene Daten erhält, die nicht in den Kundendaten enthalten sind. Wenn Microsoft*
1410 *einen neuen Unterauftragsverarbeiter für ein neues Produkt oder einen Professional Service beauftragt,*
1411 *der Kundendaten, Professional Services-Daten oder personenbezogene Daten verarbeitet, wird*
1412 *Microsoft den Kunden vor der Verfügbarkeit dieses Produkts oder Professional Services*
1413 *benachrichtigen.“*

1414 3.2.6.3. Gesprächsergebnisse

1415 In den Gesprächen mit der Arbeitsgruppe konnte Microsoft trotz anfänglicher Vorbehalte zur
1416 rechtlichen Erforderlichkeit und Praktikabilität zu einer Umstellung des bisher als Hol-Schuld des
1417 Verantwortlichen ausgestalteten Verfahrens zu organisatorischen und vertraglichen Anpassungen
1418 bewegt werden. Hierzu wurden im Wesentlichen folgende Eckpunkte vorgetragen (vgl. Anhang 3,
1419 Seiten 10 bis 15):

- 1420 - Nutzung des bestehenden Microsoft Service Messaging Center (SMC) als bestehende proaktive
1421 Benachrichtigungsmethode, die für die Servicekommunikation für Microsoft-365-Kunden
1422 verwendet wird.
- 1423 - Push-Benachrichtigung per E-Mail (Versand an zwingend benannten „Global Admin“ und (sofern
1424 zugewiesen) „Privacy Reader“ des Kunden), um diese über das Update zu informieren, ohne dass
1425 kundenseitiges Handeln erforderlich ist. Der Kunde kann diese Benachrichtigung allerdings
1426 abbestellen.
- 1427 - Die Benachrichtigung über Änderungen an der Liste der Online-Dienste-Unterauftragsverarbeiter
1428 wird mit dem zusätzlichen Hinweis „Datenschutz“ versehen. Diese Benachrichtigungen können
1429 von den Rollen Global Admin und Privacy Reader gelesen werden. Alle Dienstbenachrichtigungen
1430 sind standardmäßig zunächst für den Global Admin aktiviert.
- 1431 - Wenn die Liste der Online-Dienste-Unterauftragsverarbeiter aktualisiert wird, löst dies
1432 automatisch eine SMC-Benachrichtigung an den Global Admin und den Privacy Reader (falls
1433 Letzterer zugewiesen ist) aus. Eine E-Mail-Benachrichtigung wird auch an den Global Admin und
1434 den Privacy Reader (falls zugewiesen) gesendet, die sie über die Aktualisierung informieren, ohne
1435 dass weitere Maßnahmen erforderlich sind.

1436 Nachfolgendes Schaubild zeigt ein Umsetzungsbeispiel der SMC-Benachrichtigungs-Mail über
1437 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

1438

Abbildung

1439

1440

1441

1442 3.2.6.4. Bewertung

1443 a) Prüfungsmaßstab

1444 Art. 28 Abs. 2 Satz 2 DSGVO sieht vor, dass der Auftragsverarbeiter im Falle einer allgemeinen
1445 schriftlichen Genehmigung von Unterauftragsverhältnissen den Verantwortlichen über jede
1446 beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter
1447 informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen
1448 Einspruch zu erheben. Diese Informationspflicht wird in den Leitlinien des Europäischen
1449 Datenschutzausschusses 07/2020 ausdrücklich als „Bring-Schuld“ des durch eine solche generelle
1450 Genehmigung begünstigten Auftragsverarbeiters klargestellt:

1451 „Es sei darauf hingewiesen, dass die Pflicht des Auftragsverarbeiters, den Verantwortlichen über jede
1452 Änderung bei den Unterauftragsverarbeitern zu informieren, impliziert, dass der Auftragsverarbeiter
1453 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.

1454 b) Detailbewertung

1455 Mit der Anpassung und vertragsrechtlichen Verankerung des Unterrichtsverfahrens trägt
1456 Microsoft der Kritik des AK Verwaltung und den Anforderungen der Leitlinien des Europäischen
1457 Datenschutzausschusses Rechnung, soweit es um die Ausgestaltung als „Push“-Verfahren geht. Die
1458 oben abgebildete E-Mail verweist allerdings für den tatsächlichen Inhalt der Benachrichtigung auf eine
1459 WWW-Seite von Microsoft. Die Arbeitsgruppe versteht Art. 28 Abs. 2 DSGVO dahingehend, dass die
1460 Information des Verantwortlichen „über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung
1461 oder die Ersetzung anderer Auftragsverarbeiter“ die konkret beabsichtigte Änderung enthalten muss
1462 und nicht nur den allgemeinen Hinweis, dass Änderungen geplant sind.

1463 **3.2.6.5. Schlussfolgerungen**

1464 Für den Verantwortlichen als Vertragspartner des „Datenschutznachtrags“ 09/2022 erfordert die
1465 rechtlich gebotene Anpassung des Unterrichtsverfahrens durch Microsoft, nunmehr
1466 innerorganisatorisch einen Informationsfluss sicherzustellen, der die Weiterleitung einer
1467 Änderungsmitteilung über Unterauftragsverhältnisse an die zur datenschutzrechtlichen Bewertung
1468 dieses Sachverhalts berufenen Funktionsträger gewährleistet oder aber deren unmittelbare Nutzung
1469 des Benachrichtigungsdienstes sicherstellt.

1470 Um eine zielgenaue Bewertung z.B. im Hinblick auf die Anforderungen an Drittstaatentransfers zu
1471 ermöglichen und auch selbst inhaltlich die Anforderungen des Art. 28 zu erfüllen, bleibt freilich
1472 weiterhin auch Microsoft gefordert, die Informationen zu Unterauftragsverarbeitern zu präzisieren:
1473 Das von Microsoft bereitgestellte Muster einer Benachrichtigungs-E-Mail enthält nur eine Information
1474 über geplante Änderungen, aber nicht die konkret geplanten Änderungen. Die der Arbeitsgruppe
1475 vorgestellte Liste über Unterauftragsverhältnisse unterscheidet zudem bislang im Wesentlichen
1476 danach, für welchen Dienst bzw. welche Funktionalität Unterauftragnehmer eingesetzt sind und
1477 benennt deren Sitz und die ihnen zugänglichen Datenkategorien. Im Vergleich dazu sehen die von der
1478 EU-Kommission bereitgestellten Standardvertragsklauseln deutlich detailliertere Angaben über Name,
1479 Anschrift und Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der jeweiligen
1480 Verarbeitung vor, die eine klare Abgrenzung der Verantwortlichkeiten mehrerer eingesetzter
1481 Unterauftragsverarbeiter erlauben sollen. Microsoft wird empfohlen, die den Verantwortlichen
1482 bereitgestellten Informationen über Unterauftragsverhältnisse an diese in Anhang IV der
1483 Standardvertragsklauseln zusammengefassten Anforderungen anzupassen.

1484 Auch wenn dies — die gesetzliche Verpflichtung zur Information liegt beim Auftragsverarbeiter —
1485 außerhalb der Zuständigkeit der deutschen Aufsichtsbehörden liegt, sei der Vollständigkeit halber
1486 angemerkt, dass Microsoft auch den tatsächlichen Versand der Benachrichtigungen sicherstellen
1487 muss, insbesondere also die Möglichkeit zur Abbestellung deaktivieren sollte.

1488 3.2.7. Datenübermittlungen in Drittstaaten

1489 3.2.7.1. Feststellungen des AK Verwaltung, Untersuchungsauftrag

1490 Der AK Verwaltung hat sich in seiner Bewertung vom 15. Juli 2020 nicht zu Fragen der Übermittlung
1491 personenbezogener Daten in Drittländer geäußert. Die DSK hat in ihrem Beschluss vom 29. September
1492 2020 aber die Arbeitsgruppe beauftragt, zeitnah Anpassungen an die durch die Schrems-II-
1493 Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis
1494 öffentlicher und nicht öffentlicher Stellen zu erreichen.

1495 3.2.7.2. Aktueller Prüfungsgegenstand

1496 Der „Datenschutznachtrag“ September 2022 enthält unter „Datenübermittlungen und Speicherstelle
1497 – Datenübermittlungen“ die Regelung, dass der Kunde – unter Würdigung der in diesem Abschnitt
1498 geregelten und für verbindlich erklärten Sicherheitsmaßnahmen – Microsoft „beauftragt (...), (...)
1499 personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu
1500 übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind“. Für sämtliche
1501 Übermittlungen von insbesondere personenbezogenen Daten aus der Europäischen Union, dem
1502 Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der
1503 Produkte und Services gelten danach die von Microsoft implementierten Standardvertragsklauseln der
1504 EU-Kommission von 2021. Microsoft halte sich an die datenschutzrechtlichen Anforderungen des
1505 Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung,
1506 Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen
1507 Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz. Alle Übermittlungen
1508 personenbezogener Daten an ein Drittland oder eine internationale Organisation unterlägen
1509 geeigneten Garantien, wie sie in Art. 46 DSGVO beschrieben sind, und solche Übermittlungen und
1510 Garantien würden nach Art. 30 Abs. 2 DSGVO dokumentiert.

1511 Im Abschnitt „Datenübermittlungen und Speicherstelle – Ort der ruhenden Kundendaten“ findet sich
1512 zudem eine Regelung, wo bestimmte Daten gespeichert werden.

1513 3.2.7.3. Gesprächsergebnisse

1514 Die Gespräche der Arbeitsgruppe mit Microsoft bestätigten entsprechend den vertraglichen
1515 Regelungen, dass bei der Nutzung von Microsoft 365 personenbezogene Daten jedenfalls in die USA
1516 übermittelt werden. Eine Nutzung von Microsoft 365 ohne Übermittlungen personenbezogener Daten
1517 in die USA sei nicht möglich. Ab Dezember 2022 plane Microsoft, für alle gewerblichen und Kunden
1518 des öffentlichen Sektors, die im EU-Raum ansässig sind, anzubieten, Kundendaten, Supportdaten und
1519 sonstige personenbezogene Daten der Kunden grundsätzlich – d.h. nicht ausnahmslos, nicht etwa für
1520 bestimmte IT-Sicherheitsmaßnahmen – im EU-Raum zu speichern und zu verarbeiten.

1521 Nach Aufbau des Konzepts der „EU Data Boundary“ sollen u.a.

- 1522 • Supportleistungen „für erste Lösungen“ innerhalb der EU durch Aufstockung des Personals in der
1523 Region erbracht werden,
- 1524 • Unterauftragsverhältnisse vermindert werden, um den Zugang zu personenbezogenen Daten von
1525 EU-Kunden zu begrenzen,
- 1526 • Technologien wie eine virtuellen Desktop-Infrastruktur (VDI) eingerichtet werden, um den Schutz
1527 bei erforderlichen Support-Fernzugriffen auf personenbezogene Daten von EU-Kunden zu
1528 erhöhen und die physische Übertragung von Daten zu verhindern (vgl. im Einzelnen Anlage 4,
1529 Seiten 10 bis 15).

1530 Ergänzend ist auf die nicht spezifisch für Datenexporte geltenden Regelungen über weitere
1531 Schutzmaßnahmen für Verarbeitungen zu eigenen Geschäftstätigkeiten von Microsoft im
1532 Zusammenhang mit der Leistungserbringung zu verweisen, die in Abschnitt 3.2.2 behandelt werden.

1533 3.2.7.4. Bewertung

1534 a) Prüfungsmaßstab

1535 Nach Art. 44 DSGVO ist jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet
1536 werden oder nach ihrer Übermittlung in⁹⁷ ein Drittland oder an eine internationale Organisation
1537 verarbeitet werden sollen, nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter
1538 (einschließlich aller eventuellen Unterauftragsverarbeiter) die in Kapitel V der DSGVO niedergelegten
1539 Bedingungen einhalten und auch die sonstigen Bestimmungen der DSGVO eingehalten werden. Die
1540 Anforderungen sind auch bei Weiterübermittlungen aus einem Drittland an ein anderes Drittland
1541 einzuhalten.

1542 Zur Rechtfertigung der Übermittlung zieht Microsoft die Standardvertragsklauseln für Datenexporte
1543 2021⁹⁸ heran. Entsprechend der Rechtsprechung des EuGHs in „Schrems II“ verlangen diese
1544 Standardvertragsklauseln in Klausel 14 eine Untersuchung und Bewertung der Rechtslage und -praxis
1545 in dem jeweiligen Zielland jeglicher Übermittlungen personenbezogener Daten. Hierfür enthalten die
1546 Empfehlungen 01/2020 des Europäischen Datenschutzausschusses eine detaillierte Schritt-für-Schritt-
1547 Anleitung. Hindern die Rechtslage oder -praxis im Bestimmungsdrittland den Datenimporteur an der
1548 Erfüllung seiner Pflichten aus den Standardvertragsklauseln, sind ergänzende Schutzmaßnahmen zu
1549 treffen, die diejenigen Rechtsvorschriften oder Gepflogenheiten des Drittlandes ausgleichen, die den
1550 Datenexporteur an der Erfüllung seiner Verpflichtungen aus den Standardvertragsklauseln hindern,
1551 d.h. genau die identifizierten Rechtsschutzlücken schließe.⁹⁹ Ist es nicht möglich, diejenigen
1552 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.

1553 seiner Verpflichtungen aus den Standardvertragsklauseln hindern, vollständig auszugleichen, darf eine
1554 Übermittlung in das jeweilige Drittland nicht erfolgen.¹⁰⁰ Primär kommt es dabei auf eine Bewertung
1555 der geltenden Gesetze im Drittland an. Nur wenn insoweit Unklarheiten bestehen, besteht Raum für
1556 eine ergänzende Betrachtung der Praxis im Drittland.¹⁰¹

1557 Für die USA hat der EuGH in „Schrems II“ festgestellt, dass FISA 702 und E.O. 12333 unverhältnismäßige
1558 Zugriffsrechte für US-Geheimdienste vorsehen und für EU-Bürger kein gerichtlicher Rechtsschutz
1559 gegeben ist. Während gegen Überwachung auf der Basis von E.O. 12333 technische Maßnahmen –
1560 insbesondere Verschlüsselung – unter bestimmten Bedingungen als möglich erachtet werden,¹⁰²
1561 können Diensteanbieter und ihre Mitarbeiter, die FISA 702 unterfallen, zur Herausgabe der
1562 gewünschten Daten gezwungen werden. Der Einwand, dass die Herausgabe nach der DSGVO
1563 unzulässig ist, ist – nach der von Microsoft bestrittenen Expertenbewertung - nach US-Recht
1564 irrelevant.¹⁰³

1565 b) Detailbewertung

1566 Um die vom EuGH identifizierten am EU-Maßstab gemessenen grundrechtlichen Unzulänglichkeiten
1567 von FISA 702 auszugleichen, wäre es mithin erforderlich, Maßnahmen zu ergreifen, die den Zugriff der
1568 US-Behörden – und damit von Microsoft – auf personenbezogene Daten verhindern oder ineffektiv
1569 machen. Dies kann in bestimmten, begrenzten Anwendungsfällen möglich sein. Konkret anzuführen
1570 wären die Anwendungsfälle 1 (Datenspeicherung zu Backup- und anderen Zwecken, die nicht den
1571 Zugang zu unverschlüsselten Daten erfordern), 2 (Übermittlung pseudonymisierter Daten) und 5
1572 (Aufgeteilte Verarbeitung oder Verarbeitung durch mehrere Beteiligte, Multi-party Processing) des
1573 Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses, soweit die dort
1574 aufgestellten Bedingungen eingehalten werden.

1575 Viele der in Microsoft 365 enthaltenen Dienste erfordern allerdings einen Zugriff von Microsoft auf die
1576 unverschlüsselten, nicht pseudonymisierten Daten.¹⁰⁴ Insbesondere die naheliegende Verschlüsselung
1577 verarbeiteter Daten, die einen Zugriff von Microsoft und damit der US-Behörden verhindern würde,
1578 ist regelmäßig nicht möglich, wenn die Daten beispielsweise im Browser angezeigt werden müssen. Es
1579 handelt sich mithin um eine klassische Ausprägung des Anwendungsfalls 6 des Anhangs 2 der
1580 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.

1581 den Aufsichtsbehörden nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer
1582 Rechtmäßigkeit des Datenexports führen könnten.

1583 Die von Microsoft derzeit im Abschnitt „Ort der ruhenden Daten“ vorgesehenen Maßnahmen für die
1584 Speicherung der Daten (data at rest) führen weder zum Ausschluss einer Übermittlung noch
1585 begründen sie hinreichende Schutzmaßnahmen, da die weitergehende Verarbeitung bei den meisten
1586 der in Microsoft 365 enthaltenen Dienste technisch zwingend im Klartext erfolgen muss und die
1587 örtliche Beschränkung sich nur auf den Ort der Speicherung der Daten bezieht. Für die weiteren
1588 Verarbeitungen (abseits der Speicherung) enthält der Abschnitt „Datenübermittlung und Ort“ („Data
1589 Transfers and Location“) keine Aussagen zur Datenlokalisierung.¹⁰⁵

1590 Auch die von Microsoft im „Nachtrag zu zusätzlichen Schutzmaßnahmen“ zugesagten Maßnahmen
1591 sind nicht geeignet, die am Maßstab des EU-Rechts gemessenen grundrechtlichen Unzulänglichkeiten
1592 des US-amerikanischen Rechts auszugleichen. Am ehesten mag noch die Verpflichtung zur Anfechtung
1593 von Herausgabeanordnungen als ergänzende Schutzmaßnahme in Betracht kommen. Doch besteht
1594 diese Verpflichtung zur Anfechtung nur, wenn die Herausgabeanordnung nach demjenigen Recht
1595 unzulässig ist, dem die Behörde bzw. das Gericht unterliegt, die bzw. dass die Herausgabe anordnet,
1596 wozu auch relevante Konflikte mit dem anwendbaren EU- oder mitgliedstaatlichen Recht gehören.
1597 Da aber FISA 702, wie der EuGH festgestellt hat,¹⁰⁶ keine inhaltliche Begrenzung der
1598 Überwachungsbefugnisse vorsieht und FISA 702 unterliegende Unternehmen die Anwendung dieser
1599 Norm nicht mit dem Argument abwenden können, dadurch würde EU- oder mitgliedstaatliches Recht
1600 verletzt,¹⁰⁷ ist nicht erkennbar, wie eine Verletzung des in Art. 52 EU-Grundrechtecharta geregelten
1601 Grundsatzes der Verhältnismäßigkeit durch eine solche Herausgabeanordnung auf diesem Wege
1602 erfolgreich geltend gemacht werden könnte. Dementsprechend sehen die Empfehlungen 01/2020 des
1603 Europäischen Datenschutzausschusses derartige Maßnahmen auch nur als Ergänzung anderer
1604 Maßnahmen vor.¹⁰⁸

1605 Zu der Frage, inwieweit Microsoft sich vertraglich Offenlegungen vorbehält, die Art. 48 DSGVO
1606 widersprechen, wird auf Abschnitt 3.2.3. verwiesen.

1607 Für Übermittlungen personenbezogener Daten in andere Länder als die USA fehlt es bereits an einer
1608 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.

1609 data in the Microsoft cloud“¹⁰⁹ beschränkt sich Microsoft auf die Aussage, anzunehmen, dass die
1610 drittstaatlichen Gesetze und Gewohnheiten Microsoft in der Praxis nicht daran hindern würden, die
1611 Verpflichtungen aus den Standardvertragsklauseln einzuhalten. Insoweit ist im Übrigen darauf
1612 hinzuweisen, dass für die von Microsoft im genannten Dokument entscheidend vorgenommene
1613 Bewertung der Praxis kein Raum ist, wenn die Rechtslage bereits als problematisch identifiziert ist, wie
1614 dies in den USA der Fall ist.

1615 Zusätzliche Fragen wirft die im „Datenschutznachtrag“ vorgesehene Weisung („beauftragt (...), (...)
1616 personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu
1617 übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind“) auf, die für den Kunden
1618 regelmäßig nicht bestimmbare weitere Datenübermittlungen in Drittländer vorsieht. Selbst wenn
1619 Microsoft dem Kunden vor Vertragsschluss entsprechende Informationen bereitstellen würde,
1620 müssten auch die Informationen über neue Unterauftragsverarbeiter entsprechend ergänzt werden.
1621 Darüber hinaus müsste auch eine Information vorgesehen werden, wenn sich die Länder, in denen
1622 Microsoft selbst oder bestehende Unterauftragsverarbeiter tätig sind (und zwar unabhängig davon, ob
1623 diese Tätigkeit einen Bezug zur Auftragsverarbeitung hat), ändern.

1624 Die Arbeitsgruppe weist darauf hin, dass nach der Rechtsprechung des Bundesverwaltungsgerichts aus
1625 der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auch eine Beweislastverteilung folgt,¹¹⁰ sodass
1626 Verantwortliche bereits unabhängig von der implizit durch die Regel-Ausnahme-Formulierung der
1627 Art. 44, 45 Abs. 1 DSGVO erfolgten Beweislastregelung die Erfüllung der Anforderungen des Kapitels V
1628 DSGVO zweifelsfrei nachweisen können müssen.

1629 3.2.7.5. Schlussfolgerungen

1630 Die Nutzung von Microsoft 365 unter Geltung des „Datenschutznachtrags“ 09/2022 verlangt zwingend
1631 Weisungen des Verantwortlichen zu Übermittlungen personenbezogener Daten in Drittländer,
1632 namentlich die USA und alle anderen Länder, in denen Microsoft oder ihre Unterauftragsverarbeiter
1633 tätig sind. Jedenfalls Datenübermittlungen in die USA lassen sich auch technisch nicht verhindern.

1634 Insbesondere das US-amerikanische nationale Sicherheitsrecht in Form von FISA 702 kann die Erfüllung
1635 der Verpflichtungen aus den Standardvertragsklauseln in Frage stellen. Damit wären also ergänzende
1636 Schutzmaßnahmen zu treffen, die jeden Zugriff von US-Behörden und auch von Microsoft und seinen
1637 Mitarbeitern unmöglich oder ineffektiv machen, um so zu verhindern, dass Microsoft
1638 Herausgabeverlangen nach FISA 702 nachkommen kann.

1639 Die Nutzung der Dienste von Microsoft 365 als klassische Cloud-Dienste erfordert allerdings in vielen
1640 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/RWRq1?culture=en-us&country=US>.

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

1641 Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. Für diesen
1642 Anwendungsfall ist es den Aufsichtsbehörden nicht gelungen, ergänzende Schutzmaßnahmen zu
1643 identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten. Die von Microsoft
1644 vorgesehenen Maßnahmen sind unzureichend, da sie nicht die bestehenden Schutzlücken –
1645 insbesondere exzessive Zugriffsrechte und fehlender gerichtlicher Rechtsschutz – beheben.

1646 Nur in besonderen Ausnahmefällen kommen ergänzende Schutzmaßnahmen in Betracht, die für die
1647 erforderliche Gewährleistung eines vergleichbaren Schutzniveaus für die übermittelten Daten effektiv
1648 sind, etwa die Speicherung sicher verschlüsselter Backups in der Microsoft-Cloud, wenn der Schlüssel
1649 beim Kunden verbleibt.

1650 Die von Microsoft bereits avisierte künftige verstärkte Verlagerung der Datenverarbeitung in die EU
1651 erscheint vor diesem Hintergrund hilfreich, ist in der Umsetzung aber vor dem Hintergrund etwaiger
1652 extraterritorial wirkender Rechtsvorschriften zu beobachten und zu bewerten. Microsoft sollte auch
1653 die derzeit unbestimmte Weisung zu Datenexporten beschränken und klar bestimmt fassen.

1654 4. Gesamtbewertung, weiteres Vorgehen

1655 Auf Grundlage ihrer Gespräche mit Microsoft von Dezember 2020 bis April 2022 und Berücksichtigung
1656 des am 15. September 2022 von Microsoft veröffentlichten „Datenschutznachtrags“ unterbreitet die
1657 Arbeitsgruppe der DSK Vorschläge für eine zusammenfassende Bewertung, die gesondert zu diesem
1658 Bericht zur abschließenden Beratung vorgelegt werden.

1659 4.1.1.1. Anhang: Übersicht über die Arbeitsgespräche der Arbeitsgruppe mit
1660 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

1661