AG DSK „Microsoft-Onlinedienste“

Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung,

1. Untersuchungsauftrag, Verfahren und Untersuchungsgegenstand

Die DSK hatte am 22. September 2020 eine **Bewertung des Arbeitskreises Verwaltung** zu den dem Einsatz des Cloud-Dienstes Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service Terms (OST) sowie den Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die damalige Bewertung des AK Verwaltung kommt zum Ergebnis, *„dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“* sei.

Die DSK hat in ihrer Sitzung am 22. September 2020 eine Arbeitsgruppe unter Federführung Brandenburgs und des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gebeten, Gespräche mit Microsoft aufzunehmen, *„um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen*[1]*.“*

Daraufhin hat eine Arbeitsgruppe Ende 2020 Gespräche mit Microsoft begonnen. Teilnehmer der AG waren: Brandenburg und BayLDA (beide Leitung), BfDI, Baden-Württemberg, Berlin, Hessen, Mecklenburg-Vorpommern, Sachsen, Saarland und Schleswig-Holstein. Für Microsoft haben Beschäftigte der Microsoft Deutschland GmbH einschließlich eines Mitgliedes der Geschäftsleitung sowie je nach Schwerpunkt Ansprechpartner der Microsoft Corporation (USA) teilgenommen. Im Rahmen der Gespräche fanden 14 mehrstündige Videokonferenzen statt.

Bei den Gesprächen war zu berücksichtigen, dass federführende Datenschutzaufsichtsbehörde für Microsoft Ireland Operations, Ltd. als Partei des Auftragsverarbeitungsverarbeitungsvertrags die irische Aufsichtsbehörde ist und die deutschen Aufsichtsbehörden für die Aufsicht der jeweiligen deutschen Kunden (z.B. Unternehmen, Behörden, also die Verantwortlichen im Sinne von Art. 4 Nr. 7

[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.

DS-GVO) zuständig sind. Wesentliche Frage für die deutschen Aufsichtsbehörden war daher, ob die einzelnen Verarbeitungstätigkeiten der hiesigen Verantwortlichen (für die diese den Auftragsverarbeiter Microsoft beauftragt haben) rechtmäßig sind und ob der Auftragsverarbeitungsvertrag die Anforderungen von Art. 28 DS-GVO erfüllt. Zudem war zu berücksichtigen, dass der Cloud-Dienst Microsoft 365 in verschiedenen Funktionsumfängen, Varianten und Konfigurationen genutzt werden kann.

Grundlage der nachfolgenden Bewertungen ist der „Datenschutznachtrag zu den Produkten und Services von Microsoft“ (im Folgenden: „*Datenschutznachtrag*“) einschließlich der aktuellen Fassung vom 15. September 2022. Die Bewertung beruht auf der zum Abschluss des Berichts am 10. Oktober 2022 bestehenden Sach- und Rechtslage.

Der Bericht der Arbeitsgruppe enthält

a) eine alleine auf ausgewählte rechtliche Anforderungen der DSGVO beschränkte Bewertung, jedoch keine vollständige datenschutzrechtliche Bewertung des Cloud-Dienstes Microsoft 365,
b) im Wesentlichen eine Untersuchung, die sich auf die der sechs vom AK Verwaltung 2020 festgestellten vertraglichen Mängel beschränkt und keine darüber hinausgehenden Prüfungen enthält,
c) keine eigenständigen technischen Untersuchungen durch die Arbeitsgruppe und damit keine Prüfung der tatsächlich stattfindenden Datenflüsse und Verarbeitungen,
d) keine Untersuchung der Umsetzung der vertraglich festgelegten Verarbeitungen bzw. der tatsächlich stattfindenden Verarbeitungen,
e) keine Prüfung der Einzelkomponenten des Cloud-Dienstes, insbesondere keine Prüfung einzelner Funktionalitäten auf ihre Datenschutzkonformität (z.B. im Bereich Beschäftigtendatenschutz und Überwachung der Mitarbeitenden durch Verantwortliche),
f) keine Prüfung der einzelnen Verarbeitungstätigkeiten,
g) keine Prüfung des gesamten einschlägigen Vertragswerks von Microsoft sowie
h) keine Prüfung der datenschutzrechtlichen Anforderungen aus dem TTDSG und der Fragen, die sich aus dem Telekommunikationsrecht und des Fernmeldegeheimnisses ergeben.

Damit bietet der Bericht keine abschließenden Untersuchungen und kann anderweitige aufsichtliche Feststellungen weder ausschließen noch diesen vorgreifen. Dies gilt insbesondere im Hinblick auf

bereits von einzelnen Aufsichtsbehörden durchgeführte Untersuchungen, die teils selbständige Mängel auflisten.[2]

Die Arbeitsgruppe hat Microsoft vor dem Abschluss ihres Berichts Gelegenheit zur Stellungnahme gegeben, diese Rückmeldungen geprüft und in ihren abschließenden Bewertungen berücksichtigt.

Die folgende Zusammenfassung bietet einen Überblick über wesentliche Ergebnisse der Gespräche und die dabei gegenüber den dem Auftrag der Arbeitsgruppe zu Grunde liegenden Prüfpunkten des AK Verwaltung erreichten bzw. nicht erreichten Nachbesserungen.

2. Wesentliche Ergebnisse

Microsoft hat im September 2022 einen aktualisierten „*Datenschutznachtrag zu den Produkten und Services von Microsoft*“ (Englisch: „*Microsoft Products and Services Data Protection Addendum (DPA)*“) vorgestellt. Diese neue Version bringt vor allem Änderungen im Bereich der vertraglichen Formulierung der Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime Geschäftszwecke“ mit sich, kann als Ergebnis der Gespräche gesehen werden und adressiert damit einen Teil der Kritikpunkte des AK Verwaltung. Insgesamt konnte die Arbeitsgruppe in den vom AK Verwaltung benannten Kritikpunkten nur geringfügige Verbesserungen erreichen.

Zentrale und wiederkehrende Fragestellung der Gesprächsreihe war es, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als Verantwortlicher. Dies konnte nicht abschließend geklärt werden.

Verantwortliche müssen jederzeit in der Lage sein, ihrer **Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO** nachzukommen. Beim Einsatz von Microsoft 365 lassen sich hierbei auf Grundlage des „Datenschutznachtrags“ weiterhin Schwierigkeiten erwarten, da Microsoft nicht vollumfänglich offenlegt, **welche Verarbeitungen im Einzelnen stattfinden.** Zudem legt Microsoft weder vollständig dar, welche Verarbeitungen im Auftrag des Kunden noch welche zu eigenen Zwecken stattfinden. **Die Vertragsunterlagen sind in der Hinsicht nicht präzise** und erlauben im Ergebnis nicht abschließend bewertbare, ggf. sogar umfangreiche Verarbeitungen auch zu eigenen Zwecken.

Eine Verwendung personenbezogener Daten der Nutzenden (z.B. Mitarbeitenden oder Schüler:innen) zu eigenen Zwecken des Anbieters **schließt den Einsatz eines Auftragsverarbeiters im öffentlichen Bereich (insbesondere an Schulen) aus.** Die Rechtsgrundlage des berechtigten Interesses nach
Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).

---

1. [2] Vgl. z.B. seitens der deutschen Aufsichtsbehörden: 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.

Aufgrund der Schwierigkeit für Verantwortliche des öffentlichen Bereichs, ihrer Rechenschaftspflicht nachzukommen, ist auch Art. 6 Abs. 1 lit. e DS-GVO i.V.m. jeweiligem Spezialrecht als Rechtsgrundlage schwer begründbar.

3. Zusammenfassung der erreichten Nachbesserungen im Einzelnen

Im Folgenden werden die nach dem Auftrag der DSK erzielten Nachbesserungen an den Kritikpunkten des AK Verwaltung zusammengefasst.

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

Die Arbeitsgruppe konnte im Rahmen der Gespräche mit Microsoft **keine signifikanten Nachbesserungen** in der Vertragsgestaltung hinsichtlich der Festlegung von Arten und Zwecken der Verarbeitung sowie der Arten der verarbeiteten personenbezogenen Daten erreichen. Es bleiben Nachbesserungen erforderlich, die den Gegenstand der Auftragsverarbeitung nicht nur umfassend, sondern auch spezifisch und so detailliert als möglich beschreiben sollten.

Dies könnte etwa durch eine kundenspezifische Konkretisierung nach dem Vorbild des Anhangs II der Standardvertragsklauseln der Kommission gemäß Art. 28 Abs. 7 DS-GVO erreicht werden. Möglich wäre auch, Verweise auf ein formgerecht in den Vertrag einzubeziehendes und hinreichend detailliertes Verzeichnis der Verarbeitungstätigkeiten (VVT) des Verantwortlichen vorzusehen.

3.2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime Geschäftszwecke“ (jetzt: „Geschäftstätigkeiten“)

Zum Themenkomplex der eigenen Verantwortlichkeit Microsofts im Rahmen der Verarbeitungen „für legitime Geschäftszwecke“ konnte die Arbeitsgruppe zwar Änderungen der vertraglichen Ausgestaltung erreichen. Ungeachtet unterschiedlicher Beurteilungen der datenschutzkonformen Ausgestaltung von Verarbeitungen vertragsgegenständlicher Daten zu eigenen Zwecken des Auftragsverarbeiters durch die europäischen Aufsichtsbehörden bewirken diese Vertragsänderungen jedoch aus Sicht der Arbeitsgruppe **keine substantiellen Verbesserungen:** Der „Datenschutznachtrag“ vom September 2022 enthält als Konsequenz der Gespräche mit der Arbeitsgruppe einen begrifflich veränderten Abschnitt über Datenverarbeitungen, die Geschäftstätigkeiten Microsofts dienen sollen, der erste Ansätze zur Eingrenzung und Konkretisierung zeigt. Allerdings hat Microsoft nach eigener Aussage **keine Anpassungen an den tatsächlichen Verarbeitungen** vorgenommen.

Eine genauere Untersuchung der vertraglichen Umgestaltung zeigt aus Sicht der Arbeitsgruppe, dass Microsoft die Grundansätze des bisherigen Regelungsmodells fortführt, sich für bestimmte Verarbeitungen **unzureichend eingegrenzte Rechte zu wenig konkretisierten Verarbeitungen** der verarbeiteten personenbezogenen Daten einräumen zu lassen. Es bleibt **weiterhin unklar,** welche personenbezogenen Daten im Rahmen der von Microsoft so genannten „legitimen“ Geschäftszwecke bzw. nun „Geschäftstätigkeiten“ verarbeitet werden.

Ebenso ist unklar, auf welcher Rechtsgrundlage die Überführung der im Auftrag verarbeiteten personenbezogenen Daten in die Verantwortlichkeit von Microsoft für die anschließende Verarbeitung zu Zwecken Microsofts samt der damit verbundenen umfassenden Nachweispflichten stattfindet. Ähnliches gilt für Daten wie **Telemetrie- und Diagnosedaten**, die Microsoft nach Kenntnis der Arbeitsgruppe in großem Umfang und grundsätzlich für eigennützige Zwecke erhebt.

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

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

Der aktuelle Datenschutznachtrag vom September 2022 enthält **Veränderungen der bisherigen Bestimmungen,** die die Offenlegung von Microsoft als Auftragsverarbeiter bereitgestellten Daten im Rahmen eigener Geschäftszwecke „zur Erfüllung rechtlicher Verpflichtungen“ regeln. Dabei enthalten die Änderungen zwar neue Formulierungen, im Ergebnis bleiben die Befugnisse aber ähnlich umfangreich.

Mit der Regelung wird etwa das Weisungsrecht des Kunden in Bezug auf Offenlegungen der im Auftrag verarbeiteten Daten eingeschränkt. Der Datenschutznachtrag erlaubt die Offenlegung, wenn diese rechtlich vorgeschrieben oder im „Datenschutznachtrag“ beschrieben sind. Solche Offenlegungen sind nicht auf Weisungen des Verantwortlichen beschränkt, sodass sie vor dem Hintergrund des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a) DSGVO nur zulässig sind, wenn sie sich auf Verpflichtungen aus dem Unions- oder mitgliedstaatlichen Recht, dem Microsoft unterliegt, beschränken. Dies ist nicht der Fall. Damit **genügt die Weisungsbindung Microsofts nicht den gesetzlichen Mindestanforderungen** gemäß Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO.

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

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

Die ab 15. September 2022 geltende Version des „Datenschutznachtrags“ enthält gegenüber der vom AK Verwaltung geprüften Version **Ergänzungen zu den technisch-organisatorischen Maßnahmen**. Für ausdrücklich beschränkte bestimmte Datenkategorien (nämlich Kundendaten in „Core-Onlinediensten“ und nunmehr auch „Professional Services-Daten“) bestehen Garantie- und Datensicherheitsmaßnahmen. Zudem hat Microsoft dargelegt, dass es Interessierten nach einer Anmeldung Zugang zur Website servicetrust.microsoft.com („Servicetrust Website“), unter der Informationen über die durchgeführten technisch-organisatorischen Maßnahmen eingesehen werden können, bietet.

Es bleiben Rechtsunsicherheiten, da die Garantien über „Sicherheitsmaßnahmen“ formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten, nämlich „Kundendaten in „Core-Onlinediensten“ und „Professional-Service-Daten“, erfassen.

3.5. Löschung und Rückgabe personenbezogener Daten

Microsoft hat der Arbeitsgruppe die einzelnen Löschprozesse erläutert. Die Erläuterungen zeigen mit Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der „Cyberabwehr“, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschfristen für personenbezogene Daten nicht verlängern sollten. Zudem haben sich im Zuge der Umgestaltung des „Datenschutznachtrags“ auch Änderungen in Bezug auf Löschung ergeben, die allerdings auch Unklarheiten und Widersprüche mit sich bringen.

Nach Bewertung der Arbeitsgruppe genügt die Ausgestaltung der Rückgabe- und Löschverpflichtung **nicht in jedem Fall den gesetzlichen Anforderungen** aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO. Verantwortliche können wegen der Unklarheit der Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.

3.6. Information über Unterauftragsverarbeiter

Die Arbeitsgruppe hat mehrfach, teils kontrovers mit Microsoft die Ausgestaltung der Kontrollrechte des Verantwortlichen bei Veränderungen der Unterauftragsverarbeitungsverhältnisse diskutiert. Microsoft konnte trotz anfänglicher Vorbehalte zu einer Umstellung des bisher als Hol-Schuld des Verantwortlichen ausgestalteten Verfahrens zu organisatorischen und vertraglichen Anpassungen bewogen werden. Dies hat zu einer bereits Ende März eingeführten **Neugestaltung des Unterrichtungsverfahrens** geführt, die im aktuellen „Datenschutznachtrag“ vom September 2022 zu einer Streichung des bisherigen „Hol-Schuld“-Verfahrens geführt hat.

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

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

3.7. Datenübermittlungen in Drittstaaten

Der „Datenschutznachtrag“ vom September 2022 enthält die Regelung, dass **der Kunde Microsoft „beauftragt (…), (…) personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind“.** Für sämtliche Übermittlungen von insbesondere personenbezogenen Daten gelten danach die von Microsoft implementierten Standardvertragsklauseln der EU-Kommission von 2021.

Die Gespräche der Arbeitsgruppe mit Microsoft bestätigten entsprechend den vertraglichen Regelungen, dass bei der Nutzung von Microsoft 365 personenbezogene Daten jedenfalls in die USA übermittelt werden. **Eine Nutzung von Microsoft 365 ohne Übermittlungen personenbezogener Daten in die USA sei nicht möglich.** Ab Dezember 2022 plane Microsoft, allen Kunden im EU-Raum anzubieten, Kundendaten, Supportdaten und sonstige personenbezogene Daten der Kunden grundsätzlich – d.h. nicht ausnahmslos, nicht etwa für bestimme IT-Sicherheitsmaßnahmen – im EU-Raum zu speichern und zu verarbeiten („EU Data Boundary“).

Für die USA hat der EuGH in „Schrems II“ festgestellt, dass FISA 702 und E.O. 12333 unverhältnismäßige Zugriffsrechte für US-Geheimdienste vorsehen und für EU-Bürger kein gerichtlicher Rechtsschutz gegeben ist. Um die vom EuGH identifizierten am EU-Maßstab gemessenen grundrechtlichen Unzulänglichkeiten von FISA 702 auszugleichen, wäre es erforderlich, Maßnahmen zu ergreifen, die den Zugriff der US-Behörden – und damit von Microsoft – auf personenbezogene Daten verhindern oder ineffektiv machen. Viele der in Microsoft 365 enthaltenen Dienste erfordern einen Zugriff von Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten. Die naheliegende Möglichkeit der **Verschlüsselung der verarbeiteten Daten ist regelmäßig nicht möglich,** beispielsweise wenn die Daten im Browser angezeigt werden müssen. Microsoft hat somit regelmäßig und letztlich schon zur Erfüllung vertraglicher Leistungspflichten die Möglichkeit, Daten im Klartext zu lesen. Es handelt sich mithin um eine klassische Ausprägung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. **Für diesen Anwendungsfall ist es den Aufsichtsbehörden bislang nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten.**

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

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

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

Ob und in welchem Umfang durch die am 7. Oktober 2022 von US-Präsident Biden und Generalstaatsanwalt Garland vorgestellte Executive Order „Enhancing Safeguards for United States Signals Intelligence Activities“ und begleitende Rechtsverordnungen des US-Justizministeriums Änderungen des für die Bewertung von Drittstaatentransfers maßgeblichen Bedingungen des US-Rechts eingetreten sind, bleibt angesichts noch ausstehender Vollzugsschritte zur Implementierung dieser Regelungen im Rahmen dieses Berichts unberücksichtigt