Anlage 1

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365

vom XX.XX.XXXX

Ziel des Beschlusses ist es, eine unter den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einheitliche, intern abgestimmte Grundlage für weitere Gespräche mit Microsoft zu schaffen.

Sachverhalt:

Der AK Verwaltung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die dem Einsatz des Produktes Microsoft Office 365 zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020 – geprüft und hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) bewertet. Er kommt zu dem Ergebnis, dass auf Basis dieser Unterlagen jedenfalls mit Stand Januar 2020 kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich war. Die DSK wird auf dieser Basis mit Microsoft in den Dialog treten um die identifizierten Probleme zu lösen.
Die Folgen des Urteils des EuGH C-311/18 (Schrems II) finden in diesem Papier noch keine Berücksichtigung.

Bewertung des AK Verwaltung:

1.) Art und Zweck der Verarbeitung, Art der personenbezogenen Daten

Auch unter der Berücksichtigung der Klassifizierung des Dienstes MS Office 365 als cloud-spezifischer Dienst, wonach es ggf. sachdienlich ist, die Arten

personenbezogener Daten und deren Verarbeitungszweck verallgemeinert zu benennen, muss es dem Auftraggeber dennoch möglich sein, beides näher zu beschreiben und ggf. zu konkretisieren.

Dies betrifft insbesondere die Beschreibung personenbezogener Daten hinsichtlich der gesonderten datenschutzrechtlichen Anforderungen und Risikostufen, bspw. bei Daten nach Art. 9 DS-GVO, als auch der für den Auftraggeber maßgeblichen Zwecke.

Seitens des Auftragsverarbeitungsvertrages muss es ersichtlich sein, in welchem Umfeld (Fachverfahren) die Datenverarbeitung stattfindet und für welche Zwecke die Daten im Auftrag verarbeitet werden sollen. In diesem Zusammenhang wird Microsoft empfohlen, den Abstraktionsgrad zu verringern und Freifelder, welche erforderlichenfalls angepasst werden können, einzusetzen. Ggf. ist dadurch sogar eine konkrete Benennung im Einzelfall möglich.

2.) Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für legitime Geschäftszwecke

Microsoft verweist innerhalb der Datenschutzbestimmungen für Microsoft Online-Dienste (Data Processing Agreement (DPA)) darauf, dass soweit es personenbezogene Daten im Zusammenhang mit legitimen Geschäftstätigkeiten von Microsoft verwendet oder anderweitig verarbeitet, Microsoft ein unabhängiger Datenverantwortlicher für diese Verwendung und für die Einhaltung aller geltenden Gesetze sowie der Erfüllung der Verpflichtung als Verantwortlicher verantwortlich ist.

Auch wenn nunmehr eine Aufzählung dieser legitimen Geschäftstätigkeiten erfolgt, ist weiterhin nicht eindeutig ersichtlich, welche weiteren personenbezogenen Daten in diesem Rahmen verarbeitet werden. Dies betrifft insbesondere die Verarbeitung personenbezogener Daten in Bezug auf die Aktivitäten

Microsofts unter den Punkten 3), 4), 5) und 6) der Definition der „legitimen Geschäftstätigkeit“.[1]

Zudem besteht für die Übermittlung weiterer personenbezogener Daten vom Verantwortlichen an Microsoft, z.B. im Rahmen der Telemetrie, neben dem Auftragsverarbeitungsvertrag keine weitere Rechtsgrundlage.

Soweit Verantwortliche für die Übermittlung an Microsoft als eigenständig Verantwortlichem für die Verarbeitung der Daten vom Verantwortlichen und Dritten für „legitime Geschäftszwecke“ ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f) DS-GVO darlegen könnten, gilt dies gemäß Art. 6 Abs. 1 Satz 2 DS-GVO nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Es bedarf daher einer eigenen Rechtsgrundlage, die es der öffentlichen Verwaltung erlaubt, Daten von Beschäftigten oder Bürgerinnen und Bürgern für diese Zwecke zur Verfügung zu stellen.

Die jeweiligen Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (gemäß Art. 6 Abs. 3 lit. b DS-GVO) können dabei wegen des (aufgrund der Grundrechtsrelevanz) strengen Erforderlichkeitsgrundsatzes nur bedingt als Rechtsgrundlage herangezogen werden. Nur unter der Voraussetzung, dass z.B. ein nachhaltig sicherer Einsatz der Software lediglich möglich ist, wenn der Anbieter bestimmte personenbezogene Systemdaten verarbeiten kann, kann die entsprechende Datenverarbeitung auch zur Erfüllung der Aufgaben erforderlich sein.

Jedenfalls für öffentliche Stellen sind daher nicht alle Anwendungsfälle der „legitimen Geschäftszwecke“ abgebildet.

[1] (3) interne Berichterstattung und Modellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; (5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen

3.) Offenlegung verarbeiteter Daten – Cloud Act

In den Datenschutzbestimmungen für Microsoft Onlinedienste verweist Microsoft darauf, dass verarbeitete Daten außerhalb der Weisung des Kunden auch offengelegt werden können, wenn die Datenschutzbestimmungen es vorsehen oder dies gesetzlich vorgeschrieben wird.

Diese Beschreibung ist nicht hinreichend konkret und bestimmt nicht die durch den Auftraggeber vertraglich zu definierenden Rechte. Die Ausnahme darf sich ausschließlich auf das Recht der Union oder einzelstaatliches Recht eines Mitgliedsstaates beziehen, wobei nicht ausgeschlossen ist, dass zu diesem Recht auch Rechtshilfeabkommen gelten, die die Union oder einzelne Mitgliedsstaaten mit Drittstaaten schließen.

Die konkrete Umsetzung und die Auswirkungen des Cloud Acts, dem Microsoft als US-amerikanischer Hersteller unterliegt, auf die datenschutzrechtliche Frage zur rechtlich zulässigen Weitergabe personenbezogener Daten in diesem Kontext, sind nicht abschließend geklärt. Diese Bewertung ist auch im Lichte der jüngsten EuGH-Rechtsprechung vorzunehmen, die das Privacy Shield für unwirksam erklärt und Datenübertragungen in die USA generell in Frage stellt, vgl. EuGH, 16.7.2020 – C-311/18 “Schrems II”.

Microsoft nutzte – flankierend zur Privacy Shield Zertifizierung – auch Standardvertragsklauseln. Auch diese sind auf Basis der jüngsten EuGH-Rechtsprechung neu zu bewerten.

4.) Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO

Seitens der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder besteht Konsens, dass der Auftraggeber grundsätzlich die Umset-

zung und Beschreibung der technischen und organisatorischen Maßnahmen durch die Online-Service-Terms, die Datenschutzbestimmungen sowie weiterer durch Microsoft bereitgestellter Dokumentation prüfen und ausreichend (Zusatz-) Informationen einholen können muss. Zwar ist eine entsprechende IT-Sicherheitsrichtlinie in den DPA erwähnt (nicht in den OST), diese liegt jedoch vor Vertragsschluss nicht vor.

Grundsätzlich ist daher festzuhalten, dass in den Standard-OST seitens Microsoft keine ausreichende Darstellung erfolgt, welche dem Risiko angemessenen Maßnahmen der angebotene Onlinedienst für die Verarbeitung von personenbezogenen Daten bietet. Microsoft stellt darauf ab, dass der Verantwortliche allein für die unabhängige Entscheidung verantwortlich ist, ob die technischen und organisatorischen Maßnahmen für einen bestimmten Onlinedienst seinen Anforderungen entsprechen, einschließlich seiner Sicherheitsverpflichtungen gemäß geltenden Datenschutzvorschriften. Die derzeitigen Darstellungen zu den technischen und organisatorischen Maßnahmen in den Vertragsunterlagen allein reichen für den Verantwortlichen nicht aus (und sind durch den Verantwortlichen auch kaum zu prüfen), um eine objektive Einschätzung zu treffen, ob die Maßnahmen dem Risiko angemessen sind.

5.) Löschung und Rückgabe personenbezogener Daten

Microsoft differenziert im Rahmen der Verarbeitung zwischen den Kundendaten, die sich aus dem Auftragsverhältnis ergeben und Daten, die zur Erbringung „professioneller Dienstleistungen“ und der Verarbeitung für „legitime Geschäftszwecke“ eigenverantwortlich verarbeitet werden.

Seitens Microsoft werden entsprechend der Rolle als „Verantwortlicher“ Daten, die zu eigenen Zwecken verarbeitet werden, nicht gelöscht.

Es ist zwar nachzuvollziehen, dass diese Daten gem. Definition nicht Teil der Auftragsverarbeitung sind und demnach aufgrund einer anderen Rechtsgrundlage verarbeitet werden, dennoch ist zu hinterfragen, wie lange die Daten für eigene Zwecke vorgehalten werden. Hierzu äußert sich Microsoft nicht.

6.) Information über Unterauftragsverarbeiter

In Bezug auf die Weitergabe personenbezogener Daten an Unterauftragnehmer ist die „vorherige schriftliche Zustimmung des Kunden zur Weitervergabe der Verarbeitung von Kundendaten und personenbezogenen Daten durch Microsoft“ nur dann ausreichend, wenn eine Übersicht der zum Zeitpunkt der Unterzeichnung des Auftragsverarbeitungsvertrages vom Verantwortlichen (Kunden / Auftraggeber) genehmigten Unterauftragnehmer aufgenommen wird (siehe dazu auch 3.2.7 der Opinion 14/2019 des Europäischen Datenschutzausschusses).

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