Der Bayerische Landesbeauftragte
für den Datenschutz

Microsoft als Auftragsverarbeiter beim Einsatz von „Microsoft 365“

Handreichung

Stichwörter: Auftragsverarbeitungsvereinbarung, Microsoft 365 – Microsoft 365, Auftragsverarbeitungsvereinbarung | **Stand:** 1. September 2023

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Festlegung vom 25. November 2022 zur Arbeitsgruppe DSK „Microsoft-Onlinedienste“ festgestellt, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann. Insbesondere erfüllt dieser Datenschutznachtrag, den Microsoft seinen Kunden als Standard-Auftragsverarbeitungsvereinbarung im Rahmen der Beauftragung von Produkten und Services der Produktfamilie „Microsoft 365“ anbietet, nicht die Anforderungen von Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).[1]

Um die Verantwortlichen, die ein Microsoft 365-Produkt erwerben und in ihrem Betrieb oder ihrer Behörde einsetzen wollen, bei der Erfüllung ihrer Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu unterstützen, haben Datenschutzaufsichtsbehörden der Länder, darunter der Bayerische Landesbeauftragte für den Datenschutz, eine Handreichung entwickelt, die dabei helfen soll, die von der DSK genannten Anforderungen an eine rechtskonforme Auftragsverarbeitungsvereinbarung umzusetzen. Die Handreichung bezieht sich auf den „Datenschutznachtrag zu den Produkten und Services von Microsoft“ auf dem Stand der Aktualisierung vom 1. Januar 2023.[2] Eine Überprüfung, ob Microsoft den Datenschutznachtrag zwischenzeitlich geändert hat, ist den Verantwortlichen vor Verwendung der Handreichung stets anzuraten.

1 Vgl. Zusammenfassung des Berichts der Arbeitsgruppe DSK „Microsoft-Onlinedienste“ und Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“, Internet: https://www.datenschutz-bayern.de/inhalte/dsk_ent_t.htm.

2 Internet: https://wwlpdocumentsearch.blob.core.windows.net/prodv2/MicrosoftProductandServicesDPA(WW)(German)(Jan2023)(CR).docx?sv=2020-08-04&se=2123-08-25T14:32:38Z&sr=b&sp=r&sig=s%2BZjrTDsWc%2Bwmx5R4mf3EFYy5jiG%2FvB%2BXelznbA%2BcY0%3D.

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Handreichung
für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit Microsoft für den Einsatz von „Microsoft 365“

I. Vorbemerkung

Öffentliche Stellen (z. B. Behörden) und nicht-öffentliche Stellen (z. B. Unternehmen) stellen Microsoft beim Einsatz der Produktfamilie Microsoft 365 Daten zur Verfügung, die in Rechenzentren des Technologieunternehmens innerhalb, aber auch außerhalb der Europäischen Union gespeichert werden und auf die möglicherweise nicht nur die Auftraggeber von Microsoft Zugriff haben. Soweit unter diesen Daten auch personenbezogene Daten sind, sind die öffentlichen und nicht-öffentlichen Stellen Verantwortliche im Sinne der Datenschutz-Grundverordnung (DSGVO) und entscheiden über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten ihrer Beschäftigten oder von Dritten, mit denen sie zusammenarbeiten bzw. in geschäftlichem Kontakt stehen. Microsoft wiederum ist mit der Verarbeitung (z. B. Speicherung) der Daten in seinen Rechenzentren als Auftragsverarbeiter für die öffentlichen und nicht-öffentlichen Stellen tätig. Die Standard-Auftragsverarbeitungsvereinbarung, die Microsoft seinen Kunden (d. h. den datenschutzrechtlich Verantwortlichen) im Rahmen der Beauftragung von Produkten und Services der Produktfamilie „Microsoft 365“ anbietet (nachstehend „DPA“),[1] sieht aber auch vor, dass Microsoft personenbezogene Daten zu eigenen Geschäftszwecken verarbeitet, so z. B. zur Berechnung von Mitarbeiterprovisionen oder für die interne Berichterstattung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im November 2022 festgestellt, dass die Standardvereinbarung nicht den Anforderungen des Art. 28 Abs. 3 DSGVO entspricht.[2] Solange insbesondere die notwendige Transparenz bezüglich der Verarbeitung personenbezogener Daten aus der Auftragsdatenverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann der Nachweis, Microsoft 365 datenschutzkonform zu betreiben, von den Verantwortlichen nicht erbracht werden.

Was heißt das nun für die öffentlichen und nicht-öffentlichen Stellen, wenn diese ein Microsoft 365-Produkt erwerben und in ihrem Betrieb oder ihrer Behörde einsetzen wollen? Oder mit anderen Worten: Gehen die Feststellungen der DSK nur Microsoft etwas an oder sind auch die Kunden von Microsoft datenschutzrechtlich adressiert?

Gemäß Art. 5 Abs. 2 DSGVO sind diejenigen, die den Einsatz eines Produkts, wie Microsoft 365, verantworten, dabei auch für die Einhaltung des Datenschutzes verantwortlich und müssen diese Einhaltung nachweisen können (sog. Rechenschaftspflicht). Für die datenschutzrechtlichen Anforderungen an Auftragsverarbeitungsverträge enthält Art. 28 DSGVO Vorgaben, die von diesen zu erfüllen sind. Somit richten sich datenschutzrechtliche Anforde-

---

1 Datenschutznachtrag zu den Produkten und Services von Microsoft, deutsche Fassung, Stand 1. Januar 2023, Internet: https://wwlpdocumentsearch.blob.core.windows.net/prodv2/MicrosoftProductandServices-DPA(WW)(German)(Jan2023)(CR).docx?sv=2020-08-04&se=2123-08-07T12:52:52Z&sr=b&sp=r&sig=WLlo-SyFSWGiu0dUwFBjHJK615N6%2FvlQtBMYDMTbCHCc%3D.

2 Diese Feststellung bezog sich zuletzt auf das DPA mit Stand 15. September 2022.

rungen im Zusammenhang mit dem Einsatz von Microsoft 365 nicht nur an Microsoft als Hersteller und Vertreiber der Software, sondern auch an die einsetzenden öffentlichen und nicht öffentlichen Stellen als datenschutzrechtlich Verantwortliche.

Neben eigenen Maßnahmen, mit denen öffentliche und nicht-öffentliche Stellen sicherstellen können, dass beim Einsatz von Microsoft 365 so wenig personenbezogene Daten wie möglich verarbeitet werden, z. B. durch die Verwendung pseudonymer Mailadressen/Accounts für die Beschäftigten, ist es der Auftragsverarbeitungsvertrag mit Microsoft, der sicherstellen muss, dass personenbezogene Daten rechtmäßig verarbeitet werden, was bislang allerdings – jedenfalls ohne entsprechende vertragliche Anpassungen – nicht der Fall ist.

Änderungen oder Ergänzungen der Vertragsbedingungen mit Microsoft liegen nicht alleine in der Hand der einsetzenden öffentlichen und nicht-öffentlichen Stellen, sondern sind davon abhängig, dass Microsoft als Vertragspartner diesen zustimmt. Dessen ungeachtet obliegt es den öffentlichen und nicht-öffentlichen Stellen, die Microsoft 365 einsetzen, vor dem Hintergrund ihrer datenschutzrechtlichen Pflichten als Verantwortliche, alle ihnen zur Verfügung stehenden Möglichkeiten zu nutzen, auf datenschutzkonforme Vereinbarungen mit Microsoft hinzuwirken und eine datenschutzkonforme Nutzung zu ermöglichen. Zudem gibt es Maßnahmen, die von den öffentlichen und nicht-öffentlichen Stellen unabhängig von vertraglichen Vereinbarungen mit Microsoft getroffen werden können, um den Datenschutz beim Einsatz von Microsoft 365 zu verbessern.

Diese Maßnahmen sowie die in Betracht kommenden vertraglichen Vereinbarungen, die dazu beitragen, dass der Einsatz von Microsoft 365 datenschutzkonform erfolgen kann, sind in der folgenden Handreichung beschrieben. Die nachstehenden Hinweise sollen die Verantwortlichen dabei unterstützen, auf eine den Anforderungen des Art. 28 Abs. 3 DSGVO entsprechende Auftragsverarbeitungsvereinbarung (nachstehend: „AV-Vereinbarung“) mit Microsoft hinzuwirken. Sie knüpfen an die Problemfelder an, die die Arbeitsgruppe der DSK „Microsoft Onlinedienste“ in ihrem Bericht vom 2. November 2022[3] (nachstehend: „Bericht der DSK“) und zuvor der Arbeitskreis „Verwaltung“ der DSK in seiner Bewertung vom 15. Juli 2020[4] beschrieben haben. An diesen Hinweisen kann sich der Verantwortliche orientieren, um eine Zusatzvereinbarung zum DPA abzuschließen.

Ein Kurzüberblick über die notwendigen vertraglichen Änderungen und Maßnahmen ist nachstehend in Abschnitt II dargestellt; eine Langversion, in der der datenschutzrechtliche Handlungsbedarf einschließlich der jeweiligen Herleitung eingehend begründet und erläutert wird, findet sich in der Anlage.

Nicht Gegenstand dieser Handreichung ist eine Befassung mit der Problematik der Übermittlung personenbezogener Daten in sog. Drittländer, auch angesichts der derzeitigen Entwicklungen zum Datentransfer in die USA, deren Bewertung zum Zeitpunkt der Erstellung dieser Handreichung noch nicht abgeschlossen ist. Daher wird im Hinblick auf den Drittlandtransfer auf die vorhandenen Materialien des EDSA und der DSK verwiesen. Nicht betrachtet werden

---

[3] AG DSK „Microsoft-Onlinedienste“, Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, Stand 2. November 2022, Internet: https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf.

[4] Siehe DSK, Festlegung zu TOP 9 der Zwischenkonferenz vom 22. September 2020, Internet: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf.

konnten ferner insbesondere sämtliche technischen Funktionen von Microsoft 365 sowie Spezifika der einzelnen Anwendungen. Diese muss der Verantwortliche eigenständig einer datenschutzrechtlichen Prüfung zuführen, auch in Abhängigkeit davon, welche Funktionen er für die Verarbeitung welcher Daten einsetzen möchte. Auch das Thema „Extraterritoriale Zugriffe öffentlicher Stellen aus Drittländern“ wurde weitgehend ausgeklammert, da insofern noch offen ist, wie die Rechtmäßigkeit entsprechender Datenverarbeitungen durch eine vertragliche Gestaltung beeinflusst werden könnte.

Ferner ist zu beachten, dass aufgrund der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO jede vertraglich vereinbarte Verpflichtung auch nachweisbar umgesetzt werden muss. Die Nachweispflicht liegt beim Verantwortlichen, Microsoft sollte hier in der Praxis aber entsprechende Hilfestellungen bereitstellen.

[!] ToDo:

- Eine zwischen dem Verantwortlichen und Microsoft abzuschließende Zusatzvereinbarung zum DPA sollte klarstellen, dass diese Zusatzvereinbarung gegenüber sämtlichen entgegenstehenden Vertragstexten (des DPA, aber auch z. B. der Product Terms und der einzelnen Produktdokumentationen), die seitens Microsoft einbezogen werden, Vorrang hat und diesen im Kollisionsfalle vorgeht.
- Der Verantwortliche muss sich auch mit allen weiteren datenschutzrechtlichen Aspekten befassen, die über die reine Vertragsgestaltung der AV-Vereinbarung hinausgehen, z. B. der Prüfung der Angemessenheit der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten im konkreten Fall und ggf. der Vornahme eigener technischer und organisatorischer Maßnahmen.

II. Wesentliche Handlungshinweise

Die nachstehenden Handlungshinweise werden in der Anlage, auf deren Randnummern jeweils referenziert wird, genauer erläutert. Die Auflistung in diesem Kapitel II dient lediglich einem ersten Überblick über die wesentlichen ToDo’s.

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

Folgende Punkte betreffen insbesondere die Abschnitte „Art der Datenverarbeitung; Eigentumsverhältnisse“, „Verarbeitungsdetails“, Anhang B des DPA und Art. 28 Abs. 3 Satz 1 DSGVO:

- Hinsichtlich der Zwecke der Verarbeitung muss der Verantwortliche überprüfen, inwiefern er selbst eine Rechtsgrundlage hat, um personenbezogene Daten zu den im DPA genannten Zwecken des Verantwortlichen zu verarbeiten. Liegt dem Verantwortlichen eine solche Rechtsgrundlage nicht vor, kann er auch Microsoft nicht mit der Verarbeitung zu solchen Zwecken beauftragen. Die Verarbeitung zu solchen Zwecken durch Microsoft im Auftrag des Verantwortlichen muss also abbedungen werden. Kommt der Verantwortliche hingegen zu der Feststellung, dass er personenbezogene Daten zu den genannten Zwe-

cken verarbeiten und somit auch durch Microsoft im Auftrag verarbeiten lassen kann, können diese Zwecke im Vertrag weiterhin aufgeführt werden, jedoch muss eine Beschränkung auf das zur Leistungserbringung Erforderliche erfolgen. → vgl. Rn. 2

- Hinsichtlich der Art der Verarbeitung muss aus der Vereinbarung erkennbar sein, welche Verarbeitungsvorgänge gem. Art. 4 Nr. 2 DSGVO für den konkreten Vertrag relevant sind. → vgl. Rn. 2
- Die Angaben, welche Kategorien personenbezogener Daten welcher betroffenen Personen im Auftrag des Verantwortlichen verarbeitet werden sollen, hat der Verantwortliche in der AV-Vereinbarung einzutragen. Dies kann entweder durch eine Einbeziehung des Verzeichnisses der Verarbeitungstätigkeiten (VVT) geschehen, oder durch manuelles Ausfüllen der Tabelle aus der Anlage, Rn. 3. Der Verantwortliche muss, ausgehend davon, welche Funktionen die zu nutzende Anwendung hat, angeben, welche Kategorien personenbezogener Daten welcher Personen hierzu verarbeitet werden müssen. → vgl. Rn. 3
- Den Angaben „Kategorien personenbezogener Daten“ und „Kategorien betroffener Personen“ sollten auch direkt die Angaben zur Art und zu den Zwecken der Verarbeitung zugeordnet werden. → vgl. Rn. 3
- Der Übersichtlichkeit halber könnten alle vorgenannten Angaben in einer Tabelle aufgeführt werden; eine Zuordnung in anderer Form, z. B. im Fließtext, bleibt jedoch weiterhin möglich. → vgl. Rn. 3
- Es sollte vertraglich sichergestellt werden, dass diese abschließende Auflistung den Anhang B des DPA ersetzt. → vgl. Rn. 3

2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für Geschäftstätigkeiten, die durch Bereitstellung der Produkte und Services an den Kunden veranlasst sind (nachstehend „für Microsofts Geschäftszwecke“)

Folgende Punkte betreffen insbesondere die Abschnitte des DPA „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“ und „Art der Datenverarbeitung/Eigentumsverhältnisse“:

- Für die rechtskonforme vertragliche Formulierung wäre es am einfachsten, wenn jede Verarbeitung von personenbezogenen Daten seitens Microsoft zu eigenen Zwecken unterbliebe. Sofern Microsoft die Möglichkeit zur Verarbeitung der Daten zu eigenen Geschäftszwecken eingeräumt werden soll, muss der Verantwortliche zunächst klären, welche Verarbeitungen von welchen personenbezogenen Daten in welchem Umfang zu Microsofts eigenen Zwecken durchgeführt werden. Anschließend muss der Verantwortliche beurteilen, ob er eine Rechtsgrundlage für die Zurverfügungstellung dieser personenbezogenen Daten besitzt. Alle Verarbeitungszwecke, für welche keine Rechtsgrundlage gefunden werden konnte, sind vertraglich auszuschließen und technisch zu unterbinden. → vgl. Rn. 4 ff.
- Es muss vertraglich geregelt sein, ob es sich bei Telemetrie- und Diagnosedaten um personenbezogene Daten handelt. → vgl. Rn. 7 ff.
- Die Verarbeitung personenbezogener Daten der Nutzer zu Microsofts eigenen Zwecken muss bei einem Einsatz durch öffentliche Stellen ausgeschlossen werden bzw. müssen

die ausnahmsweise zulässigen Verarbeitungen zu Microsofts eigenen Zwecken unter Angabe der jeweiligen Rechtsgrundlage und Zwecke klar beschrieben werden.
→ vgl. Rn. 10 ff.

- Alle auf einer Einwilligung basierenden Verarbeitungsvorgänge für Microsofts eigene Zwecke müssen vom Verantwortlichen per Konfiguration aktivier- und deaktivierbar sein. Dies muss durch den Verantwortlichen geprüft und ggf. vertraglich vereinbart werden.
→ vgl. Rn. 10 ff.

3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen

Folgende Punkte betreffen die Abschnitte „Verarbeitung personenbezogener Daten, DSGVO/ Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ und „Offenlegung verarbeiteter Daten“ sowie den Anhang C des DPA und die Vorgaben gemäß Art. 28 Abs. 1 DSGVO:

- Die Regelungen des DPA zum Weisungsrecht sind widersprüchlich; dies ließe sich durch eine vertragliche Klarstellung der vorrangigen Geltung von Anlage I auflösen. Akzeptabel wäre es auch, für solche Weisungen ein Vertragsänderungsverfahren (in Abweichung von der einseitigen Erklärung der Weisungen) vorzusehen, die dazu führen würden, dass der vom Verantwortlichen bestellte Funktionsumfang erweitert werden würde.
→ vgl. Rn. 14 f.

- Ferner sollte der Begriff der Weisung restriktiv definiert werden, um zu verhindern, dass Verantwortliche ungewollt „Weisungen“ erteilen. So kann z. B. bei einer bloßen Nutzung eines Service nicht von einer dokumentierten Weisung ausgegangen werden.
→ vgl. Rn. 14 f.

- Soweit sich der Umfang der Weisungen nach der Produktdokumentation richtet, ist darauf zu achten, dass die konkrete Produktdokumentation dem Vertrag beigefügt ist oder anderweitig dokumentiert und für den Verantwortlichen leicht zugänglich ist. Auch etwaige Änderungen der Produktdokumentation müssen als Vertragsänderung dokumentiert werden. → vgl. Rn. 14 f.

- Es ist vertraglich klarzustellen, dass personenbezogene Daten der Nutzer durch Microsoft nur offengelegt werden dürfen, wenn eine gesetzliche Pflicht nach Vorgabe der DSGVO oder des Rechts der EU-Mitgliedsstaaten besteht. → vgl. Rn. 16 f.

- Im Hinblick darauf, dass Microsoft sich vorbehält, Basiskontaktinformationen an Dritte weiterzugeben (vgl. letzter Satz des Abschnittes „Offenlegung verarbeiteter Daten“) sollten Verantwortliche ihre Basiskontaktinformationen nach Möglichkeit auf nicht personenbezogene Angaben (z. B. Unternehmensadresse und/oder Funktionspostfächer) beschränken.
→ vgl. Rn. 16 f.

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

Folgende Hinweise betreffen insbesondere den Unterabschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ des Abschnitts „Datenverarbeitung; Eigentumsverhältnisse“, den Abschnitt „Datensicherheit“ und den Anhang A des DPA:

- Der Vertrag hat zu spezifizieren, welche personenbezogenen Daten neben den Nutzerdaten dem Zweck der Gewährleistung der Sicherheit dienen. Die Inhaltsdaten kann der Verantwortliche lediglich selbst benennen, für die Auflistung der darüberhinausgehenden Daten (z. B. Anmeldedaten, Diagnosedaten etc.) wird er ggf. Unterstützung von Microsoft benötigen, es sei denn, er kann abschätzen, welche Daten hier erforderlich sind. Microsoft muss ebenfalls überblickartig mitteilen, warum genau die spezifizierten Daten zur Gewährleistung der Sicherheit notwendig sind. → vgl. Rn. 18 ff.
- Ferner sollte geklärt werden, welche der benannten personenbezogenen Daten für die Zwecke „Fehlerbehebung“ und „Förderung der Sicherheit“ genutzt werden und auf welche Art und Weise diese Daten verarbeitet werden, z. B. durch einen Verweis auf konkrete Dokumente, in denen dies beschrieben ist. Auch hier gilt, dass der Verantwortliche eine Rechtsgrundlage zu den beauftragten Verarbeitungsvorgängen nachweisen muss. Andernfalls müssen diese vertraglich ausgeschlossen werden. → vgl. Rn. 18 ff.
- Zu beachten ist, dass bei der Verarbeitung der Telemetrie- und Diagnosedaten sowie in sonstigen sicherheitsrelevanten Datenverarbeitungsprozessen von Microsoft die Anforderungen an die Umsetzung der Mandantentrennung fortbestehen. Als kompensierende Maßnahmen sollten die Verantwortlichen die Möglichkeiten zur Gestaltung eigener technisch-organisatorischen Maßnahmen prüfen und dabei die relevanten Studien und Lösungsansätze berücksichtigen. → vgl. Rn. 18 ff.
- Alle unrechtmäßigen, nicht notwendigen oder unverhältnismäßigen Datenverarbeitungen müssen vertraglich ausgeschlossen und technisch unterbunden werden. → vgl. Rn. 23 ff.
- Der Verantwortliche muss die Sicherheit auch dann gewährleisten, wenn die betroffenen Personen auf die Einhaltung verzichtet haben. → vgl. Rn. 23 ff.
- Der Verantwortliche muss prüfen, ob die vertraglich vorgesehenen Maßnahmen zum angemessenen Schutz der Verarbeitung seiner personenbezogenen Daten durch Microsoft ausreichend sind und – soweit erforderlich – zwingend notwendige zusätzliche Maßnahmen ebenfalls vertraglich vereinbaren. → vgl. Rn. 23 ff.

5. Löschen personenbezogener Daten

Folgende Punkte betreffen den Abschnitt „Speicherung und Löschung von Daten“:

- Die im DPA aufgeführten Löschfristen sind vertraglich anzupassen, d. h. in der Regel zu kürzen. → vgl. Rn. 26 ff.
- Der Verantwortliche muss ggf. vertragliche Anpassungen vornehmen, um Microsoft als Auftragsverarbeiter in eigene Löschprozesse zu integrieren. → vgl. Rn. 26 ff.
- Die Ausnahmen von der Löschungsverpflichtung sollten eingeschränkt und konkretisiert werden. → vgl. Rn. 26 ff.

- Über die im DPA formulierten bzw. noch zu ergänzenden Regelungen bezüglich der Löschung von personenbezogenen Daten müssen Verantwortliche auch die verwendeten Anwendungen prüfen und ggf. spezifische Maßnahmen in ihre eigenen Löschprozessen aufnehmen. → vgl. Rn. 26 ff.
- Sonderregelungen für „Zusätzliche Professional Services“ sollten entfallen. → vgl. Rn. 26 ff.

6. Information über Unterauftragsverarbeiter

Folgende Punkte betreffen insbesondere den Abschnitt „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“:

- Die Information über Unterauftragsverarbeiter muss den Namen sowie die Anschrift des Unterauftragsverarbeiters, Namen, Funktion und Kontaktdaten der Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der betreffenden Verarbeitung und eine eindeutige Benennung des betroffenen Produkts/ der Funktion (einschließlich einer klaren Abgrenzung der Zuständigkeiten/ Verantwortungsanteile, falls mehrere Unterauftragsverarbeiter genehmigt werden) enthalten. → vgl. Rn. 32 ff.
- Dies gilt auch für die Einbindung von neuen Unterauftragsverarbeitern sowie für Änderungen im Rahmen bestehender Unterauftragsverhältnisse. → vgl. Rn. 32 ff.
- Microsoft als Auftragsverarbeiter muss sich verpflichten, den Verantwortlichen „proaktiv“ über neue Unterauftragsverarbeiter zu informieren, beispielsweise via Push-Benachrichtigung. → vgl. Rn. 32 ff.

7. Weitere Hinweise:

Die folgenden Hinweise sollten grundsätzlich von Verantwortlichen in Erwägung gezogen werden:

- Betrieb von Microsoft 365 auf eigenen IT-Strukturen („On-Premises-Lösung“): Verantwortliche sollten prüfen, ob und inwieweit Lösungen in Betracht kommen, die einen Betrieb von Microsoft-Produkten auf eigenen IT-Strukturen vorsehen, die eine Übermittlung personenbezogener Daten an Microsoft zu eigenen Zwecken unterbinden. Denkbar könnten auch Lösungen sein, die eine Übermittlung personenbezogener Daten zumindest verringern, so z. B. die Zwischenschaltung entsprechend vorkonfigurierter Terminal-Clients. → vgl. Rn. 36
- Dringend empfohlen wird die Verwendung pseudonymer Mailadressen/ Accounts und ein Verbot der Nutzung privater Microsoft-Accounts sowie des „Bring your own device“ (BYOD) im dienstlichen Bereich. Grundsätzlich sollte zudem darauf geachtet werden, den Personenbezug der verarbeiteten Daten zu minimieren. → vgl. Rn. 36
- Beim Einsatz in Bildungseinrichtungen sollte die AV-Vereinbarung mit Microsoft keine Verpflichtung des Verantwortlichen enthalten, für die Nutzung von Microsoft-Produkten eine Einwilligung von Schülerinnen und Schülern oder deren Eltern einzuholen. → vgl. Rn. 37

Anlage:
Begründung und Erläuterung

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

→ Diese Hinweise betreffen insbesondere die Abschnitte „Art der Datenverarbeitung; Eigentumsverhältnisse“, „Verarbeitungsdetails“ und Anhang B des DPA.

1 Gemäß Art. 28 Abs. 3 Satz 1 DSGVO müssen in der AV-Vereinbarung unter anderem die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen festgelegt sein.

a) Art und Zweck der Verarbeitung

2 Das DPA unterscheidet hinsichtlich des Zwecks der Verarbeitung zwischen den Verarbeitungen, die Microsoft zu eigenen Zwecken durchführt (vgl. hierzu Nr. 2 unten) und den Zwecken, die verfolgt werden, soweit Microsoft im Auftrag des Verantwortlichen handelt. Zu den Letzteren gehören nach hiesigem Verständnis die Zwecke, die im Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse“, Unterabschnitt: „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ enthalten sind. In diesem Abschnitt werden jedoch auch Zwecke genannt, die sich in der Regel nicht als Zwecke des Verantwortlichen (des Kunden von Microsoft) darstellen lassen. Hierzu gehören insbesondere die Verarbeitungszwecke, die der Produktverbesserung (z.B. Förderung der Benutzerproduktivität oder der Effektivität), dienen.

[!] ToDo:

- Hinsichtlich der Zwecke der Verarbeitung muss der Verantwortliche überprüfen, inwiefern er selbst eine Rechtsgrundlage hat, um personenbezogene Daten zu den im DPA genannten Zwecken des Verantwortlichen zu verarbeiten. Liegt dem Verantwortlichen eine solche Rechtsgrundlage nicht vor, kann er auch Microsoft nicht mit der Verarbeitung zu solchen Zwecken beauftragen. Die Verarbeitung zu solchen Zwecken durch Microsoft im Auftrag des Verantwortlichen muss also abbedungen werden. Kommt der Verantwortliche hingegen zu der Feststellung, dass er personenbezogene Daten zu diesen Zwecken verarbeiten und somit auch durch Microsoft im Auftrag verarbeiten lassen kann, können diese Zwecke im Vertrag weiterhin aufgeführt werden, jedoch muss eine Beschränkung auf das zur Leistungserbringung Erforderliche erfolgen.
- Hinsichtlich der Art der Verarbeitung muss aus der Vereinbarung erkennbar sein, welche Verarbeitungsvorgänge gem. Art. 4 Nr. 2 DSGVO für den konkreten Vertrag relevant sind, siehe auch Tabelle unten.

b) Art der personenbezogenen Daten und Kategorien der von der Verarbeitung betroffenen Personen

3 Anhang B des DPA listet die Arten personenbezogener Daten und die Kategorien der von der Verarbeitung betroffenen Personen auf, die im Rahmen der Nutzung der angebotenen Dienste theoretisch betroffen sein können. In einer AV-Vereinbarung müssen jedoch konkrete Angaben enthalten sein.

[!] ToDo:

- Die Angaben, welche Kategorien personenbezogener Daten welcher betroffenen Personen im Auftrag des Verantwortlichen verarbeitet werden sollen, hat der Verantwortliche in der AV-Vereinbarung einzutragen. Dies kann entweder durch eine Einbeziehung des Verzeichnisses der Verarbeitungstätigkeiten (VVT) geschehen, oder indem z. B. die nachfolgende Tabelle manuell ausgefüllt wird. Der Verantwortliche muss, ausgehend davon, welche Funktionen die zu nutzende Anwendung hat, angeben, welche Kategorien personenbezogener Daten welcher Personen hierzu verarbeitet werden müssen.
- Den Angaben „Kategorien personenbezogener Daten“ und „Kategorien betroffener Personen“ sollten auch direkt die Angaben zur Art und zu den Zwecken der Verarbeitung zugeordnet werden.
- Der Übersichtlichkeit halber könnten alle vorgenannten Angaben in einer Tabelle aufgeführt werden; eine Zuordnung in anderer Form, z. B. im Fließtext, bleibt jedoch weiterhin möglich:

Kategorien personenbezogener Daten	***Kategorien betroffener Personen***	***Verarbeitungen gem. Art. 4 Nr. 2 DSGVO***	***Zwecke der Verarbeitung***
Bitte eintragen	*Bitte eintragen*	*Bitte eintragen*	*Bitte eintragen*
Bitte eintragen	*Bitte eintragen*	*Bitte eintragen*	*Bitte eintragen*
Bitte eintragen	*Bitte eintragen*	*Bitte eintragen*	*Bitte eintragen*

- Es sollte vertraglich sichergestellt werden, dass diese abschließende Auflistung den Anhang B des DPA ersetzt.

2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für Geschäftstätigkeiten, die durch Bereitstellung der Produkte und Services an den Kunden veranlasst sind (nachstehend „für Microsofts Geschäftszwecke“)

→ Diese Hinweise betreffen insbesondere die folgenden Abschnitte des DPA: „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“ und „Art der Datenverarbeitung/ Eigentumsverhältnisse“.

Grundsätzlich wird Microsoft als Auftragsverarbeiter für Verantwortliche, die diese Dienste einsetzen wollen, tätig. Sofern dies der Fall ist, darf Microsoft personenbezogene Daten, auf die Microsoft Zugriff erhält, nur im Auftrag und damit auf Weisung des Verantwortlichen verarbeiten. Ein Einsatz zu eigenen Zwecken ist somit ausgeschlossen. Nach den Regelungen des DPA verarbeitet Microsoft personenbezogene Daten hingegen auch zu eigenen Zwecken. Für die rechtskonforme vertragliche Formulierung wäre es am einfachsten, wenn jede Verarbeitung von personenbezogenen Daten seitens Microsoft zu eigenen Zwecken unterbliebe. Dies beträfe alle Tätigkeiten des Abschnitts „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“ des DPA. 4

Soweit Microsoft dennoch personenbezogene Daten zu eigenen Zwecken und somit als Verantwortlicher verarbeiten will, benötigt bereits der Verantwortliche (Kunde von Microsoft) für die Bereitstellung von personenbezogenen Daten zu Microsofts Geschäftszwecken eine gesonderte Rechtsgrundlage. Ob eine solche Rechtsgrundlage besteht, ist für jeden von Microsoft definierten Verarbeitungszweck gesondert zu prüfen. Im Unterabschnitt des DPA „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an 5

den Kunden veranlasst sind“ werden diverse Verarbeitungszwecke aufgezählt, für die Microsoft die Pflichten eines Verantwortlichen übernimmt.[5] Allerdings wird das DPA insoweit den folgenden Anforderungen nicht gerecht:

- Die durch Microsoft zu eigenen Geschäftszwecken erfolgende Verarbeitungen sind nicht konkret genug beschrieben. Insbesondere bleibt unklar, welche konkreten Daten und Verarbeitungsvorgänge mit den jeweiligen Begrifflichkeiten gemeint sind (z. B. Verarbeitung von „Daten, die pseudonymisierte Identifikatoren beinhalten“).
- Über die formulierte Autorisierung bleibt unklar, wie weitreichend die Verarbeitung vereinbart wird.
- Aufgrund der Unklarheiten sowohl bei den genannten Verarbeitungszwecken als auch bei den dem DPA zufolge erhobenen Daten kann ein Verantwortlicher nicht die Rechtsgrundlage benennen, auf die er die Überlassung personenbezogener Daten an Microsoft zu Microsofts eigenen Zwecken stützen darf. Sofern öffentliche Stellen diese Dienste einsetzen, ist eine Übermittlung personenbezogener Daten an Microsoft zu Microsofts eigenen Zwecken regelmäßig auszuschließen, weil öffentliche Stellen – weder aus dem Fachrecht noch aus der DSGVO – berechtigt sind, Microsoft Daten zu diesen (unbestimmten) Zwecken zu übermitteln.[6]
- Es ist unklar, inwieweit Telemetrie- und Diagnosedaten von Microsoft zu eigenen Geschäftszwecken verarbeitet werden.

Folgendes ist für die Formulierung einer etwaigen Vertragsergänzung zu beachten:

a) Nachvollziehbarkeit der Verarbeitungszwecke durch den Verantwortlichen und Prüfung einer Rechtsgrundlage

6 Der Verantwortliche muss sich (entweder durch eigene Expertise oder unter Hinzuziehung von Microsoft) darüber klar werden, welche Kategorien personenbezogener Daten für welche eigenen Geschäftszwecke Microsofts herangezogen werden. Das umfasst auch die Feststellung, welche Daten mit pseudonymen Identifikatoren zu eigenen Zwecken Microsofts verarbeitet werden und wie häufig oder bei welchen Aktionen diese anfallen. Im letzten Schritt muss der Verantwortliche prüfen, für welche Verarbeitungszwecke er welche Daten Microsoft für Microsofts eigene Zwecke zur Verfügung stellen darf. Vertraglich „autorisiert“[7] werden dürfen nur auf eine Rechtsgrundlage gestützte zulässige Verarbeitungen zu in einer Rechtsgrundlage definierten, zulässigen Zwecken. Unzulässige Verarbeitungen sind zu unterbinden.

[!] ToDo:

Sofern Microsoft die Möglichkeit zur Verarbeitung der Daten zu eigenen Geschäftszwecken eingeräumt werden soll, muss der Verantwortliche zunächst klären, welche Verarbeitungen von welchen personenbezogenen Daten in welchem Umfang zu Microsofts eigenen Zwecken

---

5 DPA (Fn. 1), Abschnitt „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“ in Verbindung mit Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ – dort Satz 1 in Absatz 2.

6 Hierzu noch unter Rn. 10 ff.

7 Je nach vertraglicher Gestaltung müssten entweder explizit genannte unzulässige Verarbeitungszwecke aus dem Vertrag entfernt werden oder nur abschließend aufgeführte Zwecke zugelassen und die anderen explizit ausgeschlossen werden.

durchgeführt werden. Dazu könnte z. B. die folgende Tabelle genutzt werden. Anschließend muss der Verantwortliche beurteilen, ob er eine Rechtsgrundlage für die Zurverfügungstellung dieser personenbezogenen Daten besitzt. Alle Verarbeitungszwecke, für welche keine Rechtsgrundlage gefunden werden konnte, sind vertraglich auszuschließen und technisch zu unterbinden.

Lfd. Nr.	***Kategorie von personenbezogenen Daten, die von Microsoft zu eigenen Zwecken verarbeitet werden (einschl. der Daten, welche pseudonyme Identifikatoren enthalten)***	***Verarbeitungszweck laut Datenschutznachtrag***	***Zwecke der Verarbeitung***
durch Microsoft auszufüllen	*durch Microsoft auszufüllen*	*durch Microsoft auszufüllen*	*durch Microsoft auszufüllen*

b) Speziell zu Telemetrie- und Diagnosedaten

Eine besondere Schwierigkeit ergibt sich bei der Verarbeitung von Metadaten, insbesondere sog. Telemetrie- und Diagnosedaten durch Microsoft. Diese Daten werden regelmäßig durch Microsoft im Hintergrund verarbeitet, und diese Verarbeitungen lassen sich häufig nicht oder nicht komplett deaktivieren. Eine hinreichende Beschreibung der hier ablaufenden Prozesse stellt Microsoft nicht bereit. 7

Bei der Verarbeitung von Telemetrie- und Diagnosedaten ist davon auszugehen, dass personenbeziehbare Identifier in unterschiedlicher Form betroffen sein können (z. B. Werbe-ID, Lizenz-ID, Cookie-IDs, Nutzer-IDs, Rechner-IDs). Das DPA spricht diese Datenkategorien nicht ausdrücklich an. Im Rahmen einer Vertragsergänzung sollte klargestellt werden, ob Telemetrie- und Diagnosedaten auch personenbezogene Daten sind. Hiervon hängt die Anwendbarkeit der Regelungen des DPA auf diese Daten ab. 8

Die Verarbeitung von Telemetrie- und Diagnosedaten kann den Beschäftigtendatenschutz betreffen; sofern damit auch Leistungs- und Verhaltenskontrolle ausgeübt werden kann, können sich weitere (z. B. personalvertretungsrechtliche) Rechtsfolgen anschließen. 9

[!] ToDo:

Es muss vertraglich geregelt sein, ob es sich bei Telemetrie- und Diagnosedaten (s. z. B. auch die Datenschutzerklärung[8]) um personenbezogene Daten handelt.

c) Speziell zu den Rechtsgrundlagen der Verarbeitung öffentlicher Stellen

Öffentliche Stellen (insbesondere Behörden) unterliegen besonderen datenschutzrechtlichen Anforderungen, weil sie unmittelbar durch die Grundrechte verpflichtet werden.[9] 10

So können personenbezogene Daten, die Microsoft im Auftrag von öffentlichen Stellen verarbeitet, nicht ohne weiteres von Microsoft zur Verarbeitung für eigene Zwecke bzw. für Geschäftstätigkeiten genutzt werden (Art. 6 Abs. 1 Satz 2 DSGVO). Vielmehr bedarf es hierfür 11

---

8 Internet: https://privacy.microsoft.com/de-de/privacystatement, dort im Abschnitt „Von Ihrer Organisation bereitgestellte Produkte – Hinweis für Endbenutzer“.

9 Art. 1 Abs. 3 Grundgesetz.

für die öffentlichen Stellen einer besonderen Rechtsgrundlage, die die Übermittlung personenbezogener Daten an Microsoft für die Geschäftstätigkeiten des Unternehmens legitimiert.[10] Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO ist für öffentliche Stellen insbesondere dann nicht anwendbar, wenn das jeweilige Fachrecht[11] selbst Übermittlungsvorgänge an Privatunternehmen abschließend regelt.

12 Soweit eine Verarbeitung personenbezogener Daten zu Abrechnungszwecken erfolgen soll, ist diese Teil der Auftragsverarbeitung und erfolgt somit nicht zu eigenen Zwecken von Microsoft. Insoweit gelten die Ausführungen zu Rn. 1 ff. Für eine Übermittlung personenbezogener Daten durch öffentliche Stellen an Microsoft zur Erfüllung der anderen im DPA genannten Zwecke (Kontoverwaltung, Vergütung, Interne Berichterstattung, Geschäftsmodellierung und Finanzberichterstattung) wird in der Regel keine Rechtsgrundlage vorliegen. Ausnahmen muss der Verantwortliche prüfen und dokumentieren.

13 Wenn der Verantwortliche bei seiner Prüfung sodann feststellt, dass als mögliche Rechtsgrundlage allenfalls die Einwilligung von Betroffenen in Betracht kommt, darf die Verarbeitung erst nach einer solchen Einwilligung durch die Betroffenen erfolgen; diese Einwilligung kann vom Betroffenen jederzeit widerrufen werden. Zu beachten ist jedoch, dass eine Verarbeitung vor allem durch öffentliche Stellen nicht immer auf eine Einwilligung gestützt werden kann: Gerade, wenn es um personenbezogene Daten von Dritten und nicht mit dem Nutzer identischen Betroffenen geht, kann sich eine solche Einwilligung als sehr schwierig bis unmöglich erweisen. Weitere relevante Faktoren sind in diesem Zusammenhang die Freiwilligkeit und die Informiertheit der Einwilligung – an der Freiwilligkeit fehlt es gerade bei einer gegenüber einer öffentlichen Stelle erklärten Einwilligung häufig,[12] zudem ist eine Einwilligung auch nur bei hinreichender Informiertheit des Einwilligenden wirksam. Auch im Beschäftigungsverhältnis wird es in der Regel wegen der bestehenden Abhängigkeit der beschäftigten Person an der Freiwilligkeit fehlen. Eine Einwilligung kommt im Bereich der hoheitlichen Tätigkeiten ebenfalls grundsätzlich nicht als Rechtsgrundlage in Betracht.[13]

[!] ToDo:

- Die Verarbeitung personenbezogener Daten der Nutzer zu Microsofts eigenen Zwecken muss bei einem Einsatz durch öffentliche Stellen ausgeschlossen werden bzw. müssen die ausnahmsweise zulässigen Verarbeitungen zu Microsofts eigenen Zwecken unter Angabe der jeweiligen Rechtsgrundlage und Zwecke klar beschrieben werden.
- Alle auf einer Einwilligung basierenden Verarbeitungsvorgänge für Microsofts eigene Zwecke müssen vom Verantwortlichen per Konfiguration aktivier- und deaktivierbar sein. Dies muss durch den Verantwortlichen geprüft und ggf. vertraglich vereinbart werden.

---

[10] Vgl. Bundesverfassungsgericht, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13: Nicht nur Microsoft benötigt eine Rechtsgrundlage für das Abrufen von personenbezogenen Daten, sondern bereits die öffentliche Stelle für die Übermittlung von personenbezogenen Daten.

[11] Vgl. z. B. das jeweilige Landesschulgesetz oder § 80 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – für die Verarbeitung von Sozialdaten.

[12] Hierzu noch in Rn. 10 ff.

[13] Vgl. Erwägungsgrund 43 Satz 1 DSGVO.

3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen

a) Weisungsbindung

→ Diese Hinweise betreffen den Unterabschnitt „Verarbeitung personenbezogener Daten, DSGVO / Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten.

Gemäß Art. 29 DSGVO verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich nach Weisung des Verantwortlichen, es sei denn, er ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet. Diese Regelung impliziert grundsätzlich ein einseitiges Weisungsrecht des Verantwortlichen. Das muss sich aus dem jeweiligen Auftragsverarbeitungsvertrag entsprechend ergeben, vgl. Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO. Ferner sind Weisungen zu dokumentieren. 14

Die Regelungen in Microsofts DPA hierzu sind widersprüchlich: Im Unterabschnitt „Verarbeitung personenbezogener Daten, DSGVO / Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ des DPA ist geregelt, dass Weisungen, die über den dort aufgelisteten Umfang hinausgehen, einer Vertragsänderung bedürfen und gerade nicht einseitig erfolgen können. Hingegen ergibt sich aus Anlage I ein einseitiges Weisungsrecht des Verantwortlichen. 15

[!] ToDo:

- Die dargestellte Problematik ließe sich durch eine vertragliche Klarstellung der vorrangigen Geltung von Anlage I lösen. Akzeptabel wäre es auch, für solche Weisungen ein Vertragsänderungsverfahren (in Abweichung von der einseitigen Erklärung der Weisungen) vorzusehen, die dazu führen würden, dass der vom Verantwortlichen bestellte Funktionsumfang erweitert werden würde.
- Ferner sollte der Begriff der Weisung restriktiv definiert werden, um zu verhindern, dass Verantwortliche ungewollt „Weisungen“ erteilen. So kann z. B. bei einer bloßen Nutzung eines Services nicht von einer dokumentierten Weisung ausgegangen werden.
- Soweit sich der Umfang der Weisungen nach der Produktdokumentation richtet, ist darauf zu achten, dass die konkrete Produktdokumentation dem Vertrag beigefügt ist oder anderweitig dokumentiert und für den Verantwortlichen leicht zugänglich ist. Auch etwaige Änderungen der Produktdokumentation müssen als Vertragsänderung dokumentiert werden.

b) Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen

→ Dieser Hinweis betrifft insbesondere den Abschnitt „Offenlegung verarbeiteter Daten“ und den Anhang C des DPA.

Gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DSGVO darf der Auftragsverarbeiter personenbezogene Daten nur nach Weisung verarbeiten, es sei denn, er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaates zu einer konkreten Verarbeitung verpflichtet. Die aktuelle Regelung des DPA ermöglicht darüber hinaus eine Offenlegung personenbezogener Daten gegenüber Dritten, wenn dies gesetzlich vorgeschrieben ist, wobei eine solche Offenle- 16

gungspflicht auch aus den Gesetzen unsicherer Drittländer resultieren kann.[14] Diese Verpflichtung steht im Widerspruch zu den Vorgaben der DSGVO und muss daher vertraglich abbedungen werden.

17 Die in Anhang C enthaltenen zusätzlichen Schutzmaßnahmen ändern an der Unvereinbarkeit der o. g. Offenlegungsregelung mit der DSGVO nichts. Zudem ist auch nicht klar, ob sich Anhang C nur auf Konstellationen bezieht, in denen Microsoft als Verantwortlicher agiert[15] oder auch auf Konstellationen, in denen Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt.[16, 17]

[!] ToDo:

- Es ist vertraglich klarzustellen, dass personenbezogene Daten der Nutzer durch Microsoft nur offengelegt werden dürfen, wenn eine gesetzliche Pflicht nach Vorgabe der DSGVO oder des Rechts der EU-Mitgliedstaaten[18] besteht.
- Im Hinblick darauf, dass Microsoft sich vorbehält, Basiskontaktinformationen an Dritte weiterzugeben (vgl. letzter Satz des Abschnitts „Offenlegung verarbeiteter Daten“), sollten Verantwortliche ihre Basiskontaktinformationen nach Möglichkeit auf nicht personenbezogene Angaben (z. B. Unternehmensadresse und/oder Funktionspostfächer) beschränken.

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

→ Diese Hinweise betreffen insbesondere den Unterabschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“, den Abschnitt „Datensicherheit“ und den Anhang A des DPA.

18 Der Verantwortliche hat für eine ausreichende Sicherheit der von ihm in Auftrag gegebenen Verarbeitungen zu sorgen. Laut Unterabschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ des DPA ist ein solcher Zweck (zur Bereitstellung eines Produkts oder Services) auch die Gewährleistung der Sicherheit. Nach Art. 32 DSGVO müssen die ge-

---

14 Siehe auch DSK, Bericht (Fn. 3), Rn. 869–882; Rn. 917–940; Rn. 945–979.

15 So die Auslegung der DSK, siehe Bericht (Fn. 3), Rn. 811–819 mit Verweis auf die Formulierung im Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“, Unterabschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“.

16 Die Stellungnahme von Microsoft Deutschland zur datenschutzrechtlichen Bewertung von Microsoft 365 durch die DSK scheint in Abschnitt 9 für die Anwendbarkeit von Anhang C des DPA nicht danach zu differenzieren, in welcher Rolle Microsoft handelt, Internet: https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf, letzter Abruf: 29. März 2023.

17 Zusätzlich scheint Anhang C des DPA auf zusätzliche Professional Services Anwendung zu finden (siehe Abschnitt „Zusätzliche Professional Services“) – was aber zunächst von nachrangiger Bedeutung ist.

18 Auch eine Offenlegungsverpflichtung auf Grund des Rechts eines EWR (und nicht EU-)Staates wäre insoweit gleichgestellt, vgl. Gemeinsame Erklärung der Vertragsparteien zum Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/ 2018 vom 6. Juli 2018 zur Aufnahme der Verordnung (EU) 2016/ 679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung) in das EWR-Abkommen, Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A22018D1022.

troffenen Maßnahmen dafür geeignet sein, ein dem Risiko für die Rechte und Freiheiten Betroffener angemessenes Schutzniveau zu gewährleisten. Das Risiko bemisst sich nach der Schwere sowie der Eintrittswahrscheinlichkeit des möglichen Schadens.[19] „Angemessen“ bedeutet, dass zum einen eine ausreichende Schutzwirkung der Maßnahmen, die regelmäßig erst durch eine bestimmte Anzahl an Maßnahmen erreichbar ist, gewährleistet werden muss, und zum anderen die Maßnahmen selbst aber nicht zu einer übermäßigen Datenverarbeitung führen dürfen. Dieser Spielraum ist durch einen Vertrag auch nicht verhandelbar.

Zur Gewährleistung der Sicherheit behält sich Microsoft vor, alle personenbeziehbaren Daten zu verarbeiten. Einschränkungen auf nur eine Untermenge personenbeziehbarer Daten werden zur Gewährleistung der Sicherheit im DPA nicht formuliert. Es bleibt damit für Verantwortliche unklar, welche Maßnahmen in Verbindung mit welchen Kategorien personenbeziehbarer Daten zur Sicherstellung der Sicherheit genutzt werden. Anhang A des DPA spezifiziert hier ausschließlich Maßnahmen zu Kundendaten in „Core-Onlinediensten“ und „Professional Services-Daten“. Der Begriff der Core-Onlinedienste wird in den Microsoft Product Terms (Glossar) definiert.[20] Es bleibt unklar, welche personenbezogenen Daten zusätzlich zu den Nutzerdaten zu Sicherheitszwecken genutzt werden, welche weiteren Zwecke mit diesen Daten noch verfolgt werden und wie umfangreich jeweils die Verarbeitung ist. 19

In Anhang A des DPA sind speziell für die Kategorie der „Kundendaten“ Maßnahmen zur Gewährleistung der Sicherheit abschließend festgelegt. Diese Maßnahmen sind jedoch abstrakt formuliert (vgl. die Nutzung von Begriffen wie „branchenüblich“, „Branchenstandard“ und „standardmäßig“), ohne dabei die Berücksichtigung des im Datenschutz grundsätzlich geforderten Stands der Technik zu garantieren. Die vorgenommene Definition von Maßnahmenpaketen („Praktiken“) ermöglicht keine Einschätzung, ob die in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegebenen oder sonstigen branchenspezifischen Mindestanforderungen damit erfüllbar sind, und erlaubt keine risikobezogene Steuerung und Einschätzung, welche konkreten Maßnahmen zusätzlich erforderlich wären, um z. B. besondere Kategorien personenbezogener Daten oder Daten mit hohem Risiko für die Betroffenen zu verarbeiten. 20

Zudem werden im DPA weitergehende Zwecke, welche der Sicherheit dienen sollen, genannt.[21] Daher ist durch den Verantwortlichen zu klären, welche Kategorien personenbezogener Daten für Zwecke genutzt werden, die über die eigentliche Gewährleistung der Sicherheit im engeren Sinne hinausgehen. Aus Anhang A des DPA geht lediglich hervor, dass Kundendaten (als Datenkategorie) für die Gewährleistung der Sicherheit genutzt werden. Anhang A trifft aber keine Aussagen, ob Kundendaten noch für weitere Zwecke aus dem Abschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ des DPA genutzt oder ob und – falls ja – welche anderen personenbezogenen Daten für weiterführende Zwecke dieses Abschnitts verarbeitet werden. Die Zwecke „Fehlerbehebung“ und „Förderung der Sicherheit“ werden nach vertraglicher Festlegung Microsofts auf Weisung des Kunden (d. h. im Auftrag 21

---

19 Siehe dazu Näheres DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, Stand: 26. April 2018, Internet: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

20 Internet: https://www.microsoft.com/licensing/terms/product/Glossary/all.

21 Siehe DPA (Fn. 1), Abschnitt „Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“, worin „die Fehlerbehebung“ sowie die „Förderung der […] Sicherheit“ (im Englischen „enhancing […] security“) ebenfalls Verarbeitungszwecke darstellen, welche vom Verantwortlichen in Auftrag gegeben werden. Diese sind dabei nicht auf die Verarbeitung von Kundendaten eingeschränkt, wie es in Anhang A des DPA der Fall ist.

des Verantwortlichen) verfolgt und müssen für den Verantwortlichen bezüglich der genutzten Datenkategorien und des Zwecks verständlich sein. Die Klarstellung, welche Kategorien personenbezogener Daten für welche beauftragten Verarbeitungszwecke genutzt werden, dient hauptsächlich der Sicherstellung der Transparenz nach Art. 13 Abs. 1 Buchst. c und Art. 14 Abs. 1 Buchst. c DSGVO sowie der Nachweispflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchst. b, c und f DSGVO als Pflichten des Verantwortlichen.

22 Weiterhin muss der Verantwortliche abschätzen können, ob der Umfang der Erhebung erforderlich ist.

[!] ToDo:

- Der Vertrag hat zu spezifizieren, welche personenbezogenen Daten neben den Nutzerdaten dem Zweck der Gewährleistung der Sicherheit dienen. Die Inhaltsdaten kann der Verantwortliche lediglich selbst benennen, für die Auflistung der darüberhinausgehenden Daten (z. B. Anmeldedaten, Diagnosedaten etc.) wird er ggf. Unterstützung von Microsoft benötigen, es sei denn, er kann abschätzen, welche Daten hier erforderlich sind. Microsoft muss ebenfalls überblickartig mitteilen, warum genau die spezifizierten Daten zur Gewährleistung der Sicherheit notwendig sind.
- Ferner sollte geklärt werden, welche der benannten personenbezogenen Daten für die Zwecke „Fehlerbehebung“ und „Förderung der Sicherheit“ genutzt werden und auf welche Art und Weise diese Daten verarbeitet werden, z. B. durch einen Verweis auf konkrete Dokumente, in denen dies beschrieben ist. Auch hier gilt, dass der Verantwortliche eine Rechtsgrundlage zu den beauftragten Verarbeitungsvorgängen nachweisen muss. Andernfalls müssen diese vertraglich ausgeschlossen werden.
- Zu beachten ist, dass bei der Verarbeitung der Telemetrie- und Diagnosedaten sowie in sonstigen sicherheitsrelevanten Datenverarbeitungsprozessen von Microsoft die Anforderungen an die Umsetzung der Mandantentrennung fortbestehen. Als kompensierende Maßnahmen sollten die Verantwortlichen die Möglichkeiten zur Gestaltung eigener technisch-organisatorischen Maßnahmen prüfen und dabei die relevanten Studien[22] und Lösungsansätze berücksichtigen.

23 Weiterhin muss der Verantwortliche eine Rechtsgrundlage für Verarbeitungszwecke wie „Fehlerbehebung“ und „Förderung der Sicherheit“ erkennen, um die Rechtmäßigkeit der Verarbeitung nachweisen und diese Verarbeitungsvorgänge überhaupt in Auftrag geben zu können. Im zweiten Schritt muss der Verantwortliche die Notwendigkeit und Verhältnismäßigkeit des Umfangs der Datenverarbeitung seitens Microsofts in Bezug auf den Zweck prüfen. Sind alle Datenerhebungen notwendig, verhältnismäßig und rechtmäßig, ist keine weitere Ergänzung des Vertrages erforderlich.

24 Sind einzelne Datenkategorien nicht notwendig, unverhältnismäßig (da z. B. zu viele Daten für zu wenig Nutzen verarbeitet werden oder das Missbrauchspotential zu hoch ist) oder fehlt für ihre Verarbeitung die Rechtsgrundlage, müssen diese von der beauftragten Verarbeitung ausgeschlossen werden. Zusätzlich ist dabei zu beachten, dass der Betroffene gegenüber dem

---

[22] BSI, Evaluierung der Telemetrie von Microsoft Office 365, 6. Oktober 2020, Internet: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/Office_Telemetrie/telemetrie.html, mit Verweis auf eine ausführliche Studie.

Verantwortlichen nicht in den Verzicht auf die Sicherheit der Datenverarbeitung nach Art. 32 DSGVO einwilligen kann.[23]

Microsoft bietet zum Thema der Gewährleistung der Sicherheit eine Vielzahl zusätzlicher Schutzmaßnahmen und Dokumentationen an (siehe https://learn.microsoft.com/de-de/security/). Insbesondere, wenn Daten nach Art. 9 DSGVO verarbeitet werden sollen, liegen Indizien vor, dass weitere zusätzliche Maßnahmen zur Absicherung der Datenverarbeitung angemessen sind.[24] Diese Maßnahmen müssen vertraglich verbindlich vereinbart werden und dürfen nicht optional bleiben. Zu beachten ist ferner, dass Weisungen nach der aktuellen Fassung des DPA z. B. auch in – zu dokumentierenden – Konfigurationseinstellungen enthalten sein können. 25

[!] ToDo:

- Alle unrechtmäßigen, nicht notwendigen oder unverhältnismäßigen Datenverarbeitungen müssen vertraglich ausgeschlossen und technisch unterbunden werden.
- Der Verantwortliche muss die Sicherheit auch dann gewährleisten, wenn die betroffenen Personen auf die Einhaltung verzichtet hat.
- Der Verantwortliche muss prüfen, ob die vertraglich vorgesehenen Maßnahmen zum angemessenen Schutz der Verarbeitung seiner personenbezogenen Daten durch Microsoft ausreichend sind und – soweit erforderlich – zwingend notwendige zusätzliche Maßnahmen ebenfalls vertraglich vereinbaren.[25]

---

[23] Vgl. DSK, Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen, Beschluss vom 24. November 2021, Internet: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

[24] Vgl. z. B. § 17 Abs. 2 und 3 Niedersächsisches Datenschutzgesetz und vergleichbare Regelungen in den anderen Landesgesetzen.

[25] Die im Anhang A des DPA enthaltenen Praktiken reichen hierbei als Maßnahmenkatalog nicht aus. Für die Erreichung eigener Gewährleistungsziele sollte ein Maßnahmenkatalog darauf referenzierend so aufgebaut werden, dass daraus die Maßnahmen zur Gewährleistung der Sicherheit von Daten unterschiedlicher Risikoeinstufung erkennbar sind. Zum Beispiel müsste in Anhang A die zum Thema Authentifizierung beschriebene Praktik der Verwendung von Passwörtern von „mindestens acht Zeichen“ konkretisiert werden. Wenn diese Authentifizierungsmethode zum Einsatz kommen darf, sind als Passwort-Vorgaben nicht nur die Länge, sondern auch der Aufbau und die Komplexität von Passwörtern zu berücksichtigen und für die unterschiedlichen Nutzergruppen risikobezogen zu unterscheiden. Als Maßnahme könnte auch die Nutzung bestimmter Protokolle (z. B. Transportverschlüsselung älter als TLSv1.3), Funktionen oder Verfahren (z. B. DES, RSA 1024, MD5) etc. für die Verwendung von Microsoft als AVV-Partner untersagt werden. Auch die vom Verantwortlichen zu implementierenden Maßnahmen müssen soweit konkretisiert sein, dass daraus die vorzunehmende Konfiguration eines Microsoft-Produktes nachvollzogen werden kann. Für ruhende Daten enthält die aktuelle Fassung der DPA z. B. lediglich die Angabe, dass diese verschlüsselt sind. Die Microsoft-Dokumentation (Internet: https://learn.microsoft.com/de-de/microsoft-365/compliance/encryption?view=o365-worldwide) hingegen enthält unterschiedliche Verschlüsselungslösungen (Kennwortschutz, BitLocker, Customer Key, Doppelschlüssel), deren Auswahl und Ausgestaltung von Verantwortlichen als Maßnahmenausgestaltung zu treffen sind.

5. Löschen personenbezogener Daten

→ Diese Hinweise betreffen den Abschnitt „Speicherung und Löschung von Daten“.

26 In der Aktualisierung des DPA hat Microsoft festgelegt, dass gespeicherte Kundendaten und Daten, die zu eigenen Zwecken erhoben wurden („Professional Services-Daten“), den gleichen Regeln zum Löschen unterliegen.

27 Im DPA wird ein mehrstufiger Löschprozess nach Vertragsende beschrieben: Zunächst werden die Daten 90 Tage mit einer Zugriffsmöglichkeit des Verantwortlichen aufbewahrt und danach werden sie weitere 90 Tage lang nicht gelöscht. Für die Aufbewahrung für weitere 90 Tage wird in der Regel keine Rechtsgrundlage vorliegen.

28 Keine Aufbewahrungsfrist ist geregelt für die sog. „Zusätzliche Professional Services Daten“ (siehe Abschnitt „Zusätzliche Professional Services“ in Verbindung mit dem Abschnitt „Speicherung und Löschung von Daten“). Da der Begriff „Zusätzliche Professional Services“ ohnehin nicht abgrenzbar ist von dem der „Professional Services“, sollte darauf hingewirkt werden, dass Sonderregelungen für zusätzliche Professional Services (und die in ihrem Rahmen verarbeiteten Daten) insgesamt abbedungen werden.

29 Nicht im DPA geregelt sind speziellere Löschprozesse und -fristen, z. B. wenn Daten auf Verlangen (Art. 17 DSGVO) oder beim Auflösen eines einzelnen Nutzer-Kontos gelöscht werden müssen.

30 Vertraglich konkretisiert werden müsste das Löschen von „Daten, die pseudonymisierte Identifikatoren beinhalten“ (siehe Rn. 4 ff.).[26] Diese Daten können noch personenbeziehbar sein und müssen damit ggf. im Löschprozess miteinbezogen werden.

31 Nicht hinreichend konkret ist auch die Ausnahme „soweit durch das DPA zur Aufbewahrung autorisiert“, da nicht klar ist, welche Regelungen des DPA in diesem Kontext bereits als Autorisierung ausgelegt werden könnten.

[!] ToDo:

- Die im DPA aufgeführten Löschfristen sind vertraglich anzupassen, d. h. in der Regel zu kürzen.
- Der Verantwortliche muss ggf. vertragliche Anpassungen vornehmen, um Microsoft als Auftragsverarbeiter in eigene Löschprozesse zu integrieren.
- Die Ausnahmen von der Löschungsverpflichtung sollten eingeschränkt und konkretisiert werden.
- Über die im DPA formulierten bzw. noch zu ergänzenden Regelungen bezüglich der Löschung von personenbezogenen Daten müssen Verantwortliche auch die verwendeten Anwendungen prüfen und ggf. spezifische Maßnahmen in ihre eigenen Löschprozesse aufnehmen.
- Sonderregelungen für „Zusätzliche Professional Services“ sollten entfallen.

[26] Diese Daten werden in dem Abschnitt „Speicherung und Löschung von Daten“ nicht explizit behandelt.

6. Information über Unterauftragsverarbeiter

→ Diese Hinweise betreffen insbesondere den Abschnitt „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“.

Der Verantwortliche ist auch dann für den datenschutzkonformen Umgang mit personenbezogenen Daten zuständig, wenn er mit der Verarbeitung Dienstleister beauftragt. 32

Deshalb regelt Art. 28 DSGVO, dass die Einbeziehung eines Unterauftragsverarbeiters stets der Genehmigung des Verantwortlichen bedarf. Das gilt für die Einbeziehung jedes „weiteren“ Auftragsverarbeiters (also auch z. B. des Unter-Unterauftragsverarbeiters). Hat der Verantwortliche zu Beginn eine diesbezügliche allgemeine Genehmigung erteilt, steht ihm gleichwohl ein Einspruchsrecht zu, wenn der Auftragsverarbeiter einen Unterauftragsverarbeiter hinzuziehen oder ersetzen möchte. Daher muss der Auftragsverarbeiter – auch im Fall einer zuvor erteilten allgemeinen schriftlichen Genehmigung – den Verantwortlichen entsprechend informieren (vgl. Art. 28 Abs. 2 Satz 2 DSGVO). Für diese Information genügt es nicht, dem Verantwortlichen die bloße Möglichkeit einzuräumen, von entsprechenden Vorhaben Kenntnis zu nehmen. Den Verantwortlichen trifft in diesem Zusammenhang keine „Holschuld“ hinsichtlich dieser Information, vielmehr fordert Art. 28 Abs. 2 Satz 2 DSGVO, dass der Auftragsverarbeiter ihn ausdrücklich, einzelfallbezogen und aktiv informiert. Es reicht also nicht aus, wenn der Verantwortliche beispielsweise selbst diese Information von einer Website abrufen muss. Nur so wird dem Verantwortlichen auch tatsächlich die Entscheidung ermöglicht, die beabsichtigte Unterauftragsverarbeitung abzulehnen oder zu genehmigen. 33

Der Auftragsverarbeiter muss einem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegen, die im Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Dabei muss auch der Unterauftragsverarbeiter hinreichende Garantien dafür bieten, dass die Datenverarbeitung durch geeignete technische und organisatorische Maßnahmen im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt. Der Auftragsverarbeiter haftet grundsätzlich dem Verantwortlichen gegenüber für eine Verletzung von Datenschutzpflichten durch einen Unterauftragsverarbeiter (vgl. Art. 28 Abs. 4 DSGVO). 34

Um diesen Anforderungen gerecht zu werden, müsste die mit Microsoft abzuschließende AV-Vereinbarung folgende Vorgaben berücksichtigen: 35

[!] ToDo:

- Die Information über Unterauftragsverarbeiter muss den Namen sowie die Anschrift des Unterauftragsverarbeiters, Namen, Funktion und Kontaktdaten der Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der betreffenden Verarbeitung und eine eindeutige Benennung des betroffenen Produkts/ der Funktion (einschließlich einer klaren Abgrenzung der Zuständigkeiten/ Verantwortungsanteile, falls mehrere Unterauftragsverarbeiter genehmigt werden) enthalten.
- Dies gilt auch für die Einbindung von neuen Unterauftragsverarbeitern sowie für Änderungen im Rahmen bestehender Unterauftragsverhältnisse. Die bisher von Microsoft zur Verfügung gestellte Liste über Unterauftragsverhältnisse enthält demgegenüber weit weniger Angaben.

- Microsoft als Auftragsverarbeiter muss sich verpflichten, den Verantwortlichen „proaktiv“ über neue Unterauftragsverarbeiter zu informieren, beispielsweise via Push-Benachrichtigung.[27] Unzureichend wäre hingegen, wenn Microsoft beabsichtigte Hinzuziehungen oder Ersetzungen von Unterauftragsverarbeitern lediglich auf seiner Homepage veröffentlichen oder den Verantwortlichen verpflichten sollte, die Microsoft-Website regelmäßig auf beabsichtigte Änderungen von Unterauftragsverarbeitungen zu überprüfen. Aktuell erhält der Verantwortliche von Microsoft nur die Information, dass sich die Liste über Unterauftragsverhältnisse geändert habe, mit der Folge, dass der Verantwortliche die komplette Liste auf Aktualisierungen hin durchsuchen muss. Dies ist ebenfalls nicht ausreichend.

7. Weitere Hinweise

36 Der Verantwortliche hat neben den gebotenen vertraglichen Zusatzvereinbarungen zum DPA mit weiteren eigenen Maßnahmen dazu beizutragen, dass der Datenschutz beim Einsatz von Microsoft zumindest verbessert wird. So muss er prüfen, inwieweit die Weitergabe von personenbezogenen Daten von Beschäftigten oder Dritten an Microsoft durch eigene Maßnahmen unterbunden werden kann. Damit wird dem Grundsatz der Datenminimierung Rechnung getragen und es kann zudem sichergestellt werden, dass personenbezogene Daten nicht zweckwidrig oder ohne ausreichende Rechtsgrundlage verwendet werden. Soweit der Betrieb von Microsoft-Produkten auf eigenen IT-Strukturen erfolgen kann,[28] die eine Übermittlung personenbezogener Daten zu Microsofts eigenen Zwecken wirksam unterbinden, sind solche Lösungen vorrangig zu nutzen. Ist dies nicht möglich, sind andere Maßnahmen zum Schutz personenbezogener Daten zu prüfen. Unerlässlich sind dabei vor allem Maßnahmen, die eine Pseudonymisierung von E-Mailadressen/-accounts vorsehen. Anzumerken ist allerdings, dass derlei Maßnahmen nicht sämtliche datenschutzrechtlichen Bedenken beseitigen werden können, so z. B. nicht die Bedenken hinsichtlich der fehlenden Rechtsgrundlage im öffentlichen Bereich.

[!] ToDo:

- Betrieb von Microsoft 365 auf eigenen IT-Strukturen („On-Premises-Lösung“): Verantwortliche sollten prüfen, ob und inwieweit Lösungen in Betracht kommen, die einen Betrieb von Microsoft-Produkten auf eigenen IT-Strukturen vorsehen, die eine Übermittlung personenbezogener Daten zu Microsofts eigenen Zwecken unterbinden. Denkbar könnten auch Lösungen sein, die eine Übermittlung personenbezogener Daten zumindest verringern, so z. B. die Zwischenschaltung entsprechend vorkonfigurierter Terminal-Clients oder die Nutzung über einen vorkonfigurierten und abgesicherten Browser mit integrierten Schutzmaßnahmen zur weitestgehenden Anonymisierung/ Gleichschaltung der Metadaten, die Umleitung des Internetverkehrs über eine Infrastruktur im eigenen Einflussbereich mit geeigneten technischen Maßnahmen zur Verschleierung der heimischen IP-Adressen und/oder die Unterbindung der Übertragung von Telemetrie-Daten beim Einsatz von Microsoft 365 bzw. dem darunter liegenden Windows-Betriebssystem, hilfsweise die Filterung bei der Übermittlung personenbezogener Telemetriedaten über eine entsprechende Infrastruktur (Firewall).

---

[27] Die aktuelle Formulierung im DPA könnte hingegen auch als eine „Pull“-Benachrichtigung ausgelegt werden.

[28] Siehe z. B. BSI, Evaluierung der Telemetrie von Microsoft Office 365 (Fn. 22).

- Dringend empfohlen wird die Verwendung pseudonymer Mailadressen/Accounts und ein Verbot der Nutzung privater Microsoft-Accounts sowie des BYOD im dienstlichen Bereich. Grundsätzlich sollte zudem darauf geachtet werden, den Personenbezug der verarbeiteten Daten zu minimieren.

Bei einer Nutzung von Microsoft 365 durch Bildungseinrichtungen ist zu beachten, dass eine fehlende Rechtsgrundlage für die Übermittlung personenbezogener Daten jedenfalls in Zusammenhang mit dem Unterricht in der Regel nicht durch eine Einwilligung der Schülerinnen und Schüler bzw. deren Eltern ersetzt werden kann. Von der Freiwilligkeit einer Einwilligung im Sinne des Art. 7 Abs. 4 DSGVO kann regelmäßig nicht die Rede sein, wenn Schülerinnen und Schülern die Teilhabe an digitalen Unterrichts- und Lernmaterialien oder dem Unterricht selbst verwehrt bleibt, sollten ihre Eltern die Einwilligung nicht erteilen. Eine dem Verantwortlichen durch Microsoft auferlegte Verpflichtung, die u. U. zur Verarbeitung erforderliche Einwilligung der Schülerinnen und Schüler bzw. deren Eltern einzuholen, geht vor diesem Hintergrund daher ins Leere. 37

[!] ToDo:

Beim Einsatz in Bildungseinrichtungen sollte die AV-Vereinbarung mit Microsoft keine Verpflichtung des Verantwortlichen enthalten, für die Nutzung von Microsoft-Produkten eine Einwilligung von Schülerinnen und Schülern oder deren Eltern einzuholen.