DER HESSISCHE BEAUFTRAGTE FÜR
DATENSCHUTZ UND INFORMATIONSFREIHEIT

Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365

Wiesbaden, 15. November 2025

Inhalt

A) Hintergründe und Inhalte des Berichts

Im Sommer 2024 hatte das Hessische Digitalministerium (**HMD**) den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (**HBDI**) frühzeitig in seine Überlegungen zu etwaigen Nutzungsszenarien von Microsoft 365 (**M365**) in der Hessischen Landesverwaltung eingebunden. Am Beispiel des Einsatzes von MS Teams fanden in der Folge zwischen Microsoft (**MS**) – geführt durch die Microsoft Deutschland GmbH – und dem HBDI im Sommer 2024 erste Gespräche zur abstrakten Evaluierung der Anforderungen eines DS-GVO-konformen Einsatzes von M365 in der Hessischen Landesverwaltung statt.

Parallel gab es – ausgelöst durch ein aufsichtsbehördliches Verfahren des HBDI gegen eine nicht-öffentliche Stelle mit Sitz in Hessen bezüglich des Einsatzes von M365 und die vielfache Forderung des HBDI gegenüber Verantwortlichen in Hessen, sich bei MS für einen datenschutzkonformen Betrieb von M365 einzusetzen – seitens MS das Angebot, mit dem HBDI Gespräche über die grundsätzlichen Voraussetzungen eines DS-GVO-konformen Einsatzes von M365 zu führen.

Aufgrund dieser parallel stattfindenden Entwicklungen im öffentlichen und im nicht-öffentlichen Bereich vereinbarten MS und der HBDI, Gespräche aufzunehmen, um – unabhängig von konkreten Projektvorhaben oder aufsichtsbehördlichen Verfahren – über die Bedingungen eines DS-GVO-konformen Einsatzes von M365 zu sprechen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) hatte das Ergebnis ihres Gutachtens zu „Microsoft-Onlinediensten“ vom 2. November 2022[1] am 24. November 2022 in der Feststellung zusammengefasst, 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 könne.[2] MS war jedoch der Auffassung, dass die Feststellungen der DSK nicht zutreffend seien.[3]

---

1 AG DSK, „Microsoft-Onlinedienste“ – Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf.

2 DSK, Festlegung zu Tagesordnungspunk 26 im Rahmen der 104. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22. bis 24. November 2022, https://datenschutzkonferenz-online.de/media/pr/Protokoll_der_104_DSK.pdf.

3 Stellungnahme von MS Deutschland zur datenschutzrechtlichen Bewertung von M365 durch

Ziel der Gespräche sollte es nach dem gemeinsamen Willen von MS und dem HBDI sein, unter Berücksichtigung zwischenzeitlicher Entwicklungen (insb. Weiterentwicklung des Vertragswerks von MS, veröffentlichter Kundendokumentation, rechtlicher Änderungen wie dem Angemessenheitsbeschluss der Europäischen Kommission betreffend Datentransfers in die USA sowie technischer Entwicklungen wie dem Ausbau der „EU-Datengrenze“ von MS) und der Schlussfolgerungen und Forderungen der DSK zu überprüfen, ob diese Feststellung drei Jahre später noch zutrifft oder ob praxistaugliche und datenschutzkonforme Ergebnisse in Hinblick auf die Anforderungen des Art. 28 DS-GVO für den öffentlichen und den nicht-öffentlichen Bereich erarbeitet werden können.

Der vorliegende Bericht fasst die aus den Gesprächen gewonnenen Erkenntnisse zu den sieben Kritikpunkten der DSK zusammen (**Sachverhalt**), nimmt hierauf aufbauend eine datenschutzrechtliche Bewertung (**Rechtliche Erwägungen**) vor und gibt Empfehlungen für öffentliche und nicht-öffentliche Stellen mit Sitz in Hessen (**Handlungsempfehlungen**).

die DSK, https://msftstories.thesourcemediaassets.com/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf.

B) Vorgehensweise

Die DSK hatte 2020/2022 die damalige Fassung (zuletzt die Fassung vom 15. September 2022) des „Datenschutznachtrag für Produkte und Services von Microsoft“ (Data Protection Addendum, DPA) von MS untersucht und 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. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden. […].“

Gegenstand des DSK-Abschlussberichts waren folgende Themenbereiche:

(1) Festlegung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten,
(2) Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für legitime Geschäftszwecke („Geschäftstätigkeiten“),
(3) Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, CLOUD Act, FISA 702,
(4) Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO,
(5) Löschung und Rückgabe personenbezogener Daten,
(6) Information über Unterauftragsverarbeiter,
(7) Datenübermittlungen in Drittstaaten.

MS und der HBDI diskutierten daher ab Jahresbeginn 2025 in zehn Gesprächsrunden jeweils einen der sieben Kritikpunkte in Präsenz und arbeiteten an einem gemeinsamen Lösungsvorschlag, der Grundlage einer späteren Praxis von MS für hessische Kunden und einer Verwaltungspraxis des HBDI werden sollte.

In Vorbereitung auf jeden Gesprächstermin fand ein schriftliches Vorverfahren statt, in dessen Rahmen die Möglichkeit bestand, tatsächliche Informationen zu übermitteln, rechtliche Argumente auszutauschen und Fragen zur Vorbereitung des Gesprächstermins zu stellen.

Der Gesprächstermin diente sodann der inhaltlichen Vertiefung und der Erarbeitung etwaiger Lösungsvorschläge. Die wichtigsten Ergebnisse der Gespräche wurden in informellen Ergebnisprotokollen festgehalten. Mitunter kam es auch im Nachgang der Gesprächstermine zu weiterem schriftlichem Austausch und weiteren Besprechungen zu einzelnen Spezialfragen.

Die aus diesem Austausch zwischen MS und HBDI gewonnenen Erkenntnisse bilden die Grundlage des vorliegenden Berichts.

C) Abgrenzung

Die in diesem Bericht getroffenen Feststellungen zum Sachverhalt beruhen auf dem zuvor beschriebenen schriftlichen und persönlichen Austausch zwischen MS und dem HBDI.

Im Fokus standen dabei nicht einzelne Komponenten oder Produkte von M365,[4] sondern das DPA von MS (zuletzt in der Fassung vom 1. September 2025 – nachfolgend in dieser Fassung „**DPA**“) und die Frage, mit Hilfe welcher möglichen Verbesserungen die Anforderungen des Art. 28 DS-GVO erfüllt werden können. Ziel war es, vor dem Hintergrund der von der DSK geäußerten Kritikpunkte öffentlichen und nicht-öffentlichen Stellen mehr Rechtssicherheit zu bieten.

Ausgehend von der zusammenfassenden Feststellung der DSK, 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 könne und angesichts der Verantwortung der Verantwortlichen für die durch Auftragnehmer unterstützte Datenverarbeitung, sollte mit Blick auf die Handlungsmöglichkeiten von Auftragnehmern **und** Verantwortlichen geprüft werden, ob und wie die Rechtssicherheit für beide **zusammen** und sich ergänzend erreicht werden kann. Sie sollten in die Lage versetzt werden, ihre Nachweispflichten zum datenschutzkonformen Einsatz von M365 bezüglich der oben genannten Kritikpunkte der DSK erfüllen zu können. Mit dieser Blickrichtung ist dann auch das Kapitel zu den **Handlungsempfehlungen für Verantwortliche** in Kapitel F) III. zu lesen.

Der folgende Bericht zielt auf eine **normative** Bewertung

(1) des im Zuge der gemeinsamen Gespräche für öffentliche Stellen mit Sitz in Hessen fortentwickelten DPA (nachfolgend „**DPA-öS**“) sowie

(2) des DPA, das für nicht-öffentliche Stellen zum Einsatz kommt,

jeweils unter Berücksichtigung der begleitenden Dokumentation.

[4] Insbesondere auch keine produktspezifischen Erweiterungen zum DPA, die ggf. ergänzend zu den Anforderungen des DPA zu prüfen sind.

Diese Bewertung erfolgte auf der Grundlage der von MS geschilderten oder für die Zukunft zugesagten Praxis im Rahmen von M365 im Allgemeinen und in Hessen im Besonderen.

Dem Bericht liegen keine technischen Prüfungen der Datenverarbeitung in Produkten von M365,[5] wohl aber von MS-Technikern übermittelte, vertiefende Informationen zu Verarbeitungsvorgängen, zugrunde. Der HBDI geht davon aus, dass aufbauend auf dem Bericht technische Prüffragen formuliert werden können, hat sich jedoch mit MS nicht hierzu ausgetauscht.

Der Bericht behandelt keine über den zuvor beschriebenen Anwendungsbereich hinausgehende Fragen, wie etwa die zunehmend an Bedeutung gewinnenden Fragen der digitalen Souveränität.[6] MS machte in diesem Zusammenhang auf seine „European Digital Commitments“ zur Stärkung der digitalen Souveränität und Resilienz seiner Kunden in Europa aufmerksam.[7]

Er beschränkt sich auf das durch das

(1) DPA-öS geprägte Verhältnis zwischen öffentlichen Stellen und MS einerseits sowie
(2) DPA geprägte Verhältnis zwischen nicht-öffentlichen verantwortlichen Stellen (Geschäfts- und Unternehmenskunden von MS) und MS andererseits

und behandelt nicht das Verhältnis zwischen Privatkunden/Endnutzern und MS.

[5] Dies wäre mit Blick auf die zur Verfügung stehenden Ressourcen und der Produktvielfalt von M365 im Rahmen der geführten Gespräche nicht möglich gewesen und wurde auch nicht angestrebt.

[6] Bezüglich eines „digital souveränen“ Einsatzes von M365-Produkten durch öffentliche Stellen wird insoweit insbesondere auch auf die weiteren Entwicklungen rund um die Delos Cloud für den öffentlichen Dienst hingewiesen, https://www.deloscloud.de/.

[7] Zu den „European Digital Commitments” siehe unter: https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/.

D) Allgemeine Hinweise zum DPA

Diesem Bericht liegt das DPA zugrunde,[8] sofern nicht ausdrücklich das im Zuge der gemeinsamen Gespräche für öffentliche Stellen mit Sitz in Hessen fortentwickelte DPA-öS angesprochen ist.

Das DPA von MS gelangt weltweit für MS-Kunden zur Anwendung und unternimmt es, auf diverse rechtliche Fragestellungen eine globale Antwort zu geben. Dabei berücksichtigt es auch, aber eben nicht ausschließlich, die Anforderungen der DS-GVO. Das DPA von MS entspricht in Struktur und Aufbau nicht den in der Praxis weit verbreiteten Vertragsmustern zur Auftragsverarbeitung und dem Aufbau des Art. 28 Abs. 3 DS-GVO.[9] Zudem verwendet das DPA von MS teilweise eine MS-eigene Terminologie, die so in der DS-GVO nicht vorkommt. Sie ist auf den weltweiten Einsatz des DPA zurückzuführen.[10]

Für den öffentlichen Bereich hat MS im DPA-öS individuelle Anpassungen vorgenommen, um den spezifischen Anforderungen von Datenschutzaufsichts-behörden gerecht zu werden. Für die Anwendung im öffentlichen Bereich in Hessen sieht MS im DPA-öS Anpassungen vor, um die Rechtssicherheit für Kunden des öffentlichen Sektors zu gewährleisten. Diese Anpassungen werden im Folgenden berücksichtigt.

Die nachfolgend zusammengefassten Ausführungen geben einen Überblick über die grundsätzliche Struktur des DPA und einige terminologisch besonders bedeutsame Begriffe.

I. Aufbau des DPA

Das DPA folgt einem modularen Aufbau, in dem der Vertragstext durch die Anhänge A, B und C und die Anlage 1 ergänzt wird. Die Anhänge A, B und C stehen gleichstufig nebeneinander. Anlage 1 beinhaltet zusätzliche Regelungen, die sich auf die Verpflichtungen nach der DS-GVO beziehen. Diese Anlage gilt nur im Anwendungsbereich der DS-GVO. Ist der Anwendungsbereich der DS-GVO eröffnet,

---

8 DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14.

9 MS weist darauf hin, dass dies auch bei anderen Anbietern von Cloud-Dienstleistungen der Fall ist.

10 Siehe unter II. und vereinzelt im Abschnitt „Definitionen“ im DPA in der Fassung vom 1. September 2025 unter „Definitionen“, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Seite 5 ff.

ist Anlage 1 lex specialis gegenüber den allgemeinen Regelungen im DPA und seinen Anhängen, weil MS im Anhang 1 darstellt, dass und wie es die Verpflichtungen aus der DS-GVO erfüllt.

II. Erläuterung zu den Datenarten, die MS unterscheidet

Alle Daten – seien sie personenbezogen oder nicht-personenbezogen –, über die MS infolge der Bereitstellung von Online-Diensten gegenüber seinen Kunden verfügt, fallen in eine der folgenden drei Kategorien[11] (1) „**Kundendaten**“, (2) „**Professional Services Daten**“ oder (3) „**von MS generierte, abgeleitete oder gesammelte Daten**“. Diese Unterteilung spiegelt wider, wie die Daten zu MS gelangen.

(1) *„Kundendaten“*[12] sind alle Daten, einschließlich sämtlicher Text-, Ton-, Video- oder Bilddateien und Software, die MS vom oder im Namen des Kunden durch die Nutzung der Onlinedienste bereitgestellt werden. Der Begriff des Kunden ist nicht gleichbedeutend mit dem Begriff des Endnutzers oder der betroffenen Person im Sinne der DS-GVO. Der Kunde ist der Auftraggeber von MS, der die in Anspruch genommenen Onlinedienste gegebenenfalls seinerseits einer Vielzahl von Endnutzern und Betroffenen im Sinne der DS-GVO (z. B. Beschäftigten) zur Verfügung stellt.[13]

Eine wichtige Teilmenge der Kundendaten sind *„Audit-Log-Daten“*. Sie werden auf Basis derselben Daten erzeugt, die für die Erzeugung von Log-Daten genutzt werden. Audit-Log-Daten können von Kunden eingesehen werden.[14]

(2) *„Professional Services Daten“*[15] bezeichnet alle Daten, einschließlich sämtlicher Text-, Ton-, Video-, Bilddateien oder Software, die MS vom oder im Namen eines Kunden zur Verfügung gestellt werden (oder für die der Kunde MS ermächtigt, sie von einem Produkt zu erlangen) oder die anderweitig von oder im Namen von

---

11 Über die hier genannten drei Kategorien hinaus gibt es keine weiteren Kategorien.

12 Die Definition zu „Kundendaten“ findet sich im DPA in der Fassung vom 1. September 2025 unter „Definitionen“, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Seite 6.

13 Zur Klarstellung: Kundendaten schließen die Professional Services Daten nicht ein. Kopien von Kundendaten können aber zu Professional Services Daten werden, wenn der Kunde diese seinerseits (z. B. durch Anfertigung und Bereitstellung eines Screenshots) zur Erläuterung seiner Supportanfrage beifügt.

14 Zu Audit-Log-Daten vgl. Anlage 3: Taxonomie zum Datenschutznachtrag für Produkte und Services von MS.

15 Die Definition zu „Professional Services Daten“ findet sich im DPA in der Fassung vom 1. September 2025 unter „Definitionen“, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Seite 7.

Microsoft im Zuge einer Vereinbarung mit MS über die Erlangung von Professional Services erlangt oder verarbeitet werden. Sie umfassen auch Daten, die für die vom Kunden beauftragten Professional Services (kundenspezifische Beratung und kundenspezifische Entwicklung) benötigt und daher nach Beauftragung der Professional Services durch den Kunden gebildet werden. Es ist möglich, dass Kunden, die Professional Services beauftragen, MS Kopien von Audit-Log-Daten zur Verfügung stellen. In dem Falle werden die Kopien der Audit-Log-Daten den Professional Services Daten zugeordnet. Die Systeme der Professional Services sind isoliert von anderen IT-Systemen und -Diensten von MS. Die einzige Möglichkeit, dass Kopien von Kundendaten Einzug in Professional Services Daten erhalten, ist, wenn Kopien dieser Daten im Kontext der Erbringung der Professional Services bereitgestellt werden oder wenn der Kunde den MS-Mitarbeiter, der Professional Services erbringt, ausdrücklich anweist, Kopien von Kundendaten aus den Onlinediensten zu extrahieren. Bei den Kopien handelt es sich in der Folge um Professional Services Daten.

(3) *„Von MS generierte, abgeleitete oder gesammelte Daten“* sind alle Diagnose- und Log-Daten, die durch eine Handlung des Kunden systemseitig geschaffen („ausgelöst“) werden. Streng genommen stehen „von MS generierte, abgeleitete oder gesammelte Daten“ daher nicht auf einer Stufe mit den Kunden- und Professional Services-Daten, sondern werden aus Kunden- und Professional Services-Daten abgeleitet. Allerdings werden von MS generierte, abgeleitete oder gesammelte Daten nicht aus Inhaltsdaten gewonnen bzw. abgeleitet.

„Diagnose-Daten“ sind Daten, die von der Software/Anwendung von MS bei der Benutzung lokal auf dem Endgerät erzeugt werden. Dies geschieht entsprechend der Konfiguration des Kunden.

„Log-Daten“ sind Protokollierungsdaten, die im Rahmen der Nutzung der Cloud-Dienste von MS erzeugt werden.

Bei Diagnose- und Log-Daten werden auch Zusammenhänge und Abhängigkeiten zwischen den protokollierten Ereignissen festgehalten. Üblicherweise führen Aktionen in einer Anwendung (z. B. das Klicken auf „Speichern“ in Excel) zu Sequenzen von Ereignissen. Hierbei wird systemseitig protokolliert, was durch die Handlung „Speichern“ im System passiert. Bei den Diagnose-Daten kann es zu Sequenzen von Einträgen kommen.

Kundendaten, Professional Services-Daten und „von MS generierte, abgeleitete oder gesammelte Daten“ umfassen sowohl personenbezogene Daten im Sinne der DS-GVO als auch nicht-personenbezogene Daten. Dieser Bericht beschränkt sich jedoch auf die Ausführungen zu personenbezogenen Daten.

E) Zusammenfassung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte am 24. November 2022 festgestellt, dass Verantwortliche den Nachweis, M365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von MS bereitgestellten „Datenschutznachtrags“ vom 15. September 2022 (Data Protection Addendum – DPA) nicht führen könnten. Als Grund nannte die DSK, dass das DPA in sieben Kritikpunkten den Vorgaben des Art. 28 DS-GVO für Auftragsverarbeiter nicht entspreche.

Drei Jahre später untersuchten der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) und Microsoft (MS) in vielen Verhandlungsrunden, ob und wie praxistaugliche und datenschutzkonforme Ergebnisse im Hinblick auf diese Kritikpunkte erarbeitet werden können. Im Ergebnis kann der HBDI feststellen, dass – bezogen auf die sieben Kritikpunkte der DSK – ein datenschutzkonformer Betrieb möglich ist.

In den Verhandlungen konnte der HBDI feststellen, dass sich zwischenzeitlich wichtige rechtliche Vorgaben verändert haben und MS seine Datenverarbeitung an europäische Anforderungen angepasst hat. Er konnte erreichen, dass MS das DPA (für öffentliche Stellen) fortentwickelt und den Verantwortlichen zusätzliche Informationen (u. a. eine Interpretationshilfe zum DPA und das M365-Kit) zur Verfügung stellt. Das Ergebnis beruht auch auf der Erwartung, dass MS und die Verantwortlichen zusammenwirken, damit Verantwortliche M365 datenschutz-rechtskonform nutzen können.

Im Folgenden werden die sieben Kritikpunkte der DSK am DPA von 2022 genannt und die Gründe für eine neue Bewertung angesprochen:

1. fordere Art. 28 DS-GVO eine klare Feststellung von Art und Zweck der Datenverarbeitung sowie Art der personenbezogenen Daten und betroffener Kategorien. Das DPA ermögliche den Verantwortlichen nicht, personenbezogene Daten und deren Verarbeitungszweck näher zu beschreiben und gegebenenfalls zu konkretisieren. – MS hat unterschiedliche Materialien erstellt, um besser über die Datenverarbeitung zu informieren, und für öffentliche Stellen das DPA überarbeitet, so dass Verantwortliche

ausreichende Informationen über die Datenverarbeitung durch MS erlangen und in ihr Verarbeitungsverzeichnis einbinden können.

2. lasse sich MS unzureichend konkretisierte Rechte für Datenverarbeitungen für eigene Geschäftstätigkeiten einräumen. – MS hat klargestellt, dass es nur Log- und Diagnose-Daten, nicht aber Inhaltsdaten, in anonymisierter und aggregierter Form für Zwecke des Auftraggebers (des verantwortlichen Kunden) verarbeite. Diese Datenverarbeitung unterfällt entweder nicht der DS-GVO oder ist datenschutzrechtlich vertretbar.

3. behalte sich MS im DPA im Ergebnis umfangreiche Befugnisse vor, Daten ohne Weisung des Auftraggebers zu verarbeiten und Daten – auch an Drittstaaten – offenzulegen. – MS hat sich verpflichtet, personenbezogene Daten nur auf dokumentierte Anweisung des Kunden zu verarbeiten und hinsichtlich Offenlegungen sich der DS-GVO zu unterwerfen.

4. verpflichte sich MS nicht, die von der DS-GVO geforderten technischen und organisatorischen Sicherheitsmaßnahmen einzuhalten. – MS hat sich verpflichtet, die Vorgaben des Art. 32 DS-GVO ohne Abstriche einzuhalten.

5. genügten die Ausgestaltung der Rückgabe- und Löschverpflichtung im DPA nicht in jedem Fall den gesetzlichen Anforderungen des Art. 28 DS-GVO. – MS bietet einen Löschprozess an und ermöglicht allen Kunden, Daten auch selbst zu löschen oder löschen zu lassen, wenn diese schneller gelöscht werden müssen.

6. informiere MS nach dem DPA nicht über jede beabsichtigte Änderung in Bezug auf Unterauftragnehmer, wie Art. 28 DS-GVO dies fordere. – MS hält sechs Monate bzw. einen Monat im Voraus in seinem Service Trust Portal detaillierte Informationen über jeden Unterauftragnehmer bereit und informiert darüber alle Kunden, die diese Informationen problemlos zur Kenntnis nehmen können.

7. übermittle MS für den Betrieb von M365 personenbezogene Daten in unzulässiger Weise in die USA und in andere Staaten. – Inzwischen sind aufgrund des Angemessenheitsbeschlusses der Europäischen Kommission zum Data Protection Framework zwischen EU und USA die Datenübermittlungen zulässig. Außerdem hat MS seine Datenverarbeitung technisch-organisatorisch so verändert, dass sie zu einem weit überwiegenden

Anteil im Europäischen Wirtschaftsraum stattfindet. Soweit dennoch in einzelnen Fällen Datenübermittlungen an Unterauftragnehmer in allen anderen Staaten erfolgen müssen, gewährleisten Standardvertragsklauseln ein ausreichendes Datenschutzniveau.

Da ein datenschutzkonformer Betrieb von M365 nur gewährleistet ist, wenn auch die Kunden von MS als Verantwortliche und Auftraggeber ihre Pflichten ergänzend zu MS erfüllen, enthält der Bericht Handlungsempfehlungen für die verantwortlichen öffentlichen und nicht-öffentlichen Stellen mit Sitz in Hessen. Sie bieten ihnen für den datenschutzkonformen Einsatz von M365-Produkten grundlegende Rechts- und Handlungssicherheit. Hierauf aufbauend können Verantwortliche einzelne Bestandteile von M365 einer vertiefenden, datenschutzrechtlichen Betrachtung für den konkreten Einsatz unterziehen und im Erfolgsfall datenschutzrechtskonform einsetzen.

F) Ausführlicher Bericht

Der Bericht stellt im ersten Abschnitt den Sachverhalt bezogen auf das DPA, die Kritik an ihm und seine Verteidigung sowie die Praxis der Datenverarbeitung von MS dar. Im zweiten Abschnitt erfolgt eine rechtliche Bewertung von DPA sowie DPA-öS und Datenverarbeitung am Maßstab der DS-GVO. Aus dieser werden dann im dritten Abschnitt Handlungsempfehlungen für die M365 nutzenden Kunden von MS abgeleitet, um M365 datenschutzgerecht nutzen zu können. Abgeschlossen wird der Bericht mit folgenden vier Anlagen:

Anlage	**Titel**	**Inhalt**	**Autor**
1	Interpretationshilfe	Zuordnung der Ausführungen im DPA zu Anforderungen aus Art. 28 Abs. 3 DS-GVO	MS
2	M365-Kit	Eine von MS in Zusammenarbeit mit dem BayLDA erstellte Erläuterung zum M365-Kit	MS
3	Taxonomie zum Datenschutznachtrag für Produkte und Services von MS	Taxonomie der im DPA verwendeten Begriffe für unterschiedliche Datenarten	HBDI
4	Datenschutzrechtliche Anforderungen an Datenverarbeitungsverfahren	Ausführungen zu datenschutzrechtlichen Anforderungen an Datenverarbeitungsverfahren	HBDI

I. Sachverhalt

Der folgende Abschnitt beschreibt den Sachverhalt, indem er sich an den sieben Kritikpunkten der DSK orientiert, dabei aber die zwischenzeitlich eingetretenen tatsächlichen und rechtlichen Veränderungen sowie die darüber hinausgehenden Ermittlungen berücksichtigt. Zu Beginn jedes Kritikpunktes findet sich eine durch Einrahmung hervorgehobene Passage, die auf die einschlägigen Bestimmungen im DPA hinweist.

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

Die vertraglichen Bestimmungen zur Art der personenbezogenen Daten finden sich im DPA in den Abschnitten „Definitionen“ und „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO sowie im Anhang B und in der Anlage 1 im Abschnitt „Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33“, Nr. 3 (Einleitungssatz).

Die Bestimmungen zu den Kategorien verarbeiteter personenbezogener Daten finden sich im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Verarbeitungsdetails“ sowie in Anhang B – „Betroffene Personen und Kategorien personenbezogener Daten“.

Die Bestimmungen zu den Zwecken der Verarbeitung personenbezogener Daten finden sich in den Abschnitten „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Verarbeitungsdetails“ sowie „Art der Datenverarbeitung; Eigentumsverhältnisse – Verarbeitung zur Bereitstellung der Produkte und Services für Kunden“ und Unterabschnitt „Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“.

Der Abschlussbericht der DSK-Arbeitsgruppe „Microsoft-Onlinedienste“ vom 2. November 2022 rügte die fehlende Möglichkeit des Verantwortlichen, personenbezogene Daten und deren Verarbeitungszweck näher zu beschreiben und gegebenenfalls zu konkretisieren.[16] Die DSK-Arbeitsgruppe betont in ihrem Bericht,

[16] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 4. Grundlage

dass Art. 28 Abs. 3 Satz 1 DS-GVO eine klare Feststellung von Art und Zweck der Verarbeitung sowie Art der personenbezogenen Daten und betroffener Kategorien verlange. Es blieben daher Nachbesserungen am DPA erforderlich, die den Gegenstand der Auftragsverarbeitung nicht nur umfassend, sondern auch spezifisch und so detailliert als möglich beschreiben sollten. Wörtlich heißt es im Abschlussbericht: *„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.“*[17]

Die DSK-Arbeitsgruppe empfiehlt daher klare Vorgaben wie kundenspezifische Klarheit oder die Einbeziehung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 28 Abs. 7 DS-GVO.[18]

Um bezogen auf den ersten Kritikpunkt der DSK Lösungsvorschläge zu erarbeiten, die für öffentliche und nicht-öffentliche Stellen mehr Rechtssicherheit bieten, hat MS für das DPA flankierende Dokumentationen erstellt:

- **Interpretationshilfe zur Auslegung des DPA**

Auf Vorschlag des HBDI stellt MS seinen Kunden eine Interpretationshilfe zur Auslegung des DPA zur Verfügung (**Anlage 1**). Das Dokument „Zuordnung der Anforderungen aus Art. 28 Abs. 3 DS-GVO zu Ausführungen im Microsoft DPA (Stand 09/2025)“ ordnet die im DPA enthaltenen Informationen dem Anforderungskatalog des Art. 28 Abs. 3 DS-GVO zu und ermöglicht den Kunden von MS insoweit eine schnellere Orientierung und einen einfacheren Abgleich des DPA mit den nach Art. 28 Abs. 3 DS-GVO notwendigen Inhalten eines Auftragsverarbeitungsvertrags.

der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

[17] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 4.

[18] Ähnlich der EDPS: „Investigation into Use of Microsoft 365 by the European Commission (Case 2021-0518)”, https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf, Seite 25 Rn. 71 ff., Seite 37-38 Rn. 110 bis 112.

- **„M365-Kit“**

Bereits im Vorfeld der Gespräche mit dem HBDI hatte MS in Abstimmung mit dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) – unter anderem als Reaktion auf die Kritik der DSK – begonnen, das M365-Kit zu erarbeiten, das Beispieleinträge zum Verzeichnis der Verarbeitungstätigkeiten, beispielhafte Schwellwertanalysen, beispielhafte Ausführungen zu Rechtsgrundlagen der Datenverarbeitungen und eine beispielhafte Datenschutzerklärung enthält (**Anlage 2**).

- **Klärung von Datenbegriffen und deren Taxonomie**

Um ein besseres Verständnis der durch MS stattfindenden Datenverarbeitungen zu erhalten, hat der HBDI auf der Grundlage von Informationen, die MS im Rahmen der Gespräche bereitgestellt hat, und weiteren themenbezogenen Rückmeldungen von MS eine eigene Taxonomie (**Anlage 3**) speziell für die Prüfung des HBDI entwickelt. Dadurch kann der Kunde besser nachvollziehen, welche Daten von MS verarbeitet werden und auf welche Daten und Datenverarbeitungen er Einfluss nehmen kann und muss. MS betont ausdrücklich, dass die Taxonomie nach seiner Auffassung keine Auswirkungen auf die Verträge mit Kunden haben kann und die Datenverarbeitungen unter dem DPA und den dazugehörigen Produktbestimmungen und anderen MS-Verträgen mit dem jeweiligen Kunden hiervon unberührt bleiben.[19]

- **Für den öffentlichen Bereich: Anpassung des Anhangs B**

Für den öffentlichen Bereich in Hessen hat MS den Anhang B des DPA-öS, der eine Beschreibung der betroffenen Personen und Kategorien personenbezogener Daten enthält, kundengruppenspezifisch angepasst.

Zum einen erfasst der Anhang B des DPA-öS nicht mehr spezifische Inhaltsdaten, sondern führt „Inhaltsdaten“ nur noch als Sammelkategorie auf. Dies vermeidet, dass eine Aufzählung einzelner Kategorien von Inhaltsdaten unterschiedslos für alle Kunden einerseits unvollständig ist und andererseits einzelne Datenkategorien aufführt, die die jeweilige Behörde als Kunde gar nicht verarbeiten darf. Mit dieser zusammenfassenden Kategorie „Inhaltsdaten“ bringt MS zum Ausdruck, dass sich MS

[19] Aus Sicht des HBDI berührt dies Aspekte des Zivilrechts, deren Bewertung nicht Gegenstand der dem HBDI nach Art. 57 DS-GVO zugewiesenen Aufgaben ist.

zu diesen Daten agnostisch verhält, sie weder kennt noch kennen will und für ihre Verarbeitung auch keinerlei inhaltliche Verantwortung oder Haftung übernimmt.[20]

Zum anderen wurde der Anhang B des DPA-öS so abgeändert, dass bezogen auf die von der Diensterbringung betroffenen Personen und Kategorien personenbezogener Daten, die in M365 verarbeitet werden sollen, nicht mehr spezifische Kategorien betroffener Personen und Kategorien personenbezogener Daten aufgeführt werden, sondern, soweit der Kunde im Rahmen des DPA-öS über sie entscheidet, jeweils nur als Sammelkategorie. Zudem listet Anhang B des DPA-öS die von MS verarbeiteten Daten auf.

[20] Dass sich MS bzgl. der Inhaltsdaten agnostisch verhält, gilt sowohl für Kunden aus dem öffentlichen als auch aus dem nicht-öffentlichen Bereich, siehe auch Kap. F) I. 2).

2) Eigene Verantwortlichkeit von MS für „Geschäftstätigkeiten“

Die vertraglichen Bestimmungen zu den Geschäftstätigkeiten finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse – Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind“.

Die DSK-Arbeitsgruppe hält in ihrer Zusammenfassung fest, MS lasse sich „*für bestimmte Verarbeitungen unzureichend eingegrenzte Rechte zu wenig konkretisierten Verarbeitungen der verarbeiteten personenbezogenen Daten einräumen […]. Es bleibt […] unklar, welche personenbezogenen Daten im Rahmen der von Microsoft so genannten ‚legitimen […] Geschäftstätigkeiten‘ verarbeitet werden.*“[21] Auch die Rechtsgrundlage für die Überführung von im Auftrag verarbeiteten Daten in MS‘ Verantwortung sei unklar. Besondere Schwierigkeiten ergäben sich für öffentliche Stellen, da diese nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zurückgreifen könnten.[22]

Um die Datenverarbeitungen zu eigenen Geschäftstätigkeiten besser zu verstehen und beurteilen zu können, hat MS die Verarbeitungsschritte zu Geschäftstätigkeiten im Einzelnen ausführlich erläutert und Fragen des HBDI hierzu umfassend beantwortet.

Danach erfolgt die Verarbeitung zu Geschäftstätigkeiten von MS, soweit durch die Bereitstellung der Produkte und Services für den Kunden veranlasst, in vier Schritten, die nachfolgend nacheinander näher beschrieben werden. Im Einzelnen handelt es sich hierbei um die folgenden Schritte:

(1) **Erhebung** der Daten,
(2) **Pseudonymisierung** der Daten,
(3) **Aggregation** der pseudonymisierten Daten und
(4) **Verarbeitung** der pseudonymisierten, aggregierten (mithin für diesen Zweck anonymisierten) Daten.

---

[21] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 4 und 5. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

[22] Ähnlich der EDPS: „Investigation into Use of Microsoft 365 by the European Commission (Case 2021-0518)”, https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf, Seite 43 Rn. 124 ff.

Als Grundlage für die Datenverarbeitung zu Geschäftstätigkeiten dienen ausschließlich Daten ohne Nutzung oder Wiedergabe der Inhalte der vom Kunden hochgeladenen Informationen, die von **MS im Rahmen der Bereitstellung der Dienste generiert oder erfasst** (erhoben) werden („von MS generierte, abgeleitete oder gesammelte Daten“, wie z. B. Diagnosedaten oder systemgenerierte Protokolle, sog. Log-Daten). Diese Daten werden von MS in der Rolle als Auftragsverarbeiter erhoben und sind nach Aussage von MS sämtlich für die Dienstleistungserbringung gegenüber dem Kunden erforderlich. Es erfolgt ausschließlich eine Weiterverarbeitung dieser – im Rahmen der Auftragsverarbeitung „von MS generierten, abgeleiteten oder gesammelten“ – Daten zur Erfüllung der Geschäftstätigkeiten von MS. Insbesondere werden Inhaltsdaten der MS-Kunden nicht für Geschäftstätigkeiten von MS verarbeitet. MS verhält sich bezüglich der Daten seiner Kunden inhaltsagnostisch.[23]

Soweit „von MS generierte, abgeleitete oder gesammelte Daten“ einen Personenbezug aufweisen, werden diese – bereits im Rahmen der Dienstleistungserbringung gegenüber dem Kunden (Auftragsverarbeitung) – durch Tokenisierung, Verschlüsselung oder Maskierung **pseudonymisiert**. MS führt diese Pseudonymisierung in seiner Rolle als Auftragsverarbeiter durch, um die Einhaltung der Grundsätze der Datenminimierung sowie Integrität und Vertraulichkeit zu fördern. Bei der **Tokenisierung** wird eine Unique ID (UID) vergeben, die die Identifikatoren (z. B. Nutzerkennung) in den personenbeziehbaren Daten ersetzen. Die Tokenisierung ist eines der häufigsten Verfahren, das von MS zur Pseudonymisierung personenbezogener Daten eingesetzt wird. Daten, die nicht mit der UID pseudonymisiert werden, werden verschlüsselt oder maskiert.

Für die Auswertung werden die pseudonymisierten Daten in einem weiteren Schritt **aggregiert**. Der von MS geschilderte Prozess der Aggregation der pseudonymisierten Daten erfolgt so, dass die resultierenden aggregierten Daten, die MS als **R-Daten** bezeichnet, nach dem gemeinsamen Verständnis von MS und HBDI aus den Gesprächen keinen Personenbezug und auch keine Personenbeziehbarkeit mehr aufweisen. Bei diesem Prozess handelt es sich um eine Verarbeitung, in deren Rahmen insbesondere auch keine Kopien der pseudonymisierten Daten erstellt werden. MS hat insoweit versichert, dass aus den aggregierten Daten keine

[23] MS betont ausdrücklich, dass MS aus diesem Grund auch nicht kontrollieren kann, welche Kategorien personenbezogener Daten seine Kunden in M365 verarbeiten.

Rückschlüsse auf die ursprünglich „von MS generierten, abgeleiteten oder gesammelten Daten“ bzw. Personen möglich sind. Es handelt sich somit insgesamt nach dem von MS geschilderten Prozess um eine wirksame Anonymisierung durch Aggregation.

Die konkreten Zwecke, die mit der Nutzung der aus der Aggregation gewonnenen Daten verfolgt werden, können vom jeweiligen MS-Dienst abhängen. Zum Beispiel ist bei „SharePoint“ häufig die Ermittlung der aktuellen Speichernutzung zur Kapazitätsplanung relevant, während bei „MS Teams“ die Audio- und Video-Qualität auf Basis der aggregierten Daten für die Service-Qualität evaluiert wird.

Die aggregierten Daten werden nicht über den jeweiligen Zweck hinaus gespeichert (z. B. in einer Datenbank) und auch nicht für andere Zwecke genutzt. Vielmehr wird für jeden im konkreten Einzelfall verfolgten Zweck ein neuer Aggregationslauf durchgeführt. MS kann als Auftragsverarbeiter zwar auf die „von MS generierten, abgeleiteten oder gesammelten Daten“ zugreifen, aus denen (aggregierte) R-Daten generiert werden. Die aggregierten R-Daten sind jedoch als solche nicht auf die ursprünglichen „von MS generierten, abgeleiteten oder gesammelten Daten“ zurückführbar.

Die Grundprinzipien für die Aggregationsarten bauen auf den Leitlinien zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe von 2014 („Stellungnahme 5/2014 zu Anonymisierungstechniken“, 0829/14/DE) auf.[24] Diese Leitlinien wurden in die internen technischen Richtlinien von MS integriert. MS sichert zu, dass die Aggregationspraktiken den Leitlinien der Artikel-29-Datenschutzgruppe von 2014 entsprechen. Dabei ist die Aggregation eine von mehreren Optionen, um Daten zu anonymisieren.[25]

Beispiel Anonymisierung im Bereich der Entwicklung[26]

Welche Anonymisierungsart zur Anwendung gelangt, entscheidet für den Bereich der

[24] Artikel 29-Datenschutzgruppe, WP 216, „Stellungnahme 5/2014 zu Anonymisierungstechniken“ vom 10. April 2014, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/wp216_de.pdf.

[25] Sofern zum Bespiel keine Abfolge von Ereignissen relevant ist, erfolgt bereits zu einem früheren Stadium ein Überschreiben, Löschen oder Hashen von IDs. Dies erfolgt teilweise bereits auf dem lokalen Endgerät.

[26] Das nachfolgende Beispiel beschreibt das Verfahren der Erstellung von Reportings für den Bereich der Entwicklung. Die hier beschriebene Methodik und Organisation lassen sich aber auch auf andere Bereiche übertragen.

Entwicklung – unter Berücksichtigung der zuvor genannten MS-Richtlinien, welche die Leitlinien zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe integrieren – das sog. **Feature Team** in Abstimmung mit dem Privacy Champ[27] und vor dem Hintergrund der Anforderungen des jeweiligen Einzelfalls.[28] Das Feature Team besteht aus Software-Entwicklern (und/oder Engineers), die für eine bestimmte Funktionalität in einem Software-Produkt (bspw. die Ribbons[29] in MS Word) zuständig sind und diese entwickeln. Für ein Software-Produkt kann es eine Vielzahl von unterschiedlichen Feature Teams geben. Bei dem Privacy Champ handelt es sich um einen Entwickler, der eine monatliche Datenschutzschulung durchläuft, wohingegen alle anderen Entwickler jährlich eine Datenschutzschulung durchlaufen. Die Rolle des Privacy Champ unterstützt und sorgt dafür, dass die Feature Teams die internen Vorgaben (Richtlinien) einhalten.

Nur die **Feature Teams** aus dem Bereich der Entwicklung können Zugriff auf pseudonymisierte Daten erhalten und können hierfür Reportings (Aggregationen) erstellen. Wird eine bestimmte Art von Report (z. B. für die Rechnungsstellung oder andere Geschäftstätigkeiten) benötigt, muss dafür ein Antrag/Auftrag an das Feature Team erfolgen. Dieser wird dann überprüft. Ist die Anfrage berechtigt, wird eine Datenschutz-Folgenabschätzung durchgeführt und eine Report-Art entworfen. Sowohl der Antrag als auch die Report-Art durchlaufen sodann einen Datenschutzfreigabeprozess (Datenschutz-Review). Die Datenschutz-Reviews werden von der Datenschutz-Manager-Gruppe („Privacy Manager Group“) durchgeführt. Im Rahmen des Datenschutz-Reviews wird der geplante Report/die geplante Aggregation anhand der internen Richtlinien von MS bewertet und sichergestellt, dass eine Überprüfung und Genehmigung erfolgt. Es gibt insoweit einen umfassenden Prozess, den alle Reportings (Aggregationen) befolgen müssen. Sollte der Überprüfungsprozess ergeben, dass die internen technischen Richtlinien oder die

---

[27] MS verfügt über ein Datenschutzexpertenteam ("Privacy Expert Team"). Alle Entwickler müssen Datenschutztrainings durchlaufen. Jedes Feature Team (Crew) hat einen sog. "Privacy Champ", der selbst Entwickler ist. Der "Privacy Champ" berät bei der Entwicklung und bereitet die Datenschutz-Reviews vor einem Gremium (Board) vor. Diese sind erforderlich, wenn eine Software oder ein Feature für den Produktivbetrieb freigegeben werden soll. Für die verschiedenen Ebenen gibt es ein abgestuftes Schulungskonzept. Allgemein gesprochen erhält das Board mehr datenschutzspezifische Schulungen als die Privacy Champs, welche wiederum mehr Schulungen als die übrigen Entwickler erhalten.

[28] Das Verfahren gilt für alle Geschäftstätigkeiten. Nur die Feature Teams können über die für den Report sinnvollen Attribute entscheiden, weshalb diese Teams auch verantwortlich sind für die Aggregationen für Rechnungen etc.

[29] Ein Ribbon ist eine Multifunktionsleiste in Office-Anwendungen.

Leitlinien zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe von 2014 nicht eingehalten wurden, führt dies zu Empfehlungen an das Feature Team, das diese zu implementieren hat. Identifiziert der Datenschutz-Review-Prozess Probleme, gibt es eine organisatorische Anordnung, dass diese vor dem Produktivbetrieb behoben werden müssen. Die Missachtung interner Prozesse kann dabei arbeitsrechtliche Konsequenzen nach sich ziehen.

Bei jeder Änderung eines Reportings (Aggregation) muss zudem überprüft werden, ob gegebenenfalls Anpassungen vorzunehmen sind. Losgelöst davon findet mindestens einmal jährlich eine Überprüfung statt.

Das Beispiel zeigt, dass jedes Verarbeitungsszenario einer umfassenden Datenschutzprüfung unterzogen wird. Neben den MS-seitig vorgesehenen Aggregationsverfahren ist es auch möglich, dass ein Feature Team eigene Verfahren entwickelt und anwendet.

Hierfür muss ebenfalls ein umfangreicher **Review-Prozess** durchlaufen werden, durch den sichergestellt wird, dass das Aggregationsverfahren bzw. der Anonymisierungsprozess den Vorgaben der Leitlinien zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe von 2014 und den technischen Richtlinien von MS entspricht.

Für den öffentlichen Bereich in Hessen hat MS die Passage „Verarbeitung für Geschäftstätigkeiten“ im DPA-öS wie folgt neu gefasst:

„*Der Kunde weist Microsoft an, gegebenenfalls auch personenbezogene Daten zu aggregieren und Statistiken zu kalkulieren, um nicht-personenbezogene Daten für folgende Zwecke zu erstellen:*

(1) korrekte Abrechnung;
(2) kundenspezifisches Accountmanagement;
(3) interne Berichterstattung und Geschäftsmodellierung wie etwa Prognose, Umsatz, Kapazitätsplanung und Produktstrategie, um die Bereitstellung und Wartung der Produkte und Services zu unterstützen; und
(4) rechtlich erforderliche Finanzberichterstattung.

Diese Verarbeitung erfolgt in jedem Fall ohne auf den Inhalt von Kundendaten oder Professional Services-Daten zuzugreifen oder diese zu analysieren und beschränkt auf die Erreichung der vorgenannten Zwecke.“

3) Weisungsbindung und Offenlegung

Die vertraglichen Bestimmungen zur Auftragsverarbeitung finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“; „Art der Datenverarbeitung; „Eigentumsverhältnisse“ sowie „Datenübermittlung und Speicherort – Vertraulichkeitsverpflichtung des Auftragsverarbeiters“ und in Anlage 1 unter „Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33, Nr. 3 Buchst. a und Nr. 7“.

Die vertraglichen Bestimmungen zur Offenlegung personenbezogener Daten finden sich im Abschnitt „Datenschutzbestimmungen – Offenlegung verarbeiteter Daten“ und in Anhang C unter „Anfechtung von Anordnungen“.

Zum Themenkomplex „Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, CLOUD Act, FISA 702“ führt die DSK-Arbeitsgruppe aus, dass das DPA MS im Ergebnis umfangreiche Befugnisse vorbehalte.[30] Mit der Regelung werde etwa das Weisungsrecht des Kunden in Bezug auf die Offenlegungen der im Auftrag verarbeiteten Daten eingeschränkt. Der Datenschutznachtrag erlaube die Offenlegung, wenn diese rechtlich vorgeschrieben oder im „Datenschutznachtrag“ beschrieben sei. Solche Offenlegungen seien nicht auf Weisungen des Verantwortlichen beschränkt, sodass sie vor dem Hintergrund des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO nur zulässig seien, wenn sie sich auf Verpflichtungen aus dem Unions- oder mitgliedstaatlichen Recht, dem MS unterliege, beschränkten. Dies sei nicht der Fall, weshalb die Weisungsbindung durch das DPA nicht den gesetzlichen Mindestanforderungen gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO genüge. Auch behalte sich MS vertraglich weit reichende Offenlegungen vor, die im Falle ihrer Umsetzung nicht den in Art. 48 DS-GVO aufgestellten Anforderungen entsprächen.[31]

---

[30] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 5. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

[31] Ähnlich der EDPS: „Investigation into Use of Microsoft 365 by the European Commission (Case 2021-0518)”, https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf, Seite 25 Rn. 71 ff., Seite 162, Rn. 552 ff., 165, Rn. 567 ff.

Aus dem DPA ergibt sich, dass MS nur nach den dokumentierten Weisungen des Kunden handelt.[32] Für Datenverarbeitungen im Anwendungsbereich der DS-GVO verpflichtet sich MS im Anhang C zudem zu zusätzlichen Schutzmaßnahmen.[33] Beispielhaft zu nennen sind hier die „Anfechtung von Anordnungen“ zur Offenlegung personenbezogener Daten und „Änderungsmitteilungen“ über Änderungen von Rechtsvorschriften, die Auswirkungen auf die in Anlage C oder in den Standardvertragsklauseln vorgesehenen Zusicherungen und Verpflichtungen haben.

Aus dem DPA ergibt sich weiterhin, dass MS personenbezogene Daten grundsätzlich nicht offenlegt oder zugänglich macht. Ausnahmen liegen jedoch vor, wenn (1) ein Kunde die Offenlegung anweist, (2) das DPA die Offenlegung erlaubt oder (3) die Offenlegung gesetzlich vorgeschrieben ist. Schließlich ist in diesem Zusammenhang Anlage 1 des DPA zu erwähnen. MS erkennt hierin ausdrücklich die Verpflichtungen nach der DS-GVO an und nimmt Bezug auf „*das Recht der Union oder des Mitgliedstaats, dem Microsoft unterliegt*“.

MS stellt insoweit klar, dass im Geltungsbereich der DS-GVO gesetzliche Offenlegungen von Daten nur nach den Bestimmungen des Unionsrechts oder des Rechts eines Mitgliedstaates zulässig sind.[34]

Das DPA-öS sagt nunmehr[35] aus, dass die Ausübung gesetzlicher Weisungsrechte nicht beschränkt ist, soweit dies den vereinbarten Leistungsumfang nicht verändert und dass MS die DS-GVO[36] einhält, auch wenn MS durch ausländische Behörden zu einem Handeln, Dulden oder Unterlassen verpflichtet wird und dadurch gegen seine Pflichten aus dem Auftragsverarbeitungsvertrag und der DS-GVO verstoßen würde.

MS verpflichtet sich in Anlage 1 zum DPA-öS zudem, personenbezogene Daten nur auf dokumentierte Anweisung des Kunden zu verarbeiten. Um Missverständnisse zu vermeiden, war MS bereit, für öffentliche Stellen mit Sitz in Hessen im Rahmen des

---

[32] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten, Seite 13.

[33] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen, Seite 39.

[34] Rechtsvorschriften können auch solche im Sinne von Klausel 14 Buchst. a des Standardvertrags 2021/914/EU sein, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de.

[35] Wie zuvor auch bereits mit anderen öffentlichen Stellen vereinbart.

[36] Siehe auch insoweit Fn. 34.

DPA-öS unter der Überschrift „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“ in der folgenden Textpassage

„Der Kunde stimmt zu, dass der Kundenvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der **Verwendung und** der Konfiguration der Features der Produkte durch den Kunden die vollständigen und dokumentierten Weisungen des Kunden gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten oder die Dokumentation der Professional Services und die Nutzung der Professional Services durch den Kunden darstellen.“

die Worte „*Verwendung und*“ zu streichen.

Mit dieser Streichung wird klargestellt, dass zum einen eine Verwendung zum Zeitpunkt der Konfiguration noch nicht stattfindet. Zum anderen kann eine Verwendung von M365 durch einen beliebigen Mitarbeiter nicht als autorisierte Weisung interpretiert werden.[37]

[37] MS weist darauf hin, dass hiervon das Recht von MS, Features der Produkte und Dienste von MS auszuführen, unberührt bleibt, wenn der Kunde sie benutzt.

4) Umsetzung technischer und organisatorischer Maßnahmen

Die vertraglichen Bestimmungen zu den technischen und organisatorischen Maßnahmen finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Datensicherheit – Sicherheitsverfahren und Sicherheitsrichtlinien“ sowie in den Unterabschnitten „Datenverschlüsselung“ und „Datenzugriff“. Außerdem finden sich vertragliche Bestimmungen im Anhang A und Anlage 1 im Abschnitt „Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33“, Nr. 3 Buchst. c und Nr. 5 ff.

Detailinformationen zu den technischen und organisatorischen Maßnahmen stellt MS unter https://www.microsoft.com/de-de/security bereit.

Zum Kritikpunkt „Umsetzung technischer und organisatorischer Maßnahmen“ stellte die DSK-Arbeitsgruppe fest, dass das geprüfte DPA Ergänzungen zu den technisch-organisatorischen Maßnahmen enthält.[38] Für bestimmte beschränkte Datenkategorien (nämlich Kundendaten in „Core-Onlinediensten“ und nunmehr auch „Professional Services-Daten“) bestünden Garantie- und Datensicherheitsmaßnahmen. Zudem habe MS dargelegt, dass es Interessierten nach einer Anmeldung Zugang zur Website servicetrust.microsoft.com („Service Trust Portal“), unter der Informationen über die durchgeführten technisch-organisatorischen Maßnahmen anbiete. Es blieben jedoch Rechtsunsicherheiten, da die Garantien über „Sicherheitsmaßnahmen“ formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten, nämlich „Kundendaten“ in „Core-Onlinediensten“ und „Professional Service-Daten“, erfassten.

Die HBDI stellte hierzu bereits während der Gespräche im Sommer 2024 fest, dass der Auftragsverarbeiter nach Art. 28 Abs. 3 Buchst. c und f DS-GVO alle gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreifen und den Verantwortlichen (Kunden) bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten unterstützen muss. Für die Beurteilung der Sicherheit der Verarbeitung ist nach Art. 32 Abs. 1 DS-GVO u. a. der **Stand der Technik** (und nicht davon abweichende „branchenübliche Standards“ oder nicht davon abweichende „Verfahren nach Branchenstandard“, wie z. B. in Anhang A und an anderer Stelle erwähnt) zu berücksichtigen.

[38] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 5 und 6. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

MS hat klargestellt und in Anhang 1 auch festgehalten, dass die übergeordnete Prämisse besteht, dass die Anforderungen des Art. 32 DS-GVO umfassend und für sämtliche Verarbeitungsvorgänge eingehalten werden. Die Verwendung der Begriffe „branchenübliche Systeme“ oder „branchenübliche Prozesse“ führen hierbei zu keinem im Verhältnis zu dem nach Art. 32 DS-GVO geforderten „Stand der Technik“ niedrigerem Schutzniveau. Vielmehr stellt der Stand der Technik eine untere Grenze dar, die durch die Umsetzung der Maßnahmen niemals unterschritten wird. MS verpflichtet sich zusammenfassend, alle notwendigen Maßnahmen im Sinne des Art. 32 DS-GVO zu treffen. Außerdem unterstützt MS Kunden bei der Umsetzung eigener Maßnahmen und bei der Einhaltung ihrer Rechenschaftspflicht. Hierzu stellt MS u.a. umfassende Informationen über ergriffene Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DS-GVO zur Verfügung, die insbesondere geeignet sind, hierauf aufbauend eigene abgestimmte Maßnahmen zu ergreifen.

5) Löschung und Rückgabe personenbezogener Daten

Die vertraglichen Bestimmungen zur Löschung und Rückgabe von Daten finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Speicherung und Löschung von Daten“ sowie im Anhang A unter „Physische und umgebungsbezogene Sicherheit“ und Anlage 1 unter „Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33, Nr. 3 Buchst. g“.

Detailinformationen zur Löschung von Daten sämtlicher Datenkategorien stellt MS unter https://learn.microsoft.com/de-de/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview bereit.

Zum fünften Kritikpunkt zur „Löschung und Rückgabe personenbezogener Daten“ hat die DSK-Arbeitsgruppe festgestellt, die Ausgestaltung der Rückgabe- und Löschverpflichtung im DPA genüge nicht in jedem Fall den gesetzlichen Anforderungen des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. g DS-GVO.[39] Verantwortliche könnten wegen der Unklarheit der Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 Buchst. a DS-GVO nicht nachkommen.

MS sichert ausdrücklich zu, dass der Kunde alle im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten jederzeit nach Maßgabe des jeweils geltenden DPA löschen kann. Dies gilt auch nach Abschluss der Vertragsbeziehung. Der HBDI stellte fest, dass aufgrund der Zusicherung von MS davon auszugehen ist, dass die Anforderung des Art. 28 Abs. 3 UAbs. 1 Buchst. g DS-GVO erfüllt werden kann. Die geführten Gespräche wurden sodann genutzt, um sich das Verfahren der Löschung von MS näher beschreiben zu lassen.

MS setzt seine vertraglichen Verpflichtungen und die gesetzlichen Anforderungen aus der DS-GVO in technischen Richtlinien um. Diese Richtlinien enthalten Abschnitte über die Aufbewahrung der verschiedenen Datenkategorien, die MS im Auftrag verarbeitet. Die Löschung von Kundendaten und „von MS generierten, abgeleiteten und gesammelten Daten“ erfolgt kundenseitig oder systemseitig aufgrund automatisiert

[39] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung,, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 6. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

umgesetzter Löschfristen. Hierzu stehen dem Kunden unterschiedliche Tools zur Verfügung, die das Auffinden und Löschen von Daten unterstützen.

Sämtliche gespeicherte Kundendaten können jederzeit manuell gelöscht werden oder werden automatisiert durch Ablauf des Abonnements von M365 gelöscht, sofern MS nicht zur Aufbewahrung autorisiert ist.[40] Kunden, Nutzende eines Benutzeraccounts von M365 (z. B. Mitarbeiter) und Kundenadministratoren können Inhaltsdaten in diesem Rahmen jederzeit manuell löschen (**Active Deletion**). Die Ausgestaltung der jeweiligen Löschfunktion und des zugehörigen Löschprozesses richtet sich nach dem konkreten Typ der jeweiligen Daten (z. B. Nachrichten, E-Mails, Kalendereinträge) und dem Dienst, in dessen Kontext die Daten gelöscht werden. Konkret betrachtet wurde dies am Beispiel von Dateien im Kontext des Dienstes M365Office.

Beispiel M365Office[41]

Wenn ein Kunde eine Datei manuell löscht, wird diese zuerst in einen Papierkorb des Nutzers (Recovery Bin) verschoben, sofern der jeweilige Dienst das vorsieht und ggf. von Kunden entsprechend konfiguriert wurde. Dateien können aus diesem wiederhergestellt werden. Nach einer vorgegebenen oder vom Kunden konfigurierten Frist, verlängert um eine standardmäßige System-Aufbewahrungsfrist von maximal 30 Tagen, werden die Daten vollständig gelöscht, sodass eine Wiederherstellung spätestens nach Ablauf dieser Frist nicht mehr möglich ist. Der Kunde kann den Benutzeraccount so konfigurieren, dass eine Löschung auf verschiedenen Ebenen (Layer) erfolgt. Hier bleibt eine Wiederherstellung bis zur endgültigen Löschung auf der letzten Ebene (Layer) möglich. Die Zeitdauer, wie lange eine Datei in den verschiedenen Papierkörben vorgehalten wird, kann vom Kunden konfiguriert werden. Solange sich eine Datei in einem der Papierkörbe befindet, kann die Datei wiederhergestellt werden. Erst wenn sie aus (allen) Papierkörben gelöscht wurde, wird die Löschung tatsächlich durchgeführt (**Hard Delete**). Es ist möglich, dass die Löschung aus dem Papierkorb des Kunden nicht der letzte Schritt vor der tatsächlichen

[40] Nutzungsdaten sind für die konkrete Nutzung von zentralen Diensten erforderlich und werden automatisiert gelöscht, sobald sie für diese Nutzung nicht mehr benötigt werden. Eine vorzeitige manuelle Löschung ist nicht möglich und wäre auch nicht sinnvoll.

[41] Das nachfolgende Beispiel beschreibt das Verfahren der Löschung an Hand des Dienstes M365 Office. Die hier beschriebene Methodik und Organisation lassen sich aber auch auf andere Bereiche übertragen.

Löschung ist. Bei einer entsprechenden Konfiguration kann sich die Datei noch in einem für Administratoren zugänglichen Papierkorb befinden.

Vor der Löschung besteht für Kunden die Möglichkeit, alle (personenbezogenen) Daten zu identifizieren, die in den verschiedenen Anwendungen von M365 (wie z. B. in Outlook und OneDrive) gespeichert sind. Dies kann z. B. durch die Nutzung von Such- und Discovery-Tools (wie dem **eDiscovery-Tool**[42] für die Inhaltssuche) erfolgen. Kunden können für die Inhaltssuche daneben auch das **Purview Compliance-Portal**[43] von MS verwenden, um nach Daten zu suchen. Für die Löschung von Daten kann der Kunde Daten entweder manuell löschen oder andere Tools wie zum Beispiel das eDiscovery-Tool verwenden. Bei der Benutzung des eDiscovery-Tools kann angegeben werden, welche Art von Löschung erfolgen soll. Auch eine vollständige Löschung ist möglich.

Wenn ein Kunde das Abonnement der M365-Dienste beendet oder nicht verlängert, werden die Inhaltsdaten 90 Tage lang in einem eingeschränkten Funktionskonto aufbewahrt, damit Kunden, die ihre Inhaltsdaten nicht rechtzeitig vor Vertragsende extrahiert oder gelöscht haben, diese noch extrahieren können und ein ungewollter Datenverlust vermieden wird. Das Recht des Kunden, jederzeit die Löschung der gespeicherten Inhaltsdaten vorzunehmen, bleibt hiervon unberührt. Nach Ablauf der 90 Tage werden die Inhaltsdaten und die in den Onlinediensten gespeicherten personenbezogenen Daten innerhalb weiterer 90 Tage sequentiell gelöscht, es sei denn, MS ist zur Aufbewahrung autorisiert. Eine vollständige Löschung (**Passive Deletion**) erfolgt somit spätestens nach 180 Tagen.

Sequentielle Löschung bedeutet, dass die Dienste die Löschung in einer bestimmten Reihenfolge vornehmen. Generell verwalten die Dienste Verweise (Links) auf die spezifischen Inhalte der Daten, die selbst ggf. mehrfach redundant auf unterschiedlichen Servern oder Speichern vorgehalten werden. Beim Löschen einer Datei wird normalerweise als erstes dieser Verweis (Link) gelöscht (**Soft Delete**). Danach werden die Daten der Datei aktiv und gezielt überschrieben (**Hard Delete**). Dies geschieht innerhalb von 30 Tagen nach dem Soft-Delete. Der genaue Zeitpunkt des Übergangs vom Soft Delete zum Hard Delete ist für den Kunden (Benutzer) nicht

[42] Das eDiscovery-Tool ist ein Werkzeug, mit dem Administratoren Informationen in der Kunden-Umgebung (Kundendaten) durchsuchen können, siehe auch: https://learn.microsoft.com/de-de/purview/ediscovery-configure-edge-to-export-search-results.

[43] Siehe https://learn.microsoft.com/de-de/purview/purview-portal.

erkennbar, da die Verbindung (Link) zwischen dem Account und dem Kundendatum im Rahmen des Soft-Delete bereits vorab entfernt wurde.

Grundsätzlich werden „von MS generierte, abgeleitete und gesammelte Daten“ nach 18 Monaten automatisch gelöscht. Kürzere Löschfristen werden angewendet, wenn es keinen weiteren Verwendungszweck mehr für die Daten gibt. Zudem ist eine kundenseitige Löschung von generierten, abgeleiteten und gesammelten Daten denkbar, sofern MS nicht zur Aufbewahrung autorisiert ist**.** Eine Löschung von generierten, abgeleiteten und gesammelten Daten kann der Kunde zwar nicht selbst vornehmen, er kann aber einen entsprechenden Löschantrag stellen. „Von MS generierte, abgeleitete und gesammelte Daten“ werden dann in der Regel innerhalb von 30 Tagen gelöscht.

Obwohl die meisten „von MS generierten, abgeleiteten und gesammelten Daten“ eines Nutzenden bei der Löschung eines Benutzerkontos ebenfalls gelöscht werden, bleiben einige Daten erhalten, um die Konsistenz und Integrität der entsprechenden Protokolle zu schützen (z. B. bei Sicherheitsprotokollen).[44] Die verbleibenden Log-Daten können nach der Löschung des Kontos aber nicht mehr zum Nutzenden zurückverfolgt werden, da die betroffenen Daten ehemalige Identifikatoren enthalten, zu denen es nach der Löschung des zugehörigen Benutzeraccounts keinen Bezugspunkt mehr gibt.

Bei R-Daten handelt es sich um anonymisierte Daten, die nicht mehr in der Sphäre des Kunden liegen. Hier besteht keine Möglichkeit der Löschung durch den Kunden. R-Daten werden gelöscht, wenn der spezifische Zweck der Generierung erreicht wurde.

Kunden können durch die Audit-Logs Einblick in die Nutzung der Dienste nehmen und damit sicherstellen (bspw. bei einer Löschaufforderung gem. Art. 17 DS-GVO nachweisen), dass Daten wirklich gelöscht sind. Insbesondere, wenn ein Benutzer-Objekt (Benutzer-Account) gelöscht wird, gibt es eine Vielzahl von Warnungen und Hinweisen, die im Audit-Log nachvollzogen werden können.

Bei M365 gibt es kein standardmäßiges dediziertes Backup. Ein reguläres Backup muss durch einen Kunden eigenständig vorgehalten werden oder als dedizierter Dienst

[44] Weitere Informationen finden sich unter: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-office365#deleting-system-generated-logs.

von MS bestellt werden. Daten werden redundant in der Cloud gespeichert. Für bestehende Dateien, die im Dienst gespeichert sind, repliziert MS diese Dateien und bewahrt einen „Versionsverlauf“ auf, der es den Benutzern ermöglicht, zu früheren Versionen zurückzukehren.

6) Unterauftragsverarbeiter

Die vertraglichen Bestimmungen zum Einsatz von Unterauftragsverarbeitern durch MS finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ und Anhang C unter Nr. 6. Die Auflistung der Unterauftragsverarbeiter findet sich im MS Service Trust Center, abzurufen unter: https://www.microsoft.com/de-de/trust-center/privacy/data-access.

Informationen zum Prozess der Publikation von neuen oder ersetzten Auftragsverarbeitern stellt MS unter https://servicetrust.microsoft.com/DocumentPage/7a132d00-29c2-4d26-b0f5-486923c41223 bereit.

Hinsichtlich des sechsten Kritikpunkts, der Bekanntgabe des Einsatzes von Unterauftragsverarbeitern, versteht die DSK-Arbeitsgruppe Art. 28 Abs. 2 DS-GVO 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 müsse und nicht nur den allgemeinen Hinweis, dass Änderungen geplant seien.[45] Das von MS bereitgestellte Muster einer Benachrichtigungs-E-Mail enthalte nur eine Information über geplante Änderungen, aber nicht die konkret geplanten Änderungen. Die der DSK-Arbeitsgruppe vorgestellte Liste über Unterauftragsverhältnisse unterscheide zudem bislang im Wesentlichen danach, für welchen Dienst bzw. welche Funktionalität Unterauftragnehmer eingesetzt seien, benenne deren Sitz und die ihnen zugänglichen Datenkategorien. Im Vergleich dazu sähen die von der EU-Kommission bereitgestellten Standardvertragsklauseln deutlich detailliertere Angaben über Namen, Anschrift und Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der jeweiligen Verarbeitung vor, die eine klare Abgrenzung der Verantwortlichkeiten mehrerer eingesetzter Unterauftragsverarbeiter erlaubten. MS hat seit der Bewertung durch die DSK-Arbeitsgruppe die Bandbreite an über Auftragsverarbeiter zur Verfügung gestellten Informationen erweitert.

[45] AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 6. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

Der HBDI stellte im August 2024 fest, dass MS mit 47 Unterauftragsverarbeitern zusammenarbeitet. Gemessen an der Größe des Unternehmens handelt es sich somit um eine relativ geringe Anzahl an Unterauftragsverarbeitern. Änderungen der Unterauftragsverhältnisse erfolgen – aufgrund der hiermit einhergehenden Aufwände – selten, sodass der Prozess des Monitorings der Änderungen an den Unterauftragsverarbeitern mit vertretbarem Aufwand möglich erscheint. MS unterscheidet zwischen drei Kategorien von Unterauftragsverarbeitern: (1) solche, die Teile der Technologie für die MS Clouddienste bereitstellen (Anzahl 7), (2) solche, die unterstützende Dienste anbieten (Anzahl 5), und (3) solche, die Vertragspersonal zur Verfügung stellen (Anzahl 35).[46] Für jeden Unterauftragsverarbeiter werden detaillierte Informationen bereitgestellt, einschließlich Geschäftsadresse, DnB-Nummer und Mutterkonzern. Der Wechsel oder das Hinzutreten eines Unterauftragsverarbeiters wird durch ein Update der MS Online Services-Unterauftragsverarbeiterliste bekannt gegeben.

Sofern ein Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung von Kundendaten steht, verpflichtet sich MS im DPA, die entsprechenden Informationen mit einer Vorlaufzeit von sechs Monaten bereitzustellen; für sonstige personenbezogene Daten beträgt die Vorlaufzeit 30 Tage. Dies gibt dem Kunden Zeit, um dem Einsatz des Unterauftragsverarbeiters zu widersprechen oder geeignete Maßnahmen zu ergreifen.

Die Liste der Unterauftragsverarbeiter wird durch MS stets aktuell gehalten. Änderungen der Unterauftragsverarbeiter werden am Ende der Liste unter dem Punkt „Summary of Changes“ aufgeführt. Die Änderungen können auch über das Service Trust Portal[47] eingesehen werden.

Sofern der Kunde der Verarbeitung seiner Daten durch einen neuen Unterauftragsverarbeiter nicht zustimmt, wird im DPA dem Kunden vertraglich das Recht eingeräumt, den betroffenen Onlinedienst jeweils ohne Strafe oder Kündigungsgebühr zu beenden oder das betroffene Softwareprodukt zu kündigen, indem er vor dem Ablauf der entsprechenden Benachrichtigungsfrist eine schriftliche Kündigung einreicht.

---

[46] Die Liste der Unterauftragsverarbeiter findet sich unter: Service Trust Portal, https://servicetrust.microsoft.com/DocumentPage/8d295fc2-f7d9-4662-8301-99b077fc6b79.

[47] Das Service Trust Portal ist unter dem folgenden Link abrufbar: https://servicetrust.microsoft.com/.

Neben den bereits zuvor getroffenen Feststellungen weist MS ergänzend darauf hin, dass MS beim Einsatz von Unterauftragsverarbeitern dafür Sorge trage, dass deren sicherer Einsatz im Einklang mit dem DPA und der DS-GVO gewährleistet sei. MS verpflichtet sich im DPA, beim Einsatz von Unterauftragsverarbeitern mittels schriftlichen Vertrags mit diesen sicherzustellen, dass diese mindestens das Datenschutzniveau bieten, das im DPA von MS verlangt wird. MS stellt darüber hinaus nach Art. 28 Abs. 4 Satz 2 DS-GVO sicher, dass MS weiterhin für die Einhaltung der Pflichten aus dem DPA verantwortlich ist.

7) Drittlandübermittlungen

Die vertraglichen Bestimmungen zu Drittlandübermittlungen finden sich im DPA im Abschnitt „Datenschutzbestimmungen – Datenübermittlungen und Speicherort – Datenübermittlungen“.

In ihrem Bericht vom November 2022 kritisierte die DSK-Arbeitsgruppe zum siebten Kritikpunkt „Drittlandübermittlungen“, dass die Nutzung von M365 ohne Übermittlungen personenbezogener Daten in die USA nicht möglich sei, dies aber gegen das Urteil des EuGH zu Schrems II[48] und die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses (EDSA)[49] verstoßen könne.[50]

Gemäß Unterabschnitt „Datenübermittlungen“ des DPA beauftragt der Kunde MS, personenbezogene Daten in Länder zu übermitteln, in denen MS oder Unterauftragsverarbeiter tätig sind. Außerdem speichert und verarbeitet MS gemäß Abschnitt „Speicherorte von Kundendaten“, Absatz 2, für die „EU-Datengrenzen-Onlinedienste“ Kundendaten und personenbezogene Daten innerhalb der Europäischen Union „wie in den Produktbestimmungen beschrieben“. Die EU-Data Boundary erstreckt sich jedoch nicht vollumfänglich auf den technischen Support (Professional Services), sodass es in diesen Fällen zu Datenübermittlungen in Drittländer, für die die Europäische Kommission kein angemessenes Datenschutzniveau anerkannt hat, kommen kann.

Nach Aussagen von MS wird die Frage der „Datenübermittlungen in Drittstaaten“ aufgrund der Datenverarbeitung innerhalb der EU-Data Boundary und des Lock Box-Prozesses für den Fall des technischen Supports nur einen äußerst geringen Teil von personenbezogenen Datenverarbeitungen betreffen. Der Lock Box-Prozess beschreibt einen internen Prozess, nach dem ein Zugriff eines Mitarbeiters von MS auf

---

48 EuGH, Urt. vom 16. Juli 2020, C-311/18, https://curia.europa.eu/juris/document/document.jsf;jsessionid=21C1DD931AB4F8A17ABC6C2F70B9F9DF?text=&docid=228677&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=10387316.

49 EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

50 AG DSK, „Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 7. Grundlage der Bewertung durch die DSK-Arbeitsgruppe war das DPA in der Fassung vom 15. September 2022, https://www.microsoft.com/licensing/docs/view/microsoft-products-and-services-data-protection-addendum-dpa?lang=14.

Kundendaten in Produktivumgebungen im Supportfall durch die MS-interne Hierarchie freigegeben wird. Die Freigabe erfolgt aufgrund eines Antrags durch den Mitarbeiter von MS, der von einem Manager von MS geprüft wird und abgelehnt oder genehmigt werden kann. Zudem werden alle Aktionen des Supports protokolliert.

Bei der Customer Lock Box findet ein dem Lock Box-Prozess vorgelagerter Prozess statt. Im Rahmen dieses vorgelagerten Prozesses erhält der Kunde zusätzlich die Möglichkeit, den Antrag seinerseits zu genehmigen oder abzulehnen. Vom Lock Box-Prozess ausgenommen sind grundsätzlich automatisierte Verarbeitungen, bspw. Indexierung und Schad-Software-Scans.

Der HBDI legt seiner Bewertung folgendes Verständnis zugrunde: Aufgrund der EU-Data Boundary[51] finden seit dem 1. Januar 2024 Datenverarbeitungen außerhalb der EU/des EWR nur in wenigen Fällen statt, insbesondere:

(1) Vom Kunden initiierte Datenübermittlungen in Drittländer,

(2) Professional Services-Daten für Support und Beratung,

(3) Sicherheitsmaßnahmen zum Schutz vor globalen Bedrohungen der Cybersicherheit und Informationen über Sicherheitsbedrohungen (MS Threat Intelligence),

(4) Verzeichnisdaten (MS Entra Directory, vormals Azure Active Directory),

(5) Netzwerk-Transit zur Aufrechterhaltung der Routing-Ausfallsicherheit,

(6) Qualität und Management von Diensten und Plattformen.

Seit der Feststellung der DSK haben sich die politischen und rechtlichen Grundlagen verändert. Für Datenübermittlungen in die USA hat die Europäische Kommission den Angemessenheitsbeschluss für das EU-US Data Privacy Framework (EU-US DPF) angenommen.[52] Sie kommt darin zu dem Schluss, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten. Seit der Annahme des Angemessenheitsbeschlusses können wieder personenbezogene Daten aus der EU in die USA übermittelt werden, ohne dass weitere Übermittlungsinstrumente oder

[51] MS hat seit der Bewertung durch die DSK-Arbeitsgruppe die Bandbreite über Auftragsverarbeitern zur Verfügung gestellten Informationen erweitert. In deutschsprachigen Dokumenten verwendet Microsoft den Begriff „EU-Datengrenzen".

[52] EU-US Data Privacy Framework (EU-US DPF), Commission Implenting Decision EU 2023/1795 vom 10. Juli 2023, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj.

zusätzliche Maßnahmen erforderlich sind. Dies gilt jedoch nur, sofern der jeweilige US-Datenempfänger auch unter dem EU-US DPF beim US Department of Commerce zertifiziert ist. Dies müssen Datenexporteure in der EU vorab prüfen. Das US Department of Commerce veröffentlicht eine entsprechende Liste. MS ist nach dem EU-US DPF zertifiziert und zur Übermittlung von „HR und Non-HR Data“ berechtigt.[53]

Als zusätzliches Instrument zur Legitimation des Drittstaatentransfers hat MS innerhalb seiner Unternehmensgruppe sowie mit seinen Unterauftragsverarbeitern zudem Standardvertragsklauseln gemäß der Entscheidung 2021/914/EU Modul 3 abgeschlossen.[54]

Der Abschluss der Standardvertragsklauseln dient einerseits als zusätzliche Sicherheitsmaßnahme für den Fall des Wegfalls des EU-US DPF und ist zudem erforderlich, da MS – wie zuvor dargestellt – auch Mitarbeiter und Unterauftragsverarbeiter in Drittstaaten ohne ein der DS-GVO entsprechendes, angemessenes Datenschutzniveau (z. B. Indien) beschäftigt.

Für die Datenübermittlung in Drittländer sowie an nicht nach dem EU-US DPF zertifizierte US-Unternehmen gelten die Anforderungen und Prüfpflichten aus dem sog. „Schrems II“-Urteil des EuGH und die zugehörigen Empfehlungen 01/2020 des Europäischen Datenschutzausschusses weiter fort.[55]

---

53 EU-US Data Privacy Framework List, https://www.dataprivacyframework.gov/list.

54 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de.

55 EuGH, Urt. vom 16. Juli 2020, C-311/18, https://curia.europa.eu/juris/document/document.jsf;jsessionid=21C1DD931AB4F8A17ABC6C2F70B9F9DF?text=&docid=228677&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=10387316; EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

II. Rechtliche Erwägungen

Nachfolgend werden die rechtlichen Erwägungen zu Art. 28 DS-GVO, die der HBDI seiner Bewertung unter Berücksichtigung der Kritikpunkte der DSK zugrunde gelegt hat, zusammengefasst.

Verantwortlicher und Auftragsverarbeiter

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[56] Maßgeblich für die Bestimmung des Verantwortlichen ist also, wer die Entscheidungsgewalt über Zwecke und Mittel der Verarbeitung hat. Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[57] Der Auftragsverarbeiter agiert im Verhältnis zum Verantwortlichen wie ein „verlängerter Arm“.[58]

Der Kunde und MS als Verantwortliche und Auftragsverarbeiter

MS bietet seinen Kunden mit M365 einen cloudbasierten Abonnementdienst, der verschiedene Anwendungen umfasst, wie z. B. Office-Anwendungen (Word, Excel, PowerPoint, Outlook), Exchange Online (E-Mail/Kalender), MS Teams (Chat, Video, Telefonie), Sharepoint Online (Intranet und Dokumentenmanagement) und OneDrive for Business (Cloud-Speicher).[59] MS agiert hierbei je nach tatsächlicher Ausgestaltung des Verhältnisses als Auftragsverarbeiter, während die Kunden, die die von MS bereitgestellten Clouddienste nutzen, Verantwortliche sind.[60] Im Folgenden wird davon ausgegangen, dass der Kunde Verantwortlicher und MS Auftragsverarbeiter ist.

---

[56] Eine ausführliche Darstellung der Kriterien zur Bestimmung der Rolle des Verantwortlichen findet sich in den Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO Version 2.0 des Europäischen Datenschutzausschusses (EDSA), Rn. 15 ff., https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

[57] Eine ausführliche Darstellung der Kriterien zur Bestimmung der Rolle des Auftragsverarbeiters findet sich in den Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO Version 2.0 des Europäischen Datenschutzausschusses (EDSA), Rn. 73 ff., https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

[58] Nink in Spindler/Schuster, 4. Aufl. 2019, DS-GVO Art. 28 Rn. 2.

[59] Insgesamt umfasst M365 ca. 300 verschiedene Dienste.

[60] Dies entspricht sowohl der Rechtsauffassung von MS, vgl. DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Seite 13, als auch der Rechtsauffassung der AG DSK

Pflichten des Kunden als Verantwortlicher

Nach Art. 5 Abs. 2 DS-GVO ist der Verantwortliche für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten rechenschafts- und nachweispflichtig. Alle den Grundsätzen des Art. 5 Abs. 1 DS-GVO nachfolgenden materiellen Bestimmungen der DS-GVO sind auf die Umsetzung dieser Grundsätze ausgerichtet.[61] Der Verantwortliche ist somit primärer Normadressat der DS-GVO. Er trägt (weit überwiegend) die Beweislast dafür, dass die Vorschriften der DS-GVO eingehalten werden.[62]

Zu den Pflichten des Verantwortlichen zählen etwa das Führen des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO, die Gewährleistung des Datenschutzes durch Technikgestaltung gem. Art 25 DS-GVO, die Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DS-GVO und die Durchführung der Datenschutzfolgenabschätzung unter den Voraussetzungen des Art. 35 DS-GVO.

An den Pflichten des Verantwortlichen ändert sich auch dann nichts, wenn sich der Verantwortliche zur Durchführung von Verarbeitungsverfahren eines Auftragsverarbeiters – wie z. B. im Fall der Nutzung von M365-Clouddiensten – bedient. Dies verdeutlicht etwa Art. 28 Abs. 1 DS-GVO, wonach der Verantwortliche nur mit Auftragsverarbeitern zusammenarbeiten darf, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Auftragsverarbeitungsvertrag

Auch beim Einsatz von Auftragsverarbeitern muss der Verantwortliche das durch die DS-GVO garantierte Schutzniveau wahren und die ihm nach der DS-GVO obliegenden Pflichten erfüllen.[63] Um dieses Schutzniveau bei der Zusammenarbeit mit einem Auftragsverarbeiter zu garantieren, sieht Art. 28 DS-GVO als Regelfall den Abschluss

---

„Microsoft-Onlinedienste“ – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, Seite 1 f.

61 EuGH, Urt. vom 30. März 2023, C-34/21, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0034, Rn. 69; Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 5 Rn. 15.

62 EuGH, Urt. vom 14. Dezember 2023, C-340/21, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0340&qid=1762427729099, Rn. 48 ff.

63 Gabel/Lutz in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Auflage 2022, Art. 28 Rn. 2 DS-GVO.

eines Auftragsverarbeitungsvertrags vor, der den in Art. 28 Abs. 3 DS-GVO näher beschriebenen Anforderungen entsprechen muss.[64]

Soweit die Verarbeitung personenbezogener Daten aufgrund eines Auftragsverarbeitungsvertrags erfolgt (Art. 28 Abs. 3 UAbs. 1 Satz 1 1. HS DS-GVO), legt Art. 28 Abs. 3 Satz 2 DS-GVO die Mindestanforderungen an den Auftragsverarbeitungsvertrag fest. Der Auftragsverarbeitungsvertrag sieht nach Art. 28 Abs. 3 UAbs. 1 Satz 2 DS-GVO insbesondere vor, dass[65]

- der Auftragsverarbeiter personenbezogene Daten nur **auf dokumentierte Weisung** des Verantwortlichen verarbeiten darf, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet ist,
- der Auftragsverarbeitungsvertrag korrespondierende **Vertraulichkeits- und Verschwiegenheitsverpflichtungen** enthält, sofern die zur Verarbeitung der personenbezogenen Daten befugten Personen nicht ohnehin einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- **geeignete technische und organisatorische Maßnahmen nach Art. 32 DS-GVO** zu ergreifen sind, um die Sicherheit der Daten zu gewährleisten,
- die Bedingungen zum Einsatz weiterer **Unterauftragnehmer** eingehalten sind,
- der Auftragsverarbeiter den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der **Rechte der betroffenen Person** nachzukommen und die Einhaltung der Datenschutzvorschriften sicherzustellen,
- der Auftragsverarbeiter den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den **Art. 32 bis 36 DS-GVO genannten Pflichten** unterstützt,
- der Auftragsverarbeiter alle personenbezogenen Daten entweder **löschen** oder an den Verantwortlichen **zurückgeben** muss, sobald die Auftragsverarbeitung

[64] Siehe auch ErwG 81 Satz 1 und 4 DS-GVO.

[65] Siehe hierzu im Einzelnen etwa Petri in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, Art. 28 Rn. 57 ff.; Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 38 ff.; Hartung in Kühling/Buchner, 4. Aufl. 2024, DS-GVO Art. 28 Rn. 31 ff.; Spoerr in BeckOK DatenschutzR, 53. Ed. 1. August 2025, DS-GVO Art. 28 Rn. 50 ff.

beendet ist, sofern nicht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

- dem Verantwortlichen alle erforderlichen Informationen zum **Nachweis der Einhaltung** der in diesem Artikel niedergelegten Pflichten zur Verfügung gestellt werden und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beitragen wird.

Bei der Prüfung der nach Art. 28 Abs. 3 DS-GVO zu schließenden Auftragsverarbeitungsverträge ist somit besonders in den Blick zu nehmen, ob der Verantwortliche hierauf aufbauend seinen nach der DS-GVO obliegenden Pflichten (z. B. der Pflicht zur transparenten Information nach Art. 12 ff. DS-GVO oder zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DS-GVO) nachkommen kann.[66]

Dies vorweggestellt gelangt der HBDI bezüglich der Kritikpunkte der DSK im Einzelnen zu folgender Rechtsauffassung:

[66] Es ist diskutabel, ob die Einordnung eines IT-Dienstleisters mit einer bedeutenden Markmacht als „weisungsgebundener Auftragsverarbeiter“ im Sinne von Art. 28 DS-GVO des Verantwortlichen sachgerecht ist. Hier wäre es aber Aufgabe des Gesetzgebers, entsprechend tätig zu werden.

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

Nach Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO erfolgt die Verarbeitung auf der Grundlage eines Vertrags, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem:

(1) Gegenstand und Dauer der Verarbeitung,
(2) Art und Zweck der Verarbeitung,
(3) Art der personenbezogenen Daten,
(4) Kategorien betroffener Personen und die
(5) Pflichten und Rechte des Verantwortlichen

festgelegt sind.

Insbesondere die Wendung „*Beschreibung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen*“ findet sich in ähnlicher Weise auch in anderen Vorschriften der DS-GVO, die ihrerseits die insoweit bestehenden Pflichten des Verantwortlichen konkretisieren. So muss der Verantwortliche im Rahmen der Informationspflichten nach Art. 13 Abs. 1 Buchst. c DS-GVO dem Betroffenen „*die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung*“ und nach Art. 14 Abs. 1 Buchst. c und d DS-GVO zusätzlich „*die Kategorien personenbezogener Daten, die verarbeitet werden*“ mitteilen. Nach Art. 15 Abs. 1 Buchst. a und b DS-GVO sind vom Verantwortlichen „*die Verarbeitungszwecke*“ und „*die Kategorien personenbezogener Daten, die verarbeitet werden*“ zu beauskunften und nach Art. 30 Abs. 1 Satz 2 Buchst. b und c DS-GVO enthält das Verzeichnis von Verarbeitungstätigkeiten unter anderem die folgenden Angaben: „*die Zwecke der Verarbeitung*“ und „*eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten*“.

Soweit es die Informationspflichten der Art. 13 und 14 DS-GVO und das Auskunftsrecht des Art. 15 DS-GVO betrifft, ist mit Blick auf die Bereitstellung der Informationen der Transparenzmaßstab des Art. 12 Abs. 1 DS-GVO zu beachten: Alle in Art. 12 Abs. 1 DS-GVO genannten Informationen und Mitteilungen, die sich auf die Verarbeitung beziehen, müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitgestellt werden.

Wie zuvor dargestellt, muss der Verantwortliche, obwohl er seine Datenverarbeitung einem Auftragsverarbeiter anvertraut, weiterhin in der Lage sein, seinen Pflichten nach der DS-GVO gerecht zu werden. Er muss also nicht nur selbst ausreichend Kenntnisse und Informationen über die Verarbeitung haben, um die Anforderung des Art. 28 Abs. 1 und 3 DS-GVO zu erfüllen. Er muss darüber hinaus auch Betroffene oder auf Nachfrage auch die zuständige Aufsichtsbehörde hierüber informieren können.

Dieser Anforderung kann der Kunde als Verantwortlicher unter Einbeziehung der gemeinsam erarbeiteten Lösungsvorschläge und der aktuell von MS bereitgestellten Informationen gerecht werden.[67]

Produktauswahl durch den Kunden und Abschluss von Lizenzverträgen

Eingangs ist insofern zu berücksichtigen, dass der Verarbeitung personenbezogener Daten durch MS der Abschluss entsprechender Lizenzverträge zwischen MS und seinen Kunden vorausgeht, die den Gegenstand und die Dauer des Auftragsverarbeitungsvertrags näher konkretisieren können.[68] Durch die Auswahl der Produkte entscheidet der Kunde, welche Anwendungen in seinem Verantwortungsbereich zum Einsatz gelangen und welche Verarbeitungen personenbezogener Daten hieraus resultierend durch MS ermöglicht werden.

DPA und Interpretationshilfe

Das von MS verwendete DPA weist für Verantwortliche eine gewisse Komplexität auf, weil es weltweit zur Anwendung gelangt und in Aufbau und Struktur von einem „klassischen“ europäischen oder deutschen Auftragsverarbeitungsvertrag abweicht. MS hat auf Anregung des HBDI für seine Kunden daher eine „Interpretationshilfe zum DPA“ erstellt, die diesem Bericht als Anlage 1 beigefügt ist. Sie ermöglicht den Kunden bezogen auf die DS-GVO eine schnellere Orientierung und einen Abgleich des DPA mit den nach Art. 28 Abs. 3 DS-GVO notwendigen Inhalten eines Auftragsverarbeitungsvertrags. So können etwa Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen danach abgeglichen werden, an welcher Stelle des DPA sie geregelt werden. Dadurch wird mehr Klarheit und Transparenz

[67] MS weist darauf hin, dass nach seiner Auffassung auch bisher die Möglichkeit bestanden hat, die Anforderungen des Art. 28 DS-GVO zu erfüllen.

[68] Etwa MS Customer Agreement, Online Subscription Agreement, Product Terms, Service Level Agreement.

darüber geschaffen, an welcher Stelle des DPA sich Ausführungen zu den Vorgaben des Art. 28 Abs. 3 DS-GVO finden. Hierdurch können Interpretationsprobleme und Rechtsunsicherheiten bezüglich der Umsetzung der Anforderungen des Art. 28 Abs. 3 DS-GVO verringert werden. Zudem kann die Prüfung der Umsetzung der Anforderungen des Art. 28 Abs. 3 DS-GVO auf Seiten der (verantwortlichen) Kunden insgesamt effizienter und zielgerichteter erfolgen.

Taxonomie der Datenbegriffe des DPA

Im Rahmen der inhaltlichen Auseinandersetzung mit dem DPA stellte sich die Verwendung der verschiedenen Datenbegriffe im DPA als herausfordernd dar. Der HBDI hat daher – auf Grundlage des schriftlichen Austauschs sowie der mit MS geführten Gespräche und Rückmeldungen von MS – eine Taxonomie der im DPA verwendeten Datenbegriffe erarbeitet, die die im Geltungsbereich des DPA verarbeiteten personenbezogenen Daten in eine Hierarchie von Datenkategorien unterteilt (Anlage 3). Die im DPA, aber etwa auch im M365-Kit sowie in anderen Veröffentlichungen von MS verwendeten Datenbegriffe lassen sich hierdurch besser und eindeutiger verorten. Hierdurch wird die Transparenz und die Nachvollziehbarkeit der verarbeiteten Kategorien personenbezogener Daten und der stattfindenden Datenverarbeitungen verbessert. Für den (verantwortlichen) Kunden wird es dadurch leichter, seine Datenverarbeitungen verständlich und umfassend zu dokumentieren und damit nicht nur den Anforderungen nach Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO, sondern seinen DS-GVO-Pflichten insgesamt besser nachzukommen.

M365-Kit

Als Reaktion auf die von der DSK geäußerten Kritikpunkte hat MS – unabhängig von den Gesprächen zwischen MS und dem HBDI – in Abstimmung mit dem LDA Bayern und unter Einbindung des HBDI unter anderem das M365-Kit erstellt. Mit dem M365-Kit stellt MS seinen Kunden Beispiele für Verzeichnisse von Verarbeitungstätigkeiten der relevantesten cloudbasierten Abonnementdienste zur Verfügung. Das M365-Kit umfasst zudem Beispiele für Schwellwertanalysen, zu Ausführungen von Rechtsgrundlagen und für eine Datenschutzerklärung.

Diese Dokumente sind ebenso wie die Interpretationshilfe und die Taxonomie zwar nicht Gegenstand des DPA (als Auftragsverarbeitungsvertrag) im engeren Sinne. Zudem bedürfen sie seitens des Verantwortlichen einer eigenständigen

datenschutzrechtlichen Prüfung und Bewertung, da die Prüfung der datenschutzrechtlichen Zulässigkeit einer Verarbeitung personenbezogener Daten an Hand der konkreten Verarbeitungssituation erfolgen muss. Dies wird durch das konkrete Einsatzszenario eines M365-Produkts (mithin vom Kunden) bestimmt und nicht durch MS (als Auftragsverarbeiter).[69]

Die Dokumentationen leisten gleichwohl einen wichtigen Beitrag zur Verbesserung des Verständnisses der Datenverarbeitungen im M365-Umfeld und zur Umsetzung der Anforderungen des Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO. Auch sie ermöglichen den Kunden einen besseren Überblick über die Verarbeitungsvorgänge und erleichtern dem Verantwortlichen die Pflichterfüllung nach der DS-GVO.

Zur Verfügung stehende Dokumentationen zur Umsetzung der Anforderungen des Art. 28 Abs. 3 Satz 1 DS-GVO

Zur Umsetzung der Anforderungen des Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO stehen dem Verantwortlichen somit – neben diversen weiteren Informationen und Dokumentationen, die MS u. a. auf servicetrust.microsoft.com bereitstellt – die folgenden Informationen und Dokumentationen zur Verfügung:

(1) Die dem cloudbasierten Abonnementdienst zugrundeliegende **Lizenzvereinbarung zwischen MS und dem Kunden**, durch die festgelegt wird, welche Produkte vom Kunden überhaupt eingesetzt und somit in datenschutzrechtlicher Hinsicht dokumentiert und bewertet werden müssen.

(2) Das DPA, das die **vertraglichen Rahmenbedingungen der Verarbeitung personenbezogener Daten** aus einer globalen Perspektive, aber unter Berücksichtigung der Anforderungen der DS-GVO näher beschreibt.[70]

(3) Die **Interpretationshilfe zum DPA**, die es dem Verantwortlichen ermöglicht, das DPA mit den Voraussetzungen des Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DS-GVO abzugleichen.

---

[69] So macht es in der datenschutzrechtlichen Bewertung einen Unterschied, ob ein Kunde (Verantwortlicher) von MS (Auftragsverarbeiter) beispielsweise eine Schulung zu Compliance-Themen mittels MS Teams durchführt oder ob MS Teams zur Durchführung von Bewerbungs- oder Personalgesprächen genutzt werden soll. Die von MS als Auftragsverarbeiter bereitgestellte Anwendung MS Teams ist in beiden Fallkonstellationen identisch. Es ist aber Aufgabe des Kunden als Verantwortlicher zu prüfen und zu bewerten, ob beide Verarbeitungsverfahren unter Nutzung der Anwendung (des Betriebsmittels) „MS Teams“ durchgeführt werden können. MS kann und muss als Auftragsverarbeiter diejenigen Informationen zur Verfügung stellen, die zur Bewertung dieser Frage relevant sind. Die Bewertung und die Verantwortung hierfür verbleiben aber beim Kunden.

[70] Hier kommen ggf. auch noch die produktspezifischen Datenschutzbestimmungen hinzu.

(4) Die **Datentaxonomie**, die zu einem besseren Verständnis der im DPA verwendeten Datenbegriffe und Verarbeitungsvorgänge beiträgt.
(5) Das **M365-Kit**, das Beispiele für weitere datenschutzrechtliche Beschreibungen zu einzelnen, vom Kunden erworbenen Produkten enthält.

Unter Zugrundelegung der genannten Dokumente ist es für den Verantwortlichen möglich, den Gegenstand des Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 UAbs. 1 DS-GVO hinreichend konkret zu bestimmen und seinen weitergehenden Pflichten nach der DS-GVO (etwa Art. 13 ff. DS-GVO und Art. 30 DS-GVO) nachzukommen.

Abschließende Anmerkungen zur Orientierung

Hervorzuheben ist in diesem Zusammenhang, dass nach den Bestimmungen des DPA zwei Gruppen von Daten zur Erfüllung zweier verschiedener Zwecke verarbeitet werden:

(1) die Verarbeitung personenbezogener Daten zur **Bereitstellung** eines M365-Produkts und
(2) die Verarbeitung von pseudonymisierten, aggregierten (mithin für diesen Zweck anonymisierten) Daten zur Erfüllung eigener **Geschäftstätigkeiten**.[71]

Da M365-Produkte zur Erfüllung unterschiedlicher Verarbeitungstätigkeiten eingesetzt werden können, erfolgt die darüberhinausgehende Konkretisierung des Verarbeitungszwecks durch das vom Kunden gewählte Nutzungsszenario.

Die von der Verarbeitung betroffenen Personen werden ausschließlich vom (verantwortlichen) Kunden festgelegt. Er bestimmt, welchem Personenkreis die von ihm genutzten M365-Produkte zur Verfügung gestellt werden.

Gleiches gilt für die Festlegung der verarbeiteten Inhaltsdaten.[72]

Für Verantwortliche aus dem **öffentlichen Sektor** hat MS Anhang B im Rahmen des DPA-öS wie oben beschrieben[73] angepasst. Die Anpassung ist deswegen von großer Bedeutung, weil der Verantwortliche aus dem öffentlichen Bereich nach Art. 6 Abs. 1

[71] Weitere Ausführungen hierzu finden sich jeweils unter Punkt 2 Verantwortlichkeit (sowohl auf Sachverhaltsebene als auch bei den nachfolgenden rechtlichen Erwägungen).
[72] Als (wichtigste) Kategorie der Kundendaten werden Inhaltsdaten von MS zur Unterstützung der Aufgabenerfüllung gemäß der Beschreibung der jeweiligen Dienste verarbeitet. Kunden können MS im Rahmen von Professional Services den Zugriff auf Inhaltsdaten einräumen.
[73] Siehe Kap. F) I. 1).

UAbs. 1 Buchst. c und e DS-GVO Daten nur aufgrund einer Rechtsgrundlage nach Art. 6 Abs. 3 DS-GVO verarbeiten darf. Die zu verarbeitenden Daten, der zu verfolgende Zweck und die Verarbeitung der Daten werden somit durch eine Vorschrift des Unionsrechts oder des nationalen Rechts der Mitgliedstaaten festgelegt und begrenzt.[74] Er darf daher keine Datenverarbeitung beauftragen, die über die Festlegungen der jeweiligen Erlaubnisnorm hinausgehen. Daher muss er darauf achten, dass nur die Verarbeitungsschritte, Verarbeitungszwecke und die Verarbeitung solcher Daten erfolgen, die er selbst verfolgen und daher auch beauftragen darf.

Dies ist durch die Änderungen des Anhangs B im DPA-öS hinsichtlich der Kategorien betroffener Personen und personenbezogener Daten möglich.[75] Dadurch, dass der Anhang B keine spezifischen Inhaltsdaten mehr enthält, sondern die Bestimmung der Inhaltsdaten dem Verantwortlichen überlässt, vermeidet das DPA-öS, dass die Aufzählung einzelner Kategorien von Inhaltsdaten einerseits unvollständig ist und andererseits einzelne Datenkategorien aufführt, die die jeweilige Behörde als Kunde gar nicht verarbeiten darf. Welche Inhaltsdaten mit Hilfe des Betriebsmittels M365 verarbeitet werden, bestimmt allein die öffentliche Stelle. Sie kann damit einen Gleichklang zwischen den Einträgen im Verarbeitungsverzeichnis und der Nutzung von M365 herstellen. Ähnlich verfährt der Anhang B mit den Kategorien betroffener Personen und personenbezogener Daten, die von dem Verantwortlichen festgelegt werden, wenn er seine Aufgaben mit Hilfe des Betriebsmittels M365 erfüllt. Dadurch hat der Verantwortliche die Kategorien betroffener Personen und verarbeiteter personenbezogener Daten nach seinem VVT zu bestimmen, ohne in einen Widerspruch zum DPA-öS zu geraten.

Anhang B beschränkt sich daher auf die Kategorien betroffener Personen und personenbezogener Daten, die in M365 verarbeitet werden, um die gebuchten Dienste zu erbringen. Anhang B im DPA-öS wurde so verändert,[76] dass nicht mehr spezifische Kategorien betroffener Personen und personenbezogener Daten aufgeführt werden, sondern Sammelkategorien, um die erforderlichen Festlegungen zu Verarbeitungszwecken, Verarbeitungsschritten und zu verarbeitenden Daten zu

[74] Siehe z. B. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO-BDSG, 2. Aufl. 2025, DSGVO Art. 6 Abs. 3 Rn. 13 ff.
[75] Siehe Kap. F I 1).
[76] Siehe Kap. F I 1).

treffen. Durch den Anhang B und die weiteren Informationsmaterialien benennt MS dem Verantwortlichen auf einem gewissen Abstraktionsniveau diejenigen Kategorien personenbezogener Daten, die zur Dienstleistungserbringung erforderlich sind und hierzu verarbeitet werden. Diese Datenkategorien kann nur MS benennen.

Durch die Einfügung des Satzes „*Die in Anhang B beschriebenen Inhalte gehen im Fall des Widerspruchs diesem Abschnitt zu den ‚Verarbeitungsdetails' vor*" als letzter Satz zum Punkt „Verarbeitungsdetails" im DPA-öS wird die Rangfolge der Festlegungen geklärt.

2) Eigene Verantwortlichkeit Microsofts für „Geschäftstätigkeiten“

Im Folgenden wird geprüft, ob MS im Auftrag des Kunden oder im eigenen Interesse „von MS generierte, abgeleitete oder gesammelte Daten“ aggregieren und damit anonymisieren und danach für Geschäftstätigkeiten nutzen darf. Dabei wird unterstellt, dass die aggregierten und damit anonymisierten Daten – entsprechend den Angaben von MS – keinen Personenbezug aufweisen. Zu prüfen ist auch, ob MS personenbezogene „von MS generierte, abgeleitete oder gesammelte Daten“ auch ohne Auftrag des Kunden anonymisieren darf. Bei den Prüfungen wird zwischen Kunden aus dem öffentlichen Bereich und dem privaten Bereich unterschieden.

(a) Nutzung durch Aggregation anonymisierter Daten zur Verarbeitung eigener Geschäftstätigkeiten von MS

Zur Erzeugung anonymisierter R-Daten für eigene Geschäftstätigkeiten verarbeitet MS nach den zugrundeliegenden Sachverhaltsfeststellungen[77] sowie den Ausführungen in der Taxonomie ausschließlich „von MS generierte, abgeleitete oder gesammelte Daten“. Letztere werden zur Bereitstellung der M365-Produkte – nicht zur Verfolgung eigener Geschäftstätigkeiten – erhoben und pseudonymisiert. Anschließend werden die „von MS generierten, abgeleiteten oder gesammelten Daten“ in einem weiteren Verarbeitungsschritt zu R-Daten aggregiert.

Die folgende rechtliche Bewertung geht – wie auch das DPA – davon aus, dass die R-Daten nicht auf eine natürliche Person bezogen oder beziehbar sind. Sie sind daher im Sinne des ErwG 26 Satz 5 DS-GVO anonym. Ob diese Annahme ausnahmslos zutrifft, ist abhängig von einer tatsächlichen Überprüfung der Aggregation im Einzelfall.[78]

Da das Verfahren der anonymisierenden Aggregation – mithin der Entfernung des Personenbezugs – für sich genommen eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DS-GVO darstellt, ist dieser Verarbeitungsschritt an den Grundsätzen der Verarbeitung des Art. 5 Abs. 1 DS-GVO, insbesondere am Grundsatz

[77] Siehe Kap. F) I. 2).

[78] Für den Erfolg der Anonymisierung trägt der jeweils Verantwortliche die Verantwortung nach Art. 5 Abs. 2 DS-GVO. Sollte die Anonymisierung im Rahmen der Auftragsverarbeitung erfolgen, muss sich der verantwortliche Kunde von der Anonymität der R-Daten überzeugen. Er sollte sich dies von MS zusichern lassen.

der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 DS-GVO, zu prüfen und zu bewerten.[79]

(b) Rechtliche Zurechenbarkeit der Aggregation

Für die rechtliche Bewertung ist entscheidend, wem – d. h. MS (als Auftragsverarbeiter) oder seinem Kunden (als Verantwortlichem) – das Verfahren der anonymisierenden Aggregation als Datenverarbeitung i. S. d. Art. 4 Nr. 2 DS-GVO rechtlich zuzurechnen ist.

Je nachdem wie die Frage der Zurechenbarkeit beantwortet wird, sind unterschiedliche rechtliche Erlaubnistatbestände für diesen Datenverarbeitungsvorgang zu prüfen:

(1) Fällt die Anonymisierung in den Auftragsverarbeitungsvertrag und führt MS sie als Auftragsverarbeiter durch, bestimmt sich die Zulässigkeit der Datenverarbeitung nach den Regelungen, die für den Kunden als Verantwortlichen gelten.

(2) Fällt die Anonymisierung nicht in den Auftragsverarbeitungsvertrag, führt MS sie als Verantwortlicher durch und ihre Zulässigkeit bestimmt sich nach den Regeln, die für den Kunden und für MS als jeweils Verantwortlichen gelten.

Die Zuordnung der Geschäftstätigkeiten zum Datenverarbeitungsauftrag ist somit entscheidend für die Frage nach der rechtlichen Zurechenbarkeit. Diese Frage ist für öffentliche und für nicht-öffentliche Verantwortliche unterschiedlich zu beantworten.

(c) Verarbeitungserlaubnis für öffentliche Stellen

Für die Zuordnung der Geschäftstätigkeiten zum Auftragsverarbeitungsvertrag ist zu prüfen, ob im Fall einer öffentlichen Stelle (Behörde) diese als Verantwortlicher und Auftraggeber eine Datenverarbeitung für die genannten Zwecke durchführen dürfte.

Diese Zwecke sind in seltenen Fällen unmittelbar aus den gesetzlich explizit geregelten Aufgaben der Behörde abzuleiten. Für den Beschaffungsvorgang, M365-Produkte für die Erfüllung der Behördenaufgaben zu nutzen, ist zu berücksichtigen, dass jede Behörde die aus der gesetzlichen Aufgabenübertragung und dem Haushaltsrecht ableitbare übergeordnete Aufgabe hat, ihre Aufgaben mit den geeigneten Instrumenten möglichst effektiv und effizient zu erfüllen. Daher sind all die

[79] Roßnagel, Anonymisierung personenbezogener Daten und Nutzung anonymer Daten, DuD 2024, 513 ff.

Zwecke, die der Behörde eine effektive und effiziente Nutzung der erforderlichen modernen Informationstechnik ermöglichen, zulässiger Bestandteil eines Auftrags gegenüber einem Auftragnehmer.

Diese modale Zielsetzung der Aufgabenerfüllung ist hinsichtlich der Digitalisierung der Verwaltung vielen gesetzlichen Vorgaben zu entnehmen. Nach § 3 des Hessischen Gesetzes zur Förderung der elektronischen Verwaltung (Hessisches E-Government-Gesetz – HeGovG) sollen die hessischen Behörden in der Lage sein, mit Bürgerinnen und Bürgern und anderen Behörden elektronisch zu kommunizieren. Sie sollen nach § 5 HeGovG am elektronischen Zahlungsverkehr teilnehmen, nach § 6 HeGovG Nachweise elektronisch akzeptieren und nach §§ 7 und 8 HeGovG ihre Akten elektronisch führen. Ebenso übertragen die §§ 3a, 35a und 37 des Hessischen Verwaltungsverfahrensgesetzes (HVwVfG), das Onlinezugangsgesetz (OZG) und viele Fachgesetze den Behörden die Aufgaben der Digitalisierung ihrer Verwaltungstätigkeit.

Schließlich sind alle datenschutzrechtlichen Erlaubnisnormen ein Ausdruck dafür, dass die Verwaltung ihre fachlichen Aufgaben durch Datenverarbeitung erfüllen darf oder sogar erfüllen soll. Diese Aufgaben, die der hessische Gesetzgeber den Behörden des Landes auferlegt hat, sind nur zu erfüllen, wenn die Behörden über eine Plattform verfügen, die sie in die Lage versetzen, in der vorgesehenen Weise elektronisch zu handeln.

Das DPA-öS für Kunden aus dem öffentlichen Bereich[80] sieht im Abschnitt „Verarbeitung für Geschäftstätigkeiten“ Weisungen des Kunden gegenüber MS zur Aggregation von „von MS generierten, abgeleiteten oder gesammelten Daten“ für vier neu gefasste Zwecke vor.

Als Weisungen des Auftraggebers vorgesehene Geschäftstätigkeiten

Vor diesem Hintergrund sind die Zwecke der im DPA-öS als Weisungen des Auftraggebers vorgesehenen Geschäftstätigkeiten als zulässige oder unzulässige Bestandteile des Auftragsverarbeitungsvertrags einzuordnen:

- Der Zweck „korrekte Abrechnung“ ist vom Auftragsverarbeitungsvertrag gedeckt. MS kann die Dienste von M365 nur bereitstellen, wenn sie den Auftrag

[80] Siehe Kap. F) I. 2) am Ende.

der Behörde in Abgrenzung zu anderen Kunden richtig zuordnen und die jeweils erbrachten Leistungen abrechnen kann.

- Der Zweck „kundenspezifisches Accountmanagement“ fällt ebenfalls in den Auftragsverarbeitungsvertrag, weil das Accountmanagement Teil der geschuldeten Leistung von MS ist. Dies ergibt sich insbesondere aus der Definition des „Accountmanagements“ im DPA-öS. Danach bedeutet „Accountmanagement“, „*dass Microsoft-Mitarbeiter (oder Partner, die den Kunden betreuen) informierte Interaktionen mit dem Kunden haben, um ihm zu helfen, nicht personenbezogene Nutzungsmuster zu bewerten, Ausgaben effektiver zu verwalten und zukünftige Ausgaben zu optimieren und dass dieses Personal von Microsoft entsprechend auf Basis von nutzungsbasierten Metriken vergütet wird, um den Kunden zu unterstützen, den Nutzen der erworbenen Onlinedienste auszuschöpfen*“. Soweit die Aktivitäten des Accountmanagements auf die Optimierung der Ausgaben der Behörde und ihre Unterstützung in der effektiven und effizienten Nutzung der M365-Produkte ausgerichtet ist, liegt dies im Interesse der Behörde. Indirekt nützt es ebenfalls der Behörde, wenn die Mitarbeiter oder Partner von MS finanzielle Anreize nach dem Maßstab dessen erhalten, wie gut sie die Behörde in diesen Managementaufgaben unterstützt haben. Daher kann auch das so verstandene Accountmanagement als Teil des Auftrags angesehen werden.

- Der Zweck „interne Berichterstattung und Geschäftsmodellierung wie etwa Prognose, Umsatz, Kapazitätsplanung und Produktstrategie, um die Bereitstellung und Wartung der Produkte und Services zu unterstützen“ lässt sich ebenfalls dem Auftragsverarbeitungsvertrag zuordnen. Soweit es um Geschäftsmodellierung[81] geht, fällt dies in den Auftrag, weil die öffentliche Stelle (Behörde) als Kunde sicherstellen will, dass sie mit den notwendigen Leistungen im gebotenen Umfang versorgt wird. Schwieriger ist es, die interne Berichterstattung und die allgemeine Produktstrategie von MS als Teil des Auftragsverarbeitungsvertrags, in der bestellten Form und dem bestellten Umfang, zuzurechnen. Da aber auch diese nach dem DPA den Zweck verfolgt, „die Bereitstellung und Wartung der Produkte und Services zu unterstützen“,

[81] Wie etwa den aus dem bisherigen Umsatz abgeleiteten Prognosen der zu erwartenden Nachfrage nach Leistungen und daraus abgeleitete Kapazitätsplanungen von MS für den jeweiligen Kunden.

kann letztlich auch diese Geschäftstätigkeit der Unterstützung des Kunden zugerechnet werden und unterfällt damit dem Auftragsverarbeitungsvertrag.

- Der Zweck der „rechtlich erforderlichen Finanzberichterstattung“ ist ebenfalls vom Auftragsverarbeitungsvertrag umfasst, wenn die öffentliche Stelle (Behörde) MS die Erfüllung rechtlich gebotener Berichte über oder in Bezug auf die erbrachten Leistungen für diese ermöglicht.

Im Ergebnis können damit alle Zwecke für Geschäftstätigkeiten von MS, die das DPA nennt, dem Auftragsverarbeitungsvertrag zugerechnet werden und sind daher von Art. 28 Abs. 1 DS-GVO gedeckt, sofern die öffentliche Stelle (Behörde) dafür eine datenschutzrechtliche Erlaubnis hat.

Erlaubnistatbestand der Behörde

Für die Anonymisierungen, die dem Auftragsverarbeitungsvertrag zugeordnet werden können, stellt sich die Frage, auf welchen Erlaubnistatbestand die Behörde diesen Datenverarbeitungsvorgang stützen kann.

Soweit aus den pseudonymisierten „von MS generierten, abgeleiteten oder gesammelten“ Daten auf einzelne Beschäftigte der Behörde geschlossen werden kann, ist die Anonymisierung an dem Tatbestand des § 23 Abs. 1 Satz 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) zu messen.[82] Danach ist die Verarbeitung von Beschäftigtendaten zulässig, soweit sie u.a. für die „Durchführung des Beschäftigungsverhältnisses“ erforderlich ist. Dabei sind die Interessen des Dienstherrn oder Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht der oder des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt. Zu beachten ist, dass im Rahmen dieser Vorschrift die Erforderlichkeit nicht im Sinne einer absoluten Notwendigkeit zu verstehen ist, sondern eine Verhältnismäßigkeitsprüfung fordert.[83] Auf Seiten des Arbeitgebers steht insoweit das Interesse des Einsatzes eines M365-Produkts als Instrument moderner Informationstechnik zur Erfüllung der arbeits- oder dienstrechtlichen Pflichten sowie der zuvor beschriebenen Zwecke. Auf der Seite der

[82] Siehe hierzu trotz EuGH, Urt. vom 30. März 2023, C-34/21, https://curia.europa.eu/juris/document/document.jsf?text=&docid=272066&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1: Roßnagel/Wetzstein/Horlbeck, Unionsrechtliche Vorgaben für das Recht des Beschäftigtendatenschutzes – Auswirkungen des EuGH-Urteils vom 30.3.2023, DuD 2023, 429 ff.

[83] Siehe z. B. Maier-Reinhardt in Roßnagel HDSIG, 2021, § 3 Rn. 22.

Beschäftigten steht das Interesse des Schutzes ihrer Persönlichkeitsrechte. Im Rahmen der Abwägung dieser Interessen ist die Frage zu stellen, ob der vom Arbeitgeber verfolgte Zweck mit dem Verarbeitungsverfahren erreicht werden kann, ob alternativ ein gleich geeignetes, wirksames Mittel zur Verfügung steht und ob insgesamt von einem angemessenen Ausgleich der widerstreitenden Interessen ausgegangen werden kann. Da die Anonymisierung das Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO umsetzt und das Risiko der folgenden Datenverarbeitung für die Beschäftigten ausschließt oder minimiert, kann hier eine Verhältnismäßigkeit der Datenverarbeitung durch den Dienstherrn bejaht werden.

Wenn die Behörde allgemein M365 für die Erfüllung ihrer Aufgaben nutzt, ist diese Nutzung daher auch für die Durchführung des Beschäftigungsverhältnisses erforderlich.

Soweit andere Personen als Beschäftigte betroffen sein sollten und für die Anonymisierung kein spezifischer Erlaubnistatbestand besteht, kommt nur die Generalklausel des § 3 HDSIG in Frage. Sie erlaubt die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle, „wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist“. Die Vorschrift ist von hoher Abstraktheit und geringer Bestimmtheit. Als einziger Schutz der Grundrechte fordert sie, dass die Verarbeitung personenbezogener Daten für diese Aufgaben oder Befugnisse erforderlich sein muss. Dies entspricht nicht den Anforderungen an eine bestimmte, klare und bereichsspezifische Regelung der Zulässigkeit einer solchen Datenverarbeitung, wie sie das BVerfG[84] und der EuGH[85] fordern. Sie kann daher allenfalls einfache Datenverarbeitungen mit sehr geringer Eingriffsintensität rechtfertigen.[86]

Die Anonymisierung entspricht dem Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO und reduziert das Risiko der folgenden Datenverarbeitung für die

---

84 Siehe z. B. BVerfGE 65, 1 (43 f.); 141, 220 (265); 133, 277 (336).

85 Siehe z. B. EuGH, Urt. vom 8. April 2014, Rs. C-293/12, https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1; EuGH, Urt. vom 21. Dezember 2016, C-203/15, https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.

86 Siehe z. B. Roßnagel in Roßnagel, HDSIG, 2021, § 3 Rn. 2; für die gleiche Generalklausel in § 3 Abs. 1 BDSG z. B. auch BT-Drs. 18/11325, 81; Petri in Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, § 3 BDSG Rn. 9; Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, § 3 BDSG Rn. 5.

betroffene Person. Insofern ist sie nicht mit einem tiefgehenden Grundrechtseingriff verbunden, sondern schließt ihn aus oder minimiert ihn beträchtlich. Die Anonymisierung ist somit eine einfache Datenverarbeitung mit geringer Eingriffsintensität, auf die § 3 Abs. 1 HDSIG anwendbar ist. Die Datenverarbeitung ist erforderlich, um M365-Produkte für die Aufgabenerfüllung der öffentlichen Stelle (Behörde) nutzen zu können. Sie erhöht ihre Effektivität und Effizienz. Insofern ist die Anonymisierung durch die öffentliche Stelle (Behörde) zu ihrer Aufgabenerfüllung erforderlich und nach § 3 Abs. 1 HDSIG zulässig.

Hilfsweise: Verarbeitungserlaubnis außerhalb des Auftragsverhältnisses

Lediglich hilfsweise wird untersucht, auf welche Erlaubnistatbestände die Anonymisierungen gestützt werden könnten, sofern sie entgegen des bisherigen Ergebnisses nicht dem Auftragsverarbeitungsvertrag zugeordnet werden könnten. Hierbei sind rechtlich zwei Vorgänge zu unterscheiden und zu bewerten.

Obwohl für „von MS generierte, abgeleitete und gesammelte Daten“ keine faktische Übertragung der Daten erfolgt, weil MS diese Daten selbst erzeugt und mithin über diese Daten ohne vorherigen Übertragungsvorgang verfügt,[87] ist zum einen zu beachten, dass die Verantwortlichkeit für diese Daten und die folgenden Datenverarbeitungsvorgänge (Aggregation) wechselt. Die „von MS generierten, abgeleiteten oder gesammelten Daten“ sind im Bereich des Auftragsverarbeitungsvertrags der öffentlichen Stelle (Behörde) unter ihrer datenschutzrechtlichen Verantwortung entstanden. Mit der Verarbeitung in Form der Aggregation zu Geschäftstätigkeiten von MS gibt sie diese Daten nun in den Verantwortungsbereich von MS.

Dieser Vorgang ist in der unvollständigen, nur beispielhaft zusammengestellten Auflistung von Verarbeitungsvorgängen in Art. 4 Nr. 2 DS-GVO[88] nicht enthalten. Dennoch ist der Wechsel der Verantwortung für personenbezogene Daten ein Datenverarbeitungsvorgang. Diesem Wechsel der Verantwortung kommt der Begriff der „Offenlegung“ in Art. 4 Nr. 2 DS-GVO am nächsten, der als Oberbegriff für Übermittlungen, Bereitstellungen und Verbreitung zu verstehen ist.[89] Zwar fehlt hier

[87] Diese Daten werden zum Zwecke der Bereitstellung der M365-Produkte erhoben.
[88] Siehe hierzu z. B. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, Art. 4 Nr. 2 Rn. 14.
[89] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, Art. 4 Nr. 2 Rn. 26; Herbst in Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 4 Nr. 2 Rn. 29.

das Zugänglichmachen von Daten, aber ebenso wie bei der Offenlegung eröffnet die Übertragung der Verantwortung dem Empfänger Handlungsmöglichkeiten bezogen auf die betroffenen Daten.[90]

Alle diese Formen der Datenverarbeitung sind dadurch gekennzeichnet, dass die Möglichkeit, über die Daten zu verfügen, auf einen anderen Verantwortlichen übergeht. Wenn die Daten bereits im Gewahrsam des neuen Verantwortlichen sind, so beschränkt sich dieser Datenverarbeitungsvorgang auf die Übertragung der Verantwortung ohne einen tatsächlichen Transfer von Daten. Jedenfalls ist der Vorgang der Verantwortungsübertragung ein rechtfertigungsbedürftiger Datenverarbeitungsvorgang, der unter die abstrakte Definition des Art. 4 Nr. 2 DS-GVO fällt. Er sollte sinnvollerweise als ungeschriebenes Beispiel für Datenverarbeitungsvorgänge ohne Besitzübertragung auch als „Verantwortungsübertragung“ bezeichnet werden.

Die Verantwortungsübertragung an MS kann nach § 22 Abs. 2 Satz 1 Nr. 2 HDSIG zulässig sein. Danach darf eine öffentliche Stelle einer nicht öffentlichen Stelle Daten übermitteln, wenn der Empfänger „ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat“. Diese Vorschrift könnte in unionsrechtlicher Auslegung statt einer Übermittlung auch eine Verantwortungsübertragung rechtfertigen. Die Vorschriften werden auf Art. 6 Abs. 4 DS-GVO gestützt. Danach kann ein Mitgliedstaat zweckändernde Verarbeitungsvorschriften erlassen, die den Zielen des Art. 23 DS-GVO dienen.

Für die Regelungen des § 22 Abs. 2 Nr. 2 HDSIG kommt jedoch nur Art. 23 Abs. 1 Buchst. i DS-GVO in Betracht. Die eng auszulegende Ausnahme des Art. 23 Abs. 1 Buchst. i DS-GVO erlaubt allerdings nur eine Verarbeitung zum Schutz der Rechte und Freiheiten anderer Personen. Dies ist nicht identisch mit einer Verarbeitung zu berechtigten Interessen. Rein wirtschaftliche Interessen unterfallen nicht diesem Tatbestand.[91] § 22 Abs. 2 Nr. 2 HDSIG muss daher unionsrechtskonform

[90] Zur Vermeidung eines Missverständnisses, wird an dieser Stelle darauf hingewiesen, dass die „Offenlegung“ in diesem Zusammenhang lediglich die von „MS generierten, abgeleiteten und gesammelten Daten“ betrifft, nicht aber Inhaltsdaten als solche, weil diese für die Geschäftstätigkeiten von MS nicht verarbeitet werden.

[91] Siehe z. B. Dix in Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/BDSG, 2. Aufl. 2025, Art. 23 DSGVO Rn. 32.

einschränkend ausgelegt werden[92] und kann die Verantwortungsübertragung zur Durchführung von Geschäftstätigkeiten von MS nicht rechtfertigen.

Für diese Verantwortungsübertragung könnte jedoch Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Betracht kommen. Danach ist eine Datenverarbeitung zulässig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“.

Dieser Erlaubnistatbestand gilt jedoch nach Art. 6 Abs. 1 UAbs. 2 DS-GVO „nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung“. Diese Regelung knüpft an den Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO an und sichert den Gesetzesvorbehalt für das hoheitliche Handeln der Behörden.[93] Sie sollen im Rahmen der Eingriffs- und Leistungsverwaltung öffentliche Aufgaben nur dann erfüllen und öffentliche Gewalt nur dann ausüben können, wenn dies in den einschlägigen Gesetzen geregelt ist. Sie sollen diese Beschränkung nicht dadurch unterlaufen können, dass sie Datenverarbeitungen im Verhältnis Verwaltung-Bürger auf eine eigene Interessenabwägung stützen.[94] Umgekehrt bedeutet diese Regelung, dass sich Behörden auf die Interessenabwägung des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO stützen können, wenn sie durch ihre Datenverarbeitung keine öffentlichen Aufgaben erfüllen und keine hoheitlichen Befugnisse wahrnehmen. Sie können sich auf diesen Erlaubnistatbestand berufen,[95] wenn sie als Subjekte des

---

92 Siehe z. B. Richter in Roßnagel HDSIG, 2021, § 22 Rn. 14; für die gleiche Vorschrift in § 25 Abs. 2 Nr. 2 BDSG und z. B. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, § 25 BDSG Rn. 26.

93 EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 vom 8. Oktober 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf, Rn. 98.

94 Siehe ErwG 47 Satz 5 DSGVO; EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 vom 8. Oktober 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf, Rn. 99; außerdem z. B. Buchner/Petri in Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 6 Rn. 157; Schantz in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, 2. Aufl. 2025, Art. 6 Abs. 1 Rn. 97; Frenzel in Paal/Pauly, DSGVO/BDSG, 2. Aufl. 2021 Art. 6 Rn. 26; Schulz in Gola/Heckmann, DSGVO/BDSG, 3. Aufl. 2022, Art. 6 Rn. 60; Reimer in Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2022, Art. 6 Rn. 91.

95 EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 vom 8. Oktober 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf, Rn. 98 f., bietet leider keine positiven Beispiele.

Privatrechts auf dem Markt agieren,[96] insbesondere wenn die Datenverarbeitung zu Beschaffungszwecken erfolgt.[97]

Da die Behörde mit MS für die Bereitstellung von M365-Produkten einen privatrechtlichen Vertrag vereinbart hat, tritt sie in dem Beschaffungsvorgang als Privatrechtsubjekt auf. Sie überträgt nicht die Verantwortung für personenbezogene Daten aus dem Bürger-Verwaltung-Verhältnis, sondern allenfalls für personenbezogene Daten aus der Nutzung eines M365-Accounts zum Zweck der Anonymisierung. Für sie trifft demnach die Ausnahme des Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht zu.

Soweit also die Geschäftstätigkeit von MS nicht schon durch den Auftragsverarbeitungsvertrag gedeckt ist, darf die Behörde in dem privatrechtlichen Vertrag mit MS vereinbaren, dass MS „von ihr generierte, abgeleitete oder gesammelte Daten“ anonymisiert, wenn dies von der Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gedeckt ist. Dies ist in einem dreistufigen Vorgehen zu prüfen.[98]

Die betroffenen Geschäftstätigkeiten entsprechen berechtigten Interessen von MS. Diese Interessen Dritter darf auch die Behörde wahrnehmen. Die Auswertung der aggregierten Daten ist für die Zwecke von MS auch erforderlich. Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen in diesem Fall nicht, weil die Übertragung der Verantwortung auf MS nur erfolgt, um die Daten zu aggregieren und damit zu anonymisieren. Die Anonymisierung entspricht dem Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO und reduziert das Risiko der folgenden Datenverarbeitung für die betroffenen Personen. Da durch die Anonymisierung Grundrechtseingriffe ausgeschlossen oder beträchtlich minimiert werden, überwiegen die Schutzinteressen der betroffenen Personen nicht den berechtigten Interessen des Dritten (MS).

---

96 Schulz in Gola/Heckmann, DSGVO/BDSG, 3. Aufl. 2022, Art. 6 Rn. 60.
97 Siehe z. B. Reimer in Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2022, Rn. 91.
98 EuGH Urt. vom 9. Januar 2025, C-394/23, https://curia.europa.eu/juris/document/document.jsf?text=&docid=294110&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, Rn. 44 ff.; EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 vom 8. Oktober 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf, Rn. 12 ff.

Ergebnis zur Aggregation anonymisierter Daten

Im Ergebnis ist daher festzuhalten, dass die dem DPA entsprechende Datenverarbeitung zu Geschäftstätigkeiten von MS im Rahmen des Auftragsverarbeitungsvertrags erfolgt und insoweit der verantwortlichen öffentlichen Stelle (Behörde) zuzurechnen ist. Diese kann die Aggregierung und Anonymisierung „von MS generierten, abgeleiteten und gesammelten Daten“ auf § 23 Abs. 1 oder § 3 Abs. 1 HDSIG stützen.

Soweit diese Datenverarbeitung im Einzelfall nicht im Rahmen des Auftragsverarbeitungsvertrags erfolgen sollte, überträgt die Behörde die Verantwortung für die Anonymisierung der Daten für diese Zwecke auf MS. Sowohl diese Verantwortungsübertragung durch die Behörde als auch die Anonymisierung der Daten durch MS können auf die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden.

(d) Verarbeitungserlaubnis für nicht-öffentliche Stellen

Die Ausführungen lassen sich auf nicht-öffentliche Stellen, die Datenverarbeitungen zu Geschäftstätigkeiten von MS gestatten, entsprechend übertragen.

Für nicht-öffentliche Stellen gilt das DPA, das ebenfalls vier Kategorien von Geschäftstätigkeiten von MS nennt, diese aber in den einzelnen Formulierungen etwas weiter fasst. Nicht-öffentliche Stellen können jedoch ihre Verarbeitungszwecke freier auswählen und ihre Datenverarbeitung offener gestalten als öffentliche Stellen. Daher können sie auch leichter Verarbeitungsschritte, die von MS vorgenommen werden, als Teil ihrer eigenen Geschäftstätigkeiten und als Vorteil für die Weiterentwicklung ihrer IT-Konzepte ansehen. Sie können daher eher als Teil des Auftragsverarbeitungsvertrags angesehen werden.

Losgelöst von der Frage, ob die insoweit stattfindenden Verarbeitungen dem Auftragsverarbeitungsvertrag zuzurechnen sind oder nicht, gelangt für die Anonymisierung durch den Verantwortlichen oder für die Übertragung der Verantwortung für die Anonymisierung an MS als Erlaubnistatbestand Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zur Anwendung. Für die Ausführungen zur Prüfung der Voraussetzungen von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO wird auf das zuvor gefundene Untersuchungsergebnis verwiesen.

(e) Verarbeitungserlaubnis für MS

Führt MS die Verarbeitung als Verantwortlicher durch, kann diese Datenverarbeitung ebenfalls auf die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden. Insofern gelten die angestellten Überlegungen in vergleichbarer Weise.

3) Weisungsbindung und Offenlegung

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO und Art. 29 DS-GVO darf ein Auftragsverarbeiter personenbezogene Daten – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland – nur auf dokumentierte Weisung des Verantwortlichen verarbeiten (siehe sogleich zur Ausnahme). Das Weisungsrecht des Verantwortlichen ist Wesensmerkmal der Auftragsverarbeitung.[99]

Der Auftragsverarbeiter darf sich nicht eigenmächtig über die Weisung des Verantwortlichen hinwegsetzen, andernfalls haftet er für etwaige Schäden nach Art. 82 Abs. 2 Satz 2 DS-GVO.[100] Eine Ausnahme vom Prinzip der weisungsgebundenen Verarbeitung liegt vor, wenn der Auftragsverarbeiter durch das Recht der Union oder das Recht des Mitgliedstaates, dem er unterliegt, zur Verarbeitung verpflichtet ist.[101] Er verarbeitet in diesem Fall, ohne dass er eine Weisung für die Verarbeitung benötigt.[102] Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO verpflichtet den Auftragsverarbeiter jedoch, dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mitzuteilen.

Aus dem DPA[103] ergibt sich, dass MS nur nach den dokumentierten Weisungen des Kunden handelt. Für Datenverarbeitungen im Anwendungsbereich der DS-GVO verpflichtet sich MS im Anhang C des DPA zudem zu zusätzlichen Schutzmaßnahmen. Beispielhaft zu nennen sind hier die „Anfechtung von Anordnungen“ zur Offenlegung personenbezogener Daten und „Änderungsmitteilungen“ über die Änderung von Rechtsvorschriften, die Auswirkungen auf die in Anlage C oder in den Standardvertragsklauseln vorgesehenen Zusicherungen und Verpflichtungen haben.

Mit der Erklärung, dass MS nur nach den dokumentierten Weisungen des Kunden handelt, unterwirft sich MS im Rahmen der vereinbarten Auftragsverarbeitung der Weisungsherrschaft des Verantwortlichen.

---

[99] Bertermann/Peintinger in Ehmann/Selmayr, 3. Aufl. 2024, DS-GVO Art. 28 Rn. 24.
[100] Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 40.
[101] Siehe auch insoweit Fn. 34.
[102] Spoerr in BeckOK DatenschutzR, 53. Ed. 1. August 2025, DS-GVO Art. 28 Rn. 60.
[103] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO – Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten, Seite 13.

Aus dem DPA[104] ergibt sich weiterhin, dass MS personenbezogene Daten grundsätzlich nicht offenlegt oder zugänglich macht. Ausnahmen liegen jedoch vor, wenn (1) ein Kunde die Offenlegung anweist, (2) das DPA die Offenlegung erlaubt oder (3) die Offenlegung gesetzlich vorgeschrieben ist.[105]

Im Fall (1) erfolgt die Offenlegung durch MS aufgrund einer Einzelfallweisung des Kunden. Da die Offenlegung in diesem Fall ein Handeln im Rahmen der Auftragsverarbeitung ist, bestehen keine datenschutzrechtlichen Bedenken, wenn die Weisung des Verantwortlichen zur Offenlegung rechtmäßig ist.

Im Fall (2) ist die Offenlegung von Daten aufgrund des Auftragsverarbeitungsvertrags erlaubt. Hierunter sind Fälle zu verstehen, in denen die Offenlegung zur Erfüllung des Auftragsverarbeitungsvertrags notwendig ist. In Betracht kommt insoweit z. B. die Offenlegung von Daten zur Bereitstellung der M365-Produkte und im Rahmen der Tätigkeiten eines Unterauftragsverarbeiters. Da Offenlegungen ausschließlich im Rahmen des Auftragsverarbeitungsvertrags erfolgen, begegnet die Offenlegung i. S. v. (2) ebenfalls keinen datenschutzrechtlichen Bedenken.

Fall (3) erlaubt die Offenlegung von Daten, „wie gesetzlich vorgeschrieben“.[106] Anlage 1 des DPA nimmt insoweit noch einmal ausdrücklich Bezug auf „das Recht der Union oder des Mitgliedstaats, dem Microsoft unterliegt“ und stellt insoweit klar, dass gesetzliche Offenlegungen von Daten nur nach den Bestimmungen des Unionsrechts oder des Rechts eines Mitgliedstaates zulässig sind.[107]

Soweit außereuropäisches Recht MS zur Offenlegung verpflichten sollte, sichert MS zu, rechtlich gegen US-amerikanische Anordnungen vorzugehen, soweit diese MS dazu verpflichten sollten, Daten bereitzustellen oder zu übermitteln.[108] MS hat jedoch

---

[104] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse – Offenlegung verarbeiteter Daten, Seite 11.

[105] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse – Offenlegung verarbeiteter Daten, Seite 11.

[106] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Art der Datenverarbeitung; Eigentumsverhältnisse – Offenlegung verarbeiteter Daten, Seite 11.

[107] Siehe auch insoweit Fn. 34.

[108] MS hat sich öffentlich verpflichtet, jede behördliche Anforderung nach Daten von Kunden in der EU anzufechten, sofern eine rechtliche Grundlage zur Anfechtung besteht. Auch gegenüber dem HBDI

auch eingeräumt, dass eine Offenlegung auf Anordnung der US-Regierung ohne ausdrückliche Zustimmung des Verantwortlichen für die Zukunft nicht vollständig ausgeschlossen werden kann.[109]

MS hat aber Maßnahmen eingeführt, die die Verarbeitung personenbezogener Daten europäischer Kunden innerhalb des europäischen Raums ermöglichen[110] und insoweit zusätzliche Sicherheits- und Verschlüsselungsoptionen zur Verfügung gestellt.[111]

Zusammengefasst kann daher festgestellt werden, dass der Anforderung des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO entsprochen werden kann.

Gegenüber Verantwortlichen aus dem öffentlichen Sektor in Hessen verpflichtet sich MS zudem im DPA-öS ausdrücklich, Handlungen zu unterlassen, die gegen die Pflichten aus dem Auftragsverarbeitungsvertrag und der DS-GVO verstoßen.

hat MS seine Bereitschaft erklärt, rechtlich gegen Datenanforderungen aus den USA vorzugehen: https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/.

[109] Comptes rendus de la ce commande publique, Anhörung von Herrn Anton Carniaux, Direktor für öffentliche und rechtliche Angelegenheiten, und Herrn Pierre Lagarde, Technischer Direktor für den öf-fentlichen Sektor, von Microsoft France vom 9. Juni 2025, https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html#toc2.

[110] Zum „EU data boundary project“: Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency - Microsoft On the Issues, https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/.

[111] Zu den Sicherheitszusagen von MS: Microsoft announces new European digital commitments - Microsoft On the Issues, https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/; zum Umgang mit außereuropäischen Anfragen: CE Commande publique : compte rendu de la semaine du 9 juin 2025, https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html.

4) Umsetzung technischer und organisatorischer Maßnahmen

Nach Art. 28 Abs. 3 UAbs. 1 Buchst. c und f DS-GVO muss der Auftragsverarbeiter alle gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreifen und unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten unterstützen. Für die Beurteilung der Sicherheit der Verarbeitung ist nach Art. 32 Abs. 1 DS-GVO unter anderem der „Stand der Technik“ zu berücksichtigen.

Im Anhang A zum DPA erklärt MS die Einhaltung „branchenüblicher Standards“ und spricht vom „Verfahren nach Branchenstandard“. In Anlage 1 verpflichtet sich MS zur Einhaltung des Art. 32 DS-GVO („Stand der Technik“). Wie unter D) „Allgemeine Hinweise zum Datenschutznachtrag für Produkte und Services von Microsoft“ (DPA) dargestellt, ist Anlage 1 lex specialis gegenüber den allgemeinen Regelungen im DPA und seinen Anhängen. Dieses Verständnis hat MS zudem in den Gesprächen mit dem HBDI ausdrücklich bestätigt, sodass insoweit die vertragliche Anforderung des Art. 28 Abs. 3 UAbs. 1 Buchst. c und f DS-GVO durch das DPA erfüllt ist.[112]

[112] Hiervon losgelöst müssen Verantwortliche eine inhaltliche Prüfung der technischen und organisatorischen Maßnahmen vornehmen.

5) Löschung und Rückgabe personenbezogener Daten

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. g DS-GVO muss der Auftragnehmer die Daten nach Ende des Auftrags löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Nach den Bestimmungen des DPA werden Inhaltsdaten[113] 90 Tage nach Ablauf oder Beendigung des Abonnements des Kunden in einem eingeschränkten Funktionskonto aufbewahrt, damit der Kunde die Daten extrahieren kann. Nach Ablauf der 90-tägigen Aufbewahrungsfrist deaktiviert MS das Konto des Kunden und löscht die in den Onlinediensten gespeicherten Kundendaten und personenbezogenen Daten innerhalb weiterer 90 Tage, soweit MS nicht zur Aufbewahrung autorisiert ist. Während der Laufzeit des Abonnements haben Kunden zudem jederzeit die Möglichkeit, auf die gespeicherten Daten zuzugreifen, diese zu extrahieren und zu löschen.[114]

Hinsichtlich der übrigen gespeicherten Kundendaten haben Kunden ebenfalls in Abhängigkeit von den jeweiligen Datenkategorien unterschiedliche Möglichkeiten zur Löschung. So werden Bestandsdaten zu einzelnen Nutzenden spätestens zusammen mit dem zugehörigen Nutzendenaccount gelöscht. Letzteres kann vom Kunden manuell durchgeführt werden. Die Löschung von Audit-Logs kann ebenfalls durch den Kunden erfolgen. Auch die manuelle Löschung von lokalen Diagnosedaten kann vom Kunden durchgeführt werden, da die Daten dieser Kategorie auf lokalen Systemen des Kunden gespeichert sind.

Für von MS generierte, abgeleitete und gesammelte Daten wurde von MS eine maximale Speicherdauer von 18 Monaten angegeben. Eine frühere Löschung erfolgt, falls die jeweiligen Daten nicht mehr benötigt werden. Näheres hierzu wurde nicht ausgeführt. Für Kunden besteht jedoch die Möglichkeit einen Löschantrag zu stellen, welcher binnen 180 Tagen umgesetzt wird.

Die Löschung von Professional Services-Daten erfolgt, sobald der Zweck ihrer Erhebung erreicht wurde. Zusätzlich haben Kunden die Möglichkeit, die Löschung von Professional Services-Daten zu veranlassen.

---

[113] Vgl. hierzu Anlage 3: Taxonomie zum Datenschutznachtrag für Produkte und Services von MS.
[114] Eine ausführliche Darstellung des Löschverfahrens findet sich in der Sachverhaltsdarstellung in Kap. F) I. 5).

Losgelöst vom Ende der Vertragsbeziehung zwischen MS und seinem Kunden muss es dem Kunden als Verantwortlichen möglich sein, seinen Löschverpflichtungen nach Art. 17 DS-GVO jederzeit nachkommen zu können. Dies umfasst beispielsweise auch die Pflicht, personenbezogene Daten aufgrund der Wahrnehmung von Betroffenenrechten oder aufgrund einer behördlichen Maßnahme nach Art. 58 Abs. 2 Buchst. g DS-GVO zu löschen.

Aufgrund der Ausführungen und Zusicherung von MS ist davon auszugehen, dass die vertragliche Anforderung des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. g DS-GVO erfüllt werden können, da der Kunde – losgelöst von den vertraglich festgelegten Löschläufen – jederzeit auch die Möglichkeit hat, sämtliche personenbezogenen Daten seines Verantwortungsbereichs zu löschen bzw. eine Löschung zu veranlassen.

6) Unterauftragsverarbeiter

Nach Art. 28 Abs. 2, Abs. 4 und Abs. 3 UAbs. 1 Satz 2 Buchst. d DS-GVO muss der Auftragnehmer den Auftraggeber vor der Inanspruchnahme von Unterauftragnehmern über diese informieren und die Genehmigung des Auftraggebers einholen. Dies kann auch in Form einer allgemeinen schriftlichen Genehmigung erfolgen.[115] In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen nach Art. 28 Abs. 2 Satz 2 DS-GVO über jede beabsichtigte Änderung, andere Unterauftragsverarbeiter hinzuzuziehen oder Unterauftragsverarbeiter zu ersetzen, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.[116]

In der Praxis wird das Recht zum Einspruch bei standardisierten Produkten und Dienstleistungen, die für eine große Masse an Kunden bereitgestellt werden, häufig auf erhebliche oder zwingende sachliche Gründe beschränkt. Als Ausgleich für diese Einschränkung wird dann ein Sonderkündigungsrecht für den Fall des Einspruchs vorgesehen.[117]

Für jeden Unterauftragsverarbeiter werden detaillierte Informationen bereitgestellt, einschließlich Geschäftsadresse, DnB-Nummer und Mutterkonzern. Außerdem wird der Wechsel oder das Hinzutreten eines Unterauftragsverarbeiters durch ein Update der MS Online Services-Unterauftragsverarbeiterliste bekannt gegeben.[118]

MS verpflichtet sich im DPA, die entsprechenden Informationen mit einer Vorlaufzeit von sechs Monaten bereitzustellen, wenn ein Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung von Kundendaten[119] steht. Für sonstige personenbezogene Daten beträgt die Vorlaufzeit 30 Tage.[120]

Sofern der Kunde der Verarbeitung seiner Daten durch einen neuen Unterauftragsverarbeiter nicht zustimmt, wird im DPA dem Kunden vertraglich das Recht eingeräumt, den betroffenen Onlinedienst jeweils ohne Strafe oder Kündigungsgebühr

---

[115] Petri in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO – BDSG, 2. Aufl. 2025, Art. 28 Rn. 44; Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 62.

[116] Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 61; Bertermann/Peintinger in Ehmann/Selmayr, 3. Aufl. 2024, DS-GVO Art. 28 Rn. 15.

[117] Bertermann/Peintinger in Ehmann/Selmayr, 3. Aufl. 2024, DS-GVO Art. 28 Rn. 15.

[118] Änderungen der Unterauftragsverarbeiter werden am Ende der Liste der Unterauftragsverarbeiter unter dem Punkt „Summary of Changes“ aufgeführt. Die Änderungen können auch über das Service Trust Portal eingesehen werden, https://servicetrust.microsoft.com/DocumentPage/8d295fc2-f7d9-4662-8301-99b077fc6b79.

[119] Vgl. zum Begriff der Kundendaten Anlage 3: Taxonomie zum Datenschutznachtrag für Produkte und Services von MS.

[120] Servicegenerierte, abgeleitete oder gesammelte Daten oder Professional Services Daten.

zu beenden oder das betroffene Softwareprodukt zu kündigen, indem er vor dem Ablauf der entsprechenden Benachrichtigungsfrist eine schriftliche Kündigung einreicht. Das ist datenschutzrechtlich zulässig, kann aber gerade bei komplexen IT-Leistungen faktisch ein erhebliches Risiko für den Auftraggeber darstellen, das der Verantwortliche mit Blick auf sein Nutzungsszenario bewerten muss. Andererseits ist zu berücksichtigen, dass eine andere Vorgehensweise nur schwer realisierbar sein dürfte.

Im DPA verpflichtet sich MS außerdem, beim Einsatz von Unterauftragsverarbeitern sicherzustellen, dass dasselbe Datenschutzniveau wie im DPA gewährleistet wird. Hierzu schließt MS einen schriftlichen Vertrag mit seinen Unterauftragsverarbeitern. In diesem hält MS zusätzlich fest, dass MS nach Art. 28 Abs. 4 Satz 2 DS-GVO weiterhin für die Einhaltung der Pflichten aus dem DPA verantwortlich ist.

Im Ergebnis sind die Anforderungen des Art. 28 Abs. 2, Abs. 4 und Abs. 3 Buchst. c DS-GVO erfüllt, auch wenn der Kunde die Informationen über neue Unterauftragsverarbeiter im Service-Portal von MS einsehen muss. Im Zusammenwirken von MS und dem Kunden können die Vorgaben der DS-GVO erreicht werden.

7) Drittlandübermittlungen

MS hat seine Datenverarbeitung so umorganisiert, dass sie im Rahmen der EU-Data Boundary fast vollständig in der Europäischen Union und im Europäischen Wirtschaftsraum erfolgt. Insbesondere für den rund um die Uhr verfügbaren Support[121] sind aber noch Datenübermittlungen in andere Länder außerhalb dieser Grenze erforderlich. Relevant sind vor allem Datenübermittlungen in die USA, aber es gibt auch Unterauftragnehmer in anderen Drittländern, einschließlich Ländern, für welche die Europäische Kommission das Vorliegen eines angemessenen Datenschutzniveaus nicht geprüft und festgestellt hat.

Gemäß Unterabschnitt „Datenübermittlungen“ des DPA beauftragt der Kunde MS, personenbezogene Daten in Länder zu übermitteln, in denen MS oder ihre Unterauftragsverarbeiter tätig sind. Außerdem speichert und verarbeitet MS gemäß Abschnitt „Speicherorte von Kundendaten“, Absatz 2, für die „EU-Datengrenzen-Onlinedienste“ Kundendaten und personenbezogene Daten innerhalb der Europäischen Union „wie in den Produktbestimmungen beschrieben“. Die EU-Data Boundary erstreckt sich jedoch nicht vollumfänglich auf den technischen Support, sodass es in diesen Fällen zu Datenübermittlungen in Drittländer ohne ein anerkanntes angemessenes Datenschutzniveau kommen kann.

Nach dem EuGH-Urteil zu Schrems II vom 16. Juli 2020 ist die Übermittlung personenbezogener Daten in Länder ohne ein angemessenes Datenschutzniveau grundsätzlich unzulässig.[122] Mögliche Instrumente zur Legitimation einer Drittstaatenübermittlung sind u. a.:

(1) Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 Abs. 3 DS-GVO, wenn ein Land außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums über ein anerkanntes angemessenes Datenschutzniveau verfügt.[123]

[121] Mithin eine Leistung aus dem Bereich der Professional Services.
[122] EuGH, Urt. vom 16. Juli 2020, C-311/18, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.
[123] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission.

(2) Standardvertragsklauseln nach Art. 46 Abs. 2 Buchst. c DS-GVO (Datenübermittlung aufgrund eines Vertrags).[124]

MS verfügt über beide Instrumente.

Für Datenübermittlungen in die USA hat die Europäische Kommission auf Grundlage von Art. 45 Abs. 3 DS-GVO einen Angemessenheitsbeschluss für Datenübermittlungen aus der EU an unter dem sog. EU-US **Data Privacy Framework (DPF)**[125] zertifizierte Datenempfänger in den USA erlassen. Mit seiner Entscheidung vom 3. September 2025 (Rs. T-553/23) wies der EuG die Nichtigkeitsklage gegen den Angemessenheitsbeschluss der Europäischen Kommission zum DPF ab und bestätigte damit die Gültigkeit des DPF. Daher sind auch Datenübermittlungen auf der Grundlage des DPF derzeit rechtmäßig.

Zusätzlich hat MS mit MS Corporation einen **Standardvertrag** gemäß Entscheidung 2021/914/EU Modul 3 für Datenübermittlungen in die USA abgeschlossen.

Nach Aussagen von MS betrifft die Frage der Datenübermittlungen in Drittstaaten aufgrund der Datenverarbeitung innerhalb der EU-Data Boundary und des Customer Lock Box-Prozesses für den Fall des technischen Supports nur einen äußerst geringen Teil von personenbezogenen Datenverarbeitungen.[126]

Für Datenübermittlungen an Unterauftragnehmer in Drittländer, für welche die Europäische Kommission das Vorliegen eines angemessenen Datenschutzniveaus nicht geprüft und festgestellt hat, verfügt MS über **Standarddatenschutzverträge** nach Art. 6 Abs. 2 Buchst. c DS-GVO.

In Einzelfällen kann die Datenübermittlung in einen unsicheren Drittstaat auch nach Art. 49 Abs. 1 DS-GVO gerechtfertigt werden.

---

[124] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-standarddatenschutzklauseln.

[125] Siehe auch Europäische Kommission, Fragen und Antworten: Datenschutzrahmen EU-USA, https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752; DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 4. September 2023, https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf.

[126] Siehe Kap. F) I. 7).

III. Handlungsempfehlungen für Verantwortliche

Die nachfolgenden Handlungsempfehlungen richten sich an verantwortliche öffentliche und nicht-öffentliche Stellen mit Sitz in Hessen, die M365-Produkte bereits nutzen oder zukünftig nutzen wollen. Sie sollen sie darin unterstützen, ihre datenschutzrechtlichen Verpflichtungen unter Berücksichtigung des DPA, den Zusicherungen von MS und den Kritikpunkten der DSK zu erfüllen. Sie beruhen auf den Feststellungen im Sachverhalt, auf den Klarstellungen und Zusicherungen von MS (nachfolgend in den grau hinterlegten Kästchen dargestellt) und auf den rechtlichen Erwägungen. Die Handlungsempfehlungen sollen den öffentlichen und nicht-öffentlichen Stellen in Hessen bezüglich des datenschutzkonformen Einsatzes von M365-Produkten mehr Rechts- und Handlungssicherheit bieten.

Unter der Voraussetzung, dass die nachfolgenden spezifischen Handlungsempfehlungen für M365 eingehalten werden und der Verantwortliche darüber hinaus seinen allgemein nach der DS-GVO obliegenden Pflichten nachkommt, ist ein datenschutzrechtskonformer Betrieb von M365-Produkten möglich.[127]

Als Hilfestellung und Orientierung für die allgemein zu erfüllenden Pflichten stellt der HBDI den als Anlage 4 beigefügten Fragebogen „Umsetzung datenschutzrechtlicher Anforderungen an Datenverarbeitungsverfahren“ zur Verfügung.

Hervorzuheben ist der Grundsatz der Integrität und Vertraulichkeit des Art. 5 Abs. 1 Buchst. f DS-GVO, der unter anderem durch die Vorschrift zum Datenschutz durch Systemgestaltung und durch datenschutzrechtliche Voreinstellungen des Art. 25 DS-GVO weitergehende Konkretisierung erfährt.[128] Art. 25 DS-GVO betont die Bedeutung der wirksamen Umsetzung des Datenschutzes durch Systemgestaltung in dem Zeitpunkt, in dem die Zwecke und Mittel der Verarbeitung festgelegt werden. Hierzu zählt die Auswahl der für die Verarbeitung von personenbezogenen Daten eingesetzten Anwendungen und Dienste und deren Konfiguration. Verantwortliche müssen daher vor dem Einsatz von Anwendungen und Diensten diese auf ihren datenschutzrechtskonformen Einsatz hin überprüfen. Hierzu gehört insbesondere auch die Betrachtung optionaler Teilfunktionalitäten und die Deaktivierung oder anderweitige Unterbindung der Nutzung, soweit kein datenschutzrechtskonformer

[127] Erforderlich ist insoweit, dass für den Einsatz jedes einzelnen Produkts geprüft wurde, dass die Voraussetzungen erfüllt sind.

[128] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, DSGVO – BDSG, 2. Aufl. 2025, Art. 5 Rn. 169.

Einsatz möglich ist. Hierzu gehört auch die individuelle Prüfung, welchen Schutzbedarf die vorgesehene Datenverarbeitung hat und ob für diesen die Maßnahmen für die Integrität und Vertraulichkeit der Datenverarbeitung ausreichend ist.

Die Produkte von M365 sind vielfältig. Das DPA reflektiert ca. 300 verschiedene Verarbeitungsleistungen. Allein die Menge der unterschiedlichen Produkte, der insoweit stattfindenden Verarbeitungen und der Einsatzszenarien stellt Verantwortliche vor besondere Herausforderungen. Hinzukommt die Verwendung der MS-eigenen Terminologie, der globale Charakter des DPA und die Problematik, dass der Vertrag versucht, sämtliche im Zusammenhang mit der Verarbeitung personenbezogener Daten stehenden Fragen für alle M365-Produkte global zu beantworten. In der Praxis ist davon auszugehen, dass von den Verantwortlichen nur ein deutlich geringerer Teil der von MS angebotenen M365 Cloud-Anwendungen und -Dienste genutzt wird oder genutzt werden soll. Da sich die datenschutzrechtlichen Pflichten des Verantwortlichen auf die Produkte von M365 begrenzen, die er zur Verarbeitung personenbezogener Daten einsetzt, sollte dieser vorab sorgfältig seinen Bedarf ermitteln. Dabei sollte evaluiert werden, welche M365-Produkte zur Erfüllung der unternehmerischen Aufgaben unbedingt benötigt werden und eine entsprechende Produktauswahl erfolgen. Sodann sollten die datenschutzrechtliche Prüfung und Bewertung ausgehend von den zum Einsatz kommenden Produkten und den insoweit zu berücksichtigenden Funktionalitäten und Datenverarbeitungen erfolgen. Hierdurch können die ohnehin erheblichen Aufwände auf das erforderliche Maß reduziert werden, da „nur“ die datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Nutzung von M365 betrachtet werden, die mit Blick auf das eingesetzte Verarbeitungsverfahren unter Einsatz eines M365-Produkts relevant sind.

- **Ergänzender Hinweis für den öffentlichen Bereich:**

MS bietet für öffentliche Stellen den Abschluss eines **DPA-öS** an, welches spezifische Fragestellungen der Verarbeitung personenbezogener Daten durch öffentliche Stellen berücksichtigt.

Der HBDI empfiehlt allen öffentlichen Stellen mit Sitz in Hessen vor der Nutzung von M365 Produkten den Abschluss des DPA-öS als datenschutzrechtliche Grundlage für den zwischen der öffentlichen Stelle als Verantwortliche und MS als Auftragsverarbeiter zu schließenden Auftragsverarbeitungsvertrag.

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

MS hat eine Interpretationshilfe zum DPA erstellt und dem HBDI Informationen bereitgestellt, auf deren Grundlage der HBDI die DPA-Kategorien mit Hilfe von Rückmeldungen durch MS in die Logik der Taxonomie (Anlage 3) überführt hat. Zudem stellt MS seinen Kunden das M365-Kit zur Verfügung.

*Für **öffentliche Stellen** hat sich MS zusätzlich bereit erklärt, im DPA für den öffentlichen Bereich kundenspezifische Anpassungen des Anhangs B des DPA, der eine Beschreibung der betroffenen Personen und Kategorien personenbezogener Daten enthält, vorzunehmen. Hierfür wird der Anhang B so abgeändert, wie dies in Kap. F) I. 1) beschrieben ist.*

Verantwortliche müssen nach Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO in der Lage sein, Art und Zweck der Verarbeitung und die Art der personenbezogenen Daten präzise zu bestimmen.

Auf Basis der zuvor getroffenen **Produktauswahl** sollte der Verantwortliche zunächst die **zur Bestimmung erforderlichen Informationen und Dokumente** zusammentragen. Hierbei handelt es sich insbesondere um:

(1) die zwischen dem Verantwortlichen und MS geschlossenen oder noch zu schließenden Verträge (IT-Verträge),
(2) das DPA oder das DPA-öS, die Interpretationshilfe (Anlage 1) sowie die produktspezifischen Erweiterungen zum DPA,[129]
(3) die dieser Handreichung beigefügte Taxonomie (Anlage 3) und
(4) das M365-Kit (Anlage 2).[130]

Werden der Beurteilung der Anforderungen des Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO die zuvor bezeichneten Verträge und Dokumentationen vollständig zugrunde gelegt, lassen sich die Unschärfen des DPA deutlich verringern. Die Regelungen des DPA werden insoweit durch die IT-Verträge und die ergänzend bereitgestellten Dokumentationen konkretisiert und dadurch die datenschutzrechtliche Prüfung ermöglicht, sodass der Verantwortliche hierauf aufbauend die seinerseits

[129] Produktspezifische Erweiterung waren nicht Gegenstand der Betrachtung des vorliegenden Berichts.
[130] In Anlage 2 finden sich ein Verweis und weitergehende Hinweise zum Abruf des M365-Kit.

vorzuhaltenden datenschutzrelevanten Dokumentationen erstellen und seinen Prüfpflichten leichter nachkommen kann.

Zu berücksichtigen ist in diesem Zusammenhang, dass der Einsatz eines M365-Produkts für sich genommen keine Verarbeitungstätigkeit im Sinne von Art. 30 DS-GVO darstellt. Es handelt sich vielmehr um ein **technisches Hilfs- oder Betriebsmittel**, mit dessen Unterstützung unterschiedliche Verarbeitungstätigkeiten durchgeführt werden können und mit dessen Einsatz zusätzlich **produktspezifische Datenverarbeitungen** zur Bereitstellung des Dienstes einhergehen.[131] Insofern empfiehlt es sich, eine Beschreibung des M365-Produkts als „technisches Hilfs- oder Betriebsmittel“ vorzuhalten und auf die Beschreibung des M365-Produkts im Verzeichnis der Verarbeitungstätigkeiten zu verweisen.[132]

Hervorzuheben sind zudem die folgenden Aspekte:

- Da es sich bei den von MS im Rahmen von M365 zur Verfügung gestellten Produkten um **Betriebsmittel** handelt, die im Rahmen verschiedener Verarbeitungsverfahren personenbezogener Daten zum Einsatz kommen, muss die datenschutzrechtliche Bewertung vom Verantwortlichen im Kontext des jeweiligen **Einsatzzwecks** erfolgen.

- Die Bestimmung des konkret verfolgten **Einsatzzwecks** liegt ausschließlich beim Verantwortlichen. Zudem werden die insoweit durch das Betriebsmittel verarbeiteten **personenbezogenen Daten** (Inhaltsdaten) und die von der Verarbeitung **betroffenen Personen**[133] ausschließlich vom Verantwortlichen bestimmt.

- Losgelöst vom konkreten Einsatzzweck und der Verarbeitung von Inhaltsdaten, fallen bei jeder Nutzung eines M365 Produkts als Betriebsmittel „**von MS generierte, abgeleitete oder gesammelte Daten**“ d. h. Diagnosedaten oder

---

[131] EuGH, Urt. vom 10. Juli 2018, C-25/17, https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, Rn. 55 ff.; VG Wiesbaden, Beschl. vom 15. Januar 2018, 22 K 4755/17.WI.PV, https://openjur.de/u/2260322.html; HBDI, 53. Tätigkeitsbericht zum Datenschutz, Kap. 14.1 Software und IT-Dienste als Beratungsgegenstand, Seite 193 ff.

[132] Gute Beispiele und Vorlagen zur Erstellung entsprechender Dokumentation finden sich auf der Webseite des Bayerischen Landesbeauftragten für den Datenschutz: https://www.datenschutz-bayern.de/dsfa/.

[133] Hierbei handelt es sich einerseits um die Nutzerinnen und Nutzer des Verantwortlichen (z. B. Beschäftigte, Kunden, Vertragspartner) und andererseits um diejenigen, deren Daten im Rahmen der Nutzung der Produkte verarbeitet werden.

systemgenerierte Protokolle (Log-Daten) an. Bezogen auf Diagnose-Daten muss der Verantwortliche durch eine entsprechende Konfiguration und ggf. ergänzende Maßnahmen sicherstellen, dass in seinen lokalen Umgebungen lediglich die tatsächlich erforderlichen Daten erhoben und nur in pseudonymisierter Form an MS übermittelt werden.

- MS sichert zu, dass M365-Produkte ausschließlich solche „von MS generierten, abgeleiteten oder gesammelten Daten“ erheben, die zur Bereitstellung der Dienste erforderlich sind.[134] Insbesondere finden keine Erhebungen personenbezogener Daten ausschließlich mit dem Ziel statt, Daten zur Erfüllung eigener Geschäftstätigkeiten zu verarbeiten. MS **aggregiert** aber die zur Bereitstellung der Dienste erforderlichen „von MS generierten, abgeleiteten oder gesammelten Daten“, um diese anschließend für **eigene Geschäftstätigkeiten** zu nutzen.

- Die Dokumentation ist für den Verantwortlichen insofern herausfordernd, als die Verarbeitung „von MS generierten, abgeleiteten oder gesammelten Daten“ systemimmanent ist und durch MS initiiert wird. Dieser Umstand entbindet den Verantwortlichen gleichwohl nicht von seinen Verpflichtungen nach der DS-GVO. An dieser Stelle setzt die **Taxonomie** an und hilft, verschiedene Datenverarbeitungen im Kontext der „von MS generierten, abgeleiteten oder gesammelten Daten“ voneinander zu unterscheiden. In Kombination mit dem M365-Kit und einer Produktkonfiguration seitens des Verantwortlichen, die dem Prinzip des **Datenschutzes durch Technikgestaltung** Rechnung trägt, kann eine hinreichende Konkretisierung erreicht werden.

- Eine **herausgehobene Stellung** nehmen **Inhaltsdaten** ein. Für Daten dieser Kategorie verhält sich MS inhaltsagnostisch. Dies bedeutet insbesondere, dass eine inhaltliche Kenntnisnahme durch MS nicht erfolgt. Gleichzeitig haben Nutzende die Möglichkeit, Kopien von Daten dieser Kategorie zu erstellen oder die Erstellung von Kopien zu veranlassen und MS solche Kopien im Kontext anderer Kategorien zur Verfügung zu stellen. Ein Beispiel hierfür ist die Bereitstellung von Kopien von Dateien inklusive der darin enthaltenen Inhaltsdaten und die Bereitstellung der im Rahmen der Inanspruchnahme von Professional Services zur Verfügung gestellten Daten. Auch kann im Kontext

[134] Siehe Kap. F) I. 2).

von Professional Services und im Rahmen des Customer Lock Box-Prozesses ein Zugriff auf Inhaltdaten eingeräumt werden. Kunden sollten ihre Mitarbeitenden über die Konsequenzen der Bereitstellung von Inhaltsdaten sensibilisieren und organisatorische Vorgaben für die Erstellung und Bereitstellung sowie die Einräumung von Zugriffen festlegen.

- Gleiches gilt für **Audit Log-Daten**. Bei deren Bereitstellung sind insbesondere Unterschiede zu Logdaten zu beachten, auch in Bezug auf deren Pseudonymisierung.

2) Eigene Verantwortlichkeit für „Geschäftstätigkeiten“

MS versichert, keine Daten ausschließlich zur Erfüllung eigener Geschäftstätigkeiten zu erheben. MS verwendet hierfür ausschließlich aggregierte Daten – die aus (zur Bereitstellung im Rahmen der Auftragsverarbeitung erforderlichen) pseudonymisierten „von MS generierten, abgeleiteten oder gesammelten Daten“ gewonnen werden.

MS versichert, dass die Aggregationspraktiken den Leitlinien der Artikel-29-Datenschutzgruppe von 2014 entsprechen und dass aus den aggregierten Daten keine Rückschlüsse auf die ursprünglich „von MS generierten, abgeleiteten oder gesammelten Daten“ bzw. Personen möglich sind und somit eine wirksame Anonymisierung durch Aggregation erfolgt.[135]

*Für **öffentliche Stellen** in Hessen hat MS im DPA-öS zusätzlich die Passage „Verarbeitung für Geschäftstätigkeiten“*[136] *wie oben zitiert neu gefasst.*[137]

Nach Art. 28 Abs. 1 DS-GVO muss der Verantwortliche sicherstellen, dass er nur mit Auftragsverarbeitern zusammenarbeitet, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Hieraus ergeben sich bezüglich der Aggregation „von MS generierter, abgeleiteter oder gesammelter Daten“ durch MS zur Erfüllung eigener Geschäftstätigkeiten die folgenden Handlungsempfehlungen an Verantwortliche:

- Verantwortliche sollten auf eine sorgfältige Konfiguration der Übermittlung von „von MS generierten, abgeleiteten oder gesammelten Daten“ (insbesondere von Diagnose-Daten) achten, d. h.:
    - Es sollte eine differenzierte Betrachtung und Bewertung zwischen der Verarbeitung von Diagnose-Daten als notwendiger Bestandteil der Auftragsverarbeitung und zum Zwecke der Aggregation unter

[135] Siehe Kap. F) I. 2).
[136] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Art der Datenverarbeitung – Eigentumsverhältnisse – Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind, Seite 10 f.
[137] Siehe Kap. F) I 2).

Berücksichtigung der Verarbeitungsgrundsätze (z. B. Datenminimierung) erfolgen.
    - Updates sollten daraufhin geprüft werden, ob und wie sie sich auf die vorhandene Konfiguration auswirken.

- Im Rahmen von Auditierungen sollte die Möglichkeit genutzt werden, Prüffragen zum Verfahren der Aggregation, Anonymisierung und Verarbeitung zu eigenen Geschäftstätigkeiten zu formulieren, z. B.:
    - durch Prüfung einer bestimmten Report-Art oder eines bestimmten Verfahrens zum Erstellen von Reports,
    - durch Prüffragen zu Verfahren der Pseudonymisierung und Aggregation,
    - durch Einsichtnahme in interne Richtlinien und Verfahrensdokumente.

- Folgt die Verarbeitung gestützt auf den Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO, sollten die Rechtsprechung des EuGH und die Leitlinien des EDSA berücksichtigt werden.[138]
    - Hiernach ist die Verarbeitung personenbezogener Daten zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten zulässig, wenn die folgenden drei Voraussetzungen kumulativ erfüllt sind:
        (1) Von dem für die Verarbeitung Verantwortlichen oder von einem Dritten muss ein berechtigtes Interesse wahrgenommen werden,
        (2) Die Verarbeitung der personenbezogenen Daten muss zur Verwirklichung des berechtigten Interesses erforderlich sein, und
        (3) Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person dürfen gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.

[138] EuGH, Urt. vom 9. Januar 2025, C-394/23, https://curia.europa.eu/juris/document/document.jsf?text=&docid=294110&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, Rn. 44 ff.; EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 vom 8. Oktober 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf, Rn. 12 ff.

- Zudem sind die Ausführungen des EuGH zur Bedeutung der Informationspflicht des Art. 13 Abs. 1 Buchst. d DS-GVO zu berücksichtigen.[139]

[139] EuGH, Urt. vom 9. Januar 2025, C-394/23, https://curia.europa.eu/juris/document/document.jsf?text=&docid=294110&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, Rn. 29 und Rn. 46 ff.

3) Weisungsbindung und Offenlegung

MS hat sich bereiterklärt, rechtlich gegen Verpflichtungen zur Offenlegung vorzugehen, soweit MS nach US-amerikanischem Recht dazu verpflichtet sein sollte, Daten an US-Behörden bereitzustellen oder zu übermitteln.

Für öffentliche Stellen hat MS im DPA-öS zusätzlich die Verwendung von Features als Dokumentation einer Weisung gestrichen.[140]

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO muss der Auftragsverarbeitungsvertrag vorsehen, dass der Auftragsverarbeiter personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Regelungen des DPA zur Offenlegung und Weisungsbindung erfüllen die nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO bestehenden Anforderungen an den Auftragsverarbeitungsvertrag. Zu berücksichtigen ist aber, dass MS kürzlich im Rahmen einer öffentlichen Anhörung eingeräumt hat, dass eine Offenlegung auf Anordnung der US-Regierung ohne ausdrückliche Zustimmung des Verantwortlichen für die Zukunft nicht vollständig ausgeschlossen werden kann, obgleich dies in der Vergangenheit noch nie vorgekommen sei.[141]

Verantwortliche sollten daher evaluieren:

- welche Kategorien personenbezogener Daten ggf. von einer Offenlegung betroffenen sein können, und
- welche technischen und organisatorischen Maßnahmen zur Mitigation dieser Risiken ergriffen werden können.

Zudem sollte der „Government Requests for Customer Data Report“ von MS regelmäßig gesichtet und auf signifikante Änderungen und Auffälligkeiten hin überprüft

[140] Siehe Kap. F) I. 3).

[141] Comptes rendus de la ce commande publique, Anhörung von Herrn Anton Carniaux, Direktor für öffentliche und rechtliche Angelegenheiten, und Herrn Pierre Lagarde, Technischer Direktor für den öffentlichen Sektor, von Microsoft France vom 9. Juni 2025, https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html#toc2.

werden.[142] MS veröffentlicht in diesem Bericht zweimal jährlich behördliche Anfragen, die an MS global herangetragen werden.

[142] Siehe https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data?activetab=pivot_1%3aprimaryr2&culture=en-us&country=us#tab-national-security-orders-report.

4) Umsetzung technischer und organisatorischer Maßnahmen

MS hat in Anhang 1 zugesagt, die Anforderungen des Art. 32 DS-GVO einzuhalten MS hat außerdem zugesagt, dass die Verwendung der Begriffe „branchenübliche Systeme“ oder „branchenübliche Prozesse“ kein im Verhältnis zu dem nach Art. 32 DS-GVO geforderten „Stand der Technik“ niedrigeres Schutzniveau impliziert.

MS hat sich verpflichtet, alle notwendigen Maßnahmen im Sinne des Art. 32 DS-GVO zu treffen und die Kunden insoweit bei der Einhaltung ihrer Rechenschaftspflicht zu unterstützen.[143]

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. c und e DS-GVO muss der Auftragsverarbeitungsvertrag vorsehen, dass der Auftragsverarbeiter nach Art. 32 DS-GVO unter Berücksichtigung des Stands der Technik die erforderlichen Maßnahmen ergreift und den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DS-GVO unterstützt.

In rechtlicher Hinsicht ist durch die Zusicherung von MS und die Regelungen im DPA klargestellt, dass MS den Maßstab des Art. 32 DS-GVO („Stand der Technik“) beachtet.

Unabhängig hiervon sollten Verantwortliche

- die von MS bereitgestellten Dokumente zu technischen und organisatorischen Maßnahmen regelmäßig sichten, überprüfen und verproben,[144]
- zusätzlich von MS vorgehaltene Zertifizierungen und Auditierungen regelmäßig evaluieren und überprüfen und[145]
- in angemessenen Fällen ergänzend eigene Auditierungen und technische Prüfungen durchführen.

[143] Siehe Kap. F) I. 4).

[144] Zu den von MS bereitgestellten Dokumenten: siehe MS Trust Center: https://www.microsoft.com/de-de/trust-center, IT-Sicherheit: https://www.microsoft.com/de-de/security und M365 Dokumentation: https://learn.microsoft.com/de-de/microsoft-365/security/?view=o365-worldwide; zu den rechtlichen Anforderungen siehe z. B. Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 43 ff.

[145] Zu den von MS bereitgestellten Dokumenten siehe Fn. 144. Für die Auditberichte zu ISO/IEC Standards siehe https://servicetrust.microsoft.com/viewpage/ISOIEC und SOC Standards siehe https://servicetrust.microsoft.com/viewpage/SOC; zu den rechtlichen Anforderungen siehe z. B. Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 32 Rn. 79 ff; Martini in Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 61 ff.

Verantwortliche sollten außerdem überprüfen, welche zusätzlichen technischen und organisatorischen Maßnahmen sie in ihrem Verantwortungsbereich basierend auf den von MS bereitgestellten Informationen ergreifen und implementieren müssen. Hierbei ist insbesondere sicherzustellen, dass die von MS umgesetzten und die vom Verantwortlichen ergriffenen Maßnahmen aufeinander abgestimmt sind und im Zusammenwirken das jeweils erforderliche Schutzniveau gewährleisten. Zudem sollte der Verantwortliche die technischen und organisatorischen Maßnahmen auch insoweit regelmäßig einer Überprüfung und Erprobung unterziehen.

5) Löschung und Rückgabe personenbezogener Daten

MS hat zugesichert, dass der Kunde alle im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten jederzeit nach Maßgabe des jeweils geltenden DPA löschen kann. Dies gilt auch nach Abschluss der Vertragsbeziehung.[146]

Verantwortliche sollten ein Löschkonzept für sämtliche Datenarten inkl. der Etablierung von Prozessen zur manuellen Löschung von Datenkategorien erstellen. Hierbei sind insbesondere auch „von MS generierte, abgeleitete und gesammelte Daten“ zu berücksichtigen. Das Löschkonzept sollte sich mit folgenden Fragestellungen und Themen befassen:

- Bewegen sich die standardisierten Löschprozesse von M365 im Rahmen der Vorgaben des Art. 17 DS-GVO und nationaler Aufbewahrungsfristen?
- Falls das nicht der Fall ist: Festlegung eigener Löschfristen sowie Dokumentation und Beschreibung der Konfiguration oder der manuellen Löschprozesse.
- Falls MS für eingesetzte Produkte und Dienste Löschverfahren zur automatisierten Löschung anbietet, sollten diese bei der Konzeption und Umsetzung der Löschkonzepte berücksichtigt und eingesetzt werden.
- Es sollte ein Prozess dokumentiert und beschrieben sein, aus dem sich ergibt, wie im Falle einer ad-hoc-Löschung (z. B. aufgrund eines Löschgesuchs oder aufgrund einer Beendigung des Auftragsverhältnisses) vorzugehen ist.
- Die vorgesehenen manuellen Löschprozesse sollten erprobt werden.

[146] Siehe Kap. F) I. 5); weitere Informationen zur Löschung finden MS-Kunden hier: https://learn.microsoft.com/de-de/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview.

6) Unterauftragsverarbeiter

Sofern ein Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung von Kundendaten steht, verpflichtet sich MS im DPA, die entsprechenden Informationen mit einer Vorlaufzeit von sechs Monaten bereitzustellen; für sonstige personenbezogene Daten beträgt die Vorlaufzeit 30 Tage.

MS hat erklärt, die Liste der Unterauftragsverarbeiter stets aktuell zu halten.

Außerdem hat MS zugesichert, durch Abschluss entsprechender Verträge sicherzustellen, dass beim Einsatz von Unterauftragsverarbeitern das Datenschutzniveau des DPA gewährleistet wird.

Verantwortliche müssen sicherstellen, dass der Einsatz von Unterauftragsverarbeitern durch MS fortlaufend überprüft werden kann. MS sieht entsprechende Prozesse vor, die eine solche Überprüfung ermöglichen.[147]

Verantwortliche müssen insofern sicherstellen, dass sie

- rechtzeitig über die geplante oder erfolgte Änderung eines Unterauftragsverarbeiters informiert werden, indem sie die von MS bereitgestellten Kommunikationskanäle kennen und nutzen, und
- bei Hinweisen auf eine Änderung zeitnah die vorgenommene Änderung sichten, damit sie gegebenenfalls ausreichend Zeit haben, angemessen zu reagieren.
- bei Hinweisen auf Datenschutzprobleme einen anderen (z. B. in einem Supportfall später einsetzbaren) Unterauftragsverarbeiter in Anspruch nehmen.

[147] Siehe Kap. F) I. 6).

7) Drittlandübermittlungen

MS ist zur Übermittlung von „HR and Non-HR Data“ nach dem EU-US Data Privacy Framework berechtigt und hat mit der MS Corporation zusätzlich einen Standardvertrag gemäß Entscheidung 2021/914/EU Modul 3 abgeschlossen.[148]

Verantwortliche müssen sicherstellen, dass sie die rechtlichen Voraussetzungen für Datenübermittlungen in Drittländer nach Kapitel V DS-GVO beachten. Hierzu gehört zunächst ein klares Verständnis darüber, (1) in welchen Fällen personenbezogene Daten in Drittländer übermittelt werden, (2) auf welcher Transferlegitimation (z. B. Angemessenheitsbeschluss, Standardvertragsklauseln) die Übermittlung beruht und (3) welche Verarbeitungen ausschließlich innerhalb der EU-Data Boundary stattfinden.

Zur Risikominimierung sind insbesondere folgende Maßnahmen umzusetzen:

- Regelmäßige Prüfung der Rechtsgrundlagen: Die jeweils herangezogenen Transferinstrumente sind in angemessenen Abständen auf ihre Gültigkeit und Wirksamkeit hin zu überprüfen.
- Monitoring rechtlicher Entwicklungen: Der Verantwortliche sollte sicherstellen, dass aktuelle rechtliche Entwicklungen (z. B. neue Rechtsprechung, Aufsichtsbehördenleitlinien oder Änderungen von Angemessenheitsbeschlüssen) fortlaufend beobachtet und in die Bewertung der Transfers einbezogen werden.
- Datenminimierung: Es ist zu prüfen, ob Datenübermittlungen in Drittländer auf das unbedingt erforderliche Maß reduziert oder risikominimiert sind, etwa durch Verlagerung der Verarbeitung in den EU-/EWR-Raum oder durch den Einsatz von Anonymisierung bzw. Pseudonymisierung.
- Im Rahmen des IT-Supports (Professional Services) können Übermittlungen personenbezogener Daten auf ein Minimum reduziert werden, indem (1) in der Beschreibung des Support-Falls weitestgehend auf die Mitteilung personenbezogener Daten verzichtet wird und (2) der IT-Support soweit möglich nur innerhalb der Europäischen Servicezeiten genutzt wird. Sofern (ausnahmsweise) ein Supportfall gegeben sein sollte, der zwingend eine Übermittlung personenbezogener Daten in ein Drittland erfordert, können

[148] Siehe Kap. F) I. 7).

insoweit zusätzlich zu den bereits genannten Transferinstrumenten die Voraussetzungen des Art. 49 DS-GVO vorliegen.

Auf diese Weise wird gewährleistet, dass Drittstaatentransfers den Anforderungen der DS-GVO entsprechen und rechtliche sowie tatsächliche Risiken für die betroffenen Personen und das Unternehmen minimiert werden.

8) Weitere Empfehlungen

Prüfung und Betrieb alternativer Produkte (Digitale Souveränität)

Bei der Auswahl und dem Betrieb von IT-Produkten sollten ganz allgemein immer auch Aspekte der digitalen Resilienz, der Fähigkeit zur Betriebskontinuität und der digitalen Souveränität beachtet werden. Daher sollten stets auch alternative, möglichst europäische und datenschutzfreundliche Lösungen Bestandteil einer nachhaltigen IT-Strategie sein. Ziel ist es einerseits, die Abhängigkeit von einzelnen Herstellern und Anbietern zu verringern und dadurch die digitale Souveränität des Verantwortlichen zu stärken. Außerdem gilt es – angesichts geopolitischer Entwicklungen und wirtschaftlicher Monopolbildungen – die Fähigkeiten von Drittstaatenakteuren, auf Deutschland und Europa politischen Druck auszuüben, zu minimieren.[149] Andererseits ist dafür zu sorgen, im Falle von IT-Sicherheitsvorfällen weiter handlungsfähig zu bleiben.

Es wird daher empfohlen, für die zum Einsatz kommenden IT-Produkte immer auch alternative Produkte zu evaluieren, zu dokumentieren und zu verproben.[150] Dies soll die digitale Handlungsfähigkeit des Verantwortlichen für den Fall sicherstellen, dass ein im Einsatz befindliches IT-Produkt aus rechtlichen oder tatsächlichen Gründen nicht genutzt werden kann.

Sicherstellung der Einbindung von Stakeholdern (DSB, Personalvertretung)

Bei der Einführung oder wesentlichen Änderung von IT-Produkten sind relevante Stakeholder wie z. B. der Datenschutzbeauftragte, die Personalvertretung und die IT-Sicherheit frühzeitig einzubinden. So kann gewährleistet werden, dass rechtliche, organisatorische und mitbestimmungsrechtliche Anforderungen von Beginn an berücksichtigt werden.

Sicherstellung eines definierten Prüfprozesses

Vor Einführung, Änderung oder Nutzung weiterer Produkte sollte ein vorab festgelegter Prüfprozess verpflichtend zu durchlaufen sein.

---

[149] MS weist in diesem Zusammenhang ausdrücklich auf den neuen Anhang D des DPA-öS hin, wonach sich MS gegenüber geschützten Behördenkunden zur Anfechtung von Anforderungen oder verbindlichen rechtlichen Verpflichtungen zur Aussetzung von Onlinediensten verpflichtet.

[150] Insoweit wird insbesondere auch auf die weiteren Entwicklungen rund um die Delos Cloud für den öffentlichen Dienst hingewiesen, https://www.deloscloud.de/.

Prozess der Überprüfung von Änderungen an Diensten

Es sollte ein kontinuierlicher Prozess vorgehalten werden, durch den sichergestellt wird, dass Änderungen an bestehenden Diensten (z. B. Updates, Funktionsänderungen, Anbieterwechsel) überwacht und geprüft werden können. Dabei sind Auswirkungen auf Datenschutz, Informationssicherheit und Compliance systematisch zu bewerten. Grundlegende Änderungen lösen zudem eine erneute Prüfung des betroffenen Dienstes aus.

G) Anlagen

Anlage 1:

Zuordnung der Anforderungen aus Art. 28 Abs. 3 DS-GVO zu Ausführungen im Microsoft DPA (Stand 09/2025)

Nr.	Gesetzliche Anforderung der Datenschutz-Grundverordnung (DS-GVO)	Fundstelle im DPA	Textpassage im Data Protection Addendum (Datenschutznachtrag zu den Produkten und Services von Microsoft, DPA, Stand 09/2025)
Allgemeiner Hinweis: *Das DPA definiert verschiedene Kategorien von Daten, wie unter anderem Kundendaten und Supportdaten. Die gesetzlichen Anforderungen der DS-GVO gelten gleichermaßen für beide. Zu diesen zwei Datenkategorien sind aber teilweise unterschiedliche Regelungen in dem DPA getroffen worden. Um die Kategorien einfacher zu differenzieren, sind sie im ersten Teil dieses Dokuments farblich hervorgehoben (Kundendaten = blau, Supportdaten = orange).*			
1. Datenschutz- und Sicherheitsbestimmungen (Auftragsverarbeitung)			
1.1	Vertragsinhalt: **Gegenstand und Dauer** der Vereinbarung sind festzulegen (Art. 28 Abs. 3 S. 1, 2. HS. DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Verarbeitungsdetails	Gegenstand. Der Gegenstand der Verarbeitung ist auf personenbezogene Daten innerhalb des Geltungsbereichs des Abschnitts dieses DPA mit dem Titel „Art der Verarbeitung; Eigentumsverhältnisse“ weiter oben sowie der DS-GVO eingeschränkt. Dauer der Verarbeitung. Die Dauer der Verarbeitung richtet sich nach den Weisungen des Kunden sowie den Bestimmungen des DPA.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen sowie Pflichten und Rechte des Kunden werden im Lizenzvertrag des Kunden festgelegt, der die DS-GVO-Bestimmungen einschließt
1.2	Vertragsinhalt: **Art und Zweck** der Datenverarbeitung (Art. 28 Abs. 3 S. 1, 2. HS. DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Verarbeitungsdetails	Art und Zweck der Verarbeitung ist die Bereitstellung der Produkte und Services gemäß dem Kundenvertrag und für die Geschäftstätigkeiten in Verbindung mit der Bereitstellung der Produkte und Services für den Kunden (wie ausführlicher im Abschnitt dieses DPA mit dem Titel „Art der Verarbeitung; Eigentumsverhältnisse“ weiter oben beschrieben).
		DPA > Datenschutzbestimmungen > Art der Datenverarbeitung; Eigentumsverhältnisse	Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig verarbeiten, (a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zur Verfügung zu stellen und (b) für die Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind. Unter den Parteien behält sich der Kunde alle Rechte, Ansprüche und Eigentum an und für Kundendaten und Professional Services-Daten vor. Microsoft erwirbt keine Rechte an den Kundendaten oder Professional Services-Daten, mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt. […]

		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	2. […] Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen sowie Pflichten und Rechte des Kunden werden im Lizenzvertrag des Kunden festgelegt, der die DS-GVO-Bestimmungen einschließt.
1.3	Vertragsinhalt: **Art der personenbezogenen Daten** ist festzulegen (Art. 28 Abs. 3 S. 1, 2. HS. DS-GVO).	DPA > Definitionen	„Kundendaten“ sind alle Daten, einschließlich sämtlicher Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft vom oder im Namen des Kunden durch die Nutzung der Onlinedienste bereitgestellt werden. Kundendaten schließen nicht die Professional Services-Daten ein.
		DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO	Alle personenbezogenen Daten, die von Microsoft im Zusammenhang mit der Bereitstellung der Produkte und Services verarbeitet werden, werden entweder als Teil von (a) Kundendaten, (b) Professional Services-Daten oder (c) von Microsoft generierten, abgeleiteten oder gesammelten Daten erhoben, einschließlich Daten, die an Microsoft als Ergebnis der Nutzung dienstbasierter Funktionen durch einen Kunden gesendet werden oder die von Microsoft von lokal installierter Software bezogen wurden. Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung des Onlinediensts zur Verfügung gestellt werden, sind ebenfalls Kundendaten. Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung der Professional Services zur Verfügung gestellt werden, sind ebenfalls Professional Services-Daten. Pseudonymisierte Kennungen können in Daten enthalten sein, die von Microsoft im Zusammenhang mit der Bereitstellung der Produkte verarbeitet werden, und sind ebenfalls personenbezogene Daten. Bei personenbezogenen Daten, die zwar pseudonymisiert wurden oder keine direkte Identifizierung mehr ermöglichen, jedoch nicht anonymisiert wurden, sowie bei aus personenbezogenen Daten abgeleiteten personenbezogenen Daten handelt es sich ebenfalls um personenbezogene Daten. […]
		DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Verarbeitungsdetails	Kategorien von Daten. Zu den Arten von personenbezogenen Daten, die von Microsoft bei der Bereitstellung der Produkte und Services verarbeitet werden, gehören: (i) Personenbezogene Daten, die der Kunde in Kundendaten und Professional Services-Daten aufnehmen möchte; und (ii) diejenigen, die ausdrücklich in Artikel 4 DS-GVO genannt sind, die von Microsoft generiert, abgeleitet oder gesammelt werden können, einschließlich Daten, die aufgrund der Nutzung dienstbasierter Funktionen durch einen Kunden an Microsoft gesendet oder von Microsoft aus lokal installierter Software bezogen werden. Bei den Arten von personenbezogenen Daten, die der Kunde in die Kundendaten und Professional Services-Daten aufnehmen möchte, kann es sich um alle Kategorien von personenbezogenen Daten handeln, die in Aufzeichnungen genannt werden, die vom Kunden als Verantwortlicher gemäß Artikel 30 DS-GVO handelnd gepflegt werden, einschließlich der in Anhang B aufgeführten Kategorien personenbezogener Daten.

		DPA > Definitionen	„Professional Services-Daten“ bezeichnet alle Daten, einschließlich sämtlicher Text-, Ton-, Video-, Bilddateien oder Software, die Microsoft vom oder im Namen eines Kunden zur Verfügung gestellt werden (oder für die der Kunde Microsoft ermächtigt, sie von einem Produkt zu erlangen) oder die anderweitig von oder im Namen von Microsoft im Zuge einer Vereinbarung mit Microsoft über die Erlangung von Professional Services erlangt oder verarbeitet werden.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anhang B - Betroffene Personen und Kategorien personenbezogener Daten	Kategorien von Daten: Die übermittelten personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Produkte und Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte und Services die Möglichkeit hat, personenbezogene Daten aus den folgenden Kategorien in die personenbezogenen Daten aufzunehmen: • Personenbezogene Basisdaten (z. B. Geburtsort, Straßenname und Hausnummer (Adresse), Postleitzahl, Wohnort, Land der Ansässigkeit, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum) einschließlich der personenbezogenen Basisdaten von Familienmitgliedern und Kindern; • Authentifizierungsdaten (z. B. Benutzername, Kennwort oder PIN-Code, Sicherheitsfrage, Audit-Protokoll); • Kontaktinformationen (z. B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten); • Eindeutige Identifikationsnummern und Signaturen (z. B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentennummer, Patientennummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien); • Pseudonymisierte Kennungen; • Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartenname und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität); • Geschäftsinformationen (z. B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf); • Biometrische Informationen (z. B. DNA, Fingerabdrücke und Iris-Erfassungen); • Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden); • Fotos, Videos und Audio; • Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören); • Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartennummer, MAC-Adresse);

			• Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen); • Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen); • Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung); • Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis); • Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird; • Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Anklagen); oder • Alle anderen in Artikel 4 DS-GVO genannten personenbezogenen Daten.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen sowie Pflichten und Rechte des Kunden werden im Lizenzvertrag des Kunden festgelegt, der die DS-GVO-Bestimmungen einschließt.
1.4	Vertragsinhalt: **Kategorien betroffener Personen** sind festzulegen (Art. 28 Abs. 3 S. 1, 2. HS. DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Verarbeitungsdetails	Betroffene Personen. Die Kategorien betroffener Personen sind Vertreter und Endnutzer des Kunden, wie Mitarbeiter, Auftragnehmer, Partner und Kunden. Dies kann auch andere Kategorien betroffener Personen umfassen, die in Verzeichnissen genannt werden, welche vom Kunden als Verantwortlicher gemäß Artikel 30 DS-GVO geführt werden, einschließlich der in Anhang B aufgeführten Kategorien betroffener Personen.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.

1.5	Vertragsinhalt: Verarbeitung nur auf **dokumentierte Weisung** des Verantwortlichen (Art. 28 Abs. 3 S. 2 lit. a DS-GVO).	DPA > Datenschutzbestimmungen > Art der Datenverarbeitung; Eigentumsverhältnisse	Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig verarbeiten, (a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zur Verfügung zu stellen und (b) für die Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind. Unter den Parteien behält sich der Kunde alle Rechte, Ansprüche und Eigentum an und für Kundendaten und Professional Services-Daten vor. Microsoft erwirbt keine Rechte an den Kundendaten oder Professional Services-Daten, mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt. […]
		DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Auftragsverarbeiter und Verantwortlicher - Rollen und Verantwortlichkeiten	Wenn Microsoft als Auftragsverarbeiterin oder Unterauftragsverarbeiterin handelt, verarbeitet Microsoft personenbezogene Daten nur nach den dokumentierten Anweisungen des Kunden. Der Kunde stimmt zu, dass der Kundenvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Features der Produkte durch den Kunden die vollständigen und dokumentierten Anweisungen des Kunden gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten darstellen, oder die Dokumentation der Professional Services und die Nutzung der Professional Services durch den Kunden. [...] In allen Fällen, in denen die DS-GVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Anweisungen des Kunden, einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden.
		DPA > Datenschutzbestimmungen > Datenübermittlung und Speicherstelle > Vertraulichkeitsverpflichtung des Auftragsverarbeiters	Microsoft stellt sicher, dass die Mitarbeiter von Microsoft, die mit der Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden oder gemäß Beschreibung in diesem DPA verarbeiten; und (ii) sich verpflichten, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung des Beschäftigungsverhältnisses aufrechtzuerhalten. […]
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: a. personenbezogene Daten nur auf dokumentierte Anweisung des Kunden zu verarbeiten, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, sofern Microsoft nicht durch das Recht der Union oder des Mitgliedstaats, dem Microsoft unterliegt, hierzu verpflichtet ist; In solch einem Fall teilt Microsoft dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	7. Der Kunde und Microsoft unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Kunden verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. (Artikel 32(4))
1.6	Vertragsinhalt: **Vertraulichkeitsverpflichtung** oder gesetzliche Verschwiegenheitspflicht der zur Verarbeitung befugten Personen (Art. 28 Abs. 3 S. 2 lit. b DS-GVO).	DPA > Datenschutzbestimmungen > Vertraulichkeitsverpflichtung des Auftragsverarbeiters	Microsoft stellt sicher, dass die Mitarbeiter von Microsoft, die mit der Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden oder gemäß Beschreibung in diesem DPA verarbeiten; und (ii) sich verpflichten, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung des Beschäftigungsverhältnisses aufrechtzuerhalten. Microsoft führt für Mitarbeiter mit Zugriff auf Kundendaten, Professional Services-Daten und personenbezogene Daten entsprechend den geltenden Datenschutzvorschriften und Branchenstandards regelmäßige und verpflichtende Datenschutz-, Datensicherheits- und Sensibilisierungsschulungen durch.
		DPA > Anhang A - Sicherheitsmaßnahmen > Organisation der IT-Sicherheit	Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit. Microsoft-Mitarbeiter, die Zugang zu Kundendaten haben, sind zur Vertraulichkeit verpflichtet.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: b. zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
1.7	Vertragsinhalt: **Technische und Organisatorische Maßnahmen** sind festzulegen (Art. 28 Abs. 1, 3 S. 2 lit. c i.V.m. Art. 32 DS-GVO).[*Hinweis: Die technischen und organisatorischen Maßnahmen sind unter Ziffer 2 ausführlich dargestellt.]*	DPA > Datenschutzbestimmungen > Datensicherheit > Sicherheitsverfahren und Sicherheitsrichtlinien	Microsoft ergreift geeignete technische und organisatorische Maßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft stellt diese Richtlinie dem Kunden zur Verfügung, zusammen mit anderen Informationen über die Sicherheitsverfahren und -richtlinien von Microsoft, die der Kunde angemessen anfordert. *[Hinweis: Eine tabellarische Aufzählung der technischen und organisatorischen Maßnahmen für Kernonlinedienste ist Anhang A des DPA (Seiten 14 ff.) zu entnehmen.]*

		DPA > Datenschutzbestimmungen > Datensicherheit > Datenverschlüsselung	Kundendaten und Professional Services-Daten (jeweils einschließlich aller darin enthaltenen personenbezogenen Daten), die über öffentliche Netzwerke zwischen dem Kunden und Microsoft oder zwischen Microsoft-Rechenzentren übertragen werden, werden standardmäßig verschlüsselt. Microsoft verschlüsselt auch ruhende Kundendaten in Onlinediensten und ruhende Professional Services-Daten. Im Fall von Onlinediensten, in denen der Kunde oder ein Dritter, der im Namen des Kunden handelt, Anwendungen erstellen kann (z. B. bestimmte Azure-Dienste), kann die Verschlüsselung der in diesen Anwendungen gespeicherten Daten nach Ermessen des Kunden erfolgen, unter Verwendung von Funktionen, die von Microsoft bereitgestellt werden oder die der Kunden von Dritten erlangt.
		DPA > Datenschutzbestimmungen > Datensicherheit > Datenzugriff	Microsoft nutzt Zugriffsmechanismen, die auf dem Grundsatz der geringsten Berechtigung beruhen, um den Zugriff auf Kundendaten und Professional Services-Daten (einschließlich darin enthaltener personenbezogener Daten) zu kontrollieren. Eine rollenbasierte Zugriffssteuerung wird eingesetzt, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf Kundendaten und Professional Services-Daten einem angemessenen Zweck dient und unter Aufsicht des Vorgesetzten genehmigt ist. Für Core-Onlinedienste und Professional Services unterhält Microsoft Zugriffskontrollmechanismen, die in der Tabelle mit dem Titel „Sicherheitsmaßnahmen“ in Anhang A beschrieben sind; es gibt keinen ständigen Zugriff von Microsoft-Mitarbeitern auf Kundendaten und jeder erforderliche Zugriff ist zeitlich begrenzt.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: c. alle erforderlichen Maßnahmen gemäß Artikel 32 der DS-GVO zu ergreifen;
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	5. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Kunde und Microsoft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen im Falle eines physischen oder technischen Zwischenfalls rasch wiederherzustellen;

			d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (Artikel 32(1)) […]
1.8	Vertragsinhalt: Festlegung etwaiger Berechtigung zur Begründung von **Unterauftragsverhältnissen** (Art. 28 Abs. 3 S. 2 lit. d; Absatz 4 DS-GVO).	DPA > Datenschutzbestimmungen > Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern	Microsoft kann Unterauftragsverarbeiter beauftragen, bestimmte eingeschränkte oder unterstützende Dienstleistungen für Microsoft zu erbringen. Der Kunde erklärt sich einverstanden, dass eine solche Beauftragung erfolgt und dass Microsoft-Gesellschaften als Unterauftragsverarbeiter eingesetzt werden. Die oben genannten Autorisierungen stellen die vorherige schriftliche Zustimmung des Kunden zur Untervergabe der Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten durch Microsoft dar, wenn eine solche Zustimmung nach den Standardvertragsklauseln oder den Bestimmungen der DS-GVO erforderlich ist. Microsoft ist für die Einhaltung der in diesem DPA beschriebenen Verpflichtungen von Microsoft durch seine Unterauftragsverarbeiter verantwortlich. Microsoft stellt Informationen über Unterauftragsverarbeiter auf einer Microsoft-Website zur Verfügung. Bei der Beauftragung eines Unterauftragsverarbeiters stellt Microsoft durch einen schriftlichen Vertrag sicher, dass der Unterauftragsverarbeiter auf Kundendaten, Professional Services-Daten oder personenbezogene Daten nur zugreifen und diese nur dazu nutzen darf, um die Dienstleistungen zu erbringen, für die Microsoft ihn beauftragt hat; und dass es ist ihm untersagt ist, Kundendaten, Professional Services-Daten oder personenbezogene Daten für andere Zwecke zu nutzen. Microsoft wird sicherstellen, dass Unterauftragsverarbeiter durch schriftliche Vereinbarungen gebunden sind, die von ihnen verlangen, dass sie mindestens das Datenschutzniveau bieten, das dieses DPA von Microsoft verlangt, einschließlich der Beschränkungen für die Offenlegung verarbeiteter Daten. Microsoft verpflichtet sich, die Unterauftragsverarbeiter zu beaufsichtigen, um sicherzustellen, dass diese vertraglichen Verpflichtungen erfüllt werden. Von Zeit zu Zeit beauftragt Microsoft möglicherweise neue Unterauftragsverarbeiter. Microsoft wird den Kunden über jeden neuen Unterauftragsverarbeiter mindestens 6 Monate, bevor dieser Zugriff auf Kundendaten erhält, informieren und, soweit zutreffend, die Website aktualisieren und dem Kunden einen Mechanismus bereitstellen, mit dem er über diese Aktualisierung benachrichtigt wird. Darüber hinaus wird Microsoft den Kunden über jeden neuen Unterauftragsverarbeiter mindestens 30 Tage bevor er Zugriff auf Professional Services-Daten oder personenbezogene Daten erhält, die nicht in den Kundendaten enthalten sind, informieren und, soweit zutreffend, die Website aktualisieren und dem Kunden einen Mechanismus bereitstellen, mit dem er über diese Aktualisierung benachrichtigt wird. Wenn Microsoft einen neuen Unterauftragsverarbeiter für ein neues Produkt oder einen Professional Service beauftragt, der Kundendaten, Professional Services-Daten oder personenbezogene Daten verarbeitet, wird Microsoft den Kunden vor der Verfügbarkeit dieses Produkts oder Professional Services benachrichtigen. Wenn der Kunde einem neuen Unterauftragsverarbeiter für einen Onlinedienst oder für Professional Services nicht zustimmt, kann er ein etwaiges Abonnement für den betroffenen Onlinedienst oder die zutreffenden Leistungsbeschreibungen, wie z. B. einen Enterprise Services-Arbeitsauftrag, für den betreffenden Professional Services, jeweils ohne Strafe oder Kündigungsgebühr beenden, indem er vor dem Ablauf der entsprechenden Kündigungsfrist eine schriftliche

			Kündigung einreicht. Wenn der Kunde einem neuen Unterauftragsverarbeiter für Software nicht zustimmt und der Kunde die Nutzung des Unterauftragsverarbeiters nicht vernünftigerweise vermeiden kann, indem er Microsoft daran hindert, Daten wie in der Dokumentation oder dieser DPA beschrieben zu verarbeiten, kann der Kunde jede Lizenz für das betroffene Softwareprodukt durch schriftliche Kündigung vor Ablauf der jeweiligen Kündigungsfrist ohne Strafe kündigen. Der Kunde kann zusammen mit der Kündigung auch eine Erklärung der Gründe für seine Ablehnung beifügen, damit Microsoft die Möglichkeit hat, diesen neuen Unterauftragsverarbeiter anhand der vorgebrachten Bedenken neu zu bewerten. Wenn das betroffene Produkt Teil einer Suite (oder eines ähnlichen einzelnen Kaufs von Diensten) ist, gilt die Kündigung für die gesamte Suite. Nach der Kündigung entfernt Microsoft die Zahlungsverpflichtungen für jedwedes Abonnement oder sonstige entsprechende nicht bezahlte Arbeiten für die gekündigten Produkte oder Services aus den nachfolgenden Rechnungen an den Kunden oder seinen Handelspartner.
1.9	Vertragsinhalt: **Unterstützung des Verantwortlichen bei Beantwortung von Anträgen des Betroffenen** (Art. 28 Abs. 3 lit. e DS-GVO), u. A.: - Auskunftsverlangen (Art. 15 DS-GVO) - Berichtigungsverlangen (Art. 16 DS-GVO) - Löschungsverlangen (Art. 17 DS-GVO) - Verlangen der Einschränkung der Verarbeitung der Daten (Art. 18 DS-GVO) - Verlangen der Daten in portablem Format (Art. 20 DS-GVO) - Geltendmachung des Widerspruchsrechts (Art. 21 DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Rechte der betroffenen Personen; Unterstützung bei Anfragen	Microsoft ermöglicht dem Kunden, Anfragen betroffener Personen zur Ausübung ihrer Rechte nach der DS-GVO auf eine mit der Funktion der Produkte und Services und der Rolle von Microsoft als Auftragsverarbeiter personenbezogener Daten betroffener Personen konsistente Art und Weise nachzukommen. Wenn Microsoft eine Anfrage der betroffenen Person des Kunden erhält, mindestens eines ihrer Rechte nach der DS-GVO in Verbindung mit den Produkten und Services, für die Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter ist, auszuüben, verweist Microsoft die betroffene Person, damit sie ihre Anfrage direkt an den Kunden richtet. Der Kunde ist für die Beantwortung einer solchen Anfrage verantwortlich, einschließlich, falls erforderlich, durch Nutzung der Funktionalität der Produkte und Services. Microsoft kommt angemessenen Anfragen des Kunden nach Unterstützung bei der Bearbeitung von Anfragen betroffener Personen nach.
		DPA > Datenschutzbestimmungen > Speicherung und Löschung von Daten	Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu löschen. […]
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: e. angesichts der Art der Verarbeitung den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen;

1.10	Vertragsinhalt: **Unterstützung des Verantwortlichen bei der Datensicherheit** (Art. 28 Abs. 3 lit. f. DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Meldung von Sicherheitsvorfällen	Microsoft wird angemessene Anstrengungen unternehmen, um den Kunden bei der Erfüllung seiner Verpflichtung nach Art. 33 DS-GVO oder anderen anwendbaren Gesetzen oder Vorschriften zu unterstützen, nämlich die zuständige Aufsichtsbehörde und die betroffenen Personen über solche Sicherheitsvorfälle zu unterrichten.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: f. den Kunden unter Berücksichtigung der Art der Verarbeitung und der Microsoft zur Verfügung stehenden Informationen bei der Einhaltung seiner Verpflichtungen gemäß den Artikeln 32 bis 36 der DS-GVO zu unterstützen.
1.11	Vertragsinhalt: **Löschung oder Rückgabe** der Daten nach Vertragsbeendigung (Art. 28 Abs. 3 lit. g DS-GVO).	DPA > Datenschutzbestimmungen > Speicherung und Löschung von Daten	Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu löschen. Mit Ausnahme von kostenlosen Testversionen und LinkedIn-Diensten wird Microsoft Kundendaten, die in den Onlinediensten gespeichert bleiben, 90 Tage lang nach Ablauf oder Beendigung des Abonnements des Kunden in einem eingeschränkten Funktionskonto aufbewahren, damit der Kunde die Daten extrahieren kann. Nach Ablauf der 90-tägigen Aufbewahrungsfrist deaktiviert Microsoft das Konto des Kunden und löscht die in den Onlinediensten gespeicherten Kundendaten und personenbezogenen Daten innerhalb weiterer 90 Tage; es sei denn, Microsoft ist durch dieses DPA zur Aufbewahrung autorisiert. Für personenbezogene Daten in Verbindung mit der Software sowie für Professional Services-Daten gilt, dass Microsoft alle Kopien löschen wird, nachdem die geschäftlichen Zwecke erfüllt wurden, zu denen die Daten erhoben oder übermittelt wurden (auf Kundenwunsch auch früher); es sei denn, Microsoft ist durch diesen DPA zur Aufbewahrung dieser Daten autorisiert. […]
		DPA > Anhang A - Sicherheitsmaßnahmen > Physische und umgebungsbezogene Sicherheit	Entsorgung von Komponenten. Microsoft nutzt branchenübliche Prozesse, um Kundendaten und Professional Services-Daten zu löschen, wenn sie nicht mehr benötigt werden.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: g. nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Kunden sämtliche personenbezogenen Daten zu löschen oder dem Kunden zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

1.11	Vertragsinhalt: **Zurverfügungstellung aller erforderlichen Informationen** zur Nachprüfung der Einhaltung des Vertrags (Art. 28 Abs. 3 lit. h Hs. 1 DS-GVO).	DPA > Datenschutzbestimmungen > Datensicherheit > Sicherheitsverfahren und Sicherheitsrichtlinien	Microsoft ergreift geeignete technische und organisatorische Maßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft stellt diese Richtlinie dem Kunden zur Verfügung, zusammen mit anderen Informationen über die Sicherheitsverfahren und -richtlinien von Microsoft, die der Kunde angemessen anfordert.
		DPA > Datenschutzbestimmungen > Datensicherheit > Prüfung der Einhaltung	Microsoft wird Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft zur Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten nutzt, wie folgt durchführen: • Sieht eine Norm oder ein Rahmenkonzept Prüfungen vor, so wird mindestens einmal jährlich eine Prüfung dieser Kontrollnorm oder dieses Rahmenkonzepts veranlasst. • Jede Prüfung wird entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder Rahmenbestimmungen durchgeführt. • Jede Prüfung wird von qualifizierten, unabhängigen dritten Sicherheitsprüfern durchgeführt, die von Microsoft ausgewählt werden und für die Microsoft die Kosten trägt. Jede Prüfung führt zur Erstellung eines Prüfungsberichts („Microsoft-Prüfungsbericht“), den Microsoft unter https://servicetrust.microsoft.com/ oder an einem anderen von Microsoft angegebenen Ort zur Verfügung stellt […]
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: h. dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der DS-GVO beschriebenen Verpflichtungen zur Verfügung zu stellen und Überprüfungen - einschließlich Inspektionen, die vom Kunden oder einem von ihm beauftragten Prüfer durchgeführt werden - zu ermöglichen und dazu beizutragen.
1.12	Vertragsinhalt: Ermöglichung von **Überprüfungen** (Art. 28 Abs. 3 lit. h Hs. 2 DS-GVO).	DPA > Datenschutzbestimmungen > Datensicherheit > Prüfung der Einhaltung	Insoweit die Prüfanforderungen des Kunden im Rahmen der Datenschutzvorschriften durch die Prüfberichte, Dokumentationen oder Informationen zur Einhaltung nicht angemessen erfüllt werden können, die Microsoft seinen Kunden allgemein zur Verfügung stellt, reagiert Microsoft umgehend auf die zusätzlichen Prüfanweisungen des Kunden. Vor Beginn einer Prüfung vereinbaren der Kunde und Microsoft gemeinsam Umfang, Zeitpunkt, Dauer, Kontroll- und Nachweisanforderungen sowie die Gebühren für die Prüfung; das Erfordernis einer Vereinbarung gestattet Microsoft jedoch nicht, die Durchführung der Prüfung unangemessen zu verzögern. Soweit für die Durchführung der Prüfung erforderlich, stellt Microsoft die relevanten Verarbeitungssysteme, Einrichtungen und unterstützende Unterlagen zur Verfügung, die für die Verarbeitung von Kundendaten,

			Professional Services-Daten und personenbezogenen Daten durch Microsoft, die mit Microsoft verbundenen Unternehmen und Unterauftragsverarbeiter relevant sind. Eine solche Prüfung wird von einer unabhängigen, akkreditierten und externen Prüfungsgesellschaft während der normalen Geschäftszeiten mit angemessener Vorankündigung für Microsoft sowie unter Einhaltung angemessener Vertraulichkeitsverfahren durchgeführt. […]
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: h. dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der DS-GVO beschriebenen Verpflichtungen zur Verfügung zu stellen und Überprüfungen - einschließlich Inspektionen, die vom Kunden oder einem von ihm beauftragten Prüfer durchgeführt werden - zu ermöglichen und dazu beizutragen.
1.13	Vertragsinhalt: Regelung zur **Mitteilungspflicht von Verstößen** des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen (Art. 28 Abs. 3 S. 3 DS-GVO).	DPA > Datenschutzbestimmungen > Verarbeitung personenbezogener Daten; DS-GVO > Meldung von Sicherheitsvorfällen	Wenn Microsoft eine Verletzung der Sicherheit bemerkt, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf Kundendaten, Professional Services-Daten oder personenbezogene Daten während der Verarbeitung durch Microsoft führt (jeweils ein „Sicherheitsvorfall“), wird Microsoft den Kunden unverzüglich und ohne schuldhaftes Zögern (1) vom Sicherheitsvorfall benachrichtigen; (2) den Sicherheitsvorfall untersuchen und den Kunden mit detaillierten Informationen über den Sicherheitsvorfall versorgen; (3) angemessene Maßnahmen ergreifen, um die Auswirkungen zu mildern und den Schaden, der sich aus dem Sicherheitsvorfall ergibt, so gering wie möglich zu halten. […] Microsoft wird angemessene Anstrengungen unternehmen, um den Kunden bei der Erfüllung seiner Verpflichtung nach Art. 33 DS-GVO oder anderen anwendbaren Gesetzen oder Vorschriften zu unterstützen, nämlich die zuständige Aufsichtsbehörde und die betroffenen Personen über solche Sicherheitsvorfälle zu unterrichten. […]
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante GDPR-Verpflichtungen: Artikel 28, 32 und 33	Microsoft informiert den Kunden unverzüglich, falls Microsoft der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. (Artikel 28(3))
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante GDPR-Verpflichtungen: Artikel 28, 32 und 33	8. Wenn Microsoft eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet Microsoft diese dem Kunden unverzüglich. (Art. 33 Absatz 2). Eine solche Mitteilung enthält auch die Informationen, die ein Auftragsverarbeiter gemäß Artikel 33 (3) einem Datenverantwortlichen zur Verfügung stellen muss, soweit diese Informationen Microsoft in angemessener Weise zur Verfügung stehen.
		DPA > Anhang A - Sicherheitsmaßnahmen > Handhabung eines Informationssicherheits-vorfalls	Vorfallreaktionsablauf • Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens für die Wiederherstellung von Daten. • Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (wie im Abschnitt „Meldung von Sicherheitsvorfällen“ weiter oben beschrieben)

			unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens Microsofts. • Microsoft untersucht Offenlegungen von Kundendaten und Professional Services-Daten einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage.
2. Technische und organisatorische Maßnahmen (TOM)			
2.	Der Auftragsverarbeiter muss gem. Art. 28 Abs. 3 lit. c DS-GVO die **Sicherheit der Daten** des Verarbeiters gewährleisten, indem er alle erforderlichen Maßnahmen nach Art. 32 DS-GVO ergreift. Art. 32 DS-GVO zählt beispielhaft einige Maßnahmen auf. Der Auftragsverarbeiter hat im Rahmen einer Datenverarbeitung die Maßnahmen zu ergreifen, die in einem angemessenen Verhältnis von Schutzaufwand und Risiko stehen, um ein angemessenes Schutzniveau für die betroffenen personenbezogenen Daten zu gewährleisten.	DPA > Datenschutzbestimmungen > Datensicherheit > Sicherheitsverfahren und Sicherheitsrichtlinien	Microsoft ergreift geeignete technische und organisatorische Maßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft stellt diese Richtlinie dem Kunden zur Verfügung, zusammen mit anderen Informationen über die Sicherheitsverfahren und -richtlinien von Microsoft, die der Kunde angemessen anfordert. Darüber hinaus erfüllen diese Maßnahmen die Anforderungen von ISO 27001, ISO 27002 und ISO 27018. Eine Beschreibung der Sicherheitskontrollen für diese Anforderungen steht den Kunden zur Verfügung. Jeder Core-Onlinedienst entspricht auch den Kontrollstandards und -bestimmungen, die in der Tabelle in den Produktbestimmungen aufgeführt sind. Jeder Core-Onlinedienst und Professional Service implementiert und unterhält die in Anhang A dargelegten Sicherheitsmaßnahmen zum Schutz von Kundendaten und Professional Services-Daten.
		DPA > Einleitung	Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA“) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. […] Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA unterliegen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	3. […] Insbesondere ist Microsoft gehalten: c. alle erforderlichen Maßnahmen gemäß Artikel 32 der DS-GVO zu treffen.
		DPA > Anlage 1 - Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union > Relevante DS-GVO-Verpflichtungen: Artikel 5, 28, 32 und 33	5. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Kunde und Microsoft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

			c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen im Falle eines physischen oder technischen Zwischenfalls rasch wiederherzustellen; d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (Artikel 32(1)) […] 6. Bei der Beurteilung des angemessenen Schutzniveaus sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. (Artikel 32(2)) *[Hinweis: Eine tabellarische Aufzählung der technischen und organisatorischen Maßnahmen ist Anhang A des DPA (Seiten 14 ff.) zu entnehmen.]*

Anlage 2:

M365-Kit

Das M365-Kit ist unter https://www.microsoft.com/de-de/mit-sicherheit/datenschutz-ressourcen#DasMicrosoft365Kit im **Service Trust Portal** für Kunden zugänglich veröffentlicht. Hier finden sich die folgenden Dokumentationen:

- 01_Deckblatt
- 02_Verzeichnis der Verarbeitungstätigkeiten_Beispieleinträge
- 03_Beispielhafte Schwellwertanalysen
- 04_Rechtmäßigkeit der Verarbeitung
- 05_Beispielhafte Datenschutzerklärung
- 06_Erläuterungen zu Microsofts Verständnis der Anonymisierung von Daten_Microsoft_M365

Anlage 3:

Taxonomie zum Datenschutznachtrag für Produkte und Services von MS

Inhalt

A) Grundlegendes

I. Einleitung

Im Folgenden werden grundlegende Festlegungen hinsichtlich des Aufbaus der Taxonomie und der Zuordnung von Daten zu Kategorien dargestellt. Diese sind bei der Verwendung der Kategorien bzw. deren Benennungen von zentraler Bedeutung.

II. Aufbau der Taxonomie

Die vorliegende Taxonomie unterteilt die im Geltungsbereich des DPA verarbeiteten personenbezogenen Daten in eine Hierarchie von Datenkategorien (kurz: **Kategorien**). In dieser Hierarchie sind jeder Kategorie genau eine[151] übergeordnete und beliebig viele[152] untergeordnete Kategorien zugeordnet. Hieraus ergibt sich ein **Kategorienbaum** mit einem Wurzelelement und ohne zyklische Beziehungen zwischen den Kategorien.

Jede Kategorie trägt eine eindeutige Benennung und ist durch **kategoriespezifische Eigenschaften** gekennzeichnet. Die Zuordnung eines personenbezogenen Datums zu einer Kategorie bedeutet, dass das Datum der Kategorie selbst und indirekt auch allen direkt oder indirekt übergeordneten Kategorien angehört.

III. Lebenszyklus personenbezogener Daten

Jedes verarbeitete personenbezogene Datum verbleibt nach seiner einmaligen, initialen Zuordnung zu einer Kategorie in dieser bis zur Löschung des Datums. Ein personenbezogenes Datum ist immer genau einer Kategorie zugeordnet, der keine weiteren untergeordneten Kategorien zugeordnet sind. Hiermit wird das Ziel einer möglichst spezifischen Kategorienzuordnung erreicht, welche wiederum eine trennscharfe Abgrenzung im Rahmen der Verwendung der Taxonomie ermöglicht. Auch wird hierdurch eine vollständige Trennung der Daten der einzelnen Kategorien untereinander erreicht. Dies entspricht auch den Ausführungen im DPA[153]:

---

[151] Die einzige Ausnahme bildet das oberste Element der Hierarchie „Personenbezogene Daten“.
[152] Dies schließt mit ein, dass einer Kategorie keine untergeordnete Kategorie zugeordnet ist.
[153] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO, Seite 12.

„*Alle personenbezogenen Daten, die von Microsoft im Zusammenhang mit der Bereitstellung der Produkte und Services verarbeitet werden, werden entweder als Teil von (a) Kundendaten, (b) Professional Services-Daten oder (c) von Microsoft generierten, abgeleiteten oder gesammelten Daten erhoben, einschließlich Daten, die an Microsoft als Ergebnis der Nutzung dienstbasierter Funktionen durch einen Kunden gesendet werden oder die von Microsoft von lokal installierter Software bezogen wurden.*“.

Von der Entstehung eines personenbezogenen Datums bis zu seiner Zuordnung zu einer Kategorie der Taxonomie kann es zu mehreren Verarbeitungsvorgängen im Sinne des Art. 4 Nr. 2 DS-GVO kommen. Aufgrund der atomaren Vorgangsreihe kann es dennoch nicht zu Situationen kommen, in denen ein personenbezogenes Datum ohne Kategorienzuordnung verarbeitet wird.

Es besteht die Möglichkeit, dass ein Datum kopiert und die resultierende Kopie im Rahmen des Kopiervorgangs einer anderen Kategorie zugeordnet wird. Hierbei ist zu beachten, dass sich die Kategorienzuordnung des ursprünglichen Datums durch die Kopieerstellung nicht ändert. Vielmehr entsteht durch das Kopieren ein neues Datum, welches seinerseits eine Kategorienzuordnung erfährt. Diese kann von der Zuordnung des ursprünglichen Datums abweichen. Der Vorgang der Kopieerstellung und der Zuordnung zu einer Kategorie ist ebenfalls jeweils eine atomare Vorgangsreihe.

B) Datenkategorien

I. Einleitung

In den folgenden Kapiteln werden die einzelnen Kategorien der Taxonomie dargestellt. Hierbei wird ein **Top-Down-Ansatz** verfolgt, bei dem nach einer Betrachtung der Wurzelkategorie Personenbezogene Daten in jedem Folgekapitel jeweils eine derjenigen Kategorien betrachtet wird, die unmittelbar der Wurzelkategorie untergeordnet ist. Diesen wiederum untergeordnete Unterkategorien werden in jeweils eigenen Unterkapiteln adressiert.

Das einleitende Kapitel „Grundlegendes“ stellt die wesentlichen Annahmen für die Ausgestaltung und Nutzung der vorliegenden Taxonomie dar. Das Unterkapitel „Lebenszyklus personenbezogener Daten“ hält hierzu allgemeingültige und kategorienübergreifende Rahmenbedingungen für den Lebenszyklus der in der Taxonomie betrachteten Datenkategorien fest. Hierauf aufbauend erfolgt für die einzelnen im Folgenden betrachteten Kategorien auf unterster Ebene eine differenzierte Dokumentation der jeweiligen Lebenszyklen. Hierzu wird konkretisierend auf spezifische Gegebenheiten der jeweiligen Kategorie eingegangen.

Die Betrachtung der einzelnen Lebenszyklen erfolgt hinsichtlich der folgenden Aspekte:

(1) Herkunft und Entstehung von Daten der jeweils betrachteten Kategorie,
(2) Bedingungen und Umstände der Löschung der Daten der jeweiligen Kategorie.

Die Darstellungen zum ersten Aspekt haben exemplarischen Charakter und liefern Beispiele für die Entstehung von Daten der jeweiligen Kategorie. Die Menge der enthaltenen Beispiele sollte nicht als vollständig missinterpretiert werden.

II. Personenbezogene Daten

Die DS-GVO enthält in Art. 4 Nr. 1 die folgende Definition des Begriffs „personenbezogene Daten“:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck ‚personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Auch das DPA[154] enthält eine Definition des Begriffs „Personenbezogene Daten“:

„*Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“.*

Beide Definitionen sind inhaltsgleich. Daher wird im Folgenden davon ausgegangen, dass es sich bei den Abweichungen der Definition im DPA von der der DS-GVO lediglich um redaktionelle Anpassungen handelt. Für diese Taxonomie wird die Definition der DS-GVO zugrunde gelegt.

Die folgende Abbildung 1 zeigt die oberste Ebene der Taxonomie. Die Kategorie „Personenbezogene Daten“ stellt die Wurzelkategorie der Taxonomie dar.

[154] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Definitionen, Seite 6.

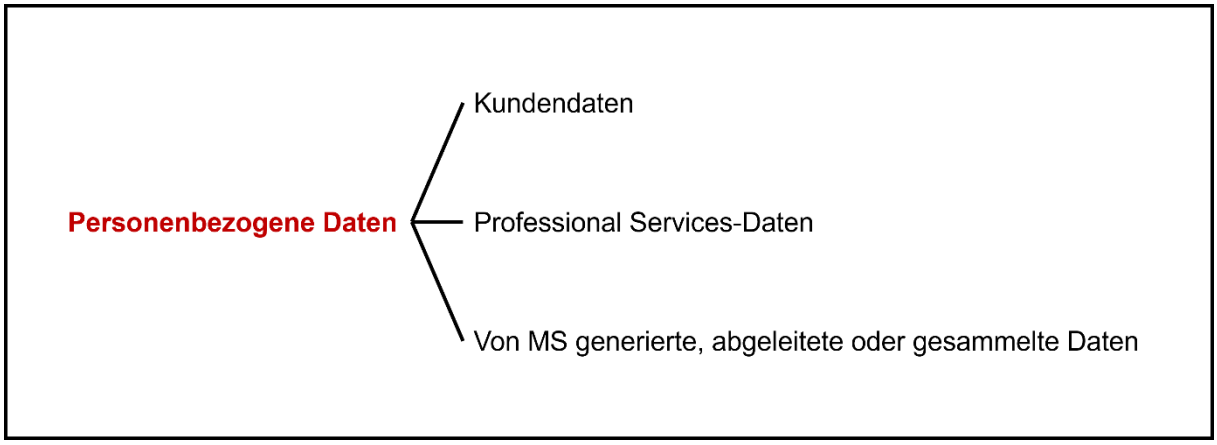

Abbildung 1: Top-Level-Kategorien

Dementsprechend sind alle übrigen Kategorien der Taxonomie unmittelbar oder mittelbar dieser Kategorie untergeordnet. Durch diesen Aufbau wird klargestellt, dass alle verarbeiteten personenbezogenen Daten entweder Kundendaten, Professional Services-Daten oder von MS generierte, abgeleitete oder gesammelte Daten sind. Dies entspricht auch den Kategorien des DPA.[155]

Die Wurzelkategorie „Personenbezogene Daten“ und die zugehörige Definition verdeutlichen, dass im Kontext der vorliegenden Taxonomie eine ausschließliche Fokussierung auf personenbezogene Daten im Sinne der DS-GVO erfolgt. Es werden also nicht alle möglichen Arten von verarbeiteten Daten und Informationen betrachtet, sondern lediglich diejenigen, welche einen Personenbezug aufweisen. Nicht-personenbezogene Daten werden demgegenüber nicht berücksichtigt, da sie außerhalb des datenschutzrechtlichen Geltungsbereichs liegen.

[155] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Datenschutzbestimmungen – Verarbeitung personenbezogener Daten; DSGVO, Seite 12.

III. Kundendaten

1) Überblick

Im DPA[156] ist der Begriff „Kundendaten“ wie folgt definiert:

„Kundendaten sind alle Daten, einschließlich sämtlicher Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft vom oder im Namen des Kunden durch die Nutzung der Onlinedienste bereitgestellt werden. Kundendaten schließen nicht die Professional Services-Daten ein.“

Die Definition enthält keinen Bezug zu personenbezogenen Daten. Vielmehr deuten u. a. der Verweis auf „alle Daten“ und das Referenzieren auf „Software“ darauf hin, dass der Definitionsbereich im DPA weiter gefasst ist und auch nicht-personenbezogene Daten einschließt. Diese Taxonomie adressiert ausschließlich die Perspektive des Datenschutzes. Daher deckt die Kategorie „Kundendaten“ in dieser Taxonomie ausschließlich diejenigen Kundendaten des DPA ab, die einen Personenbezug aufweisen. Die folgende Abbildung 2 zeigt die Einordnung der Kategorie „Kundendaten“ in die Kategorienhierarchie der Taxonomie.

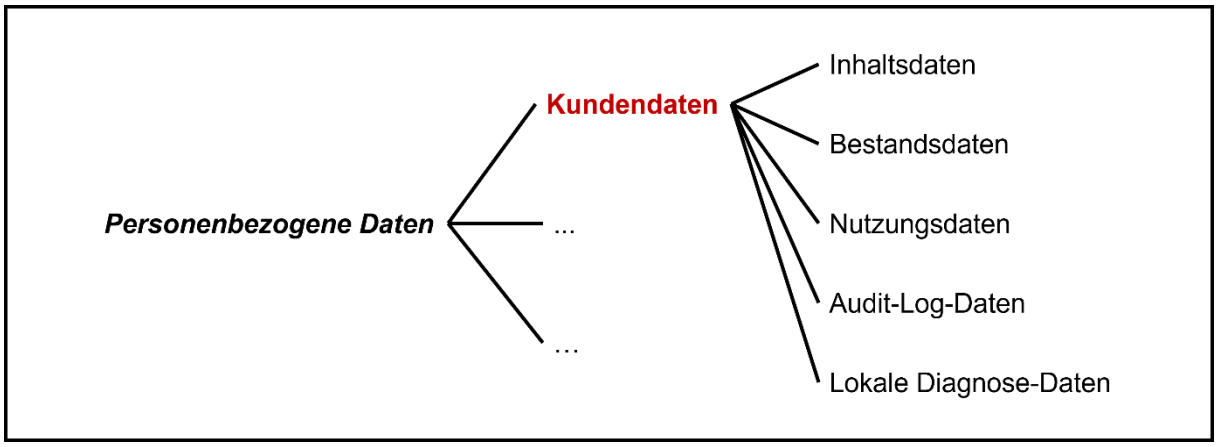

Abbildung 2: Kategorie Kundendaten

Kundendaten umfassen gemäß obiger Definition und für die Zwecke dieser Taxonomie alle personenbezogenen Daten, die MS vom oder im Namen des Kunden durch die Nutzung der Onlinedienste bereitgestellt werden. Hierbei handelt es sich um Inhaltsdaten, Bestandsdaten, Nutzungsdaten, Audit-Log-Daten und Lokale Diagnose-Daten. Diese stellen Spezialisierungen von Kundendaten dar und werden in der Taxonomie als Unterkategorien von Kundendaten repräsentiert, wie in Abbildung 2

[156] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Definitionen, Seite 6.

dargestellt. In den folgenden Unterkapiteln werden diese Unterkategorien jeweils separat spezifiziert.

2) Inhaltsdaten

Definition

Das DPA enthält keine Definition des Begriffs „*Inhaltsdaten*“. Für eine differenzierte Betrachtung der Kundendaten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Inhaltsdaten handelt es sich, wie in Abbildung 3 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen Kundendaten.

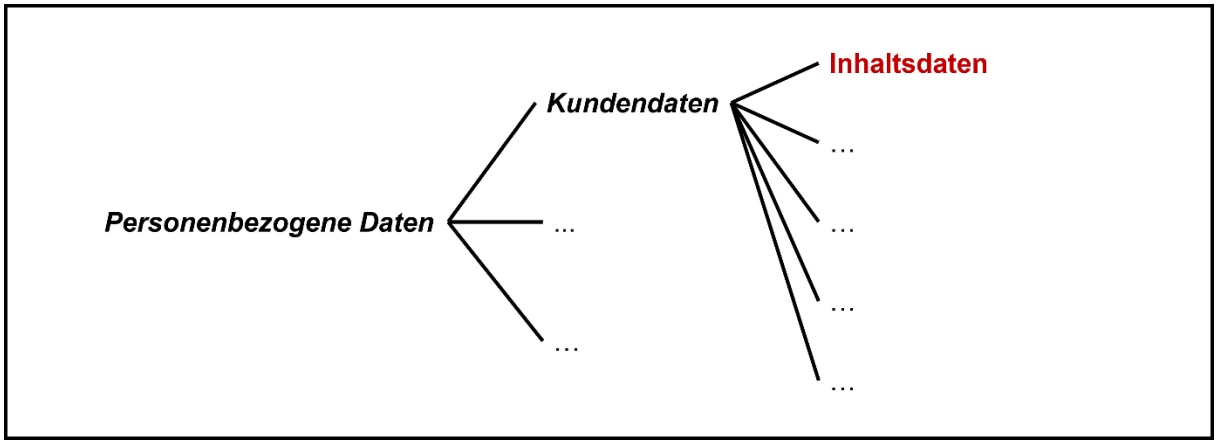

Abbildung 3: Kategorie Inhaltsdaten

Diese werden im Rahmen der Nutzung der Dienste von Anwendern mit Hilfe zentraler Dienste von MS[157] in diese hochgeladen oder mittels dieser erstellt. Nachfolgend werden Inhaltsdaten mittels der Dienste zur Aufgabenerfüllung der Nutzenden des Kunden weiterverarbeitet.

Zu Inhaltsdaten gehören bspw. Dokumente, Dateien, Textnachrichten, Audio- und Videodaten von Videokonferenzen oder weitere von Nutzenden mittels Anwendungen verarbeitete Daten, deren inhaltliche Verarbeitung der Aufgabenerfüllung des Kunden dient.

Inhaltsdaten werden von MS zur Unterstützung der Aufgabenerfüllung gemäß der Beschreibung der jeweiligen Dienste verarbeitet.

[157] Hierbei handelt es ich in aller Regel um Cloud-basierte IT-Dienste.

Kunden können im Rahmen von Professional Services den Zugriff auf Inhaltsdaten einräumen, ohne dass dabei eine Kopie erstellt würde.

Entstehung

Inhaltsdaten entstehen, indem MS vom oder im Namen des Kunden durch die Nutzung der Onlinedienste Daten bereitgestellt werden. Beispiele für die Bereitstellung von Inhaltsdaten sind:

(1) das Hochladen von Dateien oder
(2) die Erstellung von Nachrichten direkt im genutzten Dienst.

Löschung

Inhaltsdaten werden entweder manuell von Nutzenden des Kunden oder automatisiert nach der Beendigung des Vertragsverhältnisses gelöscht.

In Abhängigkeit vom konkret genutzten Dienst können Löschverfahren zur automatisierten Löschung beim Eintreten bestimmter Ereignisse hinzukommen. Ein Beispiel hierfür ist der Ablauf einer voreingestellten Aufbewahrungsfrist. All diesen Verfahren ist gemein, dass der Kunde sie kontrollieren kann.

3) Bestandsdaten

Definition

Der Begriff „*Bestandsdaten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der Kundendaten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Bestandsdaten handelt es sich, wie in Abbildung 4 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen Kundendaten.

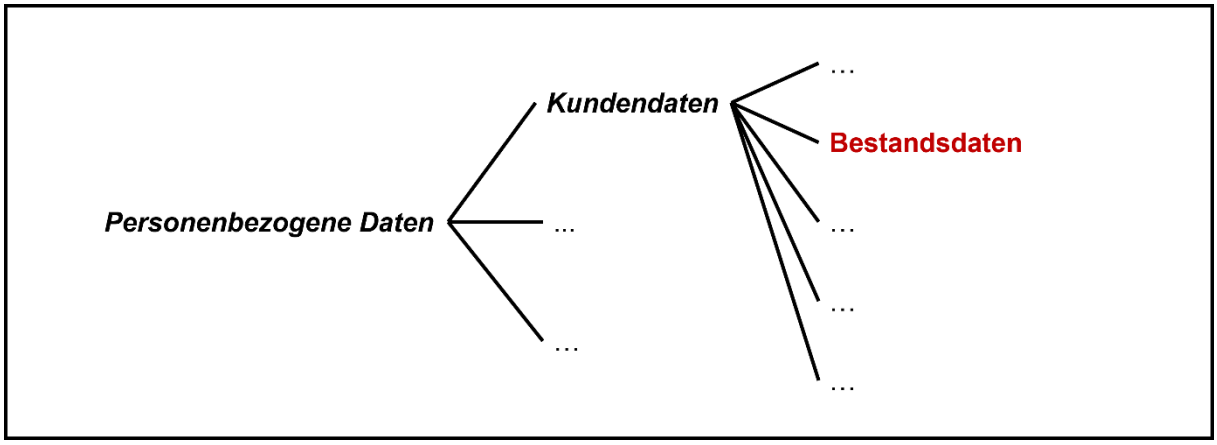

Abbildung 4: Kategorie Bestandsdaten

Bestandsdaten sind als Voraussetzung zur Nutzung von Diensten erforderlich. Es handelt sich hierbei um all diejenigen Daten, die als Datenbasis und Grundlage zur Bereitstellung und Nutzung von Diensten benötigt werden. Bestandsdaten sind somit eine Voraussetzung für die Bereitstellung und Nutzung von Diensten.

Beispiele für Bestandsdaten sind Nutzendenaccounts mit Identifikatoren, Namen und E-Mail-Adressen sowie nutzendenspezifische Einstellungen.

Entstehung

Initiale Bestandsdaten zu einem Nutzenden eines Kunden entstehen erstmalig im Rahmen der Erstellung eines Nutzendenkontos. Ergänzende Daten können im Laufe der Zeit hinzukommen. Auch können neue Nutzendendaten durch Aktionen von Nutzenden entstehen, etwa durch

(1) die Zuordnung eines Nutzendenkontos zu einer Gruppe,
(2) die Vergabe von nutzendenspezifischen Berechtigungen oder
(3) die Vornahme nutzendenspezifischer Einstellungen.

Löschung

Nutzendenaccounts werden entweder durch Administratoren von Kunden oder automatisiert nach der Beendigung des Vertragsverhältnisses gelöscht. Im Rahmen der Löschung eines Nutzendenaccounts werden auch Löschprozesse initiiert, die zur Löschung der zum Account gehörenden Bestandsdaten führen.

4) Nutzungsdaten

Definition

Der Begriff „*Nutzungsdaten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der Kundendaten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Nutzungsdaten handelt es sich, wie in Abbildung 5 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen Kundendaten.

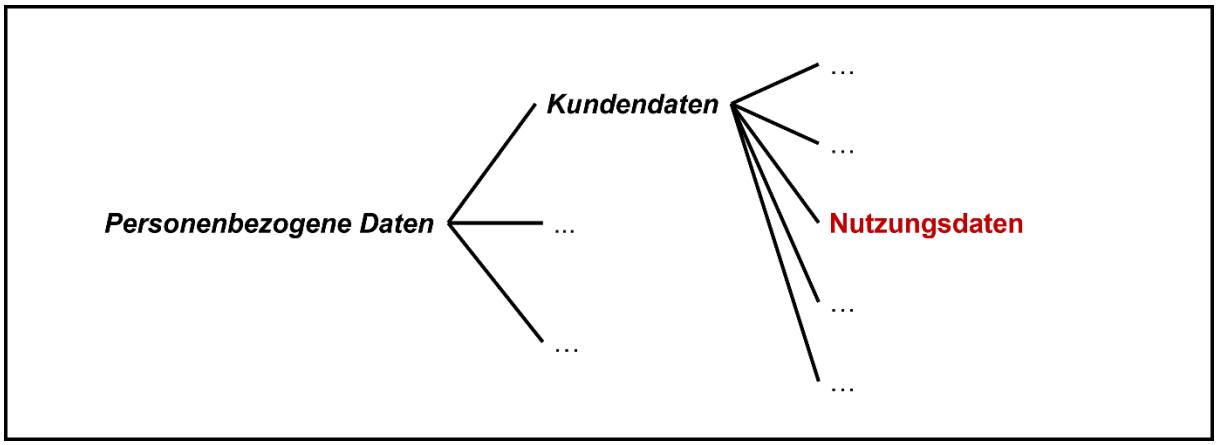

Abbildung 5: Kategorie Nutzungsdaten

Nutzungsdaten sind Daten, die für die konkrete Nutzung von zentralen Diensten erforderlich sind. Dies schließt auch Prüfung auf Kompromittierung, Session Management und ähnliches mit ein. Sie werden im Rahmen der Nutzung von zentralen Diensten zu deren unmittelbarer Erbringung verarbeitet.

Beispiele für Nutzungsdaten sind IP-Adressen, Sitzungsschlüssel und Identifikatoren als Teil der für die Kommunikation und Interaktion mit zentralen Diensten erforderlichen Daten.

Entstehung

Nutzungsdaten werden im Bedarfsfall bei der Nutzung von Anwendungen und zentralen Diensten erstellt. Hierzu werden gegebenenfalls auch Kopien von Bestandsdaten erstellt und in die Nutzungsdaten übernommen.

Löschung

Nutzungsdaten werden automatisiert gelöscht, sobald sie für die Nutzung der Anwendung bzw. des zentralen Dienstes nicht mehr benötigt werden.

5) Audit-Log-Daten

Definition

Der Begriff „*Audit-Log-Daten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der Kundendaten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Audit-Log-Daten handelt es sich, wie in Abbildung 6 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen Kundendaten.

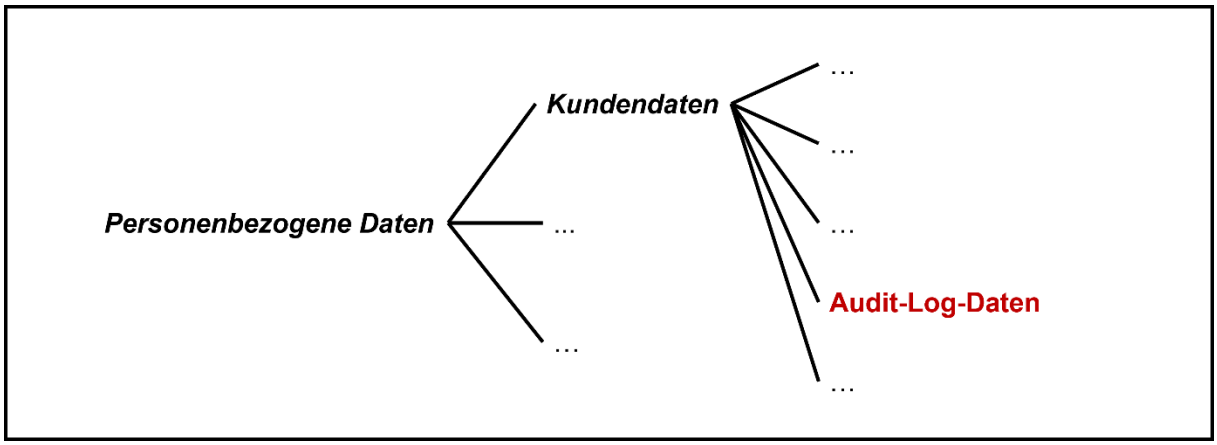

Abbildung 6: Kategorie Audit-Log-Daten

Audit-Log-Daten sind kundenspezifische Daten in der zentralen Infrastruktur von MS über die Nutzung von Diensten dieser Infrastruktur. Eine Kopie dieser Daten wird Kunden als Audit-Log-Daten bereitgestellt. Audit-Log-Daten können auch Kopien von Teilen von Bestandsdaten und Nutzungsdaten enthalten, jedoch nicht von Inhaltsdaten.

Beispiele für Audit-Log-Daten sind Ereignisprotokolle von zentralen Diensten wie Exchange Online oder Teams. In diesen können auch Object-IDs von Nutzenden oder IP-Adressen von Arbeitsplatzrechnern enthalten sein.

Entstehung

Bei der Nutzung von durch MS betriebenen zentralen Diensten werden Daten über die Nutzung dieser Dienste generiert und zu Datensätzen zusammengeführt. Zu den hierzu verwendeten Daten zählen

(1) Daten über Aktionen wie das Speichern einer Datei und
(2) Daten über Ereignisse wie das eines Fehlerfalls.

Kopien von kundenspezifischen Teilen der zusammengestellten Datensätze werden Kunden als Audit-Log-Daten zur Verfügung gestellt.

Löschung

Audit-Log-Daten kann der Kunden löschen. Ferner löscht MS Audit-Log-Daten automatisiert nach der Beendigung des Vertragsverhältnisses.

6) Lokale Diagnose-Daten

Definition

Der Begriff „*Lokale Diagnose-Daten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der Kundendaten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei lokalen Diagnose-Daten handelt es sich, wie in Abbildung 7 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen Kundendaten.

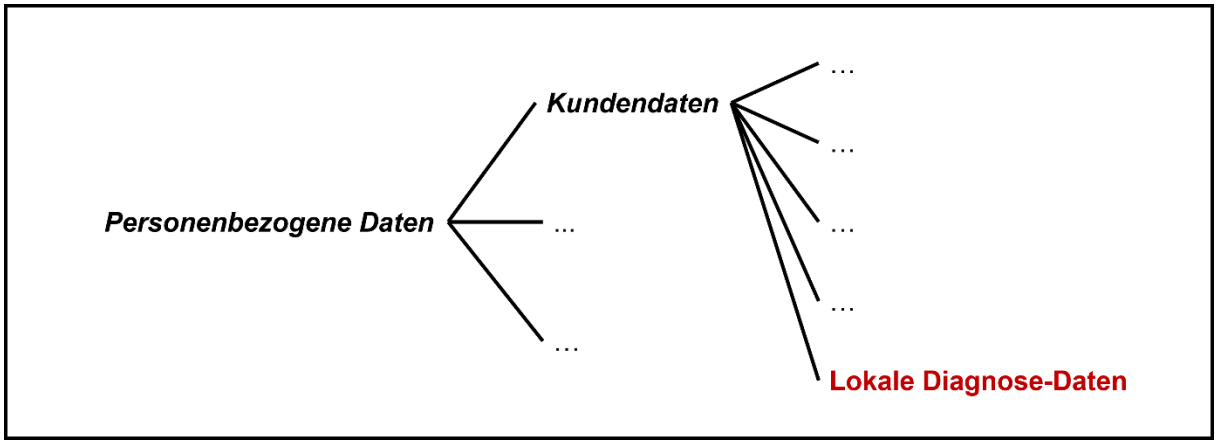

Abbildung 7: Kategorie Lokale Diagnose-Daten

Lokale Diagnose-Daten sind kundenspezifische Daten in lokalen Umgebungen von Kunden über die Nutzung von Anwendungen und zentralen Diensten. Die Grundlage für die Erzeugung von lokalen Diagnosedaten sind Daten, die in lokalen Umgebungen von Kunden bei der Nutzung von zentralen, von MS betriebenen Diensten sowie lokal installierten Anwendungen im Rahmen der Nutzung derselben anfallen bzw. erhoben werden. Die Erhebung von lokalen Diagnose-Daten erfolgt gemäß der Konfiguration des Kunden.

Ein Beispiel für Lokale Diagnose-Daten sind lokal auf Arbeitsplatzrechnern im Fehlerfall generierte und, sofern sie überhaupt gespeichert werden, dort gespeicherte Fehlerprotokolle.

MS hat keinen direkten Zugriff auf Lokale Diagnose-Daten und kann diese auch nicht unmittelbar verarbeiten. Insofern handelt es sich bei Lokalen Diagnose-Daten streng genommen auch nicht um Kundendaten, da sie MS nicht bereitgestellt werden. Allerdings bilden die Lokalen Diagnose-Daten die Grundlage zur Erzeugung von Diagnose-Daten. Daher erfolgt in der Taxonomie eine explizite Berücksichtigung der Kategorie Lokale Diagnose-Daten.

Entstehung

Während der Nutzung von lokalen und auf Systemen von Kunden bereitgestellten Anwendungen von MS werden Daten über die Nutzung der Anwendungen erhoben und zu Datensätzen zusammengeführt. Zu den hierzu verwendeten Daten zählen

(1) Daten über Aktionen wie das lokale Speichern einer Datei und
(2) Daten über Ereignisse wie das eines Fehlerfalls.

Übermittlung pseudonymisierter Lokaler Diagnose-Daten

Pseudonymisierte Lokale Diagnose-Daten werden – je nach Konfiguration des Kunden – erzeugt. Diese erzeugten Daten werden an MS übermittelt. Hierbei handelt es sich in der Folge um Diagnose-Daten.

Löschung

Die Löschung der Lokalen Diagnose-Daten obliegt dem Kunden.

IV. Professional Services-Daten

1) Überblick

Der Begriff der „*Professional Services-Daten*“ ist im DPA[158] wie folgt definiert:

„Professional Services-Daten bezeichnet alle Daten, einschließlich sämtlicher Text-, Ton-, Video-, Bilddateien oder Software, die Microsoft vom oder im Namen eines Kunden zur Verfügung gestellt werden (oder für die der Kunde Microsoft ermächtigt, sie von einem Produkt zu erlangen) oder die anderweitig von oder im Namen von Microsoft im Zuge einer Vereinbarung mit Microsoft über die Erlangung von Professional Services erlangt oder verarbeitet werden.“

Des Weiteren enthält das DPA[159] eine separate Definition des Begriffs der „Professional Services“, die wie folgt lautet:

„Professional Services bezeichnet die folgenden Dienstleistungen: (a) Beratungsdienste von Microsoft, bestehend aus der Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und aus Lösungs-/Softwareentwicklungsdiensten, die im Rahmen eines Microsoft Enterprise Services-Arbeitsauftrags, sofern in der Projektbeschreibung vereinbart, oder eines Cloud Workload Acceleration-Vertrags bereitgestellt werden, in den dieser DPA durch Verweis aufgenommen wird; und (b) technische Support-Services, die von Microsoft bereitgestellt werden und dem Kunden helfen, die Produkte betreffende Probleme zu identifizieren und zu beheben, einschließlich technischen Supports, der als Teil der Microsoft Unified Support oder Premier Support Services bereitgestellt wird, sowie alle anderen kommerziellen technischen Support-Services. Die Professional Services umfassen weder die Produkte noch, ausschließlich für die Zwecke des DPA, zusätzliche Professional Services.“

Demzufolge handelt es sich bei Professional Services entweder um Beratungs- (a) oder um Unterstützungsleistungen (b), die MS seinen Kunden erbringt. Die insoweit zur Leistungserbringung durch MS verarbeiteten Daten fallen in die Kategorie der Professional Services-Daten. Die folgende Abbildung 8 verdeutlicht die Einordnung

[158] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Definitionen, Seite 7.

[159] DPA in der Fassung vom 1. September 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14, Definitionen, Seite 6 f.

der Kategorie der Professional Services-Daten in die Kategorienhierarchie der Taxonomie.

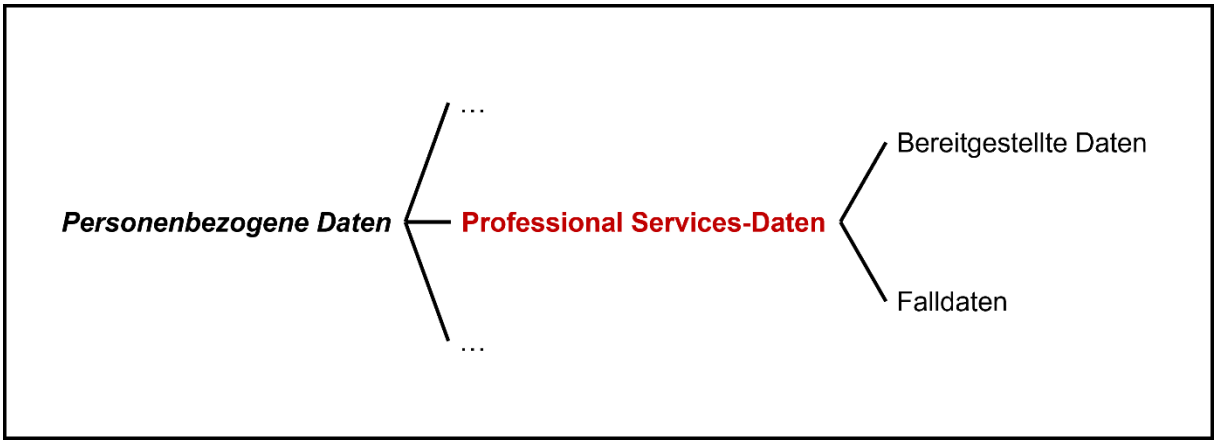

Abbildung 8: Kategorie Professional Services-Daten

Professional Services-Daten sind in die Unterkategorien Bereitgestellte Daten und Falldaten untergliedert. Diese beiden Unterkategorien werden in den folgenden beiden Unterkapiteln separat spezifiziert.

Soweit zur Inanspruchnahme von Professional Services durch den Kunden von MS bereitgestellte zentrale Dienste zum Einsatz kommen, werden analog zur Nutzung anderer Dienste im Rahmen der Nutzung solcher von MS bereitgestellten zentralen Dienste durch Kunden auch Bestandsdaten und Nutzungsdaten verarbeitet.

2) Bereitgestellte Daten

Definition

Der Begriff „*Bereitgestelle Daten*“ wird im DPA im Zuge der Definition von Professional Services-Daten nicht verwendet. Für eine differenzierte Betrachtung der Professional Services-Daten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Bereitgestellten Daten handelt es sich, wie in Abbildung 9 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der Professional Services-Daten.

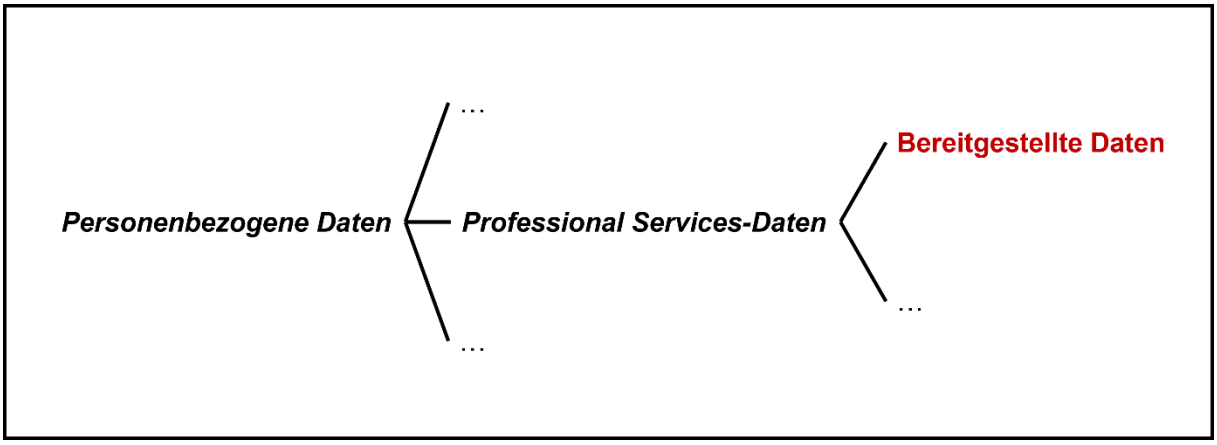

Abbildung 9: Kategorie Bereitgestellte Daten

In Bezug auf die im DPA enthaltene und in dieser Taxonomie verwendete Definition von Professional Services-Daten handelt es sich bei bereitgestellten Daten um diejenigen personenbezogenen Daten, deren Inhalt unmittelbar zur Erbringung der Professional Service-Dienstleistungen verarbeitet werden. Gemäß der Definition können Nutzende diese Daten entweder direkt bereitstellen oder einen Zugriff auf diese Daten einräumen.

Wie in der Definition von Professional Services-Daten angegeben, kann es sich bei Bereitgestellten Daten bspw. um Text-, Ton-, Video- und Bilddateien handeln. Hinzukommen können weitere, im Zusammenhang mit der konkreten Dienstleistung erforderliche Daten, wie etwa ausgetauschte Chat-Nachrichten.

Entstehung

Bereitgestellte Daten entstehen durch das Hochladen oder Bereitstellen der betreffenden Daten durch Nutzende des Kunden, die den jeweiligen Professional Service nutzen. Auch können Nutzende MS veranlassen, Daten zur Erbringung von Professional Services zu erheben.

In jedem Fall haben Kunden die Kontrolle, welche Daten sie hochladen, bereitstellen oder deren Erhebung sie veranlassen.

Löschung

In Abhängigkeit von der Art des in Anspruch genommenen Services und dem konkreten Auftrag werden Bereitgestellte Daten von MS gelöscht, sobald der Zweck der Bereitstellung erfüllt wurde.

Kunden haben die Möglichkeit, die Löschung bereitgestellter Daten früher zu veranlassen.

3) Falldaten

Definition

Der Begriff „*Falldaten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der Professional Services-Daten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Falldaten handelt es sich, wie in Abbildung 10 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der Professional Services-Daten.

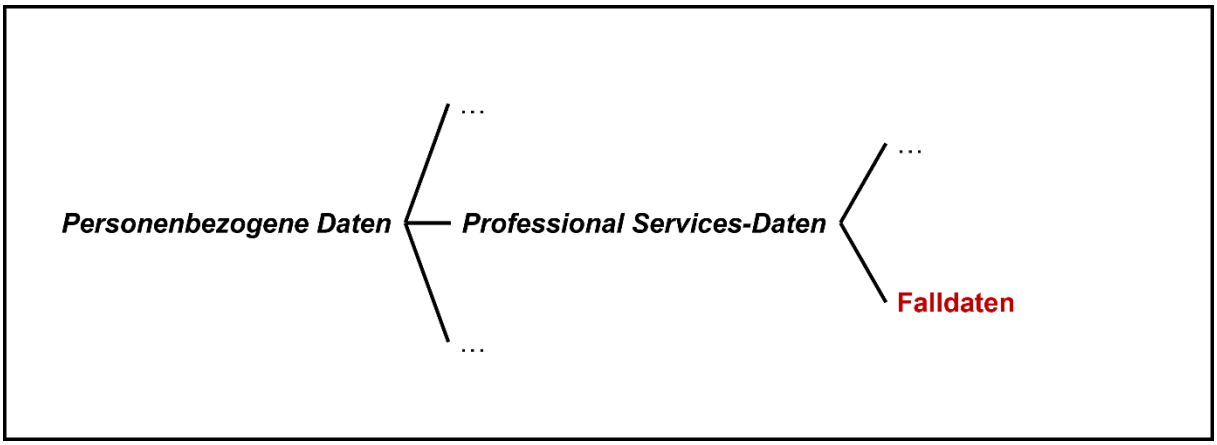

Abbildung 10: Kategorie Falldaten

Falldaten sind Professional Services-Daten, welche zur Erbringung von Professional Services-Dienstleistungen verarbeitet werden. Es handelt sich hierbei um Daten, die zu administrativen und operativen Zwecken der Dienstleistungserbringung erforderlich sind.

Ein Beispiel für Falldaten sind Kontaktdaten von Ansprechpartnern beim Kunden.

Löschung

In Abhängigkeit von der Art des in Anspruch genommenen Services und dem konkreten Auftrag löscht MS Falldaten, sobald der Zweck der Bereitstellung erfüllt wurde.

Kunden haben die Möglichkeit, die frühere Löschung von Falldaten zu veranlassen.

V. Von MS generierte, abgeleitete oder gesammelte Daten

1) Überblick

Der Begriff der „*von MS generierten, abgeleiteten oder gesammelten Daten*“ wird im DPA vereinzelt verwendet. Von zentraler Bedeutung ist die bereits in Kapitel „Lebenszyklus personenbezogener Daten“ referenzierte Erwähnung als eine der abschließenden drei in dieser Taxonomie verwendeten Unterkategorien der Kategorie Personenbezogene Daten.

Bei von MS generierten, abgeleiteten oder gesammelten Daten handelt es sich um Daten über die Nutzung von durch MS betriebenen zentralen Diensten und in lokalen Umgebungen von Kunden genutzten Anwendungen. Die folgende Abbildung 11 verdeutlicht die Einordnung der Kategorie der von MS generierten, abgeleiteten oder gesammelten Daten in die Kategorienhierarchie der Taxonomie.

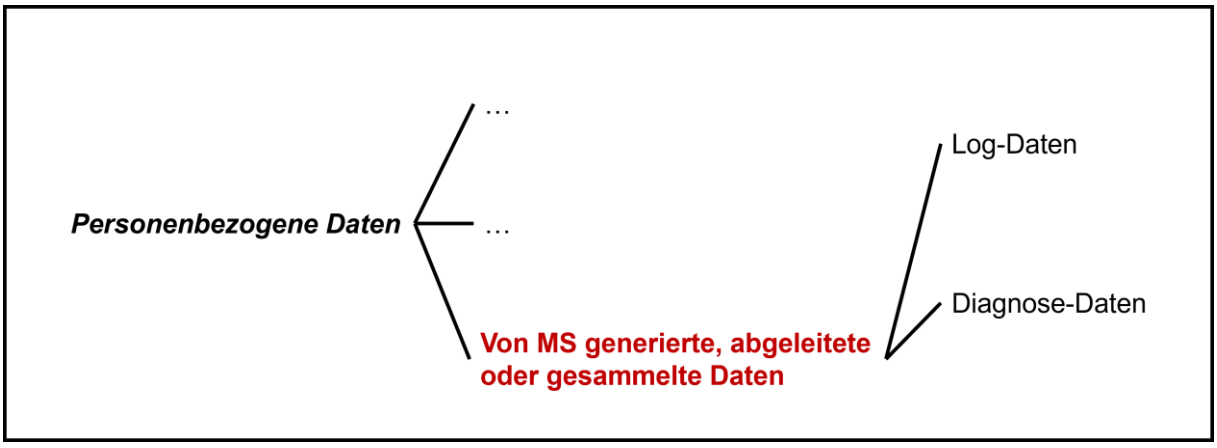

Abbildung 11: Kategorie Von MS generierte, abgeleitete oder gesammelte Daten

Die Unterscheidung zwischen in der zentralen Infrastruktur generierten, abgeleiteten oder gesammelten Daten und lokalen Daten dient als Kriterium zur Abgrenzung der Unterkategorien Log-Daten und Diagnose-Daten untereinander. Diese werden in den folgenden Unterkapiteln separat spezifiziert.

Die Speicherung der von MS generierten, abgeleiteten und gesammelten Daten erfolgt zusammengefasst in zentralen Speichersystemen von MS.

2) Log-Daten

Definition

Der Begriff „*Log-Daten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der von MS generierten, abgeleiteten oder gesammelten Daten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Log-Daten handelt es sich, wie in Abbildung 12 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen von MS generierten, abgeleiteten oder gesammelten Daten.

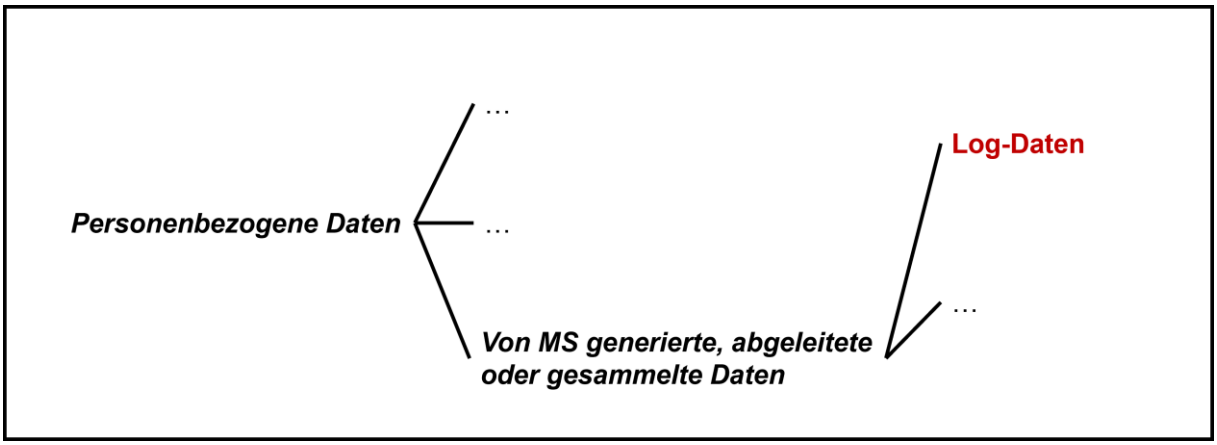

Abbildung 12: Kategorie Log-Daten

Log-Daten sind in der zentralen Infrastruktur von MS verarbeitete kundenspezifische personenbezogene Daten über die Nutzung von Diensten dieser Infrastruktur. Die Grundlage für die Erzeugung von Log-Daten sind Daten, die in der zentralen Infrastruktur von MS im Rahmen der Nutzung derselben durch den Kunden bzw. dessen Nutzende anfallen bzw. erhoben werden. Im Rahmen der Erhebung erfolgt eine Pseudonymisierung. Hierzu werden die resultierenden Log-Daten in eine Speicherinfrastruktur (im Sinne eines logischen Konstrukts) außerhalb der produktiven Dienst-Infrastruktur überführt.

Beispiele für Log-Daten sind in der zentralen Infrastruktur von MS generierte und im Anschluss bereinigte sowie pseudonymisierte Ereignis- oder Fehlerprotokolle von Diensten wie Exchange Online oder Teams.

Entstehung

Bei der Nutzung von durch MS betriebenen Diensten werden Daten über die Nutzung der Dienste generiert und zu Datensätzen zusammengeführt. Zu den hierzu verwendeten Daten zählen

(1) Daten über Aktionen wie das Speichern einer Datei und
(2) Daten über Ereignisse wie das eines Fehlerfalls.

Im Rahmen des Prozesses der Erhebung und Speicherung von Log-Daten werden diese pseudonymisiert. Die Speicherung in der zentralen Infrastruktur von MS und die anschließende Weiterverarbeitung erfolgen in pseudonymisierter Form.

Erstellung von R-Daten

Log-Daten werden von MS im Auftrag des Kunden aggregiert. Die hierdurch wirksam anonymisierten Daten – von MS als R-Daten bezeichnet – unterfallen nicht mehr dem Datenschutzrecht. Dementsprechend werden die aus der Anonymisierung resultierenden Daten und die nachfolgenden Verarbeitungen dieser im Rahmen dieser Taxonomie nicht betrachtet.

Löschung

Log-Daten werden nach spätestens 18 Monaten gelöscht. Eine vorherige Löschung erfolgt für den Fall, dass die jeweiligen Daten nicht mehr benötigt werden. Auch kann ein Kunde eine vorzeitige Löschung veranlassen, die spätestens nach 180 Tagen wirksam wird.

3) Diagnose-Daten

Definition

Der Begriff „*Diagnose-Daten*“ ist im DPA nicht definiert. Für eine differenzierte Betrachtung der von MS generierten, abgeleiteten oder gesammelten Daten und ihrer Verarbeitung ist jedoch eine Unterscheidung derselben in Form von Unterkategorien erforderlich. Bei Diagnose-Daten handelt es sich, wie in Abbildung 13 dargestellt, gemäß der Einordnung in die Kategorienhierarchie um eine Unterkategorie der personenbezogenen von MS generierten, abgeleiteten oder gesammelten Daten.

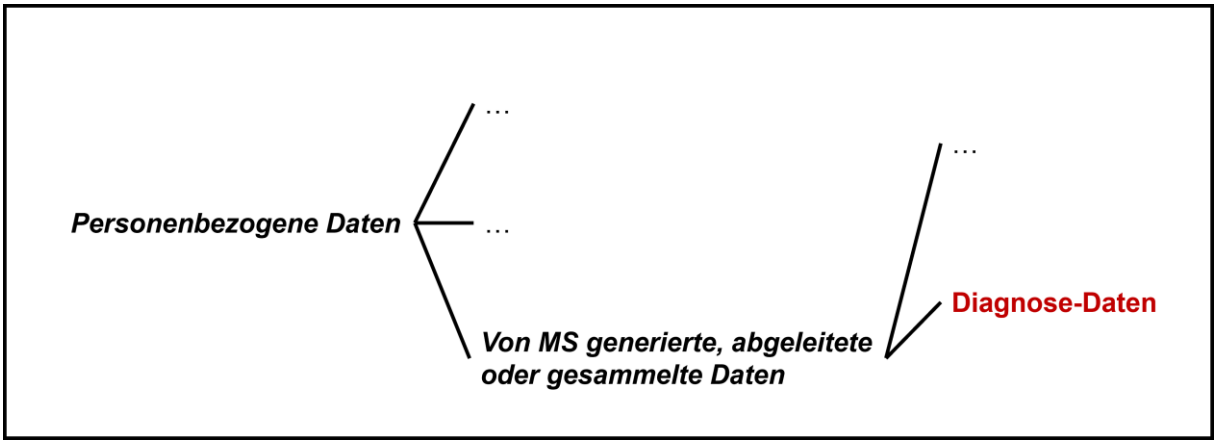

Abbildung 13: Kategorie Diagnose-Daten

Diagnose-Daten sind kundenspezifische Daten lokaler Umgebungen von Kunden über die Nutzung von Anwendungen und zentralen Diensten. Die Grundlage für die Erzeugung von Diagnose-Daten sind Lokale Diagnose-Daten.

Ein Beispiel für Diagnose-Daten sind im Fehlerfall auf Arbeitsplatzrechnern generierte Fehlerprotokolle, welche nach einer Bereinigung und Pseudonymisierung in die zentrale Infrastruktur von MS übermittelt werden.

Entstehung

Pseudonymisierte Lokale Diagnose-Daten werden – je nach Konfiguration des Kunden – erzeugt. Diese erzeugten Daten werden an MS übermittelt. Hierbei handelt es sich in der Folge um Diagnose-Daten, deren Speicherung außerhalb der produktiven Dienst-Infrastruktur erfolgt.

Erstellung von R-Daten

Diagnose-Daten werden von MS im Auftrag des Kunden aggregiert. Die hierdurch wirksam anonymisierten Daten – von MS als R-Daten bezeichnet – unterfallen nicht mehr dem Datenschutzrecht. Dementsprechend werden die aus der Anonymisierung resultierenden Daten und die nachfolgenden Verarbeitungen dieser im Rahmen dieser Taxonomie nicht betrachtet.

Löschung

Diagnose-Daten werden nach spätestens 18 Monaten gelöscht. Eine vorherige Löschung erfolgt für den Fall, dass die jeweiligen Daten nicht mehr benötigt werden. Auch kann ein Kunde eine vorzeitige Löschung veranlassen, die spätestens nach 180 Tagen wirksam wird.

Anlage 4:

Datenschutzrechtliche Anforderungen an Datenverarbeitungsverfahren

Um M365 datenschutzkonform betreiben zu können, sind neben den spezifischen Handlungsempfehlungen für M365 auch die allgemein nach der DS-GVO dem Verantwortlichen obliegenden Pflichten einzuhalten. Als Hilfestellung und Orientierung für diese allgemein zu erfüllenden Pflichten stellt der HBDI den folgenden Fragebogen „Umsetzung datenschutzrechtlicher Anforderungen an Datenverarbeitungsverfahren“ zur Verfügung. Die Beantwortung der in ihm aufgeworfenen Fragestellungen dient zunächst der Evaluierung des Datenschutzniveaus eines DV-Verfahrens durch den Verfahrensverantwortlichen selbst. Auf Nachfrage der Aufsichtsbehörde sollten die Verfahrensverantwortlichen hierzu auskunftsfähig sein und etwaig erforderliche Dokumentationen vorlegen können.

1. Auf welche Rechtsgrundlage für die Verarbeitung personenbezogener Daten aus der DS-GVO in Verbindung mit dem einschlägigen Fachrecht stützt sich das DV-Verfahren, vgl. Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 DS-GVO („**Rechtmäßigkeit der Verarbeitung**“)?[160]
2. Werden im Rahmen des DV-Verfahrens nur solche personenbezogenen Daten erhoben, die zur Erreichung des verfolgten Zwecks (dies richtet sich nach dem einschlägigen Fachrecht) erforderlich sind, vgl. Art. 5 Abs. 1 Buchst. b und Buchst. c DS-GVO („**Zweckbindung und Datenminimierung**“)?
3. Wie wird sichergestellt, dass die innerhalb des DV-Verfahrens verarbeiteten personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, vgl. Art. 5 Abs. 1 Buchst. d DS-GVO („**Richtigkeit**“)?
4. Wurde für das DV-Verfahren ein Konzept zur Löschung der personenbezogenen Daten erstellt, vgl. Art. 5 Abs. 1 Buchst. e und 17 DS-GVO („**Speicherbegrenzung**“)?

[160] EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Stand: März 2025, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en.

5. Wurde ein Prozess zum Betroffenenrechte-Management festgelegt, vgl. Art. 5 Abs. 1 Buchst. a und 12, 15 – 23 DS-GVO („**Transparenz und Verarbeitung nach Treu und Glauben**“)?[161]

6. Wurde ein Prozess zur Erfüllung der Informationspflichten festgelegt, vgl. Art. 5 Abs. 1 Buchst. a und 13, 14 DS-GVO („**Transparenz**“)?[162]

7. Wurde der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen beachtet, vgl. Art. Art. 5 Abs. 1 Buchst. f und 25 DS-GVO („**Integrität und Vertraulichkeit**“)?[163]

8. Wurden unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen[164] geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, vgl. Art. 5 Abs. 1 Buchst. f und 32 DS-GVO („**Integrität und Vertraulichkeit**“)?[165]

   i. Wurde ein Zugriffs- und Berechtigungskonzept erstellt?

   ii. Wurden Maßnahmen zur Eingabekontrolle ergriffen (Protokollierung)?

---

[161] Vgl. hierzu die folgenden Kurzpapiere der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Kurzpapier Nr. 6 „Auskunftsrecht der betroffenen Personen, Artikel 15 DS-GVO“, Kurzpapier Nr. 11 „Recht auf Löschung/“Recht auf Vergessenwerden“, https://www.datenschutzkonferenz-online.de/kurzpapiere.html, und die Veröffentlichung des EDSA, Guidelines 01/2022 on data subject rights – Right of access Version 2.1, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

[162] Vgl. hierzu das folgende Kurzpapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Kurzpapier Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“ und die Veröffentlichung des EDSA, Leitlinien für Transparenz gemäß Verordnung 2016/679, WP 260 rev. 01, https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html.

[163] Vgl. EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Version 2.0, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.

[164] Vgl. DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18 https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

[165] DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, https://www.datenschutzkonferenz-online.de/kurzpapiere.html; EDSA, Guidelines 01/2025 on Pseudonymisation, Stand März 2025, https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf sowie EDSA, Summary: pseudonymisation, when and how to apply it, https://www.edpb.europa.eu/system/files/2025-02/edpb_summary_202501_pseudonymisation_en.pdf.

iii. Wurden Maßnahmen zum Schutz vor unberechtigten Zugriffen durch Dritte ergriffen?

iv. Wurde eine Betrachtung der Risiken für Rechte und Freiheiten der betroffenen Personen und eine Analyse des erforderlichen Schutzniveaus durchgeführt?[166]

v. Gibt es ein IT-Sicherheitskonzept?

vi. Wurde ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert?

9. Wurde für das DV-Verfahren ein Verzeichnis der Verarbeitungstätigkeit nach Art. 30 DS-GVO erstellt?[167]

10. Wurde für das DV-Verfahren eine Datenschutz-Folgenabschätzung nach Art. 35 und 36 DS-GVO durchgeführt?[168]

    i. Falls nein, wurde dokumentiert, warum keine Datenschutz-Folgenabschätzung erforderlich ist?

11. Wurde ein Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 und 33, 34 DS-GVO bei der richtigen Datenschutzbehörde[169] etabliert?[170]

---

[166] Vgl. DSK, „Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

[167] Vgl. hierzu die Hinweise und Muster auf der Webseite des HBDI, https://datenschutz.hessen.de/infothek/hinweise-und-muster-zur-ds-gvo.

[168] Vgl. DSK, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Kurzpapier Nr. 5, https://www.datenschutzkonferenz-online.de/kurzpapiere.html; EDSA, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt, WP 248 Rev. 01, https://www.datenschutz-bayern.de/technik/orient/wp248.pdf.

[169] EDSA, Leitlinien 8/2022 für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202208_identifying_lsa_targeted_update_de.pdf.

[170] Vgl. hierzu etwa das Meldeverfahren auf der Webseite des HBDI: Meldungen von Verletzungen des Schutzes personenbezogener Daten durch Verantwortliche, https://datenschutz.hessen.de/service/meldung-nach-art-33-ds-gvo; Kurzübersicht EDPB (EDSA) Guidelines 9/2022 on personal data breach notification under GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en.

12. Wurden die am DV-Verfahren Beteiligten den in der DS-GVO definierten Rollen „Verantwortlicher, Gemeinsame Verantwortliche, Auftragsverarbeiter, Empfänger, Dritter und Betroffener“ zugeordnet, vgl. Art. 4 Nr. 1, 7, 8, 9 und 10 DS-GVO?[171]

13. Soweit für die am DV-Verfahren Beteiligten die Voraussetzungen der Art. 26 und 28 DS-GVO (d.h. „Gemeinsame Verantwortlichkeit oder Auftragsverarbeitung) vorliegen, wurden Verträge oder andere Rechtsinstrumente nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats geschaffen, die den Beteiligten Datenschutzpflichten im Sinne der Art. 26 und 28 DS-GVO auferlegen?[172]

14. Wurde ein Prozess zur regelmäßigen Überprüfung, Bewertung und Evaluierung der zuvor beschriebenen datenschutzrechtlichen Anforderungen (Datenschutzmanagementsystem) in Hinblick auf das DV-Verfahren implementiert, vgl. Art. 5 Abs. 2 DS-GVO („Rechenschaftspflicht“)?

15. Wurde geprüft, ob für die geplante Datenverarbeitung die Voraussetzungen des Kapitel V der DS-GVO beachtet wurden (Problematik etwaiger Drittstaatentransfers)?[173]

    Mögliche Instrumente zur Legitimation eines Drittstaatendatentransfers:

    i. Angemessenheitsbeschluss der Europäischen Kommission (d.h. ein Land außerhalb der Europäischen Union verfügt über ein anerkanntes, angemessenes Datenschutzniveau, die Europäische Kommission führt hierzu eine Liste)[174]

---

[171] Vgl. hierzu DSK, Auftragsverarbeitung, Art. 28 DS-GVO, Kurzpapier Nr. 13, und DSK, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Kurzpapier Nr. 16 (beide derzeit in Überarbeitung), https://www.datenschutzkonferenz-online.de/kurzpapiere.html; EDSA, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (auch auf Deutsch verfügbar), EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

[172] Vgl. hierzu die Hinweise und Muster auf der Webseite des HBDI, https://datenschutz.hessen.de/infothek/hinweise-und-muster-zur-ds-gvo, und auf der Webseite des LfDI Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/.

[173] Dieses Thema bedarf insbesondere beim Einsatz von Cloud-Technologien besonderer Beachtung, vgl. insgesamt zu der Thematik, https://datenschutz.hessen.de/datenschutz/internationales.

[174] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission.

- Das EU-US-Privacy Shield war ein Abkommen i. S. e. Angemessenheitsbeschlusses, das vom EuGH für ungültig erklärt wurde.[175]
- Das Folge-Abkommen, das EU-US Data Privacy Framework, wurde am 10. Juli 2023 beschlossen[176]
- US-Unternehmen können ihre Teilnahme am Datenschutzrahmen EU-USA im Rahmen einer Zertifizierung bescheinigen, indem sie sich zur Einhaltung detaillierter Datenschutzpflichten verpflichten[177]
- Dieses Abkommen könnte jedoch wieder vor dem EuGH angegriffen werden, zudem sind die Auswirkungen der derzeitigen US-amerikanischen Administration auf das Abkommen noch unklar.

ii. Binding Corporate Rules[178] (Datenübermittlung innerhalb einer Unternehmensgruppe)

iii. Standardvertragsklauseln (Datenübermittlung aufgrund eines Vertrags)[179]

iv. Ggf. sind aufgrund des EuGH-Urteils in Sachen Schrems II zusätzliche Maßnahmen für Bindung Corporate Rules und Standardvertragsklauseln zu ergreifen.[180]

v. Für die Übermittlung personenbezogener Daten an eine Behörde eines Drittlandes muss Art. 48 DS-GVO beachtet werden.[181]

---

[175] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-us-datentransfer-privacy-shield, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html.

[176] Siehe https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752; Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 4. September 2023.

[177] EU Kommission, Fragen und Antworten: Datenschutzrahmen EU-USA, https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752; EDSA, Guidelines 07/2022 on certification as a tool for transfer, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en.

[178] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/binding-corporate-rules-bcr, EDSA, Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)“, https://www.edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf.

[179] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-standarddatenschutzklauseln.

[180] Siehe https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/zusaetzliche-massnahmen-infolge-des-urteils-schrems-ii.

[181] EDSA, Guidelines 02/2024 on Article 48 GDPR, Stand 03/2025, https://www.edpb.europa.eu/system/files/2025-06/edpb_guidelines_202402_article48_v2_en.pdf.