

# Datenschutznachtrag für Produkte und Services von Microsoft

Letzte Aktualisierung: 1. September 2025

## Inhaltsverzeichnis

---

Zusammenfassung der Änderungen.....	2
Einleitung.....	2
Anwendbare DPA-Bestimmungen und -Aktualisierungen.....	3
Elektronische Benachrichtigungen.....	4
Frühere Versionen .....	4
Definitionen.....	5
Allgemeine Bestimmungen .....	8
Einhaltung von gesetzlichen Regelungen .....	8
Datenschutzbestimmungen .....	8
Umfang.....	8
Art der Datenverarbeitung; Eigentumsverhältnisse .....	9
Offenlegung verarbeiteter Daten .....	11
Verarbeitung personenbezogener Daten; DSGVO.....	12
Datensicherheit .....	15
Meldung von Sicherheitsvorfällen.....	18
Datenübermittlungen und Speicherort.....	19
Speicherung und Löschung von Daten .....	21
Vertraulichkeitsverpflichtung des Auftragsverarbeiters .....	22
Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern.....	22
Previews .....	24
Bildungseinrichtungen.....	25
CJIS-Kundenvertrag.....	25

---

HIPAA-Geschäftspartner .....	25
Telekommunikationsdaten.....	26
Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA) .....	26
Biometrische Daten.....	27
Zusätzliche Professional Services.....	27
Kontaktaufnahme mit Microsoft.....	27
Anhang A – Sicherheitsmaßnahmen .....	29
Domäne.....	29
Praktiken .....	29
Anhang B – Betroffene Personen und Kategorien personenbezogener Daten.....	36
Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen.....	39
Anhang D – Anfechtung einer Anordnung oder einer verbindlichen rechtlichen Verpflichtung zur Aussetzung von Onlinediensten .....	42
Anlage 1 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union .....	43
Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33.....	43

## Zusammenfassung der Änderungen

---

01.09.2025 – Die Europäische Freihandelsassoziation (EFTA) wurde zu den Standorten hinzugefügt, an denen Microsoft Kundendaten und personenbezogene Daten speichert und verarbeitet sowie ruhende Professional Services-Daten für EU-Datengrenzen-Dienste speichert. Dem Abschnitt zu den Telekommunikationsdaten wurde eine Formulierung hinzugefügt, die auf die Verpflichtung des Kunden hinweist, die Zustimmung des Endbenutzers einzuholen. Es wurde Text zur EU-Datenverordnung hinzugefügt. In Anhang D wurde Text bezüglich der Verpflichtung von Microsoft hinsichtlich der digitalen Resilienz in der EU hinzugefügt.

## Einleitung

---

Die Parteien stimmen überein, dass dieser Datenschutznachtrag für Produkte 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. Das DPA wird durch Bezugnahme in die Produktbestimmungen und andere Microsoft-Verträge aufgenommen. 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. Für die Nutzung von nicht von Microsoft stammenden Produkten durch den Kunden gelten gesonderte Bestimmungen einschließlich Datenschutz- und Sicherheitsbestimmungen.

Bei Konflikten oder Widersprüchen zwischen den DPA-Bestimmungen und anderen Bestimmungen des Volumenlizenzvertrags des Kunden oder anderer anwendbarer Verträge in Verbindung mit den Produkten und Services („Kundenvertrag“) haben die DPA-Bestimmungen Vorrang. Die DPA-Bestimmungen haben Vorrang vor anderslautenden Bestimmungen in der Datenschutzerklärung von Microsoft, die ansonsten möglicherweise für die Verarbeitung von Kundendaten, personenbezogenen Daten oder Professional Services-Daten (Begriffe gemäß den Definitionen in diesem DPA) gelten.

Microsoft geht die in diesem DPA beschriebenen Verpflichtungen gegenüber allen Kunden mit einem bestehenden Kundenvertrag ein. Diese Verpflichtungen sind für Microsoft in Bezug auf den Kunden bindend, unabhängig (1) von den Produktbestimmungen, die ansonsten für ein bestimmtes Produkt-Abonnement oder eine Lizenz gelten, und (2) von anderen Verträgen, die auf die Produktbestimmungen verweisen.

## Anwendbare DPA-Bestimmungen und -Aktualisierungen

### Beschränkungen für Aktualisierungen

Wenn der Kunde ein Produktabonnement verlängert oder ein neues Abonnement kauft oder einen Arbeitsauftrag für Professional Services eingeht, gelten die jeweils aktuellen DPA-Bestimmungen und werden während des Abonnements des Kunden für dieses Produkt oder die Laufzeit für diesen Professional Service nicht geändert. Wenn der Kunde eine zeitlich unbeschränkte Lizenz für die Software erwirbt, gelten die jeweils aktuellen DPA-Bestimmungen (nach den gleichen Bestimmungen zur Festlegung der jeweils geltenden Produktbedingungen für diese Software im Kundenvertrag) und ändern sich während der Laufzeit der Lizenz des Kunden für diese Software nicht.

### Neue Features, Ergänzungen oder zugehörige Software

Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen gilt, falls Microsoft neue Features, Angebote, Ergänzungen oder neue zugehörige Software einführt (d. h. die zuvor nicht

in den Produkten oder Services enthalten waren), dass Microsoft dann Bestimmungen im DPA einführen oder Aktualisierungen am DPA vornehmen kann, die sich auf die Verwendung dieser neuen Features, Angebote, Ergänzungen oder zugehörigen Software durch den Kunden beziehen. Wenn diese Bestimmungen wesentlich nachteilige Änderungen an den DPA-Bestimmungen enthalten, bietet Microsoft dem Kunden die Wahl, die neuen Features, Angebote, Ergänzungen oder zugehörige Software zu nutzen, ohne dass eine vorhandene Funktionalität eines allgemein verfügbaren Produkts oder Professional Services verloren geht. Wenn der Kunde die neuen Features, Angebote, Ergänzungen oder zugehörige Software nicht installiert oder nutzt, finden die entsprechenden neuen Bestimmungen keine Anwendung.

## Behördliche Vorschriften und Verpflichtungen

Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen gilt, dass Microsoft berechtigt ist, Produkte oder Professional Services in Ländern oder Rechtsordnungen zu ändern oder zu kündigen, in denen eine derzeitige oder künftige behördliche Vorschrift oder Verpflichtung besteht, die (1) Microsoft einer Vorschrift oder einer Auflage unterwirft, die nicht allgemein auf dort tätige Unternehmen anwendbar ist, (2) Microsoft die Fortsetzung des Betriebs der Produkte oder des Angebots der Professional Services ohne Änderung erschwert und/oder (3) Microsoft zu der Annahme veranlasst, dass die DPA-Bestimmungen oder die Produkte oder Professional Services möglicherweise im Widerspruch zu einer solchen Vorschrift oder Verpflichtung stehen.

## Elektronische Benachrichtigungen

Microsoft kann Kunden Informationen und Mitteilungen über Produkte und Services elektronisch, auch per E-Mail, über das Portal eines Onlinedienstes oder über eine von Microsoft zu benennende Website zur Verfügung stellen. Eine Benachrichtigung gilt an dem Datum als erteilt, an dem diese von Microsoft zur Verfügung gestellt wurde.

## Frühere Versionen

Die DPA-Bestimmungen gelten für aktuell verfügbare Produkte und Professional Services. Kunden können frühere Versionen der DPA-Bestimmungen unter <https://aka.ms/licensingdocs> abrufen oder beim zuständigen Handelspartner oder Microsoft-Kundenbetreuer anfordern.

## Definitionen

---

Definierte Begriffe, die in diesem DPA verwendet, jedoch nicht in diesem DPA selbst definiert werden, besitzen die im Kundenvertrag angegebene Bedeutung. In diesem DPA werden die folgenden definierten Begriffe verwendet:

„Datenschutzvorschriften“ umfasst die DSGVO, lokale EU-/EWR-Datenschutzgesetze sowie alle anwendbaren Gesetze, Verordnungen und sonstigen gesetzlichen Bestimmungen in Bezug auf (a) Datenschutz und Datensicherheit und (b) Nutzung, Erhebung, Aufbewahrung, Speicherung, Sicherheit, Offenlegung, Übermittlung, Entsorgung und die sonstige Verarbeitung personenbezogener Daten.

„DPA-Bestimmungen“ sind die Bestimmungen in diesem DPA sowie alle produktspezifischen Bedingungen in den Produktbestimmungen, die speziell die Datenschutz- und Sicherheitsbestimmungen in dem DPA für ein spezifisches Produkt (oder ein Feature eines Produkts) ergänzen oder ändern. Bei Konflikten oder Widersprüchen zwischen dem DPA und solchen produktspezifischen Bedingungen sind die produktspezifischen Bedingungen für das jeweilige Produkt (oder das Feature des jeweiligen Produkts) vorrangig.

„DSGVO“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

„DSGVO-Bestimmungen“ bezieht sich auf die Bestimmungen in Anlage 1, in der Microsoft verbindliche Zusagen in Bezug auf die Verarbeitung personenbezogener Daten nach Artikel 28 DSGVO gibt.

„EU-Kunde“ bezeichnet einen Kunden, der eine Rechnungsadresse im Europäischen Wirtschaftsraum („EWR“) hat.

„EU-Datenverordnung“ bezeichnet die Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2020/1828 (Datenverordnung).

„EU-Datenverordnungsdienst“ bezeichnet einen Onlinedienst, der an einen EU-Kunden lizenziert ist, ausgenommen einen Onlinedienst, für den der EU-Kunde sich dafür entschieden hat, Kundendaten außerhalb des EWR zu speichern.

„Exportierbare Daten und digitale Vermögenswerte“ bezeichnet Kundendaten. Zur Klarstellung: Exportierbare Daten und digitale Vermögenswerte umfassen keine Geschäftsgeheimnisse oder geistiges Eigentum von Microsoft oder Daten, die die Sicherheit oder Integrität der Onlinedienste gefährden könnten.

„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.

„Lokale EU-/EWR-Datenschutzgesetze“ bezeichnet alle untergeordneten Gesetze und Vorschriften zur Umsetzung der DSGVO.

„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.

„Preview-Daten“ bezeichnet Kundendaten oder Personenbezogene Daten, die Microsoft vom oder im Namen des Kunden durch die Nutzung einer Preview bereitgestellt werden oder durch die Nutzung einer Preview generiert werden.

„Produkt“ hat die im Volumenlizenzvertrag vorgesehene Bedeutung. Zur einfacheren Bezugnahme umfasst „Produkt“ Onlinedienste und Software, die jeweils im Volumenlizenzvertrag definiert sind.

„Produkte und Services“ bezeichnet Produkte und Professional Services. Die Verfügbarkeit von Produkten und Professional Services kann je nach Region variieren und die Anwendbarkeit dieses DPA auf bestimmte Produkte und Professional Services unterliegt den Beschränkungen im Abschnitt „Umfang“ dieses DPA.

„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.

„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.

„Standardvertragsklauseln von 2021“ bezeichnet die Standarddatenschutzklauseln (Auftragsverarbeiter-zu-Auftragsverarbeiter-Modul) zwischen Microsoft Ireland Operations Limited und Microsoft Corporation für die Übermittlung personenbezogener Daten von Auftragsverarbeitern im EWR an Auftragsverarbeiter, die in Drittländern ansässig sind, die kein angemessenes Datenschutzniveau gewährleisten, wie in Artikel 46 der DSGVO beschrieben und von der Europäischen Kommission mit Beschluss 2021/914/EG vom 4. Juni 2021 genehmigt.

„Unterauftragsverarbeiter“ bezeichnet sonstige Auftragsverarbeiter, die Microsoft zur Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten hinzuzieht, wie in Artikel 28 der DSGVO beschrieben.

„Wechsel“ bezeichnet die einmalige Übertragung von exportierbaren Daten und digitalen Vermögenswerte durch einen EU-Kunden aus einem EU-Datenverordnungsdienst an einen vom EU-Kunden benannten Cloud-Dienstleister, der nicht zu Microsoft gehört und dessen Informationen der EU-Kunde Microsoft bereitstellt, oder an die lokale IKT-Umgebung des EU-Kunden, wenn der EU-Kunde sein Abonnement kündigt und die Nutzung des EU-Datenverordnungsdienstes beendet.

„Zusätzliche Professional Services“ bezeichnet Supportanfragen, die vom Support an ein Produktentwicklungsteam zur Lösung eskaliert werden, sowie andere Beratung und Unterstützung von Microsoft, die in Verbindung mit Produkten oder einem Volumenlizenzvertrag geleistet werden, ohne dass sie in der Definition von Professional Services enthalten sind.

In diesem DPA verwendete Begriffe, die nicht definiert werden, wie „Verletzung des Schutzes personenbezogener Daten“, „Verarbeitung“, „Verantwortlicher“, „Profiling“, „personenbezogene

Daten“ und „betroffene Person“ haben die Bedeutung gemäß Artikel 4 DSGVO, unabhängig davon, ob die DSGVO anwendbar ist.

## Allgemeine Bestimmungen

---

### Einhaltung von gesetzlichen Regelungen

Microsoft befolgt alle für die Bereitstellung der Produkte und Services durch Microsoft geltenden Gesetze und Vorschriften, einschließlich Gesetzen zu Meldepflichten bei Sicherheitsverletzungen, sowie Datenschutzvorschriften. Microsoft ist jedoch nicht für die Einhaltung von Gesetzen oder Regelungen verantwortlich, die für den Kunden oder seine Branche gelten, jedoch nicht allgemein für Serviceprovider im Bereich Informationstechnologie. Microsoft ermittelt nicht, ob Kundendaten Informationen enthalten, die spezifischen Gesetzen oder Vorschriften unterliegen. Alle Sicherheitsvorfälle unterliegen den Bestimmungen für die Meldung von Sicherheitsvorfällen weiter unten.

Der Kunde muss alle Gesetze und Regelungen einhalten, die für dessen Nutzung von Produkten und Services gelten, einschließlich Gesetzen zu biometrischen Daten, zur Vertraulichkeit von Kommunikation, sowie Datenschutzvorschriften. Der Kunde ist dafür verantwortlich, zu ermitteln, ob die Produkte und Services für die Speicherung und Verarbeitung von Informationen, die spezifischen Gesetzen oder Vorschriften unterliegen, geeignet sind, und muss die Produkte und Services in einer Weise nutzen, die mit den gesetzlichen und regulatorischen Verpflichtungen des Kunden im Einklang steht. Der Kunde ist für die Beantwortung von Anfragen Dritter bezüglich der Nutzung von Produkten und Services durch den Kunden verantwortlich, z. B. die Aufforderung, Inhalte zu entfernen, die dem Digital Millennium Copyright Act der USA oder anderen anwendbaren Gesetzen unterliegen.

## Datenschutzbestimmungen

---

### Umfang

Die DPA-Bestimmungen gelten für alle Produkte und Services mit Ausnahme der in diesem Abschnitt beschriebenen Fälle.

Die DPA-Bestimmungen gelten nicht für Produkte oder Professional Services, soweit sie in den Produktbestimmungen oder im jeweiligen Arbeitsauftrag ausdrücklich als ausgeschlossen gekennzeichnet werden; für diese Produkte oder Professional Services gelten die Datenschutz-

und Sicherheitsbedingungen in den jeweiligen Produktbestimmungen bzw. der Bestimmungen des jeweiligen Arbeitsauftrags.

Zur Klarstellung wird angemerkt, dass die DPA-Bestimmungen nur für die Verarbeitung von Daten in Umgebungen gelten, die von Microsoft und den Unterauftragsverarbeitern von Microsoft kontrolliert werden. Dies umfasst Daten, die von Produkten und Services an Microsoft gesendet werden, jedoch keine Daten, die in den Räumlichkeiten des Kunden oder in vom Kunden ausgewählten Betriebsumgebungen von Drittanbietern verbleiben.

Für Zusätzliche Professional Services geht Microsoft nur die Verpflichtungen im Abschnitt „Zusätzliche Professional Services“ unten ein.

## Art der Datenverarbeitung; Eigentumsverhältnisse

Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und vorbehaltlich der weiter unten beschriebenen Einschränkungen verwenden und anderweitig verarbeiten, (a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Weisungen 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. Dieser Absatz berührt nicht die Rechte von Microsoft an Software oder Services, für die Microsoft dem Kunden eine Lizenz gewährt.

## Verarbeitung zur Bereitstellung der Produkte und Services für Kunden

Für die Zwecke dieses DPA umfasst die „Bereitstellung“ eines Produkts Folgendes:

- Die Bereitstellung von Funktionen wie vom Kunden und dessen Benutzern lizenziert, konfiguriert und verwendet, einschließlich der Bereitstellung personalisierter Benutzererfahrungen,
- Die Fehlerbehebung (Verhinderung, Erkennung und Behebung von Problemen); und
- Produkte auf dem neuesten Stand und leistungsfähig zu halten und Förderung der Benutzerproduktivität, Zuverlässigkeit, Effektivität, Qualität und Sicherheit.

Für die Zwecke dieses DPA versteht man unter der „Bereitstellung“ der Professional Services Folgendes:

- Die Bereitstellung der Professional Services, einschließlich technischem Support, professioneller Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und Lösungs-/ Softwareentwicklungsdiensten,
- Die Fehlerbehebung (Verhindern, Erkennen, Untersuchen, Abschwächen und Beheben von Problemen, einschließlich Sicherheitsvorfällen und Problemen, die bei der Bereitstellung von Professional Services in den Professional Services oder relevanten Produkten festgestellt wurden) und
- die Förderung der Bereitstellung, Wirksamkeit, Qualität und Sicherheit von Professional Services und den zugrunde liegenden Produkten basierend auf Problemen, die bei der Bereitstellung von Professional Services festgestellt wurden, einschließlich der Behebung von Softwarefehlern und der anderweitigen Aufrechterhaltung der Aktualität und Leistungsfähigkeit der Produkte und Services.

In jedem Fall erfolgt die Bereitstellung der Produkte und Services unter Berücksichtigung der datenschutzrechtlichen Sicherheitspflichten.

Bei der Bereitstellung von Produkten und Services wird Microsoft Kundendaten, Professional Services-Daten oder personenbezogene Daten nicht verwenden oder anderweitig verarbeiten für: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) Marktforschung zur Entwicklung neuer Funktionen, Dienstleistungen oder Produkte oder zu anderen Zwecken; es sei denn, eine solche Verwendung oder Verarbeitung erfolgt in Übereinstimmung mit den dokumentierten Weisungen des Kunden.

## Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind

Für die Zwecke dieses DPA bezeichnet „Geschäftstätigkeit“ die vom Kunden in diesem Abschnitt autorisierten Verarbeitungsvorgänge.

Der Kunde autorisiert Microsoft:

- zur Erstellung aggregierter statistischer, nicht personenbezogener Daten aus Daten, die pseudonymisierte Identifikatoren enthalten (wie etwa Nutzungsprotokolle, die eindeutige, pseudonymisierte Identifikatoren enthalten) und
- zur Berechnung von Statistiken bezogen auf Kundendaten oder Professional Services-Daten

in jedem Fall ohne auf den Inhalt von Kundendaten oder Professional Services-Daten zuzugreifen oder diese zu analysieren und beschränkt auf die Erreichung der folgenden Zwecke, jeweils soweit durch die Bereitstellung der Produkte und Services für den Kunden veranlasst.

Diese Zwecke sind:

- Abrechnungs- und Kontoverwaltung,
- Vergütung wie etwa Berechnung von Mitarbeiterprovisionen und Partner-Incentives,
- Interne Berichterstattung und Geschäftsmodellierung wie etwa Prognose, Umsatz, Kapazitätsplanung und Produktstrategie und
- Finanzberichterstattung.

Bei der Verarbeitung für diese Geschäftstätigkeiten wendet Microsoft die Grundsätze der Datenminimierung an und verwendet oder verarbeitet keine Kundendaten, Professional Services-Daten oder personenbezogenen Daten für: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke. Darüber hinaus unterliegt die Verarbeitung für Geschäftstätigkeiten, wie alle Verarbeitungen im Rahmen dieses DPA, den Vertraulichkeitsverpflichtungen von Microsoft und den Verpflichtungen unter Offenlegung verarbeiteter Daten.

## Offenlegung verarbeiteter Daten

Microsoft wird verarbeitete Daten nicht offenlegen oder zugänglich machen, außer: (1) wie vom Kunden angewiesen; (2) wie in diesem DPA beschrieben oder (3) wie gesetzlich vorgeschrieben. Für die Zwecke dieses Abschnitts bezeichnet „verarbeitete Daten“ Folgendes: (a) Kundendaten, (b) Professional Services-Daten, (c) personenbezogene Daten und (d) alle anderen von Microsoft im Zusammenhang mit den Produkten und Diensten verarbeiteten Daten, die vertrauliche Informationen des Kunden nach dem Kundenvertrag sind. Jegliche Verarbeitung von verarbeiteten Daten unterliegt der Verpflichtung von Microsoft zur Vertraulichkeit im Rahmen des Kundenvertrags.

Microsoft wird verarbeitete Daten gegenüber Strafverfolgungsbehörden nur offenlegen bzw. den Zugriff darauf ermöglichen, wenn dies gesetzlich vorgeschrieben ist. Wenn sich eine Strafverfolgungsbehörde mit Microsoft in Verbindung setzt und verarbeitete Daten anfordert, wird Microsoft versuchen, die Strafverfolgungsbehörde an den Kunden zu verweisen, damit sie diese Daten direkt beim Kunden anfordert. Wenn Microsoft aufgefordert wird, verarbeitete Daten an die Strafverfolgungsbehörden weiterzugeben oder diesen den Zugriff darauf einzuräumen, benachrichtigt Microsoft den Kunden unverzüglich und übermittelt eine Kopie der Anforderung, sofern dies nicht gesetzlich verboten ist.

Nach Erhalt einer sonstigen Anfrage von Dritten zur Weitergabe verarbeiteter Daten benachrichtigt Microsoft den Kunden unverzüglich, es sei denn, dies ist gesetzlich untersagt.

Microsoft wird die Anfrage ablehnen, sofern nicht gesetzlich vorgeschrieben. Wenn die Anfrage rechtsgültig ist, wird Microsoft versuchen, den Dritten weiterzuverweisen, um die Daten direkt beim Kunden anzufordern.

Microsoft wird verarbeitete Daten nur wie gesetzlich vorgeschrieben offenlegen oder zugänglich machen, vorausgesetzt, dass die Rechtsvorschriften und Gepflogenheiten den Wesensgehalt der Grundrechte und -freiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft erforderlich und verhältnismäßig sind, um gegebenenfalls eines der in Artikel 23 Absatz 1 der DSGVO aufgeführten Ziele sicherzustellen.

Microsoft wird Dritten Folgendes nicht bereitstellen: (a) einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten, (b) für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform, oder die Möglichkeit, eine solche Verschlüsselung zu umgehen, oder (c) den Zugang zu verarbeiteten Daten, wenn Microsoft bekannt ist, dass diese Daten für andere als die in der betreffenden Anfrage Dritter angegebenen Zwecke verwendet werden sollen.

Zur Unterstützung des Vorstehenden kann Microsoft die Basiskontaktinformationen des Kunden an den betreffenden Dritten weitergeben.

## **Verarbeitung personenbezogener Daten; DSGVO**

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.

Soweit Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogener Daten ist, die der DSGVO unterliegen, gelten die DSGVO-Bestimmungen in Anlage 1. Die Regelungen im Unterabschnitt „Verarbeitung personenbezogener Daten; DSGVO“ gelten ergänzend:

## Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten

Der Kunde und Microsoft vereinbaren, dass der Kunde der Verantwortliche für die personenbezogenen Daten und Microsoft der Auftragsverarbeiter dieser Daten ist, es sei denn, (a) der Kunde handelt als Auftragsverarbeiter personenbezogener Daten; in diesem Fall ist Microsoft Unterauftragsverarbeiter, oder (b) in den produktspezifischen Bedingungen oder in diesem DPA wird etwas anderes bestimmt. Wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, verarbeitet Microsoft personenbezogene Daten nur nach den dokumentierten Weisungen 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 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. Informationen zur Verwendung und Konfiguration der Produkte sind unter <https://docs.microsoft.com> (oder einer entsprechenden, dieser nachfolgenden Stelle) oder in einem anderen Vertrag, der dieses DPA einbezieht, zu finden. Zusätzliche oder andere Weisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Vertrages des Kunden. In allen Fällen, in denen die DSGVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Weisungen des Kunden einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden.

Soweit Microsoft personenbezogene Daten, die der DSGVO unterliegen, für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind, nutzt oder anderweitig verarbeitet, wird Microsoft für diese Nutzung die Pflichten eines unabhängigen Datenverantwortlichen gemäß der DSGVO erfüllen. Microsoft übernimmt die zusätzlichen Pflichten eines „für die Datenverarbeitung Verantwortlichen“ gemäß DSGVO für eine solche Verarbeitung zum: (a) Handeln in Einklang mit den regulatorischen Anforderungen, insoweit dies von der DSGVO gefordert wird, und (b) Schaffung einer erhöhten Transparenz für Kunden und Bestätigung der Rechenschaftspflicht von Microsoft für eine solche Verarbeitung. Microsoft nutzt Sicherheitsmaßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten während dieser Verarbeitung zu schützen, einschließlich

der in diesem DPA aufgeführten sowie der in Artikel 6(4) der DSGVO vorgesehenen Maßnahmen. In Bezug auf die Verarbeitung personenbezogener Daten gemäß diesem Absatz übernimmt Microsoft die im Abschnitt „Zusätzliche Sicherheitsvorkehrungen“ aufgeführten Verpflichtungen; für diese Zwecke (i) gilt jede Offenlegung personenbezogener Daten, wie im Abschnitt „Zusätzliche Schutzmaßnahmen“ beschrieben, durch Microsoft, die im Zusammenhang mit Geschäftstätigkeiten übertragen wurden, als „Relevante Offenlegung“ und (ii) finden die im Abschnitt „Zusätzliche Schutzmaßnahmen“ beschriebenen Verpflichtungen Anwendung auf diese personenbezogenen Daten.

## Verarbeitungsdetails

Die Parteien bestätigen und vereinbaren Folgendes:

- **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 DSGVO eingeschränkt.
- **Dauer der Verarbeitung.** Die Dauer der Verarbeitung richtet sich nach den Weisungen des Kunden sowie den Bestimmungen des DPA.
- **Art und Zweck der Verarbeitung.** 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 Datenverarbeitung; Eigentumsverhältnisse“ weiter oben beschrieben).
- **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 DSGVO 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 DSGVO handelnd gepflegt werden, einschließlich der in Anhang B aufgeführten Kategorien personenbezogener Daten.
- **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 DSGVO geführt werden, einschließlich der in Anhang B aufgeführten Kategorien betroffener Personen.

## Rechte der betroffenen Personen; Unterstützung bei Anfragen

Microsoft ermöglicht dem Kunden, Anfragen betroffener Personen zur Ausübung ihrer Rechte nach der DSGVO 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 DSGVO 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.

## Verzeichnis von Verarbeitungstätigkeiten

Insoweit die DSGVO von Microsoft verlangt, bestimmte Informationen im Zusammenhang mit dem Kunden zu erheben und Verzeichnisse hierüber zu führen, stellt der Kunde Microsoft diese Informationen auf Verlangen zur Verfügung und stellt sicher, dass sie stets korrekt und aktuell sind. Microsoft kann diese Informationen an Aufsichtsbehörden weitergeben, wenn dies nach der DSGVO erforderlich ist.

## 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 vom Kunden im angemessenen Umfang angeforderten Informationen über die Sicherheitsverfahren und -richtlinien von Microsoft.

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.

Microsoft implementiert die in Anhang II der Standardvertragsklauseln von 2021 festgelegten Sicherheitsmaßnahmen zum Schutz personenbezogener Daten im Anwendungsbereich der DSGVO und erhält diese aufrecht.

Microsoft kann jederzeit Branchen- oder Behördenstandards hinzufügen. Microsoft wird die ISO 27001, ISO 27002 und ISO 27018 oder die Standards oder Rahmenkonzepte aus der Tabelle der Core-Onlinedienste in den Produktbestimmungen nicht entfernen, es sei denn, sie werden in der Branche nicht mehr angewendet und durch ihnen nachfolgende Normen, Standards oder Bestimmungen ersetzt (wenn vorhanden).

## 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.

## 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.

## Pflichten des Kunden

Der Kunde ist alleine für eine unabhängige Beurteilung verantwortlich, ob die technischen und organisatorischen Maßnahmen für die Produkte und Services den Anforderungen des Kunden entsprechen, einschließlich seiner Sicherheitsverpflichtungen gemäß geltenden Datenschutzvorschriften. Der Kunde bestätigt und erklärt, dass (unter Berücksichtigung des Stands der Technik, der Einführungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung seiner personenbezogenen Daten sowie der Risiken für Einzelpersonen) die von Microsoft eingeführten und unterhaltenen Sicherheitsverfahren und Sicherheitsrichtlinien ein Sicherheitsniveau bieten, das dem Risiko in Bezug auf seine personenbezogenen Daten angemessen ist. Der Kunde ist verantwortlich für Implementierung und Aufrechterhaltung von Datenschutzvorrichtungen und Sicherheitsmaßnahmen für Komponenten, die der Kunde zur Verfügung stellt oder kontrolliert (z. B. Geräte, die bei Microsoft Intune oder im virtuellen Computer eines Microsoft-Azure-Kunden oder in einer Anwendung registriert sind).

## 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. Der Microsoft-Prüfungsbericht ist eine vertrauliche Information von Microsoft und legt alle wesentlichen Feststellungen des Prüfers eindeutig offen. Microsoft behebt umgehend alle in einem Microsoft-Prüfbericht festgestellten Probleme zur Zufriedenheit des Prüfers. Auf Verlangen des Kunden stellt Microsoft dem Kunden jeden Microsoft-Prüfbericht zur Verfügung. Der Microsoft-Prüfbericht unterliegt den Vertraulichkeits- und Verteilungseinschränkungen von Microsoft und dem Prüfer.

Insoweit die Prüfanforderungen des Kunden im Rahmen der Datenschutzvorschriften durch die Prüfberichte, Dokumentationen oder Informationen zur Einhaltung, die Microsoft seinen Kunden allgemein zur Verfügung stellt, nicht angemessen erfüllt werden können, 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. Weder der Kunde noch der Prüfer haben Zugriff auf die Daten anderer Kunden von Microsoft oder auf Microsoft-Systeme oder Einrichtungen, die nicht an der Bereitstellung der jeweiligen Produkte und Services beteiligt sind. Der Kunde ist für sämtliche Kosten und Gebühren im Zusammenhang mit dieser Prüfung verantwortlich, einschließlich aller angemessenen Kosten und Gebühren, die Microsoft für eine solche Prüfung aufwendet, zusätzlich zu den Gebühren für von Microsoft erbrachte Dienstleistungen. Wenn der als Ergebnis der Prüfung des Kunden erstellte Prüfbericht Erkenntnisse zu wesentlichen Fällen fehlender Einhaltung dokumentiert, leitet der Kunde diesen Prüfbericht an Microsoft weiter. Microsoft muss jede wesentliche fehlende Einhaltung unverzüglich beheben.

Nichts in diesem Abschnitt des DPA variiert oder modifiziert die DSGVO-Bestimmungen oder beeinträchtigt die Rechte einer Aufsichtsbehörde oder einer betroffenen Person gemäß den Datenschutzvorschriften. Microsoft Corporation ist ein beabsichtigter Drittbegünstigter dieses Abschnitts.

## 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.

Meldungen über Sicherheitsvorfälle werden dem Kunden auf von Microsoft gewählte Art und Weise übermittelt, etwa per E-Mail. Es obliegt allein dem Kunden, sicherzustellen, dass Microsoft für alle jeweiligen Produkte und Professional Services über die korrekten Kontaktinformationen des Kunden verfügt. Der Kunde ist allein verantwortlich für die Einhaltung seiner Verpflichtungen aus den für den Kunden geltenden Gesetzen zur Meldung von Vorkommnissen und für die Erfüllung von Meldepflichten im Zusammenhang mit Sicherheitsvorfällen gegenüber Dritten.

Microsoft wird angemessene Anstrengungen unternehmen, um den Kunden bei der Erfüllung seiner Verpflichtung nach Art. 33 DSGVO oder anderen anwendbaren Gesetzen oder Vorschriften zu unterstützen, nämlich die zuständige Aufsichtsbehörde und die betroffenen Personen über solche Sicherheitsvorfälle zu unterrichten.

Die Meldung eines Sicherheitsvorfalls oder die Reaktion auf einen Sicherheitsvorfall durch Microsoft gemäß diesem Abschnitt bedeutet nicht, dass Microsoft einen Fehler oder eine Haftung in Bezug auf den betreffenden Sicherheitsvorfall anerkennt.

Der Kunde ist verpflichtet, Microsoft einen möglichen Missbrauch seiner Accounts oder Authentifizierungsdaten oder sicherheitsrelevante Vorfälle im Zusammenhang mit den Produkten und Services unverzüglich mitzuteilen.

## Datenübermittlungen und Speicherort

### Datenübermittlungen

Kundendaten, Professional Services-Daten und personenbezogene Daten, die Microsoft im Auftrag des Kunden verarbeitet, dürfen nur gemäß den DPA-Bestimmungen und den nachstehend in diesem Abschnitt vorgesehenen Sicherheitsmaßnahmen an einen bestimmten geografischen Standort übermittelt und dort gespeichert und verarbeitet werden. Unter Berücksichtigung solcher Sicherheitsmaßnahmen beauftragt der Kunde Microsoft, Kundendaten, Professional Services-Daten und personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder seine Unterauftragsverarbeiter tätig sind, und Kundendaten und personenbezogene Daten zur Bereitstellung der Produkte zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den DPA-Bestimmungen beschrieben.

Sämtliche Übermittlungen von Kundendaten, Professional Services-Daten und personenbezogenen Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Produkte und Services unterliegen den Bedingungen der von Microsoft implementierten Standardvertragsklauseln von 2021. Darüber hinaus unterliegen Übermittlungen aus dem Vereinigten Königreich den Bedingungen des von Microsoft implementierten IDTA. Für die Zwecke dieses DPA bezeichnet „IDTA“ den Zusatz zur internationalen Datenübertragung zu den Standardvertragsklauseln der Europäischen Kommission für internationale Datenübertragungen, herausgegeben vom UK Information Commissioner's Office gemäß S119A(1) des UK Data Protection Act 2018. Microsoft wird die Anforderungen der Datenschutzgesetze des Europäischen Wirtschaftsraums, des Vereinigten Königreichs und der Schweiz bezüglich der Erfassung, Verwendung, Übertragung, Aufbewahrung und sonstigen Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz einhalten. Alle Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation unterliegen geeigneten Garantien, wie sie in Art. 46 DSGVO beschrieben sind, und solche Übermittlungen und Garantien werden nach Art. 30 Absatz 2 DSGVO dokumentiert.

Darüber hinaus ist Microsoft nach dem EU-U.S. und dem Schweiz-U.S. Data Privacy Framework sowie der UK Erweiterung zu dem EU-U.S. Data Privacy Framework und den damit verbundenen Verpflichtungen zertifiziert. Microsoft stimmt zu, den Kunden zu benachrichtigen, falls Microsoft der Ansicht ist, der Verpflichtung zur Bereitstellung des gleichen Schutzniveaus, das nach den Grundsätzen des Data Privacy Frameworks erforderlich ist, nicht mehr nachkommen zu können.

## Speicherorte von Kundendaten

Im Fall der Core-Onlinedienste speichert Microsoft ruhende Kundendaten („at rest“) in bestimmten größeren geografischen Gebieten (jeweils ein „Geo“), wie in den Produktbestimmungen beschrieben.

Für EU-Datengrenzen-Dienste speichert und verarbeitet Microsoft Kundendaten und personenbezogene Daten und speichert ruhende Professional Services-Daten innerhalb der Europäischen Union und der Europäischen Freihandelsassoziation (EFTA), wie in den Produktbestimmungen beschrieben.

Die Regionen, von denen aus der Kunde oder Endbenutzer des Kunden auf Kundendaten zugreifen oder diese verschieben kann, werden von Microsoft weder kontrolliert noch begrenzt.

## Speicherung und Löschung von Daten

Während der Laufzeit des Abonnements des Kunden oder dem entsprechenden Engagement des Kunden für Professional Services 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 diesen 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.

Der Onlinedienst unterstützt möglicherweise nicht die Aufbewahrung oder Extrahierung von Software, die der Kunde bereitgestellt hat. Microsoft übernimmt keine Haftung für die Löschung von Kundendaten, Professional Services-Daten oder personenbezogenen Daten, soweit die Löschung wie in diesem Abschnitt beschrieben erfolgt.

## EU-Datenverordnung

Der Wechsel ist jederzeit ohne zusätzliche Kosten über die Gebühren und sonstigen Beträge hinaus möglich, die gemäß der Vereinbarung mit dem EU-Kunden ansonsten fällig sind. EU-Kunden können jederzeit auf exportierbare Daten und digitale Vermögenswerte zugreifen, diese exportieren und löschen, einschließlich des Zugriffs und Exports auf exportierbare Daten und digitale Vermögenswerte bis zu 90 Tage lang nach Beendigung des Abonnements, wie in der Bestimmung zur Speicherung und Löschung von Daten dargelegt. Der EU-Kunde entscheidet, wann und in welchem Zeitrahmen mit dem Export von exportierbaren Daten und digitalen Vermögenswerten begonnen werden soll. Für das tatsächliche Extrahieren und Exportieren von exportierbaren Daten und digitalen Vermögenswerten durch EU-Kunden können je nach der spezifischen Konfiguration des Kunden, der Datenmenge, dem Ziel des Wechsels und anderen Umständen, die außerhalb der Kontrolle von Microsoft liegen, mehr als 30 Tage erforderlich sein. EU-Kunden sollten den Wechsel vor der Kündigung des EU-Datenverordnungsdienstes

abschließen, die der EU-Kunde unter Einhaltung einer Kündigungsfrist von 60 Tagen gegenüber Microsoft und der Zahlung aller gemäß der Vereinbarung des EU-Kunden noch geschuldeten Beträge vornehmen kann. Microsoft wird angemessene Unterstützung für den Wechsel leisten und mit der gebotenen Sorgfalt vorgehen, wie in den Abschnitten zur Datensicherheit und anderen Abschnitten des DPA sowie im Rahmen der Vereinbarung des Kunden dargelegt, um die EU-Datenverordnungsdienste während des Wechsels und bei paralleler Nutzung bereitzustellen. Ein EU-Kunde kann gemäß den Bestimmungen der Verordnung eine Reduzierung der Datenextraktionsgebühren im Zusammenhang mit dem Wechsel und der parallelen Nutzung erhalten. Diese Bestimmungen der EU-Datenverordnung gelten nicht für Vorschauen.

Unterstützende Materialien zum Datenexport und den Methoden sowie Informationen zur IKT-Infrastruktur von Microsoft, die zur Bereitstellung von EU-Datenschutzdiensten verwendet wird, und dazu, wie Microsoft auf behördliche Datenzugriffsanfragen reagiert, finden Sie in den Produktbestimmungen.

## **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 Weisung 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.

## **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 DSGVO-Bestimmungen 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 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 Service jeweils ohne Strafe oder Kündigungsgebühr beenden, indem er vor dem Ablauf der entsprechenden Benachrichtigungsfrist 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 Benachrichtigungsfrist 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.

## Previews

Previews können eventuell weniger oder andere Datenschutz- und Sicherheitsmaßnahmen vorsehen als die, die normalerweise in den Produkten und Services vorhanden sind. Wenn nicht anders angegeben, sollte der Kunde Previews nicht zur Verarbeitung Personenbezogener Daten oder anderer Daten verwenden, die gesetzlichen oder regulatorischen Konformitätsanforderungen unterliegen. Mit Ausnahme von Previews, die die Verarbeitung personenbezogener Daten für Produkte zulassen, gelten die folgenden Bedingungen dieser DPA nicht für Previews: Verarbeitung personenbezogener Daten; DSGVO, Datensicherheit und HIPAA-Geschäftspartner. Für Professional Services gilt, dass die Angebote, die als Preview oder Limited Release bezeichnet werden, nur die Bedingungen der Zusätzlichen Professional Services erfüllen.

Für Previews, die die Verarbeitung personenbezogener Daten zulassen, gelten alle Bedingungen in diesem DPA vorbehaltlich der folgenden Bestimmungen:

- Preview-Daten dürfen in die Vereinigten Staaten von Amerika oder in jedes andere Land, in dem Microsoft oder seine Unterauftragsverarbeiter tätig sind, übertragen, dort gespeichert und verarbeitet werden. Dementsprechend gilt der Speicherort der Kundendaten nicht für Previews, da dadurch die Länder eingeschränkt würden, in die bzw. in denen Microsoft Preview-Daten übertragen, speichern oder verarbeiten kann.
- Previews speichern Preview-Daten möglicherweise nicht über die Dauer einer Preview hinaus. Wenn eine Preview endet oder der Kunde die Teilnahme an einer Preview anderweitig beendet, kann Microsoft Preview-Daten löschen, auch wenn die Preview anschließend allgemein kommerziell verfügbar gemacht wird. Dementsprechend gilt die

Datenaufbewahrung und -löschung nicht für Previews, da sie das Recht von Microsoft zum Löschen von Preview-Daten einschränken würde.

Die Previews unterliegen möglicherweise zusätzlichen Bedingungen, die separat als Teil dieser Previews aufgeführt werden.

## Bildungseinrichtungen

Wenn der Kunde eine Bildungsanstalt oder Bildungseinrichtung ist, für die die Bestimmungen des „Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g („FERPA“) gelten, bestätigt Microsoft, dass Microsoft für die Zwecke des DPA gemäß der Definitionen Begriffe im FERPA und dessen Durchführungsbestimmungen ein „Schulfunktionär“ mit „legitimen pädagogischen Interessen“ an den Kundendaten und Professional Services-Daten ist. Microsoft stimmt zu, die Einschränkungen und Anforderungen einzuhalten, die den Schulfunktionären durch 34 CFR 99.33(a) auferlegt werden.

Der Kunde nimmt zur Kenntnis, dass Microsoft unter Umständen über keine oder nur über eingeschränkte Kontaktinformationen der Schüler des Kunden und deren Eltern verfügt. Daher ist der Kunde dafür verantwortlich, die Zustimmung der Eltern für die Nutzung der Produkte und Services durch den Endanwender einzuholen, die nach dem anwendbaren Recht möglicherweise erforderlich ist, und den Schülern (oder im Fall von Schülern unter 18 Jahren, die keine postsekundäre Bildungseinrichtung besuchen, den Eltern des Schülers) im Namen von Microsoft eine Benachrichtigung über eine gerichtliche Anordnung oder eine rechtmäßig ausgestellte Vorladung bereitzustellen, die die Offenlegung von im Besitz von Microsoft befindlichen Kundendaten und Professional Services-Daten verlangt.

## CJIS-Kundenvertrag

Microsoft stellt bestimmte Verwaltungs-Cloud-Services („abgedeckte Services“) in Übereinstimmung mit der Sicherheitsrichtlinie der FBI Criminal Justice Information Services („CJIS-Richtlinie“) zur Verfügung. Die CJIS-Richtlinie regelt die Nutzung und Übertragung von Strafjustizinformationen. Alle abgedeckten CJIS-Services von Microsoft unterliegen den Bestimmungen des CJIS-Management-Agreement.

## HIPAA-Geschäftspartner

Wenn der Kunde eine „betroffene Einrichtung“ oder ein „Geschäftspartner“ ist und „geschützte Gesundheitsinformationen“ in Kundendaten oder Professional Services-Daten enthält, wie diese Begriffe im Health Insurance Portability and Accountability Act von 1996 in der jeweils geltenden

Fassung und in den darunter veröffentlichten Vorschriften (zusammen „HIPAA“) definiert sind, umfasst die Ausführung des Kundenvertrags die Ausführung des HIPAA Business Associate Agreement („BAA“). Der vollständige Text des BAA identifiziert die Onlinedienste oder Professional Services, für die er gilt, und ist verfügbar unter <http://aka.ms/BAA>. Der Kunde kann sich vom BAA abmelden, indem er die folgenden Informationen in einer schriftlichen Mitteilung an Microsoft sendet (gemäß den Bedingungen des Kundenvertrags):

- den vollständigen Firmennamen des Kunden und aller verbundenen Unternehmen, die den BAA ausschließen und
- falls der Kunde mehrere Verträge hat, den Kundenvertrag, auf den die Widerspruchsklausel zutrifft.

## Telekommunikationsdaten

Soweit Microsoft Verkehrsdaten, Inhaltsdaten und andere personenbezogene Daten bei der Bereitstellung von Produkten und Services verarbeitet, die nach geltendem Recht als Telekommunikationsdienste gelten, können besondere gesetzliche Verpflichtungen gelten. Microsoft befolgt alle für die Bereitstellung der Produkte und Services durch Microsoft geltenden telekommunikationsspezifischen Gesetze und Vorschriften, einschließlich Gesetzen zu Meldepflichten bei Sicherheitsverletzungen, sowie Datenschutzvorschriften und Geheimhaltungspflichten für Telekommunikationsdaten. Der Kunde ist verantwortlich für die Einholung der jeweiligen Zustimmung der Endnutzer in Verbindung mit der Nutzung von Produkten und Services, die als Telekommunikationsdienste gelten.

## Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA)

Wenn Microsoft personenbezogene Daten im Geltungsbereich des CCPA verarbeitet, geht Microsoft die folgenden zusätzlichen Verpflichtungen gegenüber dem Kunden ein. Microsoft verarbeitet Kundendaten, Professional Services-Daten und personenbezogene Daten im Namen des Kunden und wird diese Daten nicht für andere als die in diesen DPA-Bestimmungen genannten und nach dem CCPA zulässigen Zwecke aufbewahren, verwenden oder offenlegen, einschließlich Ausnahmeregelungen für den „Verkauf“. Unter keinen Umständen verkauft Microsoft solche Daten. Diese CCPA-Bestimmungen begrenzen oder verringern nicht die Datenschutzverpflichtungen, die Microsoft gegenüber dem Kunden in den DPA-Bestimmungen, den Produktbestimmungen oder in anderen Vereinbarungen zwischen Microsoft und dem Kunden eingegangen ist.

## **Biometrische Daten**

Wenn der Kunde Produkte und Services nutzt, um biometrische Daten zu verarbeiten, ist er für Folgendes verantwortlich: (i) er muss betroffene Personen darüber informieren, einschließlich über Aufbewahrungsfristen und Vernichtung, (ii) er muss die Einwilligung der betroffenen Personen einholen und (iii) er muss die biometrischen Daten löschen, jeweils soweit angemessen und nach den geltenden Datenschutzvorschriften erforderlich. Microsoft wird diese biometrischen Daten gemäß den dokumentierten Weisungen des Kunden (wie im Abschnitt „Rollen und Verantwortlichkeiten von Auftragsverarbeiter und Verantwortlichem“ oben beschrieben) verarbeiten und diese biometrischen Daten gemäß den Datensicherheits- und -schutzbestimmungen dieses DPA schützen. Für die Zwecke dieses Abschnitts hat „biometrische Daten“ die Bedeutung, die in Artikel 4 DSGVO und gegebenenfalls in entsprechenden Bestimmungen in anderen Datenschutzvorschriften dargelegt ist.

## **Zusätzliche Professional Services**

Bei Verwendung in den unten aufgeführten Abschnitten umfasst der definierte Begriff „Professional Services“ Zusätzliche Professional Services und der definierte Begriff „Professional Services-Daten“ umfasst Daten, die für Zusätzliche Professional Services erhalten wurden.

Für Zusätzliche Professional Services gelten die folgenden Abschnitte des DPA in gleicher Weise wie für Professional Services: „Einleitung“, „Einhaltung von gesetzlichen Regelungen“, „Art der Datenverarbeitung; Eigentumsverhältnisse“, „Offenlegung verarbeiteter Daten“, „Verarbeitung personenbezogener Daten; DSGVO“, erster Absatz von „Sicherheitsverfahren und Sicherheitsrichtlinien“, „Pflichten des Kunden“, „Meldung von Sicherheitsvorfälle“, „Datenübermittlung“ (einschließlich der Bestimmungen zu den Standardvertragsklauseln 2021), der dritte Absatz von „Speicherung und Löschung von Daten“, „Vertraulichkeitsverpflichtung des Auftragsverarbeiters“, „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“, „HIPAA-Geschäftspartner“ (soweit im BAA anwendbar), „Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA)“, „Biometrische Daten“, „Kontaktaufnahme mit Microsoft“, „Anhang B – Betroffene Personen und Kategorien personenbezogener Daten“ und „Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen“.

## **Kontaktaufnahme mit Microsoft**

Wenn der Kunde der Ansicht ist, dass Microsoft seinen Datenschutz- und Sicherheitsverpflichtungen nicht nachkommt, kann der Kunde Microsoft über den

Kundensupport oder über das Datenschutzformular über <http://go.microsoft.com/?linkid=9846224> kontaktieren. Postanschrift von Microsoft:

**Microsoft Enterprise Service-Privacy**

Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052, USA

Microsoft Ireland Operations Limited ist der Datenschutzvertreter von Microsoft für den Europäischen Wirtschaftsraum und die Schweiz. Der Datenschutzbeauftragte von Microsoft Ireland Operations Limited kann unter folgender Adresse erreicht werden:

**Microsoft Ireland Operations, Ltd.**

Attn: Data Privacy  
One Microsoft Place  
South County Business Park  
Leopardstown  
Dublin 18, D18 P521, Ireland

## Anhang A – Sicherheitsmaßnahmen

---

Microsoft hat für Kundendaten in den Core-Onlinediensten und für Professional Services-Daten die folgenden Sicherheitsmaßnahmen getroffen, die in Verbindung mit den Sicherheitsverpflichtungen in diesem DPA (einschließlich der DSGVO-Bestimmungen) die einzige Verantwortung von Microsoft in Bezug auf die Sicherheit dieser Daten darstellen, und wird diese Maßnahmen aufrechterhalten.

Domäne	Praktiken
Organisation der IT-Sicherheit	<p><b>Verantwortung für die Sicherheit.</b> Microsoft hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitsregeln und -verfahren verantwortlich sind.</p> <p><b>Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.</b> Microsoft-Mitarbeiter, die Zugang zu Kundendaten oder Professional Services-Daten haben, sind zur Vertraulichkeit verpflichtet.</p> <p><b>Risikomanagementprogramm.</b> Microsoft hat vor der Verarbeitung der Kundendaten oder dem Start des Onlinedienstes und vor der Verarbeitung von Professional Services-Daten oder dem Start der Professional Services eine Risikobewertung durchgeführt.</p> <p>Microsoft archiviert Sicherheitsunterlagen im Rahmen der Aufbewahrungspflichten, nachdem sie nicht mehr in Kraft sind.</p>
Asset-Management	<p><b>Anlagenbestand.</b> Microsoft führt einen Bestand aller Medien, auf denen Kundendaten oder Professional Services-Daten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf Microsoft-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind.</p> <p><b>Asset-Handling</b></p> <ul style="list-style-type: none"><li>• Microsoft klassifiziert Kundendaten und Professional Services-Daten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs darauf zu ermöglichen.</li></ul>

Domäne	Praktiken
	<ul style="list-style-type: none"> <li>• Microsoft legt Einschränkungen für das Drucken von Kundendaten und Professional Services-Daten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die solche Daten enthalten.</li> <li>• Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie Kundendaten oder Professional Services-Daten auf tragbaren Geräten speichern, remote auf solche Daten zugreifen oder solche Daten außerhalb der Einrichtungen von Microsoft verarbeiten.</li> </ul>
Personalsicherheit	<p><b>Sicherheitsschulungen.</b> Microsoft informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen. Microsoft informiert seine Mitarbeiter auch über mögliche Folgen einer Verletzung der Sicherheitsregeln und -verfahren. Microsoft verwendet in der Schulung nur anonyme Daten.</p>
Physische und umgebungsbezogene Sicherheit	<p><b>Physischer Zugang zu Einrichtungen.</b> Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen.</p> <p><b>Physischer Zugriff auf Komponenten.</b> Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten.</p> <p><b>Schutz vor Unterbrechungen.</b> Microsoft nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern.</p> <p><b>Entsorgung von Komponenten.</b> Microsoft nutzt branchenübliche Prozesse, um Kundendaten und Professional Services-Daten zu löschen, wenn sie nicht mehr benötigt werden.</p>

Domäne	Praktiken
<p>Kommunikations- und Betriebsmanagement</p>	<p><b>Betriebsrichtlinie.</b> Microsoft führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter beschrieben sind, die Zugang zu Kundendaten oder Professional Services-Daten haben.</p> <p><b>Datenwiederherstellungsverfahren</b></p> <ul style="list-style-type: none"> <li>• Microsoft erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es haben im betreffenden Zeitraum keine Aktualisierungen stattgefunden) mehrere Kopien von Kundendaten und Professional Services-Daten, aus denen solche Daten wiederhergestellt werden können.</li> <li>• Microsoft bewahrt Kopien von Kundendaten und Professional Services-Daten und Datenwiederherstellungsverfahren an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die die Kundendaten und Professional Services-Daten verarbeitet werden.</li> <li>• Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten und Professional Services-Daten regeln.</li> <li>• Microsoft prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. Ausgenommen hiervon sind Verfahren für Professional Services und für Azure Government Services, die alle zwölf Monate geprüft werden.</li> <li>• Microsoft protokolliert Datenwiederherstellungsmaßnahmen. Dabei werden Informationen zur verantwortlichen Person, die Beschreibung der wiederhergestellten Daten sowie gegebenenfalls Angaben zu den Daten, die bei der Datenwiederherstellung manuell eingegeben werden mussten, aufgezeichnet.</li> </ul> <p><b>Malware.</b> Microsoft nimmt Anti-Malware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Kundendaten und Professional Services-</p>

Domäne	Praktiken
	<p>Daten erhält, einschließlich bössartiger Software aus öffentlichen Netzwerken.</p> <p><b>Daten außerhalb von Landesgrenzen</b></p> <ul style="list-style-type: none"> <li>• Microsoft verschlüsselt Kundendaten und Professional Services-Daten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung.</li> <li>• Microsoft schränkt den Zugriff auf Kundendaten und Professional Services-Daten in Medien ein, die die Einrichtungen von Microsoft verlassen.</li> </ul> <p><b>Ereignisprotokollierung.</b> Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten oder Professional Services-Daten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.</p>
Zugriffskontrolle	<p><b>Zugriffsrichtlinie.</b> Microsoft führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Kundendaten oder Professional Services-Daten haben.</p> <p><b>Zugriffsberechtigung</b></p> <ul style="list-style-type: none"> <li>• Microsoft führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf Microsoft-Systeme autorisiert sind, die Kundendaten oder Professional Services-Daten enthalten.</li> <li>• Microsoft deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.</li> <li>• Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.</li> <li>• Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten oder Professional Services-Daten enthalten sind, stellt Microsoft sicher,</li> </ul>

Domäne	Praktiken
	<p>dass diese Personen über separate Kennungen/Anmeldedaten verfügen.</p> <p><b>Geringste Rechte</b></p> <ul style="list-style-type: none"> <li>• Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten und Professional Services-Daten nur gestattet, wenn dies erforderlich ist.</li> <li>• Microsoft schränkt den Zugriff auf Kundendaten und Professional Services-Daten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.</li> </ul> <p><b>Integrität und Vertraulichkeit</b></p> <ul style="list-style-type: none"> <li>• Microsoft weist Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen, die sich unter der Kontrolle von Microsoft befinden, verlassen oder wenn Computer anderweitig unbeaufsichtigt sind.</li> <li>• Microsoft speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind.</li> </ul> <p><b>Authentifizierung</b></p> <ul style="list-style-type: none"> <li>• Microsoft verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.</li> <li>• Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.</li> <li>• Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss.</li> <li>• Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden.</li> <li>• Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf</li> </ul>

Domäne	Praktiken
	<p>Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung.</p> <ul style="list-style-type: none"> <li>• Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden.</li> <li>• Microsoft verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern während der Zuweisung und Verteilung sowie während der Speicherung wahren sollen.</li> </ul> <p><b>Netzwerkdesign.</b> Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Kundendaten oder Professional Services-Daten zu erhalten, auf die sie nicht zugreifen dürfen.</p>
<p>Handhabung eines Informationssicherheitsvorfalls</p>	<p><b>Vorfallreaktionsablauf</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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 Microsoft.</li> <li>• 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.</li> </ul>

Domäne	Praktiken
	<b>Dienstüberwachung.</b> Das Microsoft-Sicherheitspersonal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Abhilfemaßnahmen vorzuschlagen.
Geschäftsfortführungsmanagement	<ul style="list-style-type: none"><li>• Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft-Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten.</li><li>• Bei Microsoft sind redundante Speicherung und ihre Verfahren zur Datenwiederherstellung so konzipiert, dass versucht wird, Kundendaten und Professional Services-Daten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.</li></ul>

## Anhang B – Betroffene Personen und Kategorien personenbezogener Daten

---

**Betroffene Personen:** Betroffene Personen sind die Vertreter des Kunden und Endnutzer sowie Angestellte, Auftragnehmer, Mitarbeiter und Kunden des Kunden. Zu den betroffenen Personen können auch Personen gehören, die personenbezogene Daten an Nutzer der von Microsoft bereitgestellten Services übermitteln oder Kontakt zu solchen Nutzern aufnehmen möchten. Microsoft bestätigt, dass sich der Kunde je nach Nutzung der Produkte und Services dafür entscheiden kann, personenbezogene Daten der folgenden Arten von betroffenen Personen in die personenbezogenen Daten aufzunehmen:

- Mitarbeiter, Auftragnehmer und Zeitarbeitnehmer (derzeitige, ehemalige, zukünftige) des Kunden;
- Angehörige der oben genannten Personen;
- Partner/Kontaktpersonen des Kunden (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeitnehmer von Partnern/Kontaktpersonen (juristische Personen) (derzeitige, ehemalige, zukünftige),
- Benutzer (z. B. Kunden, Klienten, Patienten, Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen des Kunden sind,
- Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern des Kunden zusammenarbeiten, kommunizieren oder anderweitig interagieren und/oder Kommunikationsmittel wie Anwendungen und Websites verwenden, die vom Kunden bereitgestellt werden;
- Stakeholder oder einzelne Personen, die passiv mit dem Datenexporteur interagieren (z. B. weil sie Gegenstand einer Untersuchung oder Studie sind oder in Dokumenten oder in Korrespondenz mit dem Datenexporteur erwähnt werden);
- Minderjährige Personen; oder
- Berufsgeheimnisträger (z. B. Ärzte, Anwälte, Notare, Kirchenmitarbeiter usw.).

**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, Straßename 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, Studentenummer, Patientenummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien);
- Pseudonymisierte Kennungen;
- Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartename 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-Kartenummer, 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 DSGVO genannten personenbezogenen Daten.

## Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen

---

Durch diesen Nachtrag zu zusätzlichen Schutzmaßnahmen zum DPA („Nachtrag“) bietet Microsoft dem Kunden zusätzliche Schutzmaßnahmen für die Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO durch Microsoft im Auftrag des Kunden und zusätzliche Rechtsbehelfe für die betroffenen Personen, auf die sich personenbezogene Daten beziehen.

Dieser Nachtrag ergänzt das DPA und ist Teil desselben. Er ändert oder modifiziert dieses jedoch nicht.

1. **Anfechtung von Anordnungen.** Für den Fall, dass Microsoft von einem Dritten eine Anordnung zur zwingenden Offenlegung von personenbezogenen Daten erhält, die im Rahmen dieses DPA verarbeitet werden, wird Microsoft:
  - a. alle angemessenen Anstrengungen unternehmen, um den Dritten bezüglich der Anforderung von Daten direkt an den Kunden zu verweisen;
  - b. den Kunden unverzüglich benachrichtigen, es sei denn, dies ist nach dem für den anfragenden Dritten geltenden Recht verboten, und im Falle eines Verbots, den Kunden zu benachrichtigen, alle rechtmäßigen Anstrengungen zu unternehmen, um das Recht zu erhalten, auf das Verbot zu verzichten, um dem Kunden so schnell wie möglich so viele Informationen wie möglich zu übermitteln; und
  - c. alle rechtmäßigen Anstrengungen unternehmen, um die Aufforderung zur Offenlegung auf der Grundlage von Rechtsmängeln nach dem Recht der anfragenden Partei oder von relevanten Konflikten mit dem anwendbaren Recht der Europäischen Union oder dem anwendbaren Recht der Mitgliedstaaten anzufechten.

Wenn Microsoft oder eines seiner verbundenen Unternehmen nach den unter a. bis c. oben beschriebenen Schritten weiterhin zur Offenlegung personenbezogener Daten verpflichtet ist, wird Microsoft nur die Mindestmenge dieser Daten offenlegen, die erforderlich ist, um der Anordnung zur zwingenden Offenlegung nachzukommen.

Für die Zwecke dieses Abschnitts umfassen rechtmäßige Anstrengungen keine Handlungen, die nach den Gesetzen der relevanten Rechtsordnung zu zivil- oder strafrechtlichen Sanktionen, wie etwa Missachtung des Gerichts, führen würden.

2. **Entschädigung betroffener Personen.** Vorbehaltlich der Abschnitte 3 und 4 hat Microsoft einer betroffenen Person jeglichen materiellen oder immateriellen Schaden zu ersetzen, der

der betroffenen Person dadurch entsteht, dass Microsoft personenbezogene Daten der betroffenen Person offenlegt, indem diese als Reaktion auf eine Aufforderung einer öffentlichen Stelle oder einer Strafverfolgungsbehörde außerhalb der EU/des EWR unter Verletzung der Verpflichtungen von Microsoft gemäß Kapitel V der DSGVO übermittelt wurden (eine „Relevante Offenlegung“). Ungeachtet des Vorstehenden ist Microsoft nicht verpflichtet, die betroffene Person gemäß dieses Abschnitts 2 zu entschädigen, soweit die betroffene Person bereits eine Entschädigung für denselben Schaden erhalten hat, sei es von Microsoft oder anderweitig.

3. **Bedingungen für die Entschädigung.** Die Entschädigung nach Abschnitt 2 setzt voraus, dass die betroffene Person zur angemessenen Zufriedenheit von Microsoft Folgendes nachweist:
- Microsoft hat eine Relevante Offenlegung vorgenommen,
  - die Relevante Offenlegung war die Grundlage eines offiziellen Verfahrens der öffentlichen Stelle oder Strafverfolgungsbehörde in einem Land außerhalb der EU/des EWR gegen die betroffene Person und
  - die Relevante Offenlegung führte direkt zu materiellen oder immateriellen Schäden für die betroffene Person.

Die betroffene Person trägt die Beweislast in Bezug auf die Bedingungen a) bis c).

Ungeachtet des Vorstehenden ist Microsoft nicht verpflichtet, die betroffene Person gemäß Abschnitt 2 freizustellen, wenn Microsoft nachweist, dass die Relevante Offenlegung nicht gegen seine Verpflichtungen aus Kapitel V der DSGVO verstoßen hat.

4. **Umfang des Schadensersatzes.** Die Freistellung nach Abschnitt 2 ist auf materielle und immaterielle Schäden gemäß DSGVO beschränkt und schließt Folgeschäden und alle anderen Schäden aus, die nicht das Ergebnis eines Verstoßes von Microsoft gegen die DSGVO sind.
5. **Ausübung von Rechten.** Rechte, die betroffenen Personen in diesem Nachtrag gewährt werden, können von den betroffenen Personen unabhängig von den Beschränkungen in den Abschnitten 3 oder 6 der Standardvertragsklauseln Microsoft gegenüber durchgesetzt werden. Die betroffene Person darf einen Anspruch nach diesem Nachtrag nur auf individueller Basis erheben und nicht als Teil einer Muster-, Sammel-, Gruppen- oder Verbandsklage. Rechte, die betroffenen Personen im Rahmen dieses Nachtrags gewährt werden, sind nur für die betroffene Person bestimmt und nicht abtretbar.
6. **Änderungsmitteilung.** Microsoft stimmt zu und gewährleistet, dass Microsoft keinen Grund zu der Annahme hat, dass die für Microsoft oder seine Unterauftragsverarbeiter geltenden Rechtsvorschriften, einschließlich in jedem Land, in das Microsoft oder seine

Unterauftragsverarbeiter personenbezogene Daten übermitteln, Microsoft daran hindern, die vom Kunden erhaltenen Weisungen und seine Verpflichtungen aus dieser Ergänzung oder aus den Standardvertragsklauseln 2021 zu erfüllen, und dass Microsoft im Fall einer Änderung dieser Rechtsvorschriften, die wahrscheinlich erhebliche nachteilige Auswirkungen auf die in dieser Ergänzung oder in den Standardvertragsklauseln vorgesehenen Zusicherungen und Verpflichtungen haben werden, den Kunden unverzüglich über die Änderung informieren wird, sobald diese Microsoft bekannt ist; in diesem Fall ist der Kunde berechtigt, die Datenübermittlung auszusetzen und/oder den Vertrag zu kündigen.

## Anhang D – Anfechtung einer Anordnung oder einer verbindlichen rechtlichen Verpflichtung zur Aussetzung von Onlinediensten

---

Mit diesem Anhang geht Microsoft gegenüber nationalen, bundesstaatlichen und regionalen Behördenkunden der Mitgliedstaaten der Europäischen Union („EU“) sowie der EU-Beitrittsländer, der Mitglieder der Europäischen Freihandelsassoziation, des Vereinigten Königreichs, Monacos, des Vatikans und der Europäischen Kommission („geschützte Behördenkunden“) die folgenden Verpflichtungen ein.

1. Für den Fall, dass gegenüber Microsoft eine Anordnung ergeht oder Microsoft anderweitig einer verbindlichen rechtlichen Verpflichtung einer staatlichen Stelle, Behörde, Kommission oder quasi-staatliche Einrichtung unterliegt, die Microsoft dazu verpflichtet, die Bereitstellung von Onlinediensten (einschließlich, aber nicht beschränkt auf die Bereitstellung von Microsoft Azure-Diensten, Microsoft Dynamics 365-Diensten oder Office 365-Diensten) für den geschützten Behördenkunden ganz oder teilweise auszusetzen oder einzustellen, wird Microsoft im eigenen Namen und im Namen seiner verbundenen Unternehmen:
  - a. alle verfügbaren Mittel einzusetzen, um die freiwillige Rücknahme, Aufhebung oder Rückgängigmachung einer solchen Anordnung zu erreichen; und
  - b. alle rechtmäßigen Anstrengungen unternehmen, um die Anordnung vor den Gerichten des Lands anzufechten, dessen Behörde die Anordnung erlassen hat, und zwar auf der Grundlage von Rechtsmängeln nach dem Recht der anfordernden Partei oder von relevanten Konflikten mit dem Recht der Europäischen Union oder dem anwendbaren nationalen Recht.

Microsoft wird bei Bedarf einen dauerhaften und zeitweiligen Unterlassungsanspruch erwirken, um die kontinuierliche und ununterbrochene Bereitstellung der entsprechenden Onlinedienste sicherzustellen, bis eine rechtskräftige Entscheidung über die rechtmäßigen Anstrengungen zur Anfechtung der Anordnung oder der sonstigen oben genannten verbindlichen rechtlichen Verpflichtung ergangen ist.

2. Rechte, die dem Kunden im Rahmen dieser Bestimmung gewährt werden, sind nur für den geschützten Behördenkunden bestimmt und nicht abtretbar.

# Anlage 1 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union

---

Microsoft geht die in diesen Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union („DSGVO-Bestimmungen“) enthaltenen Verpflichtungen gegenüber allen Kunden mit Wirkung vom 25. Mai 2018 ein. Diese Verpflichtungen sind für Microsoft in Bezug auf den Kunden bindend, unabhängig (1) von der Version der Produktbestimmungen und des DPA, die anderweitig für ein bestimmtes Produktabonnement oder eine bestimmte Lizenz gilt, oder (2) von anderen Verträgen, die auf diese Anlage verweisen.

Für Zwecke dieser DSGVO-Bestimmungen sind sich Kunde und Microsoft darin einig, dass der Kunde der Verantwortliche für die personenbezogenen Daten und Microsoft der Auftragsverarbeiter dieser Daten ist, es sei denn, der Kunde handelt als Auftragsverarbeiter personenbezogener Daten; in diesem Fall ist Microsoft Unterauftragsverarbeiter. Diese DSGVO-Bestimmungen gelten für die Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO durch Microsoft im Auftrag des Kunden. Diese DSGVO-Bestimmungen beschränken oder verringern nicht die Datenschutzverpflichtungen, die Microsoft gegenüber dem Kunden in den Produktbestimmungen oder in anderen Verträgen zwischen Microsoft und dem Kunden eingeht. Diese DSGVO-Bestimmungen gelten nicht in den Fällen, in denen Microsoft der Verantwortliche für personenbezogene Daten ist.

## Relevante DSGVO-Verpflichtungen: Artikel 5, 28, 32 und 33

1. Microsoft unterstützt die Rechenschaftspflichten des Kunden über diesen DPA und die dem Kunden bereitgestellte Produktdokumentation und wird dies auch während der Laufzeit des Abonnements des Kunden oder des entsprechenden Professional Services-Vertrags gemäß Unterabschnitt 3(h) unten tun. (Artikel 5(2))
2. Microsoft darf ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung durch den Kunden keine weiteren Auftragsverarbeiter in Anspruch nehmen. Im Fall einer allgemeinen schriftlichen Genehmigung wird Microsoft den Kunden immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. (Artikel 28(2))
3. Die Verarbeitung durch Microsoft unterliegt diesen DSGVO-Bestimmungen nach dem Recht der Europäischen Union (nachfolgend „Union“ genannt) oder der Mitgliedstaaten. Sie sind

für Microsoft in Bezug auf den Kunden verbindlich. 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 DSGVO-Bestimmungen einschließt. Insbesondere ist Microsoft gehalten:

- a. personenbezogene Daten nur auf dokumentierte Weisung 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;
- b. zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- c. alle erforderlichen Maßnahmen gemäß Artikel 32 der DSGVO zu ergreifen;
- d. die Bedingungen einzuhalten, auf die in den Ziffern 1. und 3. dieser Anlage bezüglich der Inanspruchnahme eines weiteren Auftragsverarbeiters verwiesen wird;
- 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 DSGVO genannten Rechte der betroffenen Person nachzukommen;
- 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 DSGVO zu unterstützen;
- g. nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Kunden alle personenbezogenen Daten entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- h. dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der DSGVO 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.

Microsoft informiert den Kunden unverzüglich, falls Microsoft der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Artikel 28(3)).

4. Falls Microsoft die Dienste eines weiteren Auftragsverarbeiters in Anspruch nimmt, um im Namen des Kunden bestimmte Verarbeitungstätigkeiten auszuführen, werden diesen weiteren Auftragsverarbeitern durch einen Vertrag oder ein anderes Rechtsinstrument nach dem Recht der Union oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesen DSGVO-Bestimmungen beschrieben sind. Insbesondere muss hinreichende Garantie dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Sollte jener Auftragsverarbeiter seinen Datenschutzverpflichtungen nicht nachkommen, haftet Microsoft gegenüber dem Kunden für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters (Artikel 28(4)).
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)).
7. Der Kunde und Microsoft unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Weisung des Kunden verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet (Artikel 32(4)).

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.