Volumenlizenz

# Microsoft-Onlinedienste Nachtrag zum Datenschutz Letzte Aktualisierung: 21. Juli 2020

Am 21. Juli 2020 in englischer Sprache veröffentlicht. Übersetzungen werden von Microsoft veröffentlicht, sobald sie verfügbar sind. Diese Bestimmungen sind für Microsoft seit dem 16. Juli 2020 verbindlich.

Microsoft

# Inhaltsverzeichnis

**EINLEITUNG ..... 3**

Anwendbare DPA-Bestimmungen und -Aktualisierungen ..... 3
Elektronische Benachrichtigungen ..... 3
Frühere Versionen ..... 3

**DEFINITIONEN ..... 4**

**ALLGEMEINE BESTIMMUNGEN ..... 6**

Einhaltung von gesetzlichen Regelungen ..... 6

**DATENSCHUTZBESTIMMUNGEN ..... 6**

Umfang ..... 6
Art der Datenverarbeitung; Eigentumsverhältnisse ..... 6
Offenlegung verarbeiteter Daten ..... 7
Verarbeitung personenbezogener Daten; DSGVO ..... 7
Datensicherheit ..... 8
Meldung von Sicherheitsvorfällen ..... 10
Datenübermittlungen und Speicherstelle ..... 10
Speicherung und Löschung von Daten ..... 11
Vertraulichkeitsverpflichtung des Auftragsverarbeiters ..... 11
Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern 11
Bildungseinrichtungen ..... 12
CJIS-Kundenvertrag ..... 12
HIPAA-Geschäftspartner ..... 12
Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA) ..... 12
Biometrische Daten ..... 12
Kontaktaufnahme mit Microsoft ..... 12

**ANHANG A – SICHERHEITSMAßNAHMEN ..... 14**

**ANLAGE 1 – HINWEISE ..... 17**

**PROFESSIONAL SERVICES ..... 17**
Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA) ..... 20
Biometrische Daten ..... 20

**ANLAGE 2 – DIE STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER) ..... 21**

**ANLAGE 3 – BESTIMMUNGEN DER DATENSCHUTZ-GRUNDVERORDNUNG DER EUROPÄISCHEN UNION ..... 28**

# Einleitung

Die Parteien stimmen zu, dass dieser Nachtrag zum Datenschutz für Microsoft-Onlinedienste (Data Protection Addendum, DPA) ihre Verpflichtungen in Bezug auf die Verarbeitung und die Sicherheit von Kundendaten und personenbezogenen Daten in Verbindung mit den Onlinediensten regelt. Dieser DPA wird durch Bezugnahme Bestandteil der Bestimmungen für Onlinedienste (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten). 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 unterliegt. 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 Bestimmungen dieses DPA und anderen Bestimmungen des Volumenlizenzvertrags des Kunden hat dieser DPA Vorrang. Die Bestimmungen dieses DPA 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. Der Klarheit halber wird festgehalten, dass – entsprechend Klausel 10 der Standardvertragsklauseln in Anlage 2 – die Standardvertragsklauseln Vorrang vor anderen Bestimmungen des DPA haben.

Microsoft geht die in diesem DPA beschriebenen Verpflichtungen gegenüber allen Kunden mit Volumenlizenzverträgen ein. Diese Verpflichtungen sind für Microsoft in Bezug auf den Kunden bindend, unabhängig (1) von den Nutzungsbedingungen, die ansonsten für ein bestimmtes Onlinedienstabonnement gelten, und (2) von anderen Verträgen, die auf die OST verweisen.

## Anwendbare DPA-Bestimmungen und -Aktualisierungen

### Beschränkungen für Aktualisierungen

Wenn ein Kunde ein Onlinedienstabonnement verlängert oder kauft, gelten die zu diesem Zeitpunkt aktuellen DPA-Bestimmungen, die während der Laufzeit dieses Onlinedienstabonnements unverändert bleiben.

### Neue Features, Ergänzungen oder zugehörige Software

Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen gilt, falls Microsoft neue Features, Ergänzungen oder neue zugehörige Software einführt (d. h. die zuvor nicht im Abonnement enthalten waren), dass Microsoft dann Bestimmungen im DPA einführen oder Aktualisierungen am DPA vornehmen kann, die sich auf die Verwendung dieser neuen Features, Ergänzungen oder zugehörige 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, Ergänzungen oder zugehörige Software zu nutzen, ohne dass eine vorhandene Funktionalität eines allgemein verfügbaren Onlinedienstes verloren geht. Wenn der Kunde die neuen Features, Ergänzungen oder zugehörige Software nicht nutzt, finden die entsprechenden neuen Bestimmungen keine Anwendung.

### Behördliche Vorschriften und Verpflichtungen

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

## Elektronische Benachrichtigungen

Microsoft kann Kunden Informationen und Mitteilungen über Onlinedienste elektronisch, auch per E-Mail, über das Portal des 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 Onlinedienste. 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 Volumenlizenzvertrag angegebene Bedeutung. In diesem DPA werden die folgenden definierten Begriffe verwendet:

„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 Daten zu Professional Services ein.

„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 spezifischen Bestimmungen für Onlinedienste in den Nutzungsrechten, die speziell die Datenschutz- und Sicherheitsbestimmungen in dem DPA für einen spezifischen Onlinedienst (oder ein Feature eines Onlinediensts) ergänzen oder ändern. Bei Konflikten oder Widersprüchen zwischen dem DPA und solchen spezifischen Bedingungen für Onlinedienste sind die spezifischen Bedingungen für Onlinedienste für den jeweiligen Onlinedienst (oder das Feature des jeweiligen Onlinediensts) vorrangig.

„Diagnosedaten“ sind Daten, die Microsoft aus Software erhebt oder erhält, die vom Kunden im Zusammenhang mit dem Onlinedienst lokal installiert wurde. Diagnosedaten werden teilweise auch als Telemetriedaten bezeichnet. Kundendaten, Dienstgenerierte Daten und Professional Services Daten sind keine Diagnosedaten.

„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).

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

„DSGVO-Bestimmungen“ bezieht sich auf die Bestimmungen in Anlage 3, in der Microsoft verbindliche Zusagen in Bezug auf die Verarbeitung personenbezogener Daten nach Artikel 28 DSGVO gibt.

„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.

„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 Onlinedienst 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. Professional Services Daten schließen Supportdaten ein.

„Dienstgenerierte Daten“ sind Daten, die Microsoft im Zuge des Betriebs eines Onlinediensts generiert oder ableitet. Dienstgenerierte Daten umfassen keine Kundendaten, Diagnosedaten oder Professional Services Daten.

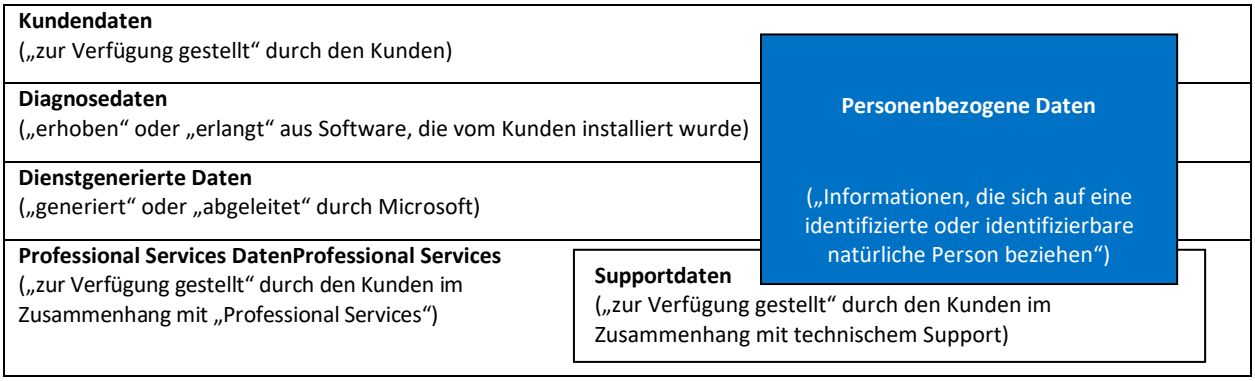
„Standardvertragsklauseln“ sind die Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern ansässig sind, die keinen angemessenen Grad an Datenschutz gewährleisten, wie in Artikel 46 der DSGVO beschrieben und durch die Entscheidung 2010/87/EG der Europäischen Kommission vom 5. Februar 2010 genehmigt. Die Standardvertragsklauseln befinden sich in Anlage 2.

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

„Supportdaten“ sind alle Daten, einschließlich sämtlichen Text-, Ton-, Video- und Bilddateien oder Software, die Microsoft vom oder im Namen des Kunden im Zuge der Beauftragung von Microsoft zur Erlangung von technischem Support für von diesem Vertrag abgedeckte Onlinedienste bereitgestellt werden (oder zu deren Erhebung über einen Onlinedienst der Kunde Microsoft berechtigt). Supportdaten sind eine Teilmenge der Professional Services Daten.

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. Die Begriffe „Datenimporteur“ und „Datenexporteur“ haben die in den Standardvertragsklauseln angegebenen Bedeutungen.

Zur Klarstellung wird festgehalten, dass, wie oben ausführlich dargelegt, Daten, die als Kundendaten, Diagnosedaten oder Dienstgenerierte Daten definiert sind, ebenso wie Professional Services Daten personenbezogene Daten enthalten können. Zur Veranschaulichung ist dies in der Übersicht zusammengefasst:




Oben sind die im DPA definierten Datentypen visuell dargestellt. Alle personenbezogenen Daten werden als Teil eines der anderen Datentypen (die jeweils auch nicht-personenbezogene Daten umfassen) verarbeitet. Supportdaten sind eine Teilmenge der Professional Services Daten. Die DPA-Bestimmungen konzentrieren sich auf Kundendaten und personenbezogene Daten (mit Professional Services Daten, einschließlich Supportdaten sowie jegliche personenbezogene Daten in Professional Services Daten und Supportdaten, die in Anlage 1 abgedeckt sind).

Inhaltsverzeichnis / Allgemeine Geschäftsbedingungen

# Allgemeine Bestimmungen

### Einhaltung von gesetzlichen Regelungen

Microsoft befolgt alle für die Bereitstellung der Onlinedienste 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 Onlinediensten gelten, einschließlich Gesetzen zu biometrischen Daten, zur Vertraulichkeit von Kommunikation, sowie Datenschutzvorschriften. Der Kunde ist dafür verantwortlich, zu ermitteln, ob die Onlinedienste für die Speicherung und Verarbeitung von Informationen geeignet sind, die spezifischen Gesetzen oder Vorschriften unterliegen, und dafür dass er die Onlinedienste nur in einer Weise nutzt, die mit den rechtlichen und regulatorischen Verpflichtungen des Kunden im Einklang steht. Der Kunde ist für die Beantwortung von Anfragen Dritter bezüglich der Nutzung eines Onlinediensts 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

Dieser Abschnitt des DPA umfasst die folgenden Unterabschnitte:

- Umfang
- Art der Datenverarbeitung; Eigentumsverhältnisse
- Offenlegung verarbeiteter Daten
- Verarbeitung personenbezogener Daten; DSGVO
- Datensicherheit
- Meldung von Sicherheitsvorfällen
- Datenübermittlungen und Speicherstelle
- Speicherung und Löschung von Daten
- Vertraulichkeitsverpflichtung des Auftragsverarbeiters
- Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern
- Bildungseinrichtungen
- CJIS-Kundenvertrag
- HIPAA-Geschäftspartner
- Bestimmungen des kalifornischen Datenschutzgesetzes (California Consumer Privacy Act, CCPA)
- Biometrische Daten
- So kontaktieren Sie Microsoft
- Anhang A – Sicherheitsmaßnahmen

### Umfang

Die DPA-Bestimmungen gelten für alle Onlinedienste mit Ausnahme der in Anlage 1 der OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) ausdrücklich genannten Onlinedienste, die den Datenschutz- und Sicherheitsbestimmungen in den spezifischen Bestimmungen des jeweiligen Onlinediensts unterliegen.

Für Previews werden unter Umständen weniger oder andere Datenschutz- und Sicherheitsmaßnahmen eingesetzt als dies bei Onlinediensten normalerweise der Fall ist. Wenn nicht anders angegeben, sollte der Kunde Preview-Versionen nicht zur Verarbeitung personenbezogener Daten oder anderer Daten verwenden, die gesetzlichen oder regulatorischen Compliance-Anforderungen unterliegen. Die folgenden Bestimmungen in diesem DPA gelten nicht für Preview-Versionen: Verarbeitung personenbezogener Daten; DSGVO, Datensicherheit und HIPAA Business Associate.

Anlage 1 des DPA enthält die Datenschutz- und Sicherheitsbestimmungen für Professional Services Daten (einschließlich der in diesen enthaltenen personenbezogenen Daten) im Zusammenhang mit der Erbringung von Professional Services. Wenn nicht ausdrücklich in Anlage 1 als anwendbar festgelegt, gelten die Bestimmungen in diesem DPA daher nicht für die Erbringung von Professional Services.

### Art der Datenverarbeitung; Eigentumsverhältnisse

Microsoft wird Kundendaten und personenbezogene Daten nur verwenden und anderweitig verarbeiten, (a) um dem Kunden die Onlinedienste gemäß den dokumentierten Anweisungen des Kunden bereitzustellen, und (b) um legitime Geschäftstätigkeiten von Microsoft zu verfolgen, die mit der Bereitstellung der Onlinedienste für den Kunden verbunden sind und im Folgenden detailliert aufgeführt und eingegrenzt werden. Zwischen den Parteien behält der Kunde alle Rechte und das Eigentum an den Kundendaten. Mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt, erwirbt Microsoft keine weiteren Rechte an Kundendaten. Dieser Absatz berührt nicht die Rechte von Microsoft an Software oder Dienstleistungen, für die Microsoft dem Kunden eine Lizenz gewährt.

#### Verarbeitung zur Bereitstellung der Onlinedienste für den Kunden

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

- Die Bereitstellung von Funktionen wie vom Kunden und dessen Benutzern lizenziert, konfiguriert und verwendet, einschließlich der Bereitstellung personalisierter Benutzererfahrungen,
- Die Problembehandlung (Verhinderung, Erkennung und Behebung von Problemen); und
- Die kontinuierliche Verbesserung (Installieren der neuesten Updates und Verbesserungen in Bezug auf Benutzerproduktivität, Zuverlässigkeit, Effektivität und Sicherheit).

Bei der Bereitstellung von Onlinediensten wird Microsoft Kundendaten oder personenbezogene Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (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 nach den dokumentierten Anweisungen des Kunden.

#### Verarbeitung für legitime Geschäftstätigkeiten von Microsoft

Für die Zwecke dieses DPA umfassen „legitime Geschäftstätigkeiten von Microsoft“ die folgenden Aktivitäten, jeweils mit der Bereitstellung der Onlinedienste für den Kunden verbunden: (1) Abrechnungs- und Kontoverwaltung; (2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives); (3) interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; (5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im Folgenden beschriebenen Beschränkungen für die Offenlegung verarbeiteter Daten).

Bei der Verarbeitung für legitime Geschäftstätigkeiten von Microsoft wird Microsoft Kundendaten oder personenbezogene Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke.

### Offenlegung verarbeiteter Daten

Microsoft wird verarbeitete Daten ausschließlich wie folgt offenlegen oder den Zugang dazu ermöglichen: (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) personenbezogene Daten; und (c) alle weiteren Daten, die von Microsoft im Zusammenhang mit dem Onlinedienst verarbeitet werden und bei denen es sich nach Maßgabe des Volumenlizenzvertrags um vertrauliche Informationen des Kunden handelt. Die gesamte Verarbeitung der verarbeiteten Daten unterliegt der Vertraulichkeitsverpflichtung von Microsoft gemäß des Volumenlizenzvertrags.

Microsoft wird verarbeitete Daten gegenüber Strafverfolgungsbehörden nur offenlegen bzw. den Zugang dazu 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 gezwungen wird, verarbeitete Daten an die Strafverfolgungsbehörden weiterzugeben oder diesen den Zugang dazu einzuräumen, benachrichtigt Microsoft den Kunden unverzüglich und übermittelt eine Kopie der Anforderung, sofern dies nicht gesetzlich verboten ist.

Bei Erhalt einer sonstigen Anfrage von Dritten zur Offenlegung verarbeiteter Daten benachrichtigt Microsoft den Kunden unverzüglich; es sei denn, dies ist gesetzlich untersagt. Microsoft wird die Anfrage ablehnen, sofern Microsoft nicht gesetzlich verpflichtet ist, ihr nachzukommen. Wenn die Anfrage rechtsgültig ist, wird Microsoft versuchen, den Dritten zu verweisen, um die Daten direkt beim Kunden anzufordern.

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 verarbeitete 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 von Microsoft im Zusammenhang mit den Onlinediensten verarbeiteten personenbezogenen Daten werden als Kundendaten, Diagnosedaten oder Dienstgenerierte Daten empfangen. Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung des Onlinediensts zur Verfügung gestellt werden, sind ebenfalls Kundendaten. Pseudonymisierte Kennungen können in Diagnosedaten oder Dienstgenerierten Daten enthalten sein 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 ein Auftragsverarbeiter oder Unterauftragsverarbeiter der personenbezogenen Daten im Sinne der DSGVO ist, regeln die DSGVO-Bestimmungen in Anlage 3 die Verarbeitung und die Parteien stimmen zudem den nachfolgenden Bestimmungen in diesem Unterabschnitt zu („Verarbeitung personenbezogener Daten; DSGVO“):

#### 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 spezifischen Bestimmungen des jeweiligen Onlinediensts oder in diesem DPA wird etwas anderes bestimmt. Wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, verarbeitet Microsoft personenbezogene Daten nur nach den dokumentierten Anweisungen des Kunden. Der Kunde stimmt zu, dass sein Volumenlizenzvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Features der Onlinedienste durch den Kunden die vollständigen und dokumentierten Anweisungen des Kunden gegenüber Microsoft in Bezug auf

die Verarbeitung personenbezogener Daten darstellen. Informationen zur Verwendung und Konfiguration der Onlinedienste sind unter https://docs.microsoft.com/en-us/ oder einer entsprechenden, dieser nachfolgenden Stelle zu finden. Zusätzliche oder andere Anweisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Volumenlizenzvertrages des Kunden. In allen Fällen, in denen die DSGVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Anweisungen des Kunden, einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden.

Insoweit Microsoft der DSGVO unterliegende personenbezogene Daten zu legitimen Geschäftstätigkeiten von Microsoft, die mit der Bereitstellung der Onlinedienste für den Kunden verbunden sind, verwendet oder anderweitig verarbeitet, erfüllt Microsoft hinsichtlich dieser Verwendung die Pflichten eines unabhängigen Datenverantwortlicher gemäß der DSGVO. Microsoft akzeptiert die folgenden zusätzlichen Verantwortlichkeiten eines Daten-„Verantwortlichen“ für die Verarbeitung in Verbindung mit legitimen Geschäftstätigkeiten von Microsoft: (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 Verantwortlichkeit von Microsoft für eine solche Verarbeitung. Microsoft implementiert Sicherheitsmaßnahmen, um Kundendaten und personenbezogene Daten während der Verarbeitung zu schützen, einschließlich der in diesem DPA aufgeführten sowie der in Artikel 6, Absatz 4 DSGVO vorgesehenen Maßnahmen.

### 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 Anweisungen des Kunden sowie den Bestimmungen des DPA.
- **Art und Zweck der Verarbeitung.** Art und Zweck der Verarbeitung ist die Bereitstellung des Onlinediensts gemäß dem Volumenlizenzvertrag des Kunden und für die legitimen Geschäftstätigkeiten von Microsoft in Verbindung mit der Bereitstellung der Onlinedienste für den Kunden (wie ausführlicher im Abschnitt dieses DPA mit dem Titel „Art der Verarbeitung; Eigentumsverhältnisse“ weiter oben beschrieben).
- **Kategorien von Daten.** Zu den Arten von personenbezogenen Daten, die von Microsoft bei der Bereitstellung des Onlinediensts verarbeitet werden, gehören: (i) Personenbezogene Daten, die der Kunde in die Kundendaten aufnehmen möchte; und (ii) die in Artikel 4 DSGVO ausdrücklich genannten personenbezogenen Daten, die möglicherweise in Diagnosedaten oder dienstgenerierten Daten enthalten sind. Bei den Arten von personenbezogenen Daten, die der Kunde in die Kundendaten 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 1 zu Anlage 2 (Standardvertragsklauseln (Auftragsverarbeiter) des DPA) 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 1 zu Anlage 2 (Standardvertragsklauseln (Auftragsverarbeiter) des DPA) 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 des Onlinediensts und der Rolle von Microsoft als Auftragsverarbeiter personenbezogener Daten betroffener Personen konsistente Art und Weise nachzukommen. Wenn Microsoft die Anfrage einer betroffenen Person des Kunden erhält, um eines oder mehrerer ihrer Rechte aus der DSGVO in Verbindung mit einem Onlinedienst auszuüben, für den Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter ist, 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 des Onlinedienstes. 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 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 Beschreibungen der für den Onlinedienst geltenden Sicherheitskontrollen und anderen Informationen, die vom Kunden in Bezug auf die Sicherheitsverfahren und Sicherheitsrichtlinien von Microsoft angemessen angefordert werden.

Darüber hinaus müssen diese Maßnahmen den Anforderungen in ISO 27001, ISO 27002 und ISO 27018 entsprechen. Jeder Core-Onlinedienst erfüllt außerdem die in der Tabelle in Anlage 1 zu den OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) aufgeführten Kontrollstandards und -bestimmungen und setzt die in Anhang A beschriebenen Sicherheitsmaßnahmen zum Schutz von Kundendaten um.

Microsoft kann jederzeit Branchen- oder Verwaltungsstandards hinzufügen. Microsoft entfernt ISO 27001, ISO 27002 und ISO 27018 oder die Standards oder Bestimmungen in der Tabelle in Anlage 1 zu den OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) nicht; es sei denn, sie werden in der Branche nicht mehr angewendet und durch ihnen nachfolgende Normen, Standards oder Bestimmungen ersetzt (wenn vorhanden).

### Datenverschlüsselung

Kundendaten (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 Kundendaten, die im Ruhezustand („at rest“) in Onlinediensten gespeichert werden. 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 bereitstellt 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 (einschließlich darin enthaltener personenbezogener Daten) zu kontrollieren. Für Core-Onlinedienste unterhält Microsoft Zugriffskontrollmechanismen, die in der Tabelle „Sicherheitsmaßnahmen“ in Anhang 1 – Hinweise beschrieben sind; Microsoft-Mitarbeiter haben keinen ständigen Zugriff auf Kundendaten. Eine rollenbasierte Zugriffssteuerung wird eingesetzt, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf Kundendaten einem angemessenen Zweck dient, dass dieser Zugriff zeitlich begrenzt ist und unter Aufsicht des Vorgesetzten genehmigt ist.

### Pflichten des Kunden

Der Kunde ist allein für eine unabhängige Beurteilung verantwortlich, ob die technischen und organisatorischen Maßnahmen für einen bestimmten Onlinedienst 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 registriert sind oder im virtuellen Computer eines Microsoft Azure Kunden oder in einer Anwendung).

### Prüfung der Einhaltung

Microsoft wird Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft zur Verarbeitung von Kundendaten 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, die für Microsoft und den Prüfer gelten.

Insoweit die Prüfanforderungen des Kunden im Rahmen der Standardvertragsklauseln oder der Datenschutzvorschriften durch die Prüfberichte, Dokumentationen oder Informationen zur Einhaltung nicht angemessen erfüllt werden können, die Microsoft seinen Kunden allgemein zur Verfügung stellt, reagiert Microsoft umgehend auf die zusätzlichen Prüfanweisungen des Kunden. Vor Beginn einer Prüfung vereinbaren der Kunde und Microsoft gemeinsam Umfang, Zeitpunkt, Dauer, Kontroll- und Nachweisanforderungen sowie die Gebühren für die Prüfung; das Erfordernis einer Vereinbarung gestattet Microsoft jedoch nicht, die Durchführung der Prüfung unangemessen zu verzögern. Soweit für die Durchführung der Prüfung erforderlich stellt Microsoft die relevanten Verarbeitungssysteme, Einrichtungen und unterstützende Unterlagen zur Verfügung, die für die Verarbeitung von Kundendaten 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 den Onlinediensten 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.

Wenn die Standardvertragsklauseln gelten, findet dieser Absatz zusätzlich zu Klausel 5, Absatz f und Klausel 12, Absatz 2 der Standardvertragsklauseln Anwendung. Keine Bestimmung in diesem Abschnitt des DPA ändert die Standardvertragsklauseln oder die DSGVO-Bestimmungen oder beeinträchtigt die Rechte einer Aufsichtsbehörde oder einer betroffenen Person gemäß den Standardvertragsklauseln oder den Datenschutzvorschriften. Microsoft Corporation ist ein Drittbegünstigter der Regelungen 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 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 einem oder mehreren Administratoren des Kunden auf von Microsoft gewählte Art und Weise übermittelt, etwa per E-Mail. Es obliegt allein dem Kunden, sicherzustellen, dass die Administratoren des Kunden stets die korrekten Kontaktinformationen auf jedem betreffenden Portal für Onlinedienste pflegen. 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 sicherheitsrelevanter Vorfälle im Zusammenhang mit einem Onlinedienst unverzüglich mitzuteilen.

### Datenübermittlungen und Speicherstelle

#### Datenübermittlungen

Kundendaten 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 und personenbezogenen Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind, und Kundendaten und personenbezogenen Daten zur Bereitstellung der Onlinedienste zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den DPA-Bestimmungen beschrieben.

Für sämtliche Übermittlungen von Kundendaten und personenbezogenen Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz, um die Onlinedienste bereitzustellen, gelten die Standardvertragsklauseln in Anlage 2.

Microsoft hält sich an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung, Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz. 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. Privacy Shield und den damit verbundenen Verpflichtungen zertifiziert, auch wenn sich Microsoft im Hinblick auf das Urteil des Europäischen Gerichtshofs im Verfahren C-311/18 nicht auf das EU-U.S.-Privacy Shield Framework als rechtliche Grundlage für die Übermittlung von personenbezogenen Daten stützt. Microsoft stimmt zu, den Kunden zu

benachrichtigen, falls Microsoft der Ansicht ist, der Verpflichtung zur Bereitstellung des Grads an Schutz, der nach den Privacy-Shield-Regelungen erforderlich ist, nicht mehr nachkommen zu können..

### Ort der ruhenden Kundendaten

Im Fall der Core-Onlinedienste speichert Microsoft ruhende Kundendaten („at rest“) in bestimmten größeren geografischen Gebieten (jeweils „Geo“) wie in Anlage 1 zu den OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) beschrieben.

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

## Speicherung und Löschung von Daten

Während der Laufzeit des Abonnements des Kunden hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten 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 Kundendaten und personenbezogenen Daten innerhalb weiterer 90 Tage; es sei denn, Microsoft ist zur Aufbewahrung dieser Daten nach anwendbarem Recht berechtigt oder verpflichtet, oder durch diesen DPA 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 oder personenbezogenen Daten, soweit die Löschung wie in diesem Abschnitt beschrieben erfolgt.

## Vertraulichkeitsverpflichtung des Auftragsverarbeiters

Microsoft stellt sicher, dass die Mitarbeiter von Microsoft, die mit der Verarbeitung von Kundendaten und personenbezogenen Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden oder gemäß Beschreibung in diesem DPA verarbeiten; und (ii) sich verpflichten, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung des Beschäftigungsverhältnisses aufrechtzuerhalten. Microsoft führt für Mitarbeiter mit Zugriff auf Kundendaten 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 und personenbezogenen Daten durch Microsoft dar, wenn eine solche Zustimmung nach den Standardvertragsklauseln oder den Bestimmungen der DSGVO 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 oder personenbezogene Daten nur zugreifen und diese nur dazu nutzen darf, um die Dienstleistungen zu erbringen, für die Microsoft ihn beauftragt hat; und dass es ist ihm untersagt ist, Kundendaten 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.

Microsoft beauftragt gelegentlich möglicherweise neue Unterauftragsverarbeiter. Über jeden neuen Unterauftragsverarbeiter informiert Microsoft den Kunden mindestens 6 Monate bevor dieser Zugriff auf Kundendaten erhält (durch Aktualisierung der Website und Bereitstellung eines Mechanismus zur Benachrichtigung des Kunden über diese Aktualisierung). Darüber hinaus informiert Microsoft den Kunden über jeden neuen Unterauftragsverarbeiter mindestens 30 Tage bevor er Zugriff auf andere personenbezogene Daten erhält, die nicht in den Kundendaten enthalten sind. Wenn Microsoft einen neuen Unterauftragsverarbeiter für einen neuen Onlinedienst beauftragt, informiert Microsoft den Kunden vor der Verfügbarkeit dieses Onlinedienstes.

Wenn der Kunde einem neuen Unterauftragsverarbeiter nicht zustimmt, kann der Kunde alle Abonnements für den betreffenden Onlinedienst ohne Zahlung einer Strafe vor Ablauf der geltenden Kündigungsfrist mit schriftlicher Mitteilung 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 der betroffene Onlinedienst 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 des gekündigten Onlinedienstes aus den nachfolgenden Rechnungen an den Kunden oder seinen Handelspartner.

### 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 Definition dieser Begriffe im FERPA und dessen Durchführungsbestimmungen ein „Schulfunktionär“ mit „legitimen pädagogischen Interessen“ an den Kundendaten 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 des Onlinediensts 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 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-Kundenvertrags unter: http://aka.ms/CJISCustomerAgreement.

### HIPAA-Geschäftspartner

Wenn es sich bei dem Kunden um eine betroffene Einrichtung („covered entity“) oder einen Geschäftspartner („business associate“) handelt und dieser in seinen Kundendaten geschützte Gesundheitsinformationen („protected health information“) einbringt, wobei die entsprechenden Begriffsdefinitionen in 45 CFR § 160.103 maßgeblich sind, beinhaltet die Ausfertigung des Volumenlizenzvertrages des Kunden ebenfalls die Ausfertigung des HIPAA-Vertrags für Geschäftspartner (HIPAA Business Associate Agreement, „BAA“), dessen vollständiger Text die abgedeckten Onlinedienste aufführt und unter http://aka.ms/BAA verfügbar ist. Der Kunde kann den BAA ausschließen, indem er Microsoft die folgenden Informationen in einer schriftlichen Mitteilung (gemäß den Bestimmungen des Volumenlizenzvertrags des Kunden) zukommen lässt:

- den vollständigen Firmennamen des Kunden und aller verbundenen Unternehmen, die den BAA ausschließen; und
- wenn der Kunde mehrere Volumenlizenzverträge besitzt, muss mitgeteilt werden, für welchen Volumenlizenzvertrag der Ausschluss gilt.

### 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 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 aller 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, Nutzungsrechten oder in anderen Vereinbarungen zwischen Microsoft und dem Kunden eingegangen ist.

### Biometrische Daten

Wenn der Kunde einen Onlinedienst 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 Anweisungen 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.

### 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

Inhaltsverzeichnis / Allgemeine Bestimmungen

# Anhang A – Sicherheitsmaßnahmen

Microsoft hat für Kundendaten in den Core-Onlinediensten 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 | **Verantwortung für die Sicherheit.** Microsoft hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitsregeln und -verfahren verantwortlich sind.<br><br>**Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.** Microsoft-Mitarbeiter, die Zugang zu Kundendaten haben, sind zur Vertraulichkeit verpflichtet.<br><br>**Risikomanagementprogramm.** Microsoft führte eine Risikobewertung durch, bevor die Kundendaten verarbeitet oder die Onlinedienste-Leistungen gestartet wurden.<br><br>Microsoft archiviert Sicherheitsunterlagen im Rahmen der Aufbewahrungspflichten, nachdem sie nicht mehr in Kraft sind. |
| Asset-Management | **Anlagenbestand.** Microsoft führt einen Bestand aller Medien, auf denen Kundendaten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf Microsoft-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind.<br><br>**Asset-Handling**<br><br>- Microsoft klassifiziert Kundendaten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs auf Kundendaten zu ermöglichen.<br>- Microsoft legt Einschränkungen für das Drucken von Kundendaten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die Kundendaten enthalten.<br>- Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie Kundendaten auf tragbaren Geräten speichern, remote auf Kundendaten zugreifen oder Kundendaten außerhalb der Einrichtungen von Microsoft verarbeiten. |
| Personalsicherheit | **Sicherheitsschulungen.** 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. |
| Physische und umgebungsbezogene Sicherheit | **Physischer Zugang zu Einrichtungen.** Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Kundendaten verarbeitende Informationssysteme befinden, auf identifizierte, autorisierte Personen.<br><br>**Physischer Zugriff auf Komponenten.** Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/der zugelassenen Empfänger, Datum und Uhrzeit, der Anzahl von Medien und der darin enthaltenen Arten von Kundendaten.<br><br>**Schutz vor Unterbrechungen.** Microsoft nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern.<br><br>**Entsorgung von Komponenten.** Microsoft verwendet branchenübliche Prozesse, um Kundendaten zu löschen, wenn sie nicht mehr benötigt werden. |
| Kommunikations- und Betriebsmanagement | **Betriebsrichtlinie.** Microsoft führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter beschrieben sind, die Zugang zu Kundendaten haben.<br><br>**Datenwiederherstellungsverfahren**<br><br>- Microsoft erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es wurden im betreffenden Zeitraum keine Kundendaten aktualisiert) mehrere Kopien von Kundendaten, aus denen Kundendaten wiederhergestellt werden können.<br>- Microsoft bewahrt Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die Kundendaten verarbeitet werden.<br>- Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten regeln.<br>- Microsoft prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. Ausgenommen hiervon sind Verfahren für Azure Government Services, die alle zwölf Monate geprüft werden. |

| Domäne | Praktiken |
|---|---|
| | - 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.<br><br>**Malware.** Microsoft nimmt Anti-Schadsoftware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Kundendaten erhält, einschließlich bösartiger Software aus öffentlichen Netzwerken.<br><br>**Daten außerhalb von Landesgrenzen**<br><br>- Microsoft verschlüsselt Kundendaten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung.<br><br>- Microsoft schränkt den Zugriff auf Kundendaten in Medien ein, die die Einrichtungen von Microsoft verlassen.<br><br>**Ereignisprotokollierung.** Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung. |
| Zugriffskontrolle | **Zugriffsrichtlinie.** Microsoft führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Kundendaten haben.<br><br>**Zugriffsberechtigung**<br><br>- Microsoft führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf Microsoft-Systeme autorisiert sind, die Kundendaten enthalten.<br><br>- Microsoft deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.<br><br>- Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.<br><br>- Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen.<br><br>**Geringste Rechte**<br><br>- Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur gestattet, wenn dies erforderlich ist.<br><br>- Microsoft schränkt den Zugriff auf Kundendaten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.<br><br>**Integrität und Vertraulichkeit**<br><br>- 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.<br><br>- Microsoft speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind.<br><br>**Authentifizierung**<br><br>- Microsoft verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.<br><br>- Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.<br><br>- Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss.<br><br>- Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden.<br><br>- Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung.<br><br>- Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden.<br><br>- 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. |

| Domäne | Praktiken |
|---|---|
| | **Netzwerkdesign.** Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Kundendaten zu erhalten, auf die sie nicht zugreifen dürfen. |
| Handhabung eines Informationssicherheitsvorfalls | **Vorfallreaktionsablauf**<br>- 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.<br>- 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.<br>- Microsoft untersucht Offenlegungen von Kundendaten, einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage.<br>**Dienstüberwachung.** Das Microsoft-Sicherheitspersonal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Abhilfemaßnahmen vorzuschlagen. |
| Geschäftsfortführungsmanagement | - Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft Informationssysteme befinden, die Kundendaten verarbeiten.<br>- Der redundante Speicher von Microsoft sowie die Verfahren von Microsoft zur Wiederherstellung von Daten sind so konzipiert, dass versucht wird, Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren. |

Inhaltsverzeichnis / Allgemeine Bestimmungen

# Anlage 1 – Hinweise

## Professional Services

Für die Erbringung von Professional Services gelten die nachstehenden „Bestimmungen für Professional Services“. Wenn jedoch die Erbringung von Professional Services aufgrund einer separaten Vereinbarung erfolgt, gelten die Bestimmungen dieser separaten Vereinbarung für jene Professional Services.

Die Professional Services, auf die sich dieser Hinweis bezieht, sind keine Onlinedienste. Die übrigen Bestimmungen der Nutzungsrechte und des DPA gelten nur, wenn dies in den Bestimmungen für Professional Services weiter unten ausdrücklich festgelegt ist.

### Verarbeitung von Professional Services Daten; Eigentum

Microsoft wird Professional Services Daten nur verwenden und anderweitig verarbeiten, (a) um dem Kunden die Professional Services gemäß den dokumentierten Anweisungen des Kunden bereitzustellen; und (b) um legitime Geschäftstätigkeiten von Microsoft in Verbindung mit der Bereitstellung der Professional Services für den Kunden zu verfolgen, die nachstehend detailliert aufgeführt und eingegrenzt werden. Zwischen den Parteien behält der Kunde alle Rechte und das Eigentum an den Professional Services Daten. Microsoft erwirbt keine Rechte an Professional Services Daten, mit Ausnahme der Rechte, die der Kunde Microsoft gewährt, um die Professional Services für den Kunden bereitzustellen. Dieser Absatz berührt nicht die Rechte von Microsoft an Software oder Dienstleistungen, für die Microsoft dem Kunden eine Lizenz gewährt.

#### Verarbeitung zur Bereitstellung der Professional Services für Kunden

Für die Zwecke dieses DPA besteht die „Bereitstellung“ von Professional Services aus:

- der Bereitstellung der Professional Services, einschließlich technischem Support, professioneller Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und Lösungs-/Softwareentwicklung;
- der Problembehandlung (Verhinderung, Erkennung, Untersuchung, Minderung und Behebung von Problemen einschließlich Sicherheitsvorfällen); und
- der kontinuierlichen Verbesserung (Wartung der Professional Services einschließlich der Installation der neuesten Updates sowie Verbesserung von Zuverlässigkeit, Effektivität, Qualität und Sicherheit).

Bei der Bereitstellung von Professional Services wird Microsoft Professional Services Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (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 nach den dokumentierten Anweisungen des Kunden.

#### Verarbeitung für legitime Geschäftstätigkeiten von Microsoft

Für die Zwecke dieses DPA umfassen „legitime Geschäftstätigkeiten von Microsoft“ Folgendes: (1) Abrechnungs- und Kontoverwaltung; (2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives); (3) interne Berichterstattung und Geschäftsmodellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; (5) Verbesserung der Kernfunktionalität von Barrierefreiheit, Datenschutz oder Energieeffizienz; und (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im Folgenden beschriebenen Offenlegungsbeschränkungen), jeweils verbunden mit der Bereitstellung der Professional Services für den Kunden.

Bei der Verarbeitung für legitime Geschäftstätigkeiten von Microsoft wird Microsoft Professional Services Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke.

### Offenlegung von Professional Services Daten

Die Bestimmung „Offenlegung von verarbeiteten Daten“ der Datenschutzbestimmungen in diesem DPA gilt für den Auftrag des Kunden über Professional Services in Bezug auf Professional Services Daten.

### Verarbeitung personenbezogener Daten; DSGVO

Personenbezogene Daten, die Microsoft vom oder im Namen des Kunden im Zuge einer Vereinbarung mit Microsoft zur Verfügung gestellt werden, um Professional Services zu erlangen, sind ebenfalls Professional Services Daten.

Soweit Microsoft ein Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogener Daten im Sinne der DSGVO ist, regeln die DSGVO-Bestimmungen in Anlage 3 diese Verarbeitung. Die Parteien vereinbaren außerdem die folgenden Bestimmungen in diesem Unterabschnitt („Verarbeitung personenbezogener Daten; DSGVO“):

### Rollen und Verantwortlichkeiten von Auftragsverarbeiter und Verantwortlichem

Der Kunde und Microsoft vereinbaren, dass der Kunde der Verantwortliche für die personenbezogenen Daten ist, die in den Professional Services Daten enthalten sind, und Microsoft der Auftragsverarbeiter; es sei denn, (a) der Kunde handelt als Auftragsverarbeiter für personenbezogene Daten; in diesem Fall ist Microsoft Unterauftragsverarbeiter; oder (b) in diesen Bestimmungen für Professional Services wird etwas anderes bestimmt. Wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, verarbeitet Microsoft personenbezogene Daten nur nach den dokumentierten Anweisungen des Kunden. Der Kunde stimmt zu, dass sein Volumenlizenzvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit jeder zwischen den Parteien vereinbarten Servicevereinbarung die vollständigen und endgültig dokumentierten Anweisungen des Kunden an Microsoft für die Verarbeitung personenbezogener Daten darstellen, die in den Professional Services Daten enthalten sind. Zusätzliche oder abweichende Anweisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Volumenlizenzvertrags oder der Servicevereinbarungen des Kunden. In allen Fällen, in denen die DSGVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Anweisungen des Kunden, einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden.

Insoweit Microsoft Professional Services Daten, die der DSGVO unterliegen, im Zusammenhang mit legitimen Geschäftstätigkeiten von Microsoft verbunden mit der Bereitstellung der Professional Services für den Kunden verwendet oder anderweitig verarbeitet, erfüllt Microsoft hinsichtlich dieser Verwendung die Pflichten eines unabhängigen Datenverantwortlichen gemäß der DSGVO. Microsoft akzeptiert die folgenden zusätzlichen Verantwortlichkeiten eines Daten-„Verantwortlichen“ für die Verarbeitung in Verbindung mit seinen legitimen Geschäftstätigkeiten: (a) in Einklang mit den regulatorischen Anforderungen zu handeln, insoweit dies von der DSGVO gefordert wird; und (b) eine erhöhte Transparenz für Kunden zu schaffen und die Verantwortlichkeit von Microsoft für eine solche Verarbeitung zu bestätigen. Microsoft implementiert Sicherheitsmaßnahmen, um Professional Services Daten während der Verarbeitung zu schützen, einschließlich der in diesem DPA aufgeführten sowie der in Artikel 6, Absatz 4 DSGVO vorgesehenen Maßnahmen.

### Verarbeitungsdetails

Die Parteien bestätigen und vereinbaren Folgendes:

- **Gegenstand.** Der Gegenstand der Verarbeitung ist auf personenbezogene Daten innerhalb des Geltungsbereichs des Abschnitts dieser Bestimmungen für Professional Services mit dem Titel „Verarbeitung von zu Professional Services Daten; Eigentum“ weiter oben sowie auf personenbezogene Daten innerhalb des Geltungsbereichs der DSGVO eingeschränkt.
- **Dauer der Verarbeitung.** Die Dauer der Verarbeitung richtet sich nach den Anweisungen des Kunden und nach diesen Bestimmungen für Professional Services.
- **Art und Zweck der Verarbeitung.** Art und Zweck der Verarbeitung bestehen in der Bereitstellung von Professional Services gemäß dem Volumenlizenzvertrag des Kunden und sämtlicher Servicevereinbarungen sowie in legitimen Geschäftstätigkeiten von Microsoft in Verbindung mit der Bereitstellung der Professional Services für den Kunden (wie weiter im Abschnitt dieser Bestimmungen für Professional Services mit dem Titel „Verarbeitung von Professional Services Daten; Eigentum“ weiter oben beschrieben).
- **Kategorien von Daten.** Zu den Arten von personenbezogenen Daten, die von Microsoft im Zusammenhang mit der Bereitstellung von Professional Services verarbeitet werden, gehören (i) die personenbezogenen Daten, die der Kunde in die Professional Services Daten aufnimmt; sowie (ii) die personenbezogenen Daten, die in Artikel 4 DSGVO ausdrücklich genannt werden. Bei den Arten von personenbezogenen Daten, die der Kunde in die Professional Services Daten einbezieht, kann es sich um alle Arten personenbezogener Daten handeln, die in Verzeichnissen genannt werden, die der Kunde als Verantwortlicher gemäß Artikel 30 DSGVO führt, einschließlich der in Anhang 1 zu Anlage 2 (Standardvertragsklauseln (Auftragsverarbeiter) des DPA) aufgeführten Kategorien personenbezogener Daten.
- **Betroffene Personen.** Die Kategorien betroffener Personen sind Vertreter und Endanwender des Kunden, wie Mitarbeiter, Auftragnehmer, Partner und Kunden. Sie können auch andere Kategorien betroffener Personen umfassen, die vom Kunden als Verantwortlicher gemäß Artikel 30 DSGVO handelnd gepflegt werden, einschließlich der in Anhang 1 zu Anlage 2 (Standardvertragsklauseln (Auftragsverarbeiter) des DPA) aufgeführten Kategorien betroffener Personen.

### Rechte betroffener Personen; Unterstützung bei Anträgen

In Bezug auf die Professional Services Daten, die der Kunde in einem Onlinedienst speichert, hält sich Microsoft an die Verpflichtungen, die im Abschnitt „Rechte des Betroffenen; Unterstützung bei Anfragen“ des Abschnitts Datenschutzbestimmungen des DPA festgelegt sind. In Bezug auf andere Professional Services Daten löscht Microsoft alle Kopien der Professional Services Daten oder gibt sie zurück, im Einklang mit dem Abschnitt „Datenlöschung oder -rückgabe“ weiter unten.

### 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 Professional Services Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft stellt diese Richtlinie dem Kunden zur Verfügung, zusammen mit anderen Informationen über die Sicherheitspraktiken und -richtlinien von Microsoft, die der Kunde angemessen anfordert.

### Pflichten des Kunden

Die Bestimmung „Kundenpflichten“ des Abschnitts Datenschutzbestimmungen des DPA gilt für den Auftrag des Kunden für Professional Services in Bezug auf Professional Services Daten. Darüber hinaus stimmt der Kunde zu, in Bezug auf den Auftrag des Kunden über Professional Services keine anderen Professional Services Daten als Supportdaten an Microsoft zu übermitteln, die den Vorschriften des Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) oder des Health Insurance Portability and Accountability Act von 1996 (Pub. L. 104-191) (HIPAA) unterliegen würden.

## Meldung von Sicherheitsvorfällen

Die Bestimmung „Meldung von Sicherheitsvorfällen“ des Abschnitts Datenschutzbestimmungen des DPA gilt für den Auftrag des Kunden über Professional Services in Bezug auf Professional Services Daten.

## Datenübermittlungen

Professional Services-Daten, die Microsoft im Auftrag des Kunden verarbeitet, dürfen nur gemäß den Professional Services-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, Professional Services-Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind, und Professional Services-Daten zur Bereitstellung der Professional Services zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den Professional Services-Bestimmungen beschrieben.

Für sämtliche Übermittlungen von Professional Services-Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Professional Services gelten die Standardvertragsklauseln in Anlage 2.

Microsoft hält sich an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung, Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz. 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. Privacy Shield und den damit verbundenen Verpflichtungen zertifiziert, auch wenn sich Microsoft im Hinblick auf das Urteil des Europäischen Gerichtshofs im Verfahren C-311/18 nicht auf das EU-U.S.-Privacy Shield Framework als rechtliche Grundlage für die Übermittlung von personenbezogenen Daten stützt. Microsoft stimmt zu, den Kunden zu benachrichtigen, falls Microsoft der Ansicht ist, der Verpflichtung zur Bereitstellung des Grads an Schutz, der nach den Privacy-Shield-Regelungen erforderlich ist, nicht mehr nachkommen zu können.

## Datenlöschung oder Rückgabe

Microsoft löscht alle Kopien von Professional Services Daten oder gibt diese zurück, nachdem die geschäftlichen Zwecke erfüllt wurden, zu denen die Professional Services Daten erhoben oder übermittelt wurden (auf Kundenwunsch auch früher); es sei denn, Microsoft ist zur Aufbewahrung dieser Daten nach geltendem Recht berechtigt oder verpflichtet, oder durch diesen DPA autorisiert.

## Vertraulichkeitsverpflichtung des Auftragsverarbeiters

Microsoft stellt sicher, dass die Mitarbeiter von Microsoft, die mit der Verarbeitung von Professional Services Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden oder gemäß der Beschreibung in diesen Bestimmungen für Professional Services verarbeiten und (ii) verpflichtet sind, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung des Beschäftigungsverhältnisses aufrechtzuerhalten. Microsoft führt für Mitarbeiter mit Zugriff auf Professional Services 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 vorgenannten Berechtigungen stellen die vorherige schriftliche Zustimmung des Kunden zur Vergabe von Unteraufträgen zur Verarbeitung von Professional Services Daten durch Microsoft dar, wenn diese Zustimmung nach den Standardvertragsklauseln oder Bestimmungen der DSGVO erforderlich ist.

Microsoft ist für die Einhaltung der in Anlage 1 des DPA beschriebenen Verpflichtungen von Microsoft durch seine Unterauftragsverarbeiter von Professional Services Daten verantwortlich. Microsoft stellt durch einen schriftlichen Vertrag sicher, dass der Unterauftragsverarbeiter auf die Professional Services Daten nur zugreifen und diese nutzen darf, um die Dienste zu erbringen, mit deren Erbringung Microsoft ihn beauftragt hat, und es ist ihm untersagt, diese Daten für andere Zwecke zu verwenden. Microsoft stellt sicher, dass Unterauftragsverarbeiter durch schriftliche Vereinbarungen dazu verpflichtet werden, mindestens das mit diesen Bestimmungen für Professional Services von Microsoft verlangte Datenschutzniveau zu gewährleisten. Microsoft verpflichtet sich, die Unterauftragsverarbeiter zu beaufsichtigen, um sicherzustellen, dass diese vertraglichen Verpflichtungen erfüllt werden.

In Bezug auf Professional Services Daten außer Supportdaten ist eine Liste der Unterauftragsverarbeiter auf Anfrage bei Microsoft erhältlich. Wenn eine solche Liste angefordert wird, wird Microsoft mindestens 30 Tage, bevor neue Unterauftragsverarbeiter die Berechtigung für den Zugriff auf personenbezogene Daten erhalten, die Liste aktualisieren und den Kunden informieren, damit er die Aktualisierung zur Kenntnis nehmen kann.

Wenn der Kunde einem neuen Unterauftragsverarbeiter nicht zustimmt, kann der Kunde den betroffenen Auftrag über Professional Services kündigen, indem er vor Ablauf der Kündigungsfrist eine schriftliche Kündigung einreicht. 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.

In Bezug auf Supportdaten unterliegt die Verwendung von Unterauftragsverarbeitern durch Microsoft im Zusammenhang mit der Bereitstellung von technischem Support für Onlinedienste denselben Einschränkungen und Verfahren, die für die Verwendung von Unterauftragsverarbeitern in Verbindung mit den Onlinediensten gelten, wie in der Bestimmung „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ im DPA beschrieben.

### Zusätzliche Bedingungen für Supportdaten

#### Sicherheit der Supportdaten

Microsoft ergreift geeignete technische und organisatorische Maßnahmen zum Schutz der Supportdaten und hält diese aufrecht. Diese Maßnahmen müssen den Anforderungen der ISO 27001, ISO 27002 und ISO 27018 entsprechen.

#### Bildungseinrichtungen

Die Bestätigungen und Verträge von Microsoft und die Pflichten des Kunden zur Einholung der elterlichen Zustimmung und Übermittlung der Benachrichtigung, die im Abschnitt „Bildungseinrichtungen“ in den Datenschutzbestimmungen des DPA dargelegt sind, gelten auch für Supportdaten.

### 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 Professional Services 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, Nutzungsrechten oder in anderen Vereinbarungen zwischen Microsoft und dem Kunden eingegangen ist.

### Biometrische Daten

Wenn der Kunde eine Professional 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 Anweisungen 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.

# Anlage 2 – Die Standardvertragsklauseln (Auftragsverarbeiter)

Die Ausführung des Volumenlizenzvertrags durch den Kunden umfasst die Ausführung dieser Anlage 2, die von der Microsoft Corporation gegengezeichnet ist.

In Ländern, in denen eine behördliche Zulassung für den Einsatz von Standardvertragsklauseln erforderlich ist, können die Standardvertragsklauseln nicht gemäß der EU-Verordnung der Europäischen Kommission 2010/87/EU (vom Februar 2010) geltend gemacht werden, um den Datenexport aus dem Land zu legitimieren, es sei denn, der Kunde verfügt über die erforderliche behördliche Genehmigung.

Ab dem 25. Mai 2018 und danach werden Verweise auf verschiedene Artikel der Richtlinie 95/46/EG in den nachstehenden Standardvertragsklauseln als Verweise auf die relevanten und entsprechenden Artikel in der DSGVO behandelt.

Gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist, haben der Kunde (als Datenexporteur) und die Microsoft Corporation (als Datenimporteur, deren Unterschrift unten zu finden ist) folgende Vertragsklauseln (die „Klauseln“ oder „Standardvertragsklauseln“) vereinbart, um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

**Klausel 1. Begriffsbestimmungen**

**Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:**

(a) die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

(b) der „Datenexporteur“ ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

(c) der „Datenimporteur“ ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

(d) der „Unterauftragsverarbeiter“ ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

(e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

(f) die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere, wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

**Klausel 2. Einzelheiten der Übermittlung**

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

**Klausel 3. Drittbegünstigtenklausel**

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

**Klausel 4. Pflichten des Datenexporteurs**

Der Datenexporteur erklärt sich bereit und garantiert, dass:

(a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

(b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

(c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

(d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

(e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

(f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

(g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

(h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

(i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und;

(j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

**Klausel 5. Pflichten des Datenimporteurs**

Der Datenimporteur erklärt sich bereit und garantiert, dass

(a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

(b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

(c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

(d) er den Datenexporteur unverzüglich informiert über:

(i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

(ii) jeden zufälligen oder unberechtigten Zugang und

(iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

(e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

(f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

(g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

(h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

(i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

(j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

**Klausel 6. Haftung**

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

**Klausel 7. Schlichtungsverfahren und Gerichtsstand**

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

**Klausel 8. Zusammenarbeit mit Kontrollstellen**

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

**Klausel 9. Anwendbares Recht.**

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

**Klausel 10. Änderung des Vertrags**

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

**Klausel 11. Vergabe eines Unterauftrags**

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6, Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

**Klausel 12. Pflichten nach Beendigung der Datenverarbeitungsdienste**

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

**Anhang 1 zu den Standardvertragsklauseln**

**Datenexporteur:** Kunde ist Datenexporteur. Der Datenexporteur ist ein Nutzer der im DPA und in den OST definierten Onlinedienste oder Professional Services.

**Datenimporteur:** Der Datenimporteur ist die MICROSOFT CORPORATION, ein weltweit tätiger Hersteller von Software und Services.

**Betroffene Personen:** Betroffene Personen sind die Vertreter des Datenexporteurs und Endnutzer, einschließlich Angestellte, Auftragnehmer, Mitarbeiter und Kunden des Datenexporteurs. Zu den betroffenen Personen können auch Personen gehören, die personenbezogene Daten an Benutzer der vom Datenimporteur bereitgestellten Dienste übermitteln möchten oder Kontakt mit solchen Benutzern aufnehmen möchten. Microsoft bestätigt, dass sich der Kunde je nach Nutzung des Onlinedienstes oder der Professional Services dafür entscheiden kann, personenbezogene Daten von einer der folgenden Arten von betroffenen Personen in die personenbezogenen Daten aufzunehmen:

- Mitarbeiter, Auftragnehmer und Zeitarbeiter (aktuelle, ehemalige, zukünftige) des Datenexporteurs;
- Angehörige der oben genannten Personen;
- Partner/Kontaktpersonen des Datenexporteurs (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeiter von Partnern/Kontaktpersonen (juristische Personen) (aktuelle, ehemalige, zukünftige),
- Benutzer (z. B. Kunden, Klienten, Patienten, Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen des Datenexporteurs sind,
- Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern des Datenexporteurs zusammenarbeiten, kommunizieren oder anderweitig interagieren und/oder Kommunikationsmittel wie Anwendungen und Websites verwenden, die vom Datenexporteur 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
- Spezialisten mit beruflichen Privilegien (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 Onlinedienste oder Professional Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung des Onlinedienstes oder der Professional Services die Möglichkeit hat, personenbezogene Daten aus einer der folgenden Kategorien in die personenbezogenen Daten aufzunehmen:

- Personenbezogene Basisdaten (z. B. Geburtsort, Straßenname und Hausnummer (Adresse), Postleitzahl, Wohnort, Land der Ansässigkeit, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum) einschließlich der personenbezogenen Basisdaten von Familienmitgliedern und Kindern;
- Authentifizierungsdaten (z. B. Benutzername, Kennwort oder PIN-Code, Sicherheitsfrage, Audit-Trail);
- Kontaktinformationen (z. B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten);
- Eindeutige Identifikationsnummern und Signaturen (z. B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentennummer, Patientennummer, Signatur, eindeutige Kennung bei der Verfolgung von Cookies oder ähnliche Technologien);
- Pseudonymisierte Kennungen;
- Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartenname und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität);
- Geschäftsinformationen (z. B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf);
- Biometrische Daten (z. B. DNS, Fingerabdrücke und Iris-Scans),
- Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden);
- Fotos, Videos und Audio;
- Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören);
- Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartennummer, MAC-Adresse);
- Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen);
- Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und

Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen);

- Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung);
- Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis);
- Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird;
- Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Straftaten); oder
- Alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten.

**Verarbeitung:** Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

**a. Dauer und Ziel der Datenverarbeitung.** Die Dauer der Datenverarbeitung entspricht dem Zeitraum, der im geltenden Volumenlizenzvertrag zwischen dem Datenexporteur und der Microsoft-Gesellschaft, dem diese Standardvertragsklauseln angefügt sind („Microsoft“), festgelegt ist. Das Ziel der Datenverarbeitung ist die Erbringung von Onlinediensten und Professional Services.

**b. Umfang und Zweck der Datenverarbeitung.** Umfang und Zweck der Verarbeitung personenbezogener Daten werden im Abschnitt „Verarbeitung personenbezogener Daten; DSGVO“ des DPA beschrieben. Der Datenimporteur betreibt ein globales Netzwerk von Rechenzentren und Verwaltungs-/Unterstützungseinrichtungen und die Verarbeitung kann in jedem Land erfolgen, in dem der Datenimporteur oder seine Unterauftragsverarbeiter solche Einrichtungen in Übereinstimmung mit dem Abschnitt „Sicherheitsverfahren und -richtlinien“ des DPA betreiben.

**c. Zugriff auf Kundendaten und personenbezogene Daten.** Für die im entsprechenden Volumenlizenzvertrag angegebene Laufzeit verpflichtet sich der Datenimporteur nach eigener Wahl und nach Maßgabe des anwendbaren Rechts zur Umsetzung von Artikel 12(b) der EU-Datenschutzrichtlinie entweder: (1) dem Datenexporteur die Möglichkeit zu geben, Kundendaten und personenbezogene Daten zu berichtigen, zu löschen oder zu sperren, oder (2) diese Berichtigungen, Löschungen oder Sperrungen in dessen Namen vorzunehmen.

**d. Anweisungen des Datenexporteurs.** Für Onlinedienste und Professional Services handelt der Datenimporteur ausschließlich auf Weisung des Datenexporteurs wie von Microsoft vermittelt.

**e. Löschung oder Rückgabe von Kundendaten und personenbezogenen Daten.** Nach Ablauf oder Beendigung der Verwendung der Onlinedienste oder Professional Services durch den Datenexporteur kann der Datenexporteur Kundendaten und personenbezogene Daten extrahieren und der Datenimporteur löscht die Kundendaten und personenbezogenen Daten, jeweils in Übereinstimmung mit den für den Vertrag geltenden DPA-Bestimmungen.

**Unterauftragsverarbeiter:** Nach dem DPA kann der Datenimporteur andere Unternehmen damit beauftragen, im Namen des Datenimporteurs begrenzte Dienstleistungen zu erbringen, z. B. Kundensupport. Solchen Vertragspartnern ist es gestattet, Kundendaten und personenbezogene Daten nur für die Bereitstellung der Dienste zu erhalten, mit deren Bereitstellung der Datenimporteur sie beauftragt hat, und es ist ihnen untersagt, Kundendaten und personenbezogene Daten für andere Zwecke zu nutzen.

**Anhang 2 zu den Standardvertragsklauseln**

Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die vom Datenimporteur im Einklang mit Klausel 4(d) und 5(c) implementiert wurden:

1. **Mitarbeiter.** Die Mitarbeiter des Datenimporteurs verarbeiten Kundendaten oder personenbezogene Daten nicht ohne Genehmigung. Die Mitarbeiter sind verpflichtet, die Vertraulichkeit solcher Kundendaten und personenbezogenen Daten zu wahren. Diese Verpflichtung besteht auch nach dem Ende der Beschäftigung fort.

2. **Kontaktperson für Datenschutz.** Der Datenschutzbeauftragte des Datenimporteurs ist unter folgender Adresse erreichbar:

Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052, USA

3. **Technische und organisatorische Maßnahmen.** Der Datenimporteur hat geeignete technische und organisatorische Maßnahmen, interne Kontrollen und IT-Sicherheitsroutinen eingerichtet und wird diese aufrechterhalten, um Kundendaten und personenbezogene Daten, so wie sie im

Abschnitt „Sicherheitsverfahren und Sicherheitsrichtlinien“ des DPA definiert sind, gegen unbeabsichtigten Verlust, Zerstörung oder Veränderung, unbefugte Offenlegung oder unbefugten Zugriff oder unrechtmäßige Zerstörung wie folgt zu schützen: Die technischen und organisatorischen Maßnahmen, internen Kontrollen und IT-Sicherheitsroutinen, die im Abschnitt „Sicherheitsverfahren und Sicherheitsrichtlinien“ des DPA dargelegt sind, werden hiermit durch diesen Verweis in diesen Anhang 2 aufgenommen und sind für den Datenimporteur verbindlich, als ob sie in diesem Anhang 2 in ihrer Gesamtheit dargelegt wären.

**Unterzeichnung der Standardvertragsklauseln, Anlage 1 und Anlage 2 im Namen des Datenimporteurs:**

Signature 851B7BFC2840456 Rajesh Jha DocuSigned By: Rajesh Jha .....

Rajesh Jha, Executive Vice President

Microsoft Corporation

One Microsoft Way, Redmond, WA 98052, USA

Inhaltsverzeichnis / Allgemeine Bestimmungen

# Anlage 3 – 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 OST und des DPA, die anderweitig für ein bestimmtes Onlinedienstabonnement gelten, 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 Bestimmungen für Onlinedienste 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-Pflichten: Artikel 28, 32 und 33**

**1.** 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))

**2.** 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 Anweisung des Kunden zu verarbeiten, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, sofern Microsoft nicht durch das Recht der Union oder des Mitgliedstaats, dem Microsoft unterliegt, hierzu verpflichtet ist; In solch einem Fall teilt Microsoft dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

**(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 sämtliche personenbezogenen Daten zu löschen oder dem Kunden zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

**(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))

**3.** 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))

**4.** 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))

**5.** 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))

**6.** Der Kunde und Microsoft unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Kunden verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. (Artikel 32(4))

**7.** 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.

Inhaltsverzeichnis / Allgemeine Geschäftsbedingungen