Microsoft Professional   
Services-Datenschutznachtrag

September 2022

Am 20. September 2022 in englischer Sprache veröffentlicht. Übersetzungen werden von Microsoft unter https://aka.ms/professionalservicesdpa veröffentlicht, sobald sie verfügbar sind. Diese Bestimmungen sind für Microsoft seit dem 20. September 2022 verbindlich.

**Inhalt**

[Einführung 3](#_Toc116951047)

[Anwendbare DPA-Bestimmungen und -Aktualisierungen 3](#_Toc116951048)

[Elektronische Benachrichtigungen 3](#_Toc116951049)

[Frühere Versionen 3](#_Toc116951050)

[Definitionen 4](#_Toc116951051)

[Allgemeine Bestimmungen 5](#_Toc116951052)

[Einhaltung von gesetzlichen Regelungen 5](#_Toc116951053)

[Datenschutzbestimmungen 5](#_Toc116951054)

[Umfang 5](#_Toc116951055)

[Art der Datenverarbeitung; Eigentumsverhältnisse 6](#_Toc116951056)

[Offenlegung verarbeiteter Daten 6](#_Toc116951057)

[Verarbeitung personenbezogener Daten; DSGVO 6](#_Toc116951058)

[Datensicherheit 7](#_Toc116951059)

[Meldung von Sicherheitsvorfällen 9](#_Toc116951060)

[Datenübermittlungen 9](#_Toc116951061)

[Löschung von Professional Services Daten 9](#_Toc116951062)

[Vertraulichkeitsverpflichtung des Auftragsverarbeiters 10](#_Toc116951063)

[Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern 10](#_Toc116951064)

[Bestimmungen des kalifornischen Datenschutzgesetzes   
(California Consumer Privacy Act, CCPA) 10](#_Toc116951065)

[Biometrische Daten 10](#_Toc116951066)

[So kontaktieren Sie Microsoft 11](#_Toc116951067)

[Anhang A – Sicherheitsmaßnahmen 12](#_Toc116951068)

[Anhang B – Betroffene Personen und Kategorien personenbezogener Daten 15](#_Toc116951069)

[Anhang C – Nachtrag zu zusätzlichen   
Schutzmaßnahmen 17](#_Toc116951070)

[Anlage 1 – Bestimmungen der Datenschutz-Grundverordnung der Europäischen Union 18](#_Toc116951071)

Einführung

Die Parteien stimmen überein, dass dieser Nachtrag zum Datenschutz für Microsoft Professional Services (Data Protection Addendum, DPA) ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Professional Services Daten im Zusammenhang mit Professional Services festlegt. Das DPA wird durch Bezugnahme in den Enterprise Services-Arbeitsauftrag oder den Microsoft Business Support Services-Arbeitsauftrag (oder die Nachfolge-Arbeitsaufträge) aufgenommen. Für die Nutzung anderer Produkte und Dienstleistungen durch den Kunden gelten gesonderte Bestimmungen einschließlich unterschiedlicher Datenschutz- und Sicherheitsbestimmungen.

Im Falle eines Widerspruchs oder einer Ungereimtheit zwischen diesem DPA und anderen Bestimmungen im Kundenvertrag hat dieses DPA Vorrang. Die Bestimmungen dieses DPAs ersetzen alle widersprüchlichen Bestimmungen der Microsoft-Datenschutzbestimmungen, die ansonsten für die Verarbeitung von Professional Services Daten oder personenbezogenen Daten, wie hier definiert, gelten könnten.

Microsoft gibt in diesem DPA gegenüber allen Kunden Zusagen bezüglich der Professional Services. Diese Zusagen sind für Microsoft in Bezug auf den Kunden verbindlich, unabhängig von (1) der Version des DPAs, die ansonsten für jeden Kunden gilt, oder (2) jedes anderen Vertrags, der auf dieses DPA verweist.

Anwendbare DPA-Bestimmungen und -Aktualisierungen

**Beschränkungen für Aktualisierungen**

Wenn der Kunde vorhandene Professional Services im Rahmen eines Arbeitsauftrags verlängert oder kauft, gelten die dann aktuellen DPA-Bestimmungen und bleiben während der Laufzeit dieser Professional Services unverändert.

**Neue Features, Ergänzungen oder zugehörige Software**

Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen gilt, dass dann, wenn Microsoft neue Angebote, Funktionen oder Ergänzungen einführt (d. h. die zuvor nicht enthalten waren), Microsoft Bestimmungen in den DPA einführen oder Aktualisierungen am DPA vornehmen kann, die sich auf die Nutzung dieser neuen Features, Ergänzungen oder zugehörige Software durch den Kunden beziehen. Wenn diese Bestimmungen wesentliche nachteilige Änderungen des DPA enthalten, die für die Nutzung von Professional Services durch den Kunden gelten, bietet Microsoft dem Kunden die Möglichkeit, die Nutzung der neuen Features, Ergänzungen oder zugehörige Software abzulehnen. Wenn der Kunde die neuen Features, Ergänzungen oder zugehörige Software nicht nutzt, haben neue Bestimmungen oder Aktualisierungen dieses DPA mindestens das gleiche Datenschutzniveau wie die aktuellen Bestimmungen.

**Behördliche Vorschriften und Verpflichtungen**

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

Elektronische Benachrichtigungen

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

Frühere Versionen

Die DPA-Bestimmungen gelten für aktuell verfügbare Professional Services. Kunden können frühere Versionen der DPA-Bestimmungen unter <http://aka.ms/MPSDPA-Archive> nachsehen oder ihren Microsoft-Kundenbetreuer kontaktieren.

Definitionen

Begriffe mit großen Anfangsbuchstaben, die in diesem DPA verwendet, aber nicht definiert werden, haben die im Vertrag verwendeten Bedeutungen. In diesem DPA werden die folgenden definierten Begriffe verwendet:

„Vertrag“ bedeutet, soweit zutreffend, die Description of Services (Beschreibung der Services) und alle Exponate, Arbeitsaufträge, Enterprise Services-Arbeitsaufträge, Microsoft Business Support Services-Arbeitsaufträge und den entsprechenden Microsoft-Rahmenvertrag, wie z. B. Den Microsoft Business- und Service-Vertrag.

„Datenschutzvorschriften“ umfasst die DSGVO, die lokalen EU/EWR-Datenschutzgesetze und alle anwendbaren Gesetze, Vorschriften und sonstigen rechtlichen Anforderungen in Bezug auf (a) Datenschutz und Datensicherheit und (b) Nutzung, Erhebung, Aufbewahrung, Speicherung, Sicherheit, Offenlegung, Übermittlung, Entsorgung und sonstige Verarbeitung Personenbezogener Daten.

„DPA-Bestimmungen“ oder „DPA“ bezeichnet die Bestimmungen dieses DPAs.

„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 und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

„DSGVO-Bestimmungen“ sind die Bestimmungen in Anlage 2, nach denen Microsoft verbindliche Zusagen hinsichtlich der Verarbeitung personenbezogener Daten nach Art. 28 DSGVO macht.

„Lokale EU/EWR-Datenschutzgesetze“ bedeutet jede untergeordnete Gesetzgebung und Rechtsvorschrift zur Umsetzung der DSGVO.

„Personenbezogene Daten“ bezeichnet 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, Standortdaten oder einer Online-Kennung, oder zu einem oder mehreren besonderen Merkmal(en), die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

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

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

„Professional Services-Daten“ bezeichnet alle Daten, einschließlich Text-, Ton-, Video-, Bilddateien oder Software, die Microsoft von oder im Namen eines Kunden zur Verfügung gestellt werden (oder in Bezug auf die der Kunde Microsoft berechtigt, sie aus einem Produkt zu beziehen) oder die anderweitig von oder im Namen von Microsoft durch einen Vertrag mit Microsoft zum Erhalt von Professional Services bezogen oder verarbeitet werden.

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

„Unterauftragsverarbeiter“ bezeichnet sonstige Auftragsverarbeiter, die Microsoft zur Verarbeitung von Professional Services Daten hinzuzieht, einschließlich aller Unterauftragnehmer, die Professional Services Daten verarbeiten.

In diesem DPA verwendete, im Quelltext kleingeschriebene Begriffe, die nicht definiert werden, wie „Verletzung des Schutzes personenbezogener Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Profilierung“, „personenbezogene Daten“ und „betroffene Person“ haben die Bedeutung gemäß Art. 4 DSGVO, unabhängig davon, ob die DSGVO anwendbar ist. Die Begriffe „Datenimporteur“ und „Datenexporteur“ haben die in den Standardvertragsklauseln angegebenen Bedeutungen.

Allgemeine Bestimmungen

Einhaltung von gesetzlichen Regelungen

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

Der Kunde muss alle Gesetze und Vorschriften einhalten, die für seine Nutzung von Professional Services gelten, einschließlich Gesetzen zu biometrischen Daten, zur Vertraulichkeit der Kommunikation sowie Datenschutzvorschriften. Der Kunde muss ermitteln, ob die Professional Services für die Speicherung und Verarbeitung von Informationen, die einem bestimmten Gesetz oder einer bestimmten Vorschrift unterliegen, geeignet sind, und muss die Professional Services in einer Weise nutzen, die mit den gesetzlichen und regulatorischen Verpflichtungen des Kunden vereinbar ist. Der Kunde ist dafür verantwortlich, auf alle Anfragen Dritter bezüglich der Nutzung der Professional Services durch den Kunden zu antworten.

Datenschutzbestimmungen

Dieser Abschnitt des DPA umfasst die folgenden Absätze:

* Umfang
* Art der Datenverarbeitung; Eigentumsverhältnisse;
* Offenlegung verarbeiteter Daten
* Verarbeitung personenbezogener Daten; DSGVO
* Datensicherheit
* Meldung von Sicherheitsvorfällen
* Datenübermittlungen
* Löschung von Daten
* Vertraulichkeitsverpflichtung des Auftragsverarbeiters
* Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern
* 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 Professional Services mit Ausnahme der in diesem Abschnitt beschriebenen Fälle.

**Vorschauversionen oder Services mit eingeschränkter Freigabe**

Vorschauversionen oder Services mit eingeschränkter Freigabe können eventuell weniger oder andere Datenschutz- und Sicherheitsmaßnahmen vorsehen als die, die normalerweise in den Professional Services vorhanden sind. Sofern nicht anders angegeben, sollte der Kunde eine sorgfältige Abwägung vornehmen, bevor er Vorschauversionen oder Services mit eingeschränkter Freigabe zur Verarbeitung von personenbezogenen oder anderen Daten nutzt, die gesetzlichen oder verwaltungsrechtlichen Anforderungen unterliegen.

Vorschauen erfüllen nur die Bestimmungen der Abschnitte „Verarbeitung personenbezogener Daten; DSGVO“, „Datenübermittlung“, des ersten Absatzes des Abschnitts „Sicherheitsverfahren und Sicherheitsrichtlinien“ unter „Datensicherheit“, der ersten beiden Absätze der „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“, Anhang B, Anhang C und der DSGVO-Bestimmungen (Anlage 1).

Vorschauversionen oder Services mit eingeschränkter Freigabe bezeichnet eine Vorschau, eine Beta-Version, Angebote zur optionalen Evaluierung oder andere Services oder Funktionen zur Vorabveröffentlichung oder eingeschränkten Freigabe, einschließlich aller als solche bezeichneten oder etikettierten Versionen.

**Eskalationsunterstützung**

Der Datenschutznachtrag für Produkte und Dienste von Microsoft, verfügbar unter <http://aka.ms/mpstomosdpa>, enthält die Datenschutz- und Sicherheitsbestimmungen für die Eskalationsunterstützung, d. h. Supportanfragen, die zur Lösung an die Produktentwicklung oder den Betrieb weitergeleitet wurden, einschließlich aller darin enthaltenen personenbezogenen Daten („Eskalationsunterstützung“). Daher gelten die Bestimmungen in diesem DPA nicht für die Bereitstellung von Eskalationsunterstützung.

Art der Datenverarbeitung; Eigentumsverhältnisse

Microsoft wird die Professional Services Daten nur nutzen und anderweitig verarbeiten, um dem Kunden die Professional Services gemäß den dokumentierten Anweisungen des Kunden bereitzustellen. Zwischen den Parteien behält der Kunde alle Rechte und das Eigentum an den Professional Services Daten. Microsoft erwirbt keine Rechte an den Professional Services Daten, mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt. Dieser Absatz berührt nicht die Rechte von Microsoft an Produkten, für die Microsoft dem Kunden eine Lizenz erteilt.

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

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

* der Bereitstellung der Professional Services, einschließlich technischem Support, professioneller Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und Lösungs-/Softwareentwicklung. Um Zweifel auszuschließen, die Bereitstellung von technischem Support umfasst Verbesserungen an den zugrunde liegenden Produkten und Services von Microsoft, die vom Kunden abonniert oder genutzt werden, basierend auf Problemen, die während der Bereitstellung von Professional Services festgestellt wurden.
* der Fehlerbehebung (Verhindern, Erkennen, Untersuchen, Mindern und Beheben von Problemen, einschließlich Sicherheitsvorfällen und Problemen, die bei der Bereitstellung von Professional Services festgestellt wurden) und
* der laufenden Verbesserung der vom Kunden abonnierten oder genutzten Professional Services (Aufrechterhaltung der Professional Services, Verbesserung der Zuverlässigkeit, Effizienz, Qualität und Sicherheit der Professional Services und Behebung von Softwaremängeln).

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 Erstellung neuer Funktionen, Services oder Produkte oder zu anderen Zwecken, es sei denn, eine solche Verwendung oder Verarbeitung erfolgt nach den dokumentierten Anweisungen des Kunden.

Offenlegung verarbeiteter Daten

Microsoft wird keine verarbeiteten Daten offenlegen oder Zugang zu ihnen gewähren, außer: (1) wie vom Kunden angewiesen; (2) wie in diesem DPA beschrieben; oder (3) wie gesetzlich vorgeschrieben. Für die Zwecke dieses Abschnitts bezeichnet „verarbeitete Daten“ Folgendes: (a) Professional Services Daten, (b) in Professional Services Daten enthaltene Personenbezogene Daten und (c) alle weiteren Daten, die von Microsoft im Zusammenhang mit den Professional Services verarbeitet werden und bei denen es sich um vertrauliche Informationen des Kunden im Rahmen des Vertrags handelt. Die gesamte Verarbeitung der verarbeiteten Daten unterliegt der Vertraulichkeitsverpflichtung von Microsoft gemäß dem Vertrag.

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

Nach Erhalt einer sonstigen Anfrage von Dritten zur Weitergabe verarbeiteter Daten benachrichtigt Microsoft den Kunden unverzüglich; es sei denn, dies ist gesetzlich untersagt. Microsoft wird die Anfrage ablehnen, sofern nicht gesetzlich vorgeschrieben. Wenn die Anfrage zulässig 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 Zugriff auf 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 dem Dritten die Basiskontaktinformationen des Kunden zur Verfügung stellen.

Verarbeitung personenbezogener Daten; DSGVO

Alle personenbezogenen Daten, die in den Professional Services Daten enthalten sind und die Microsoft vom Kunden oder im Namen des Kunden durch eine Vereinbarung mit Microsoft zum Erhalt von Professional Services zur Verfügung gestellt werden, sind ebenfalls Professional Services Daten. Pseudonymisierte Identifikatoren können auch durch IT-Systeme im Zusammenhang mit Professional Services generiert werden und sind ebenfalls personenbezogene Daten. Alle personenbezogenen Daten, pseudonymisiert oder nicht identifiziert, aber nicht anonymisiert, oder aus personenbezogenen Daten abgeleitete, personenbezogene Daten sind ebenfalls personenbezogene Daten.

Soweit Microsoft ein Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogener Daten im Sinne der DSGVO ist, regeln die Bestimmungen der DSGVO in Anlage 1 die Verarbeitung, und die Parteien stimmen zudem den nachfolgenden Bestimmungen in diesem Unterabschnitt zu („Verarbeitung personenbezogener Daten; DSGVO“):

**Rollen und Verantwortlichkeiten von Auftragsverarbeiter und Verantwortlichem**

Der Kunde und Microsoft stimmen überein, dass der Kunde der für die personenbezogenen Daten Verantwortliche und Microsoft der Auftragsverarbeiter dieser Daten ist, es sei denn, der Kunde handelt als Auftragsverarbeiter der personenbezogenen Daten; in diesem Fall ist Microsoft Unterauftragsverarbeiter. Wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter von Personenbezogenen Daten handelt, wird Microsoft Personenbezogene Daten nur nach den dokumentierten Anweisungen des Kunden verarbeiten. Der Kunde stimmt zu, dass sein Vertrag (einschließlich dieser DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Dokumentation der Professional Services und der Nutzung von Professional Services durch den Kunden die vollständigen dokumentierten Anweisungen des Kunden für Microsoft in Bezug auf die Verarbeitung Personenbezogener Daten darstellt. Zusätzliche oder andere Weisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Vertrages des Kunden. In allen Fällen, in denen die DSGVO Anwendung findet und der Kunde ein Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Anweisungen des Kunden, einschließlich der Benennung von Microsoft als zum Auftragsverarbeiter oder Unterauftragsverarbeiter, von dem jeweiligen Verantwortlichen genehmigt wurden.

**Verarbeitungsdetails**

Die Parteien bestätigen und vereinbaren Folgendes:

* **Gegenstand.** Der Gegenstand der Verarbeitung ist auf personenbezogene Daten innerhalb des Geltungsbereichs des Abschnitts dieses DPAs mit dem Titel „Art der Datenverarbeitung; Eigentumsverhältnisse“ sowie der DSGVO beschränkt.
* **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 Erbringung der Professional Services in Anwendung des Vertrags mit dem Kunden (wie weiter oben im Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse“ dieses DPA beschrieben).
* **Kategorien von Daten.** Zu den Arten von Personenbezogenen Daten, die von Microsoft bei der Bereitstellung von Professional Services verarbeitet werden, gehören: (i) personenbezogene Daten, die der Kunde in die Professional Services Daten aufnehmen möchte; und (ii) die in Art. 4 DSGVO ausdrücklich genannten Daten. Bei den Arten personenbezogener Daten, die der Kunde in die Professional Services-Daten aufnimmt, kann es sich um alle Kategorien personenbezogener Daten handeln, die in den vom Kunden als für die Verarbeitung Verantwortlicher nach Artikel 30 der DSGVO geführten Aufzeichnungen genannt werden, einschließlich der in Anhang B unter „Betroffene Personen und Kategorien personenbezogener Daten“ aufgeführten Kategorien personenbezogener Daten.
* **Betroffene Personen.** Bei den Kategorien betroffener Personen handelt es sich um Vertreter und Endanwender des Kunden, wie Mitarbeiter, Auftragnehmer, Partner und Kunden. Sie können auch andere Kategorien betroffener Personen umfassen, die in den vom Kunden als für die Verarbeitung Verantwortlicher nach Artikel 30 der DSGVO geführten Aufzeichnungen genannt werden, einschließlich der unter „Betroffene Personen und Kategorien personenbezogener Daten“ in Anhang B aufgeführten Kategorien betroffener Personen.

**Rechte der betroffenen Personen; Unterstützung bei Anfragen**

Microsoft ermöglicht dem Kunden in einer Weise, die mit der Funktionalität der Professional Services und der Rolle von Microsoft als Auftragsverarbeiter von persönlichen Daten der betroffenen Personen vereinbar ist, die Möglichkeit, die Gesuche der betroffenen Personen auf Ausübung ihrer Rechte nach der DSGVO zu befürworten. Wenn Microsoft eine Anfrage der betroffenen Person des Kunden erhält, mindestens eines ihrer Rechte nach der DSGVO in Verbindung mit den Professionellal Services, für die Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter ist, auszuüben, leitet Microsoft die betroffene Person weiter, damit sie ihre Anfrage direkt an den Kunden richten kann. Der Kunde ist dafür verantwortlich, auf eine solche Anfrage zu antworten, einschließlich, falls erforderlich, der Nutzung der dem Kunden zu diesem Zweck zur Verfügung gestellten Funktionalität. Microsoft kommt angemessenen Anfragen des Kunden nach Unterstützung bei der Bearbeitung von Anfragen betroffener Personen nach.

**Aufzeichnung der 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 und hält diese aufrecht, um die Professional Services Daten vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten zu schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft wird diese Richtlinie dem Kunden zusammen mit Beschreibungen der Sicherheitskontrollen für die Professional Services und anderen Informationen zur Verfügung stellen, die vom Kunden in angemessener Weise bezüglich der Sicherheitsverfahren und -richtlinien von Microsoft angefordert werden.

Darüber hinaus erfüllen diese Maßnahmen die Anforderungen in ISO 27001, ISO 27002 und ISO 27018. Professional Services implementiert und unterhält die in Anhang A dargelegten Sicherheitsmaßnahmen zum Schutz von Professional Services-Daten.

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 der OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) nicht; es sei denn, sie werden in der Branche nicht mehr angewendet und durch nachfolgende Normen, Standards oder Bestimmungen ersetzt (wenn vorhanden).

**Datenverschlüsselung**

Professional Services Daten (einschließlich aller darin enthaltenen Personenbezogenen Daten), die über öffentliche Netzwerke zwischen dem Kunden und Microsoft oder zwischen Microsoft-Rechenzentren übertragen werden, werden standardmäßig verschlüsselt.

**Datenzugriff**

Microsoft nutzt Zugriffsmechanismen, die auf dem Grundsatz der geringsten Berechtigung beruhen, um den Zugriff auf Professional Services Daten (einschließlich darin enthaltener Personenbezogener Daten) zu kontrollieren. Microsoft unterhält Zugriffskontrollmechanismen, die in der Tabelle „Sicherheitsmaßnahmen“ in Anhang A – Benachrichtigungen beschrieben sind. Eine rollenbasierte Zugriffssteuerung wird eingesetzt, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf Professional Services Daten einem angemessenen Zweck dient und unter Ausicht des Vorgesetzten genehmigt ist.

**Pflichten des Kunden**

Der Kunde ist für eine unabhängige Beurteilung verantwortlich, ob die technischen und organisatorischen Maßnahmen für die Professional Services den Anforderungen des Kunden entsprechen, einschließlich seiner Sicherungsverpflichtungen gemäß geltenden Datenschutzvorschriften. Der Kunde bestätigt und erklärt, dass (unter Berücksichtigung des Stands der Technik, der Einführungskosten und der Art, des Umfangs, des Umstandes 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 die Implementierung und Aufrechterhaltung von Datenschutzvorrichtungen und Sicherheitsmaßnahmen für Komponenten, die er bereitstellt oder kontrolliert.

**Prüfung der Einhaltung**

Microsoft wird Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft bei der Verarbeitung von Professional Services 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 von 2010 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. In dem für die Durchführung der Prüfung erforderlichen Umfang stellt Microsoft die relevanten Verarbeitungssysteme, Einrichtungen und unterstützende Unterlagen zur Verfügung, die für die Verarbeitung von Professional Services Daten durch Microsoft, ihre verbundenen Unternehmen und ihre 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 Zugang zu Daten von anderen Kunden von Microsoft oder zu Systemen oder Einrichtungen von Microsoft, die nicht an den Professional Services beteiligt sind. Der Kunde ist für sämtliche Kosten und Gebühren Zusammenhang mit einer solchen Prüfung verantwortlich, einschließlich aller angemessenen Aufwendungen und Honorare für die Arbeitszeit, 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.

Keine Bestimmung in diesem Abschnitt des DPA ändert die Standardvertragsklauseln von 2021 oder die DSGVO-Bestimmungen oder beeinträchtigt die Rechte einer Aufsichtsbehörde oder einer betroffenen Person gemäß den Standardvertragsklauseln von 2021 oder den Datenschutzvorschriften. Microsoft Corporation ist ein Drittbegünstigter der Regelungen dieses Abschnitts.

Meldung von Sicherheitsvorfällen

Wenn Microsoft von einer Sicherheitsverletzung Kenntnis erlangt, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugriff auf Professional Services Daten während der Verarbeitung durch Microsoft führt (jeweils ein „Sicherheitsvorfall“), wird Microsoft den Kunden unverzüglich und ohne schuldhaftes Verzögern (1) über den Sicherheitsvorfall informieren; (2) den Sicherheitsvorfall untersuchen und dem Kunden detaillierte Informationen über den Sicherheitsvorfall zur Verfügung stellen; (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 mindestens einem Ansprechpartner des Kunden für die Professional Services auf von Microsoft gewählte Art und Weise übermittelt, etwa per E-Mail. Es liegt in der alleinigen Verantwortung des Kunden sicherzustellen, dass die Ansprechpartner des Kunden korrekte Kontaktinformationen aufrechterhalten.

Der Kunde ist allein verantwortlich für die Einhaltung seiner Verpflichtungen gemäß den für ihn geltenden Gesetzen zur Benachrichtigung über Sicherheitsvorfälle und die Erfüllung der Benachrichtigungspflichten gegenüber Dritten im Zusammenhang mit Sicherheitsvorfällen.

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

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

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

Datenübermittlungen

Professional Services Daten, die Microsoft im Auftrag des Kunden verarbeitet, dürfen in die USA oder in jedes andere Land, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind, übertragen, dort gespeichert und verarbeitet werden. Der Kunde beauftragt Microsoft mit der Durchführung einer solchen Übertragung von Professional Services Daten in ein solches Land und mit der Speicherung und Verarbeitung von Professional Services Daten, um die Professional Services zu erbringen.

Für sämtliche Übermittlungen von Professional Services-Daten, einschließlich personenbezogener Daten, aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Professional Services gelten die von Microsoft implementierten Standardvertragsklauseln von 2021. Darüber hinaus unterliegen Übertragungen aus dem Vereinigten Königreich dem von Microsoft implementierten IDTA. Für die Zwecke dieses DPA bezeichnet „IDTA“ das International Data Transfer Addendum (Zusatz zur internationalen Datenübermittlung) zu den Standardvertragsklauseln der Europäischen Kommission für internationale Datenübermittlungen, herausgegeben vom UK Information Commissioner’s Office gemäß Paragraf 119A(1) des UK Data Protection Act 2018.

Microsoft hält sich an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums, des Vereinigten Königreichs 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 Schweiz-U.S. Privacy Shield und den damit verbundenen Verpflichtungen zertifiziert, auch wenn sich Microsoft im Hinblick auf das Urteil des Europäischen Gerichtshofs in der Rechtssache C-311/18 nicht auf das EU-U.S.-Privacy Shield-Abkommen als rechtliche Grundlage für die Übermittlung von Personenbezogenen Daten stützt. Microsoft stimmt zu, den Kunden zu benachrichtigen, falls Microsoft der Ansicht ist, der zur Bereitstellung des Grads an Schutz, der nach den Privacy-Shield-Regelungen erforderlich ist, nicht mehr nachkommen zu können.

Löschung von Professional Services Daten

Der Kunde hat während der gesamten Dauer seines Professional Services Engagements die Möglichkeit, auf Professional Services Daten zuzugreifen, sie zu extrahieren und zu löschen.

Microsoft löscht alle Kopien von Professional Services Daten nach Erfüllung der Geschäftszwecke, für die die Professional Services Daten erhoben oder übermittelt wurden, oder auf schriftlichen Antrag des Kunden auch früher.

Vertraulichkeitsverpflichtung des Auftragsverarbeiters

Microsoft stellt sicher, dass die Mitarbeiter, die mit der Verarbeitung von Professional Services Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden oder wie in diesem DPA beschrieben verarbeiten und (ii) sich verpflichten, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung der Beschäftigungsverhältnisses zu wahren. Microsoft führt für Mitarbeiter mit Zugriff auf Professional Services Daten entsprechend der geltenden und für Microsoft anwendbaren Datenschutzvorschriften und Branchenstandards regelmäßige und verpflichtende Datenschutz-, Datensicherheits- und Sensibilisierungsschulungen durch.

Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern

Microsoft kann Unterauftragsverarbeiter beauftragen, Dienstleistungen in ihrem Namen 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 von 2010 oder Bestimmungen der DSGVO erforderlich ist.

Microsoft ist für die Einhaltung der Verpflichtungen von Microsoft in diesem DPA 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 nur auf diejenigen Professional Services Daten zugreifen und diese nutzen darf, um die Services zu erbringen, mit denen Microsoft ihn beauftragt hat, und es ihm untersagt ist, Professional Services Daten für andere Zwecke zu nutzen. Microsoft wird sicherstellen, dass Unterauftragsverarbeiter an 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.

Bezüglich Support Services steht eine Liste der aktuellen Unterauftragsverarbeiter von Microsoft zur Verfügung: https://aka.ms/servicesapprovedsuppliers. Von Zeit zu Zeit kann Microsoft neue Unterauftragsverarbeiter einsetzen. Microsoft benachrichtigt den Kunden (durch Aktualisierung der Website und Bereitstellung eines Mechanismus zur Benachrichtigung des Kunden über diese Aktualisierung) über jeden neuen Unterauftragsverarbeiter mindestens 30 Tage vor dem Zeitpunkt, zu dem der Unterauftragsverarbeiter Zugang zu Professional Services Daten erhält.

Bezüglich Beratungsleistungen sind die Hinweise zum Einsatz von Unterauftragsverarbeitern, die für die Ausführung von Arbeiten eingesetzt werden, auf Verlangen unter <https://aka.ms/consultingapprovedsuppliers> erhältlich. Der Kunde kann auch verlangen, über Aktualisierungen zu den Unterauftragsverarbeitern, die für die Ausführung von Arbeiten eingesetzt werden, informiert zu werden. Kunden, die eine Benachrichtigung über Aktualisierungen zu den Unterauftragsverarbeitern, die für die Ausführung von Services eingesetzt werden, angefordert haben, gewährt Microsoft den Zugang zu den Professional Services Daten erst nach schriftlicher Genehmigung oder 30 Tage nach der Benachrichtigung.

Wenn der Kunde einen neuen Unterauftragsverarbeiter nicht billigt, kann er die zutreffenden Leistungsbeschreibungen, wie z. B. einen Enterprise Services-Arbeitsauftrag, für die betroffenen Professional Services ohne Kündigungsgebühr beenden, indem er vor dem Ablauf der entsprechenden Kündigungsfrist eine schriftliche Kündigung einreicht. Der Kunde kann zusammen mit der Kündigung auch eine Erklärung der Gründe für seine Ablehnung beifügen, um es Microsoft zu ermöglichen, diesen neuen Unterauftragsverarbeiter anhand der vorgebrachten Bedenken neu zu bewerten. Nach der Kündigung wird Microsoft die Zahlungsverpflichtungen für alle zutreffenden unbezahlten Arbeiten im Zusammenhang mit den gekündigten Professional Services in den Folgerechnungen an den Kunden streichen.

Bestimmungen des kalifornischen Datenschutzgesetzes (California Consumer Privacy Act, CCPA)

Wenn Microsoft Personenbezogene Daten im Rahmen des kalifornischen Verbraucherdatenschutzgesetzes (California Consumer Privacy Act – CCPA) verarbeitet, geht Microsoft gegenüber dem Kunden die folgenden zusätzlichen Verpflichtungen 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, nutzen oder offenlegen, einschließlich Ausnahmeregelungen für den „Verkauf“. Unter keinen Umständen verkauft Microsoft solche Daten. Diese CCPA-Bestimmungen beschränken oder verringern nicht die Datenschutzverpflichtungen, die Microsoft gegenüber dem Kunden in den DPA-Bestimmungen oder in anderen Verträgen zwischen Microsoft und dem Kunden eingeht.

Biometrische Daten

Wenn der Kunde 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 Datenschutzbestimmungen 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.

So kontaktieren Sie 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 unter <http://go.microsoft.com/?linkid=9846224> verfügbare Datenschutzformular 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: Datenschutz

One Microsoft Place

South County Business Park

Leopardstown

Dublin 18, D18 P521, Irland

Anhang A – Sicherheitsmaßnahmen

Microsoft hat die folgenden Sicherheitsmaßnahmen für Professional Services Daten 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.  **Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.** Microsoft-Mitarbeiter mit Zugang zu den Professional Services Daten sind zur Vertraulichkeit verpflichtet.  **Risikomanagement-Programm.** Microsoft führte vor der Verarbeitung von Professional Services Daten eine Risikobewertung durch. Microsoft archiviert ihre Sicherheitsunterlagen gemäß ihren Aufbewahrungspflichten auf, nachdem sie nicht mehr in Kraft sind. |
| Asset-Management | **Anlagenbestand.** Microsoft führt einen Bestand aller Medien, auf denen Professional Services Daten gespeichert sind. Der Zugriff auf die Bestände dieser Medien ist auf Mitarbeiter von Microsoft beschränkt, die schriftlich dazu berechtigt sind.  **Handhabung von Beständen.**  - Microsoft klassifiziert Professional Services Daten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs darauf zu ermöglichen.  - Microsoft legt Beschränkungen für das Drucken von Professional Services Daten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die Professional Services Daten enthalten.  - Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie Professional Services Daten auf tragbaren Geräten speichern, remote auf Professional Services Daten zugreifen oder Professional Services Daten 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 ökologische Sicherheit | **Physischer Zugang zu Einrichtungen.** Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Professional Services Daten verarbeiten, auf identifizierte, autorisierte Personen.  **Physischer Zugang zu Komponenten.** Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Professional Services Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Daten von Professional Services Daten.  **Schutz vor Unterbrechungen.** Microsoft nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern.  **Entsorgung von Komponenten.** Microsoft nutzt branchenübliche Prozesse, um Professional Services Daten zu löschen, wenn sie nicht mehr benötigt werden. |
| Kommunikation und Betriebsführung | **Betriebsrichtlinie.** Microsoft führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die relevanten Verfahren und Verantwortlichkeiten der Mitarbeiter, die Zugang zu Professional Services Daten haben, beschrieben werden.  **Verfahren zur Datenwiederherstellung**  - Microsoft erstellt kontinuierlich, mindestens aber einmal pro Woche (es sei denn, in diesem Zeitraum wurden keine Professional Services Daten aktualisiert), mehrere Kopien von Professional Services Daten an, aus denen Professional Services Daten wiederhergestellt werden können.  - Microsoft bewahrt Kopien von Professional Services Daten und Datenwiederherstellungsverfahren getrennt von dem Ort auf, an dem sich die primären Computergeräte, die die Professional Services Daten verarbeiten, befinden.  - Microsoft verfügt über bestimmte Verfahren für den Zugriff auf Kopien von Professional Services Daten.  - Microsoft prüft die Datenwiederherstellungsverfahren mindestens jährlich.  - Microsoft protokolliert die 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.  **Malware.** Microsoft nimmt Anti-Malware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Professional Services Daten erhält, einschließlich Schadsoftware, die aus öffentlichen Netzwerken stammt.  **Daten über Landesgrenzen hinweg**  - Microsoft verschlüsselt Professional Services-Daten, die über öffentliche Netzwerke übertragen werden, oder ermöglicht es dem Kunden, diese zu verschlüsseln.  - Microsoft schränkt den Zugriff auf Professional Services Daten in Medien ein, die die Einrichtungen von Microsoft verlassen.  **Ereignisprotokollierung**  - Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Professional Services Daten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung. |
| Zugriffskontrolle | **Zugriffsrichtlinie.** Microsoft führt ein Verzeichnis der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Professional Services Daten haben.  **Zugriffsberechtigung**  - Microsoft führt und aktualisiert einen Datensatz der Mitarbeiter, die zum Zugriff auf Microsoft-Systeme berechtigt sind, die Professional Services Daten enthalten.  - Microsoft deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.  - Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.  - Microsoft stellt sicher, dass in den Fällen, in denen mehr als eine Person Zugang zu Systemen hat, die Professional Services Daten enthalten, die einzelnen Personen über separate Kennungen/Anmeldedaten verfügen.  **Geringste Rechte**  - Technischen Supportmitarbeitern ist der Zugriff auf Professional Services Daten nur gestattet, wenn dies erforderlich ist.  - Microsoft schränkt den Zugriff auf Professional Services Daten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.  **Integrität und Vertraulichkeit**  - 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.  - Microsoft speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind.  **Authentifizierung**  - Microsoft verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.  - Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen.  - Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss.  - Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden.  - Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht Kunden eine solche Überwachung.  - Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden.  - 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.  **Netzwerkdesign.** Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Professional Services Daten zu erhalten, auf die sie nicht zugreifen dürfen. |
| Handhabung von Informationssicherheitsvorfällen | **Vorfallreaktionsablauf**  - Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe 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.  - Microsoft untersucht Offenlegungen von Professional Services Daten einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage.  **Dienstüberwachung.** Das Microsoft-Sicherheitspersonal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Wartungsmaßnahmen vorzuschlagen. |
| Geschäftsfortführungsmanagement | - Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft-Informationssysteme befinden, die Professional Services Daten verarbeiten.  - Bei Microsoft sind redundante Speicherung und ihre Verfahren zur Datenwiederherstellung so konzipiert, dass versucht wird, Professional Services Daten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren. |

Anhang B – Betroffene Personen und Kategorien personenbezogener Daten

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

* (Derzeitige, ehemalige, zukünftige) Mitarbeiter, Auftragnehmer und Zeitarbeitnehmer des Kunden;
* Angehörige der oben genannten Personen;
* Partner/Kontaktpersonen des Kunden (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 Kunden sind,
* Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern des Kunden zusammenarbeiten, kommunizieren oder anderweitig interagieren und/oder Kommunikationsmittel wie Anwendungen und Websites verwenden, die vom Kunden bereitgestellt werden;
* Stakeholder oder einzelne Personen, die passiv mit dem Kunden interagieren (z. B. weil sie Gegenstand einer Untersuchung oder Studie sind oder in Dokumenten oder in Korrespondenz mit dem Kunden erwähnt werden);
* Minderjährige Personen; oder
* Spezialisten mit beruflichen Privilegien (z. B. Ärzte, Anwälte, Notare, Kirchenmitarbeiter usw.).

**Kategorien von Daten:** Die personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Professional Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung 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 Informationen (z. B. DNA, Fingerabdrücke und Iris-Erfassungen);
* Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden);
* Fotos, Videos und Audio;
* Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören);
* Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartennummer, MAC-Adresse);
* Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen);
* Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen);
* Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung);
* Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis);
* Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird;
* Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Straftaten); oder
* Alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten.

Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen

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

Dieser Nachtrag ergänzt den DPA und ist Teil desselben. Er ändert oder modifiziert diesen jedoch nicht.

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

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

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

1. **Freistellung betroffener Personen.** Vorbehaltlich der Abschnitte 3 und 4 stellt Microsoft eine betroffene Person von jeglichen materiellen oder immateriellen Schäden frei, die der betroffenen Person dadurch entstehen, dass Microsoft personenbezogene Daten der betroffenen Person offenlegt, die als Reaktion auf eine Anordnung einer Nicht-EU-/EWR-Regierungsstelle oder einer Strafverfolgungsbehörde unter Verletzung der Verpflichtungen von Microsoft gemäß Kapitel V der DSGVO übermittelt wurden (eine „Relevante Offenlegung“). Ungeachtet des Vorstehenden ist Microsoft nicht verpflichtet, die betroffene Person gemäß dieses Abschnitt 2 zu entschädigen, soweit die betroffene Person bereits eine Entschädigung für denselben Schaden erhalten hat, sei es von Microsoft oder anderweitig.
2. **Freistellungsbedingungen.** Die Freistellung nach Abschnitt 2 setzt voraus, dass die betroffene Person zur angemessenen Zufriedenheit von Microsoft Folgendes nachweist:
3. Microsoft hat eine Relevante Offenlegung vorgenommen;
4. Die Relevante Offenlegung war die Grundlage eines offiziellen Verfahrens der Behörde oder Strafverfolgungsbehörde in einem Land außerhalb der EU/des EWR gegen die betroffene Person und
5. die Relevante Offenlegung führte unmittelbar zu materiellen oder immateriellen Schäden für die betroffene Person.

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

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

1. **Schadensausmaß.** Die Freistellung nach Abschnitt 2 ist auf materielle und immaterielle Schäden gemäß DSGVO beschränkt und schließt Folgeschäden und alle anderen Schäden aus, die nicht das Ergebnis eines Verstoßes von Microsoft gegen die DSGVO sind.
2. **Rechtsausübung.** Rechte, die betroffenen Personen in diesem Nachtrag gewährt werden, können von den betroffenen Personen unabhängig von den Beschränkungen in den Abschnitten 3 oder 6 der Standardvertragsklauseln Microsoft gegenüber durchgesetzt werden. Die betroffene Person darf einen Anspruch nach diesem Nachtrag nur auf individueller Basis erheben und nicht als Teil einer Klassen-, Sammel-, Gruppen- oder Repräsentativklage. Rechte, die betroffenen Personen im Rahmen dieses Nachtrags gewährt werden, sind nur für die betroffene Person bestimmt und nicht abtretbar.
3. **Änderungsmitteilung.** Microsoft stimmt zu und gewährleistet, dass Microsoft keinen Grund zu der Annahme hat, dass die für Microsoft oder ihre Unterauftragsverarbeiter geltenden Gesetze, einschließlich in jedem Land, in das Microsoft oder ihre Unterauftragsverarbeiter personenbezogene Daten übermitteln, Microsoft daran hindern, die vom Kunden erhaltenen Weisungen und ihre Verpflichtungen aus dieser Ergänzung oder aus den Standardvertragsklauseln 2021 zu erfüllen, und dass Microsoft im Fall einer Änderung dieser Gesetze, die wahrscheinlich erhebliche nachteilige Auswirkungen auf die in dieser Ergänzung oder in den Standardvertragsklauseln vorgesehenen Zusicherungen und Verpflichtungen haben werden, den Kunden unverzüglich über die Änderung informieren wird, sobald diese Microsoft bekannt ist; in diesem Fall ist der Kunde berechtigt, die Datenübermittlung auszusetzen und/oder den Vertrag zu kündigen.

Anlage 1 – Bestimmungen der Datenschutz-Grundverordnung der Europäischen Union

Microsoft geht die in den Bestimmungen der DSGVO 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 des DPA, die ansonsten für einen bestimmten Auftrag anwendbar ist, 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 kundeneigenen, personenbezogenen Daten und Microsoft die Auftragsverarbeiterin dieser Daten ist, es sei denn, der Kunde handelt als Auftragsverarbeiter personenbezogener Daten; in diesem Fall ist Microsoft Unterauftragsverarbeiterin. 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 im Microsoft Professional Services-Datenschutznachtrag 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 spezifische oder allgemeine schriftliche Genehmigung des Kunden keine weiteren Auftragsverarbeiter hinzuziehen. Im Fall einer allgemeinen schriftlichen Genehmigung wird Microsoft den Kunden 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 Bestimmungen der DSGVO nach dem Recht der Europäischen Union (nachfolgend „Union“ genannt) oder des Mitgliedstaats. Diese sind für Microsoft in Bezug auf den Kunden verbindlich. Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Art der Personenbezogenen Daten, die Kategorien betroffener Personen sowie die Pflichten und Rechte des Kunden sind im Kundenvertrag festgelegt, einschließlich dieser DSGVO-Bestimmungen. Insbesondere ist Microsoft verpflichtet:

**(a)** personenbezogene Daten nur entsprechend den dokumentierten Anweisungen von Seiten des Kunden zu verarbeiten. Das schließt die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation ein, es sei denn, die Übermittlung wird vom Recht der EU oder einem Mitgliedstaat verlangt. In solch einem Fall wird Microsoft den Kunden vor der Verarbeitung über jene rechtliche Anforderung informieren, es sei denn, dieses Recht verbietet eine derartige Informationsübertragung aufgrund wichtigen öffentlichen Interesses.

**(b)** sicherzustellen, dass sich Personen mit der Genehmigung, personenbezogene Daten zu verarbeiten, zu Vertraulichkeit verpflichten oder einer angemessenen gesetzlichen Verpflichtung zu Vertraulichkeit unterliegen.

**(c)** alle notwendigen Maßnahmen gemäß Artikel 32 der DSGVO zu treffen.

**(d)** die Bedingungen anzuerkennen, auf die in den Paragraphen 1 und 3 bezüglich der Beauftragung eines weiteren Auftragsverarbeiters verwiesen wird.

**(e)** die Art der Verarbeitung zu berücksichtigen, den Kunden durch angemessene technische und organisatorische Maßnahmen soweit wie möglich zu unterstützen und im Sinne der Kundenverpflichtung auf Anfragen zur Ausübung der Rechte der betroffenen Person, wie in Kapitel III der DSGVO festgelegt, zu reagieren.

**(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 Beendigung der Leistungserbringung auf Wunsch des Kunden sämtliche personenbezogenen Daten mit Bezug auf die Verarbeitung zu löschen oder dem Kunden zurückzugeben. Des Weiteren werden vorhandene Kopien gelöscht, es sei denn, das Recht der EU oder eines Mitgliedstaates verlangt die Speicherung der personenbezogenen Daten.

**(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 zu unterstützen.

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

**3.** Falls Microsoft die Dienste eines weiteren Auftragsverarbeiters in Anspruch nimmt, um im Auftrag des Kunden bestimmte Verarbeitungstätigkeiten auszuführen, werden diesem weiteren Auftragsverarbeiter durch einen Vertrag oder ein anderes Rechtsinstrument nach dem Recht der EU 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 die Anforderungen der DSGVO erfüllt. Sollte jener Auftragsverarbeiter seinen Datenschutzverpflichtungen nicht nachkommen, bleibt Microsoft gegenüber dem Kunden für die Erfüllung der Pflichten des genannten Auftragsverarbeiters uneingeschränkt verantwortlich. (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 zur zeitnahen Wiederherstellung der Verfügbarkeit und zum Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls sowie

**(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.** Microsoft benachrichtigt den Kunden unverzüglich, sobald Microsoft Kenntnis in Bezug auf einen Datenschutzverstoß erlangt. (Art. 33 Absatz 2). Diese Benachrichtigung enthält auch die Informationen, die ein Auftragsverarbeiter einem Verantwortlichen nach Artikel 33, Absatz 3 zur Verfügung stellen muss, soweit diese Informationen Microsoft in angemessener Weise zur Verfügung stehen.