Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Bauten und Logistik
Abteilung Beschaffung

Rahmenvertrag
(20007) 608 Public Clouds Bund

Firma: Microsoft Schweiz GmbH

Inhaltsverzeichnis

Nr. 13 und 14 (entfernt): Vorbestehende Vertragswerke; BK nicht zuständig

*Diese Dokumente sind direkt dem Rahmenvertrag angehängt

Unterzeichnung:

A [redacted]

Microsoft Volume Licensing

Zusatzvereinbarung zu den Vertragsunterlagen

Agreement Nummer [redacted] 7-XR7BIUMGD

Diese Zusatzvereinbarung („Zusatzvereinbarung") wird zwischen den auf dem beigefügten Programmunterschriftsblatt verzeichneten Parteien geschlossen. Sie ergänzt den oben genannten Beitritt oder Vertrag. Alle in dieser Zusatzvereinbarung verwendeten, aber nicht definierten Begriffe haben dieselben Bedeutungen wie in jenem Beitritt oder Vertrag.

Konzernvertrag

Zusatzvereinbarung ID - CTM Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

Publiziert auf der Plattform www.simap.ch (Nr. 204859 am 07.12.2020)

[redacted]

Inhaltsverzeichnis

[redacted]

Ausgangslage, Projektbeschreibung und Ziele

Auf Grundlage der öffentlichen Ausschreibung sowie der dazugehörigen Unterlagen vom 07.12.2020 auf der Publikationsplattform www.simap.ch hat die Firma ein Angebot zu den von der Vergabestelle nachgefragten Leistungen eingereicht. Der Firma wurde mit Publikation Nr. 1202937 auf www.simap.ch am 24.06.2021 der Zuschlag erteilt. Die diesbezüglichen vertraglichen Bedingungen werden in der vorliegenden Vertragsurkunde sowie den dazugehörigen Bestandteilen geregelt.

Definitionen

BBL	Bundesamt für Bauten und Logistik
Bedarfsstelle	BK - DTI
Beschaffungsstelle	BBL
Bezugsberechtigte	siehe Definition in Ziff.2 dieses Rahmenvertrags
Beitrittsunternehmen	Beschaffungsstelle, Bedarfsstelle, Vergabestelle, oder Bezugsberechtigte, die einen Beitritt unter diesem Rahmenvertrag abgeschlossen haben
BK	Bundeskanzlei
DTI	Bereich Digitale Transformation und IKT-Lenkung
Firma	Microsoft Ireland Operations Ltd (Ausnahme: Microsoft Schweiz GmbH für den Konzern-Erwerbsvertrag)
Kunde	BBL und Verbundene Unternehmen
Rahmenvertrag	die eingangs identifizierte Zusatzvereinbarung
Verbundene Unternehmen	siehe Definition in Ziff.2 dieses Rahmenvertrags
Vergabestelle	BBL & BK/DTI je einzeln oder gemeinsam

Sofern nicht anders im Rahmenvertrag definiert, gelten die übrigen Definitionen gemäss den Vertragsbestandteilen gemäss Ziff. 4.

[redacted]

1 Rahmenvertrag als Abrufrahmen

1.1. Die zu beziehenden Cloud-Services können zum Zeitpunkt des Vertragsabschlusses nicht bestimmt werden. Infolge dieser Ausgangslage vereinbaren die Parteien einen Rahmenvertrag, der bis 31.08.2026 gültig ist. Beitritte (Enrollments) gelten ebenso bis maximal 31.08.2026.

1.2. Gestützt auf den vorliegenden Rahmenvertrag werden mit Bezug auf die Realisierung einzelner Projekte jeweils Abrufe bei der Firma getätigt. Die Modalitäten der Abrufe ergeben sich aus Anhang Abrufverfahren. Verbindliche Leistungen ergeben sich jeweils erst aus den einzelnen Abrufen; aus der vorliegenden Vereinbarung ergibt sich keine Bezugspflicht der Vergabestelle noch eine diesbezügliche Leistungspflicht der Firma.

2 Bezugsberechtigung

2.1. Bezugsberechtigt sind die Verwaltungseinheiten der Bundesverwaltung gemäss Art. 8 der Regierungs- und Verwaltungsorganisationsverordnung (RVOV; SR 172.010.1), wie in Anhang 1 zur RVOV (https://www.fedlex.admin.ch/eli/cc/1999/170/de#annex_1/lvl_d4e138) aufgelistet. Zusätzlich gelten als Bezugsberechtigte: die Parlamentsdienste, die Bundesanwaltschaft, das Bundesgericht, das Bundesverwaltungsgericht, das Bundespatentgericht und das Bundesstrafgericht.

2.2. Im Folgenden wird der Begriff "Bezugsberechtigte" eingesetzt für sowohl grundsätzlich bezugsberechtigte Verwaltungseinheiten der Bundesverwaltung als auch für Verwaltungseinheiten der Bundesverwaltung, die tatsächlich Leistungen von der Firma beziehen und gemäss diesem Rahmenvertrag sowie der Beitritt(e) dazu berechtigt sind. In Abweichung von der Definition gemäss Microsoft Business- und Service-Vertrags ("**MBSA**") handelt es sich bei einem "Verbundenen Unternehmen" um eine bezugsberechtigte Verwaltungseinheit, die tatsächlich Leistungen von der Firma bezieht. Im Innenverhältnis entscheidet die Bedarfsstelle (BK-DTI) darüber, welche Bezugsberechtigten tatsächlich Leistungen beziehen dürfen und übernimmt die Verantwortung dafür.

2.3. Weiterhin verpflichten sich die Beitrittsunternehmen die volle Verantwortung für die Erfüllung des jeweiligen Beitritts (Enrollment) zu übernehmen und alle Vertragsbestimmungen an die Bezugsberechtigten zu überbinden.

3 Vertragsgegenstand

3.1. Der vorliegende Rahmenvertrag, im Zusammenspiel mit den in Ziffer 4 erwähnten Vertragsbestandteilen, regelt grundsätzlich die Rechte und Pflichten der Parteien für die Erbringung von Leistungen im Umfeld Public Cloud Services.

3.2. Er bezweckt insbesondere die Herstellung eines koordinierten Prozesses im Rahmen der Realisierung von Einzelabrufen sowie die Harmonisierung der Abläufe.

4 Vertragsbestandteile

4.1. Die weiteren Vertragsbestandteile sind im Dokument Server und Cloud Beitritt aufgeführt.

4.2. Die Rangfolge gemäss Kapitel 7.1 des Konzernvertrags wird in seiner Gesamtheit ersetzt durch:

[redacted]

Rangfolge. Im Falle eines Widerspruchs zwischen den in diesem Vertrag genannten Dokumenten, der in den Dokumenten nicht ausdrücklich geregelt ist, gelten deren Bestimmungen in der folgenden absteigenden Reihenfolge: (1) dieser Rahmenvertrag, (2) das MBSA, (3) der für diesen Rahmenvertrag durch das Unterschriftenblatt speziell generierte Konzernvertrag, (4) die einzelnen Beitritte, (5) die Produktbestimmungen, (6) der Datenschutznachtrag zu den Produkten und Services von Microsoft ("**DPA**") (7) die unter diesem Vertrag übermittelten Bestellungen und (8) alle anderen Dokumente in diesem Vertrag. Die Bestimmungen in einer Zusatzvereinbarung haben Vorrang vor dem geänderten Dokument und allen vorherigen Änderungen des gleichen Vertragsgegenstandes. Klärend halten wir fest, dass dieser Vertrag und alle Ergänzenden Verträge (wie im MBSA definiert) oder Servicevereinbarungen, die seine Bestimmungen einbeziehen, nur durch einen offiziellen schriftlichen Vertrag, der von beiden Parteien unterzeichnet wurde, geändert werden können.

4.3. Hintergrund dieser Vertragsbeziehung sind die Ausschreibungsunterlagen WTO (20007) 609 und das Angebot der Firma vom 28.01.2021. Diese beiden Dokumente werden hier zu Informationszwecken referenziert.

4.4. Das standard Leistungsangebot der Firma darf die anderen Vertragsbestandteile nicht modifizieren. Es dient nur der Konkretisierung von Punkten, welche in den anderen Vertragsbestandteilen nicht hinreichend geregelt sind.

4.5. Der guten Ordnung halber wird festgehalten, dass alle zwischen der Firma und der Vergabestelle bestehenden Verträge, die nicht den Vertragsgegenstand gemäss Ziffer 3 dieses Rahmenvertrags betreffen, untangiert weiterbestehen, sofern nicht abweichend in diesem Rahmenvertrag geregelt.

5 *Bezugsregelung*

5.1. Verbindliche Leistungen ergeben sich jeweils erst aus einem Abruf gemäss Anhang Abrufverfahren.

5.2. Bevor zu einem konkreten Bedarfsfall Leistungen bezogen werden, wird in der Bundesverwaltung ein bestimmter Prozess durchlaufen (**Abrufverfahren**). Das Abrufverfahren richtet sich nach den Regeln in Anhang Abrufverfahren.

5.3. Da nicht absehbar ist, welcher der fünf (5) Zuschlagsempfänger der Ausschreibung (20007) 608 Public Clouds Bund für die einzelnen Leistungen berücksichtigt wird, gilt für jeden der fünf Zuschlagsempfänger das Kostendach von CHF 110'000'000.00 (exkl. MwSt.). Sobald die Summe sämtlicher bezogener Leistungen über alle 5 Zuschlagsempfänger gerechnet das Kostendach erreicht, werden die Zuschlagsempfänger über die vollständige Ausschöpfung informiert. Die Einhaltung des Kostendachs liegt nicht in der Verantwortung der Firma. Allfällige über das Kostendach hinausgehende Leistungsbezüge sind der Firma vollumfänglich zu vergüten.

6 *Schlüsselfunktionen*

6.1. Auf Seite der Firma liegt die Gesamtverantwortung (single point of contact, SPOC) bei:

Funktion	Client Director für die Bundesverwaltung

Schlüsselfunktionen bei der Firma

6.2. Auf Seite der Bedarfsstelle liegt die Gesamtverantwortung bei:

Funktion	Bundeskanzlei Bereich DTI

[redacted]

Schlüsselfunktionen bei der Bedarfsstelle

7 Eskalationsverfahren

7.1. Im Falle von Uneinigkeiten erfolgt die Bereinigung gemäss dem nachstehenden Eskalationsverfahren.

7.2. Eskalationsstufen auf Seiten der Vergabestelle:

Eskalationsstufe	Beteiligte
1	Auftraggeberin Transformation und Interoperabilität
2	Direktion

Eskalationsstufen seitens Vergabestelle

7.3. Eskalationsstufen auf Seiten der Firma:

Eskalationsstufe	Beteiligte
1	ATU Leader Government and Health Switzerland
2	Public Sector Lead Microsoft Schweiz
3	General Manager Microsoft Schweiz

Eskalationsstufen seitens Firma

7.4. Das Eskalationsverfahren hat keinen Einfluss auf die geltende Unterschriftenregelung. Sobald eine Einigung erzielt werden konnte, ist für allfällige Vertragsanpassungen oder rechtsverbindliche Vertragsauslegungen innert angemessener Frist die Zustimmung der jeweils zeichnungsberechtigten Personen einzuholen. Die Parteien wenden das Eskalationsverfahren nach Treu und Glauben mit dem gemeinsamen Ziel der einvernehmlichen Bereinigung von Meinungsdifferenzen an. Jede Partei trägt dabei ihren eigenen Aufwand.

7.5. Sollte binnen 30 Tage innerhalb einer Stufe keine Einigung erzielt werden können, so ist jede Partei berechtigt, die Meinungsdifferenz der nächsthöheren Ebene schriftlich zu unterbreiten. Dabei sind mindestens zu nennen: Inhalt der Meinungsverschiedenheit, Ursache aus Sicht der betreffenden Partei, Auswirkungen auf das Preis- und Leistungsverhältnis, Lösungsvorschlag bzw. -ansätze.

7.6. Jede Partei verpflichtet sich, eine allfällige Streitigkeit erst dann dem zuständigen Gericht zu unterbreiten, wenn innerhalb der höchsten Eskalationsstufe keine Einigung erzielt werden konnte.

7.7. Das Eskalationsverfahren muss nicht durchlaufen werden, sofern es offensichtlich sinnlos bzw. zwecklos ist (namentlich Konkursfall der Firma, Vertrauensverhältnis zwischen den Parteien tief erschüttert etc.).

8 Vergütung

Die Firma führt eine allgemein gültige und öffentlich zugängliche Preisliste. Für die Bezugsberechtigten gelten maximal die in der aktuell gültigen Preisliste aufgeführten Preise [redacted]

- [redacted]
- [redacted]
- [redacted]

10 Datenschutz und Datensicherheit

10.1. Die Firma verpflichtet sich zur Einhaltung der Bestimmungen zu Datenschutz und Datensicherheit gemäss den Bestimmungen in den anwendbaren Vertragswerken der Firma, insbesondere des DPA und der Zusatzvereinbarungen M329 und M905.

10.2. Die Firma lässt zu, dass Bezugsberechtigte ihre Daten verschlüsseln können. Sie lässt insbesondere Verschlüsselungsmethoden zu, bei denen ausschliesslich die Bezugsberechtigte den Masterkey besitzt bzw. diesen Masterkey kennt. In den letztgenannten Fällen liegt die alleinige Verantwortung bezüglich des Masterkeys bei der Bezugsberechtigten.

11 Vertraulichkeit der Daten

11.1. Die Firma ist verpflichtet, die Vertraulichkeit der Daten der Bezugsberechtigten zu gewährleisten. Die entsprechenden Pflichten sind nachfolgend, in der Zusatzvereinbarung M905 und im DPA im Abschnitt "Vertraulichkeitsverpflichtungen des Auftragsverarbeiters" bzw. in "Anhang A – Sicherheitsmassnahmen" geregelt.

11.2. Ziffer 3 MBSA "Vertraulichkeit" wird wie folgt ersetzt:

- "Vertrauliche Informationen" sind nicht öffentliche Informationen, die als "vertraulich" bezeichnet werden oder die eine verständige Person als „vertraulich" nachvollziehen sollte, einschliesslich Kundendaten, Daten zu Professionellen Dienstleistungen und der Bestimmungen der Microsoft-Verträge. Die Bestimmungen für Onlinedienste können zusätzliche Verpflichtungen und Beschränkungen für die Offenlegung und Nutzung von Kundendaten vorsehen. Vertrauliche Informationen umfassen keine Informationen, die (1) ohne Verletzung dieses Vertrages öffentlich erhältlich sind oder werden, (2) vom Empfänger der Informationen rechtmässig von einer anderen Quelle ohne Vertraulichkeitsverpflichtung empfangen wurden, (3) unabhängig entwickelt werden oder (4) aus einem Kommentar oder einem Vorschlag bestehen, den eine Partei freiwillig über das Geschäft, die Produkte oder Services der anderen Partei macht.

- Jede Partei wird angemessene Massnahmen zum Schutz der Vertraulichen Informationen der anderen Partei ergreifen und die Vertraulichen Informationen der anderen Partei nur für Zwecke der Geschäftsbeziehung der Parteien verwenden. Keine Partei wird diese Vertraulichen Informationen Dritten gegenüber offenlegen, ausser gegenüber ihren Mitarbeitern, Verbundenen Unternehmen, Vertragspartnern oder Beratern ("Vertreter") und dies auch nur auf einer "need-to-know"-Basis mit Vertraulichkeitsverpflichtungen, die einen mindestens gleichwertigen Schutz bieten wie dieser Vertrag. Jede Partei bleibt für die Nutzung der Vertraulichen Informationen durch ihre Vertreter verantwortlich und muss im Falle der Entdeckung einer unbefugten Nutzung oder Offenlegung die andere Partei unverzüglich benachrichtigen.

[redacted]

- Eine Partei kann die Vertraulichen Informationen der anderen Partei offenlegen, wenn dies gesetzlich vorgeschrieben ist; dies jedoch erst, nachdem sie die andere Partei (soweit gesetzlich zulässig) benachrichtigt hat, damit die andere Partei einen Schutzbeschluss einholen kann.
- Keine der Parteien ist verpflichtet, Arbeitszuweisungen ihrer Vertreter, die Zugang zu Vertraulichen Informationen hatten, einzuschränken. Jede Partei erklärt sich damit einverstanden, dass die Verwendung von Informationen, die die Vertreter ohne Hilfsmittel im Gedächtnis behalten, bei der Entwicklung oder der Bereitstellung der jeweiligen Produkte oder Services der Parteien keinerlei Haftung unter diesem Vertrag oder unter Gesetzen zu Geschäftsgeheimnissen nach sich zieht, und jede Partei verpflichtet sich, die der anderen Partei gegenüber offengelegten Informationen dementsprechend zu beschränken.
- Diese Verpflichtungen gelten (1) im Falle von Kundendaten so lange, bis diese in den Onlinediensten gelöscht werden und (2) im Falle aller anderen Vertraulichen Informationen (beispielsweise Produktroadmaps, Architektur-Blueprints, kommerzielle Aspekte dieses Vertrages) für die Dauer von fünf Jahren, nachdem eine Partei die Vertrauliche Information erhalten hat.

12 Migration und Löschung der Daten

Die Firma ermöglicht der Vergabestelle sowie den Bezugsberechtigten den Export (aus der Cloud heraus) und die unwiderrufliche Löschung ihrer Daten. Das DPA, insbesondere der Abschnitt "Speicherung und Löschung von Daten" regelt die Einzelheiten.

13 Informationspflichten

Die Parteien informieren sich gegenseitig nach Treu und Glauben bei Vorkommnissen, die den angebotenen Leistungsumfang betreffen oder die die Integrität oder Vertraulichkeit der ausgetauschten Daten beeinträchtigen. Die Firma informiert die Vergabestelle, unter Vorbehalt anderweitiger Regelungen, umgehend bei Vorkommnissen, die den angebotenen Leistungsumfang betreffen oder die die Integrität oder Vertraulichkeit der Daten der Vergabestelle oder der Bezugsberechtigten beeinträchtigen. Die einzelnen Informationspflichten und Fristen sind im DPA, insbesondere im Abschnitt "Meldung von Sicherheitsvorfällen", in der Zusatzvereinbarung M905 sowie in den Microsoft Produktbestimmungen unter "Ausserdienststellung von Diensten und Features" geregelt.

14 Kontrollrechte (Audit)

Die Firma gewährt der Bedarfsstelle und von ihr beauftragte Verwaltungseinheiten der Bundesverwaltung Kontrollrechte. Das DPA, insbesondere im Abschnitt "Prüfung der Einhaltung" und in Anlage 2, sowie die Zusatzvereinbarung M905 regeln die Einzelheiten.

15 Zugriff auf Daten durch Unberechtigte

Die Firma verpflichtet sich auf Massnahmen zur Aufrechterhaltung der Kontrollbefugnisse über Kundendaten und Professional Services-Daten der Bezugsberechtigten, soweit die Leistungserbringung der Firma einen Bezug zu diesen Kundendaten und Professional Services-Daten der Bezugsberechtigten aufweist. Das DPA, insbesondere im Abschnitt "Datenzugriff", "Anhang A – Sicherheitsmassnahmen" und "Anhang C – Nachtrag zu zusätzlichen Schutzmassnahmen" sowie die Zusatzvereinbarung M905 regeln die Einzelheiten.

16 Technische Anforderungen

16.1. Die Firma verpflichtet sich zur Einhaltung der Bestimmungen zu den technischen Anforderungen gemäss anwendbaren Vertragswerken der Firma, insbesondere des DPA, insbesondere im Abschnitt "Datensicherheit" sowie in "Anhang A – Sicherheitsmassnahmen" und seinen Zusatzvereinbarungen.

16.3. Des Weiteren gelten die in der WTO-20007 beschriebenen "Katalog der Technischen Spezifikationen" Kriterien TS 01-05.

17 Integritätsklausel

17.1. Die Parteien verpflichten sich, alle erforderlichen Massnahmen zur Vermeidung von Korruption zu ergreifen, so dass insbesondere keine Zuwendungen oder andere Vorteile angeboten oder angenommen werden.

17.2. Die Firma nimmt zur Kenntnis, dass ein Verstoss gegen die Integritätsklausel in der Regel zu einer Auflösung des Vertrages aus wichtigen Gründen durch die Vergabestelle führt.

18 Offenlegungspflicht

18.1. Die Firma hat zur Kenntnis genommen, dass die Vergabestelle auf Gesuch hin Dritten Zugang zu diesem Vertrag und allfälligen Nachträgen oder Anhängen zu gewähren hat, wenn die Vorgaben des Öffentlichkeitsgesetzes (BGÖ) erfüllt sind.

18.2. Die Vergabestelle konsultiert die Firma, wenn es die Gewährung des Zugangs in Betracht zieht, und gibt ihr Gelegenheit zur Stellungnahme innert zehn Tagen. Art. 7 Abs. 1. Lit. g. BGÖ bleibt vorbehalten.

18.3. Die Vergabestelle informiert die Firma über ihren Entscheid zum Zugangsgesuch (Artikel 11 BGÖ). Wenn die Vergabestelle gegen den Willen der Firma Dritten den Zugang zum Vertrag ganz oder teilweise zu gewähren hat, kann die Firma innert 20 Tagen nach Empfang des Entscheids der Vergabestelle dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten schriftlich einen Schlichtungsantrag stellen (Artikel 13 BGÖ).

18.4. Regeln dieser Ziff. 17.2 gehen den Regeln der Firma mit Pflichten der Bezugsberechtigten oder von anderen Stellen in der Bundesverwaltung zur Wahrung einer von der Firma erwarteten Vertraulichkeit vor.

19 Veränderung der rechtlichen Rahmenbedingungen

19.1. Die Firma anerkennt, dass es während der Vertragsdauer zu Änderungen der rechtlichen Rahmenbedingungen zum Schutz wichtiger Schutzziele der Bezugsberechtigten insbesondere zu den folgenden Themen kommen kann:

- Gesetzliche Regeln zum Amts- oder Berufsgeheimnis (Vorgaben in der Schweiz)
- Gesetzliche Regeln betreffend Zugriff auf den Datenbestand von Bezugsberechtigten im Ausland, insbesondere in Bezug auf die Begründung einer Meldepflicht in der betreffenden Rechtsordnung
- Gesetzliche Regeln betreffend IT-Sicherheit
- Gesetzliche Regeln betreffend den Datenschutz

19.2. Die Firma und die Bezugsberechtigten werden jeweils sämtliche anwendbaren Gesetze und Regelungen einhalten (einschliesslich der geltenden Gesetze zur Benachrichtigung bei Sicherheitsverletzungen). Die Firma ist jedoch nicht für die Einhaltung von Gesetzen oder Regelungen verantwortlich, die für die Bezugsberechtigten oder ihre Branche und nicht gleichzeitig allgemein für Serviceprovider im Bereich Informationstechnologie gelten.

20 Weitere Bestimmungen

20.1. Arbeitsschutzbestimmungen, Arbeitsbedingungen, Lohngleichheit und Umweltrecht

Die Firma hat mit Erklärung vom 18.12.2020 die Einhaltung der Arbeitsbedingungen, der Arbeitsschutzbestimmungen sowie der Lohngleichheit von Frau und Mann bestätigt. Zudem verpflichtet sich die Firma in Ziff. 11 m. (i) des MBSA zur Einhaltung sämtlicher auf sie anwendbaren Gesetze und Regelungen. Des Weiteren publiziert die Firma ihre global ausgerichteten Corporate Social Responsibility Grundsätze unter https://www.microsoft.com/en-us/corporate-responsibility.

20.2. Sozialversicherungen

Die Firma verpflichtet sich zur Einhaltung sozialversicherungsrechtlicher Bestimmungen gemäss Ziff. 10.b. und 11 i.(i) des MBSA.

20.3. Ausführung und Information

Die Firma verpflichtet sich zu einer sorgfältigen, getreuen und sachkundigen Vertragserfüllung gemäss Ziffer 4.a. des MBSA.

20.4. Dokumentation und Instruktion

Die Firma liefert der Vergabestelle elektronisch oder in Papierform zusammen mit der vereinbarten Leistung eine vollständige, kopierbare Dokumentation in den vereinbarten Sprachen und in vereinbarter Anzahl.

Die Vergabestelle darf die Dokumentation für den vertragsgemässen Gebrauch kopieren und verwenden.

Sofern vereinbart, übernimmt die Firma gegen separate Vergütung eine nach Umfang und Adressatenkreis zu bestimmende erste Instruktion.

20.5. Gewährleistung

Die Bestimmungen zur Gewährleistung der Firma gemäss Ziffer 4 MBSA "Gewährleistungen" wird wie folgt ersetzt:

a. Beschränkte Garantien und Rechtsmittel.

(i) Software. Microsoft gewährleistet, dass jede Version der Software für ein Jahr ab dem Datum, an dem der Kunde zum ersten Mal für diese Version eine Lizenz erhält, im Wesentlichen funktioniert, wie in der jeweiligen Produktdokumentation beschrieben. Wenn dies nicht der Fall ist und der Kunde Microsoft innerhalb der Gewährleistungsfrist darüber informiert, wird Microsoft nach dessen Wahl entweder (1) den vom Kunden für diese Softwarelizenz bezahlten Preis zurückerstatten oder (2) die Software reparieren oder ersetzen.

(ii) Onlinedienste. Microsoft gewährleistet, dass jeder Onlinedienst während der Nutzung durch den Kunden in Übereinstimmung mit der geltenden SLA erbracht wird. Die Ansprüche des Kunden bei Verletzung dieser Gewährleistung sind in der SLA genannt.

(iii) Professionelle Dienstleistungen. Microsoft gewährleistet, dass sie die Professionellen Dienstleistungen mit professioneller Sorgfalt und Sachkenntnis erbringt. Wenn Microsoft dem nicht nachkommt und der Kunde Microsoft innerhalb von 90 Tagen ab dem Datum der Erbringung der Professional Services benachrichtigt, wird Microsoft nach eigenem Ermessen entweder die Professional Services erneut erbringen oder den für sie vom Kunden bezahlten Preis zurückerstatten.

Die oben genannten Rechtsmittel stellen die einzigen Rechtsmittel dar, die dem Kunden bei Verstössen gegen die Garantien in diesem Abschnitt zur Verfügung stehen. Der Kunde

verzichtet auf die Anmeldung von Gewährleistungsansprüchen, die nicht während der Gewährleistungsfrist geltend gemacht wurden.

b. Ausschlüsse. Die Gewährleistungen in diesem Vertrag gelten nicht bei Problemen, die auf einen Unfall, Missbrauch oder auf eine Verwendung in einer Weise zurückzuführen sind, die mit diesem Vertrag nicht im Einklang steht, darunter die Nichteinhaltung der Mindestsystemanforderungen. Diese Gewährleistungen gelten nicht für kostenlose Produkte, Test-, Vorabversions- oder Beta-Produkte oder für Komponenten von Produkten, die der Kunde weitervertreiben darf.

c. Haftungsausschluss. Ausser wie in den eingeschränkten Garantien oben beschrieben übernimmt Microsoft keine anderen Gewährleistungen oder Garantien und schliesst alle anderen ausdrücklichen, konkludenten oder gesetzlichen Gewährleistungen oder Garantien, wie beispielsweise Gewährleistungen oder Garantien der Qualität, des Eigentums, der Nichtverletzung von Rechten Dritter, der Handelsüblichkeit oder der Eignung für einen bestimmten Zweck aus.

20.6. Geheimhaltung

Die Parteien behandeln alle Tatsachen und Informationen vertraulich, die weder offenkundig noch allgemein zugänglich sind, gemäss den Bestimmungen des MBSA, den Bestimmungen in Ziffer 11 des vorliegenden Rahmenvertrags sowie gemäss Ziff. 1 der Zusatzvereinbarung M905. Vorbehalten bleiben zwingende Offenlegungspflichten des schweizerischen Rechts (z.B. nach BGÖ[1], BöB[2]).

Ohne schriftliche Einwilligung der Vergabestelle darf die Firma mit der Tatsache, dass eine Zusammenarbeit mit der Vergabestelle besteht oder bestand, nicht werben und die Vergabestelle auch nicht als Referenz angeben.

Die Parteien überbinden die Geheimhaltungspflicht auf ihre Mitarbeitenden, Subunternehmer, Unterlieferanten sowie weitere beigezogene Dritte.

20.7. Schutzrechte

Die Bestimmungen betreffend Schutzrechte (Immaterialgüter- und Leistungsschutzrechte sowie Anwartschaften an solchen) an den vereinbarten Leistungen und/oder im Rahmen der Vertragserfüllung entstandenen Arbeitsergebnissen sind in Ziffer 2 MBSA geregelt.

20.8. Verletzung von Schutzrechten

Die Firma wehrt Ansprüche Dritter wegen Verletzung von Schutzrechten gemäss den Bestimmungen in Ziffer 5 MBSA ab. Ziffer 5 MBSA "Abwehr von Ansprüchen Dritter" wird wie folgt ersetzt:

Die Parteien verteidigen sich gegenseitig gegen die in diesem Abschnitt beschriebenen Ansprüche Dritter und zahlen den Betrag eines sich daraus ergebenden nachteiligen rechtskräftigen Urteils oder eines anerkannten Vergleichs, jedoch nur, wenn die beklagte Partei unverzüglich schriftlich über die Forderung informiert wird und das Recht hat, die Verteidigung und einen Vergleich zu steuern. Die verteidigte Partei muss der beklagten Partei nachgesuchte Hilfeleistung, Informationen und Ermächtigungen zur Verfügung stellen und alle angemessenen Massnahmen ergreifen, um ihre Verluste aus der Forderung der Drittpartei abzuschwächen. Die beklagte Partei erstattet der anderen Partei angemessene Auslagen, die dieser bei der Erbringung von Hilfeleistung entstehen. Dieser Abschnitt beschreibt die alleinigen Rechtsmittel der Parteien und die gesamte Haftung für solche Ansprüche.

a. Unterschrift Microsoft. Microsoft verteidigt den Kunden gegen alle Ansprüche Dritter insoweit darin vorgebracht wird, dass ein Produkt, ein Arbeitsergebnis oder Fix, das/der von Microsoft gegen eine Gebühr bereitgestellt und im Umfang der unter diesem Vertrag gewährten Lizenz verwendet wird (unverändert in der von Microsoft bereitgestellten Form und mit nichts anderem kombiniert), widerrechtlich ein Geschäftsgeheimnis verwendet oder direkt ein Patent, Urheberrecht, eine Marke oder ein anderes Schutzrecht eines Dritten verletzt. Falls Microsoft nicht dazu in der Lage ist, unter kommerziell vernünftigen Bedingungen eine Behauptung, dass ein Verstoss vorliegt, zu entkräften, darf Microsoft (1)

[1] SR 152.3
[2] SR 172.056.1

[redacted]

entweder das Produkt, den Fix oder die Service-Arbeitsergebnisse ändern oder durch eine funktional gleichwertige Leistung ersetzen oder (2) die Lizenz des Kunden kündigen und etwaige im Voraus gezahlte Lizenzgebühren für zeitlich unbeschränkte Lizenzen (abzüglich einer fünfjährigen linearen Abschreibung) bzw. Bei Onlinediensten und den für die Nutzungszeit nach dem Kündigungsdatum gezahlten Betrag zurückzahlen. Microsoft haftet nicht für Ansprüche oder Schäden, wenn der Kunde weiterhin ein Produkt, eine Lösung oder lieferbare Dienste nutzt, nachdem ihm wegen Fremdlieferantenansprüchen ein Stopp auferlegt wurde.

b. Unterschrift Kunde. Der Kunde verteidigt Microsoft in dem nach anwendbarem Recht zulässigen Umfang gegen Ansprüche Dritter, insoweit darin vorgebracht wird, dass (1) Kundendaten oder Nicht-Microsoft-Software, gehostet in einem Onlinedienst von Microsoft im Auftrag des Kunden, zweckentfremden ein Geschäftsgeheimnis oder verletzen direkt ein Patent, ein Urheberrecht, eine Marke oder ein anderes Eigentumsrecht eines Dritten; oder (2) die Nutzung eines Produkts, einer Lösung oder lieferbarer Dienste alleine oder in Kombination mit anderen Dingen verstösst gegen das Gesetz oder schädigt Dritte.

20.9. Haftung

Die Parteien haften gemäss den Haftungsbestimmungen in [redacted] sowie der nachfolgenden Ergänzung:

[redacted]

20.10. Geltendmachung von Ansprüchen

Jedes Beitrittsunternehmen und jede Bezugsberechtigte ist berechtigt, die ihr zustehenden Ansprüche aus dem Rahmenvertrag, im Zusammenspiel mit dem in Ziff 4 erwähnten Vertragsbestandteilen, direkt gegenüber der Firma geltend zu machen. Sofern derselbe Sachverhalt betroffen ist, sind die Ansprüche gegenüber der Firma zentralisiert über die Vergabestelle geltend zu machen.

Weder die Vergabestelle noch ein Beitrittsunternehmen oder eine Bezugsberechtigte sind berechtigt, einen Anspruch gegen die Firma geltend zu machen, wenn die Firma im Rahmen dieses Rahmenvertrags bereits von der Vergabestelle, einem Beitrittsunternehmen oder einer Bezugsberechtigten für denselben Schaden in Anspruch genommen wurde.

21 Anwendbares Recht / Gerichtsstand

21.1. Die Bestimmungen zu anwendbarem Recht und Gerichtsstand ergeben sich aus den Ziffer 11(e) und 11(h) MBSA und werden wie folgt ersetzt:

"In der Ziffer 11(e) mit der Überschrift "Streitbeilegung" wird der folgende Satz:

(iii) Falls der Kunde die Klage gegen ein verbundenes Unternehmen von Microsoft mit Sitz innerhalb von Europa erhebt, sind die Gerichte von Ireland zuständig.

durch den neuen Satz ersetzt:

(iii) Falls der Kunde die Klage gegen ein verbundenes Unternehmen von Microsoft mit Sitz innerhalb von Europa erhebt, sind die Gerichte von der Schweiz zuständig.

Für alle anderen Fälle gelten die Regelungen unter 11(e) in unveränderter Form.

21.2. Klärend kann festgehalten werden, dass die Gerichte in der Schweiz zuständig sind, falls der Kunde eine Servicevereinbarung mit Microsoft Schweiz GmbH abschliesst.

21.3. Klärend wird zudem zusätzlich festgehalten, dass als Verbundenes Unternehmen von Microsoft, das die Services erbringt, jeweils dasjenige Verbundene Unternehmen von Microsoft gilt, mit welchem der Kunde die Servicevereinbarung abgeschlossen hat.

21.4. Ziffer 11(h) mit der Überschrift "Anwendbares Recht" wird der folgende Satz:

Die Bestimmungen dieses Vertrages und/oder Ergänzender Verträge, die mit einem Verbundenen Unternehmen von Microsoft mit Sitz in Europa geschlossen wurden, unterliegen dem Recht von Irland und werden nach dem Recht von Irland ausgelegt.

durch den neuen Satz ersetzt:

Die Bestimmungen dieses Vertrages und/oder Ergänzender Verträge, die mit einem Verbundenen Unternehmen von Microsoft mit Sitz in Europa geschlossen wurden, unterliegen dem Schweizer Recht und werden nach Schweizer Recht ausgelegt.

21.5. Für alle anderen Fälle gelten die Regelungen unter 11(h) in unveränderter Form.

Klärend wird festgehalten, dass als Verbundenes Unternehmen von Microsoft, dass die Services erbringt, jeweils dasjenige Verbundene Unternehmen von Microsoft gilt, mit welchem der Kunde die Servicevereinbarung abgeschlossen hat.

22 Inkrafttreten / Rahmenvertragsdauer / Rahmenvertragsänderungen

22.1. Der vorliegende Vertrag tritt mit dessen Unterzeichnung durch alle Parteien in Kraft.

22.2. Er ist gültig bis zum 31.08.2026.

22.3. Änderungen und Ergänzungen dieses Rahmenvertrages und dessen Vertragsbestandteile sind nur gültig, wenn sie von den Parteien schriftlich vereinbart werden. Dies gilt auch für die Aufhebung dieses Schriftlichkeitsvorbehaltes.

23 Kündigung

23.1. Jede Partei ist berechtigt, den Rahmenvertrag und/oder die Einzelverträge gemäss den Bestimmungen in Ziffer 8 des MBSA sowie Ziffer 6 des Konzernvertrags zu kündigen.

23.2. Die Vergabestelle ist insbesondere berechtigt, den Rahmenvertrag aus wichtigem Grund zu kündigen, wenn

- über die Firma der Konkurs eröffnet wird oder sie ein Gesuch um Nachlassstundung einreicht oder in Liquidation tritt;
- die Firma die Liquidation (ausgenommen der Fall einer freiwilligen Liquidation zum Zweck der Fusion oder einer Reorganisation) erklärt;
- die Firma mit der Beschlagnahme ihres Vermögens konfrontiert wird; oder wenn
- die Firma die Teilnahmebedingungen gemäss Ausschreibungsunterlagen WTO (20007) 609 nicht mehr erfüllt.

24 Anhänge

- M905 – Amtsgeheimnis
- M329 – Datenschutz Schweiz
- Abrufverfahren

[redacted]

Berufsgeheimnis und Amtsgeheimnis – Branchenspezifische Bedingungen (Schweiz) – Gov Only

24.1 Zusatzvereinbarung ID M905

Kunde unterliegt branchenspezifischen Geheimhaltungsverpflichtungen. In Anbetracht dieser Verpflichtungen vereinbaren die Parteien, dass diese Zusatzvereinbarung bestimmte Bedingungen in der anwendbaren Zusatzvereinbarung zum Datenschutz der Microsoft Produkte und Services ("**DPA**"), den anwendbaren Produktbedingungen oder dem Business- und Service-Vertrag von Microsoft oder der Kundenvereinbarung von Microsoft, je nach Anwendbarkeit ("**Vertrag**"), klarstellt und/oder ändert. Alle in diesem Vertrag verwendeten Begriffe, die hierin nicht definiert sind, haben dieselbe Bedeutung, die in dem anwendbaren DPA, den Produktbestimmungen oder dem Vertrag für sie festgelegt wurde. Für die Zwecke dieses Vertrags bezeichnet „Kunde" ein registriertes verbundenes Unternehmen und alle verbundenen Unternehmen, die diesen branchenspezifischen Verpflichtungen unterliegen.

1. Vertraulichkeit

Microsoft ist sich bewusst, dass Kundendaten und Professional Services möglicherweise dem Berufs- oder Amtsgeheimnis unterliegen (z. B. Art. 320 oder Art. 321 des Schweizerischen Strafgesetzbuchs vom 21. Dezember 1937) oder Informationen sein können, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung einer offiziellen Behörde ausgeführt wird. Daher hält sich Microsoft an seine Vertraulichkeitsverpflichtungen gemäss dem Abschnitt "Vertraulichkeit" des Vertrags sowie an die Vertraulichkeitsverpflichtungen in der DPA und dieser Zusatzvereinbarung.

Keine Partei ist verpflichtet, Arbeitsaufträge ihrer Vertreter zu beschränken, die Zugriff auf Vertrauliche Informationen hatten. Jede Partei erklärt sich damit einverstanden, dass die Verwendung von Informationen, die die Vertreter ohne Hilfsmittel im Gedächtnis behalten, bei der Entwicklung oder der Bereitstellung der jeweiligen Produkte oder Services der Parteien keinerlei Haftung unter diesem Vertrag oder des Geschäftsgeheimnisgesetzes begründet, vorausgesetzt, dass keine Informationen offengelegt werden, die eine Identifizierung der anderen Partei oder einer anderen natürlichen oder juristischen Person ermöglichen.

Microsoft ist verpflichtet, Kundendaten und Professional Services-Daten so lange vertraulich zu behandeln, wie es die auf diese Daten anwendbaren Berufs- oder Amtsgeheimnisgesetze erfordern.

2. Kundendaten und Daten über Professional Services

Der Zugriff auf den Inhalt von Kundendaten und Professional Services-Daten, die gemäss einem Enterprise Services-Arbeitsauftrag bereitgestellt werden, ist Microsoft (zur Vermeidung von Zweifeln einschliesslich Unterauftragsverarbeitern) für die Verarbeitung von Geschäftsvorgängen nicht gestattet, es sei denn, dies ist erforderlich, um die rechtlichen Verpflichtungen von Microsoft zu erfüllen.

Wenn Kundendaten oder Professional Services-Daten, die im Rahmen eines Enterprise Services-Arbeitsauftrags bereitgestellt werden, in Verbindung mit dem Geschäftsbetrieb von Microsoft oder mit der Bereitstellung der Produkte und Dienste durch Microsoft an den Kunden verarbeitet werden, gelten dieselben Massnahmen in dieser Zusatzvereinbarung und in der DSGVO sowie alle anderen relevanten Zusatzvereinbarungen, die für den Schutz personenbezogener Daten gelten, wenn diese von Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter verarbeitet werden, entsprechend für den Schutz dieser Kundendaten oder Professional Services-Daten, die im Rahmen eines Enterprise Services-Arbeitsauftrags bereitgestellt werden.

3. Aufbewahrung und Löschung von Kundendaten

Wenn Microsoft nach anwendbarem Recht berechtigt oder verpflichtet ist oder nach dem DPA befugt ist, Kundendaten, Professional Services-Daten oder personenbezogene Daten aufzubewahren, wird

Microsoft die in dieser Zusatzvereinbarung und dem DPA festgelegten Verpflichtungen erfüllen, bis diese Daten endgültig gelöscht werden.

4. *Kunden-Lockbox*

Für bestimmte Kern-Onlinedienste stellt Microsoft seinen Kunden Dienste (mit der Bezeichnung "Kunden-Lockbox" oder einer Nachfolgebezeichnung) zur Verfügung, die von den Kunden so konfiguriert werden können, dass der Zugriff auf Kundendaten wie in diesem Absatz beschrieben weiter eingeschränkt und kontrolliert wird.

Wenn sich der Kunde für die Lizenzierung der Kunden-Lockbox entscheidet und diese entsprechend aktiviert, wird Microsoft unbeschadet anderer Rechte von Microsoft gemäss dem Vertrag nicht auf Kundendaten zugreifen oder diese nutzen, es sei denn, (a) sie ist vom Kunden gemäss dem Rest dieses Absatzes dazu berechtigt oder (b) sie ist gesetzlich dazu verpflichtet.

Lehnt der Kunde eine Anfrage von Microsoft auf Zugriff auf Kundendaten, die der Anfrage unterliegen, nicht innerhalb des relevanten Zeitraums ab oder genehmigt er sie nicht über die Kunden-Lockbox-Funktionalität, läuft die Anfrage automatisch ab, ohne dass Microsoft-Personal vom Kunden Zugriff auf Kundendaten gewährt wird.

Wenn der Kunde Microsoft den Zugriff auf Kundendaten gewährt, die der Kunden-Lockbox unterliegen, wird der Zugriff des Microsoft-Personals auf die Kundendaten protokolliert und überprüfbar sein und automatisch nach der für die Erledigung der jeweiligen Aufgabe vorgesehenen Zeit widerrufen. Zur Klarstellung sei angemerkt, dass die anderen in dem Vertrag festgelegten Beschränkungen für den Zugriff auf oder die Nutzung von Kundendaten durch Microsoft weiterhin gelten, wenn der Kunde eine Anfrage von Microsoft auf Zugriff auf Kundendaten genehmigt.

5. *Kundendaten-at-rest für Azure Kerndienste*

Zur Klarstellung: Wenn der Kunde einen bestimmten Microsoft Azure-Kerndienst derart konfiguriert, dass er in einem Rechenzentrum innerhalb einer Grossregion (jeweils als "Geo" bezeichnet) bereitgestellt wird, speichert Microsoft die Kundendaten-at-rest nur innerhalb dieses bestimmten Geo. Bestimmte Dienste ermöglichen es dem Kunden möglicherweise nicht, die Bereitstellung in einem bestimmten Geo oder ausserhalb der Vereinigten Staaten zu konfigurieren, und können Backups an anderen Orten speichern. Weitere Informationen finden Sie im Microsoft Trust Center (das Microsoft von Zeit zu Zeit aktualisieren kann, aber Microsoft wird keine Ausnahmen für bestehende Dienste in der allgemeinen Version hinzufügen).

6. *Änderungen und Verfügbarkeit der Onlinedienste*

Microsoft ist berechtigt, von Zeit zu Zeit wirtschaftlich angemessene Änderungen an jedem Onlinedienst vorzunehmen. Microsoft ist berechtigt, einen Onlinedienst in Ländern zu ändern oder zu kündigen, in denen Microsoft einer behördliche Regelung, Verpflichtung oder sonstigen Anforderung unterliegt, die (1) 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 diese Bestimmungen oder der Onlinedienst möglicherweise im Widerspruch zu einer solchen Anforderung oder Verpflichtung stehen. Microsoft wird eine solche Änderung oder Beendigung eines Onlinedienstes so rechtzeitig wie möglich ankündigen. Solche wirtschaftlich a ngemessenen Änderungen haben keine Auswirkungen auf die Version des DPA, der Produktbedingungen und/oder dieser Zusatzvereinbarung, die für den Onlinedienst gilt, der Gegenstand der Änderung ist. Wenn Microsoft einen Onlinedienst aus aufsichtsrechtlichen Gründen kündigt, erhalten Kunden eine Gutschrift über alle im Voraus für den Zeitraum nach der Kündigung bezahlten Beträge.

7. *Prüfrecht*

Soweit die Gesetze und Regelungen für Kunde vorschreiben, dass Kunde direkte Prüfungen durch die zuständigen Aufsichtsbehörden sicherstellen muss, und diese Prüfungsanforderungen nicht in angemessener Weise durch die in dem DPA festgelegten Verfahren erfüllt werden können, können

[redacted]

Prüfungen von der zuständigen Aufsichtsbehörde selbst auf Kosten von Kunde und wie in dem DPA weiter festgelegt durchgeführt werden.

24.2 Zusatzvereinbarungs-ID M329

Zusatzvereinbarung für die Schweiz in Bezug auf den Datenschutz für Microsoft Produkte und -Dienste (Addendum)

Mit dieser Zusatzvereinbarung werden bestimmte Bedingungen des Microsoft Products and Services Data Protection Addendum ("DPA") wie folgt präzisiert und abgeändert:

Definitionen

Zum Zwecke der Klarstellung und mit Ausnahme von Anhang 1 des DPA bezeichnet "Microsoft" im DPA das jeweilige verbundene Unternehmen von Microsoft, das (a) den Vertrag, mit dem Beitrittsunternehmen die Produkte und Dienste jeweils abonniert werden, oder gegebenenfalls (b) den entsprechenden Arbeitsauftrag für die Unternehmensdienste abgeschlossen hat.

Die Definition des Begriffs "Datenschutzanforderungen" wird durch folgende Definition ersetzt:

"Datenschutzanforderungen" bezeichnet die DSGVO, die lokalen EU/EWR Datenschutzgesetze, die *schweizerischen Datenschutzgesetze soweit anwendbar* sowie alle anwendbaren Gesetze, Verordnungen und sonstigen rechtlichen Anforderungen in Bezug auf (a) den Datenschutz und die Datensicherheit und (b) die Verwendung, Erhebung, Aufbewahrung, Speicherung, Sicherheit, Offenlegung, Übertragung, Entsorgung und sonstige Verarbeitung personenbezogener Daten."

Der Begriff "personenbezogene Daten" ist wie folgt zu definieren:

Die Definition von "Personendaten" sowie die in diesem DPA verwendete kleingeschriebene Verwendung von "Personendaten" umfasst alle betroffenen Personen im Sinne des Schweizerischen Bundesgesetzes über den Datenschutz (DSG).

Die Definition von "2021 Standardvertragsklauseln" erhält folgende Fassung:

"2021 Standardvertragsklauseln" bezeichnet die Standarddatenschutzklauseln (Modul "Auftragsverarbeiter") zwischen Microsoft Ireland Operations Limited und Microsoft Corporation für die Übermittlung personenbezogener Daten von Auftragsverarbeitern im EWR an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten, wie in Artikel 46 der Datenschutz-Grundverordnung beschrieben und von der Europäischen Kommission in der Entscheidung 2021/914/EG vom 4. Juni 2021 genehmigt, *in der von Microsoft Ireland Operations Limited und Microsoft Corporation gemäss den vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Leitlinien vom 27. August 2021 für Datenübermittlungen, die dem Schweizerischen Bundesgesetz über den Datenschutz unterliegen (EDÖB-Leitlinien), geänderten Fassung.*

[redacted]

Datenschutzbestimmungen

Dokumentierte Anweisungen

Zur Klarstellung: Die "dokumentierten Anweisungen" des Kunden, auf die in der DPA Bezug genommen wird, umfassen nicht die Weisungen des Kunden an Microsoft, Kundendaten oder Professional Services-Daten für die Geschäftstätigkeiten von Microsoft zu verarbeiten.

Datenübertragung und Standort

In Übereinstimmung mit dem EDÖB-Leitfaden werden die Standardvertragsklauseln von 2010 nicht für Überweisungen aus der Schweiz gelten.

Verweise auf die Datenschutz-Grundverordnung

Verweise im DPA auf die DSGVO gelten auch als Verweise auf das schweizerische Datenschutzrecht und seine entsprechenden Bestimmungen, und die DSGVO-Bestimmungen und der Unterabschnitt "Verarbeitung personenbezogener Daten; DSGVO" des DSG gelten auch, wenn eine Datenverarbeitung dem schweizerischen Datenschutzrecht unterliegt.

Anhang C des DPA - Zusätzliche Sicherheitsvorkehrungen (Nachtrag)

Die Präambel des Anhangs C erhält folgende Fassung:

"Mit diesem Nachtrag für die zusätzlichen Sicherheitsbevorkehrungen zum DPA (dieser "Zusatz") bietet Microsoft dem Kunden zusätzliche Garantien für die Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO *oder des DSG* durch Microsoft im Namen des Kunden und zusätzliche Rechtsmittel für die betroffenen Personen, auf die sich diese personenbezogenen Daten beziehen."

Klausel 1: Aufforderung zur Bestellung

Abschnitt 1.c: Wenn der Kunde in der Schweiz ansässig ist, wird der Abschnitt durch den folgenden ersetzt:

"alle rechtmässigen Anstrengungen zu unternehmen, um die Anordnung zur Offenlegung auf der Grundlage von Rechtsmängeln nach dem Recht der ersuchenden Partei oder von Konflikten mit dem *Recht der Schweiz*, dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten anzufechten."

Klausel 2: Entschädigung der betroffenen Personen

Wenn der Kunde in der Schweiz ansässig ist, wird die Klausel durch die folgende ersetzt:

Vorbehaltlich der Abschnitte 3 und 4 entschädigt Microsoft eine betroffene Person für jeden materiellen oder immateriellen Schaden, der der betroffenen Person dadurch entsteht, dass Microsoft personenbezogene Daten der betroffenen Person offenlegt, die auf Anordnung einer nicht-

[redacted]

schweizerischen Regierungsstelle oder einer Strafverfolgungsbehörde unter Verletzung der Verpflichtungen von Microsoft nach Kapitel V der Datenschutz-Grundverordnung *oder entsprechender Bestimmungen des DSG* (eine "relevante Offenlegung") übermittelt wurden. Microsoft ist ungeachtet des Vorstehenden nicht dazu verpflichtet, die betroffene Person gemäss diesem Abschnitt 2 zu entschädigen, soweit die betroffene Person bereits eine Entschädigung für denselben Schaden erhalten hat, ob es von Microsoft oder anderweitig."

24.3 Abrufverfahren

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

Publiziert auf der Plattform www.simap.ch (Nr. 204859 am 07.12.2020)

Präambel

Die Parteien wollen das Abrufverfahren zum Bezug von Leistungen in der genannten Beschaffung gemeinsam regeln. Es soll ein für alle Zuschlagsempfängerinnen einheitliches Abrufverfahren vereinbart werden.

Das Vergabeverfahren für das Projekt (20007) 608 Public Clouds Bund (publiziert als Projekt 204859, simap vom 7. Dezember 2020) ist mit Zuschlag vom 24. Juni 2021 rechtskräftig abgeschlossen worden. Bei dem in diesem Anhang geregelten Abrufverfahren handelt es sich somit um die Abwicklung der Vertragsbeziehung, die im Anschluss an das genannte Vergabeverfahren mit separatem Rahmenvertrag begründet wurde.

Die Parteien wollen mit dem vorliegenden Dokument diese Abrufe von Bezugsberechtigten transparent regeln.

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1 Vorgehen im Überblick

Nach Erstellen des behördeninternen, bedarfsabhängigen und anbieterneutralen Pflichtenhefts (Ziff. 2.1) und nach durchgeführter Evaluation der vorhandenen Leistungsangebote (Ziff. 3.1) wählt die Bezugsberechtigte die Leistung oder die Leistungen aus (Ziff. 3.2, Entscheid) und ruft diese ab (Ziff. 3.3, Leistungsbezug).

2 Bestimmung des Bedarfs und der Abrufkriterien

2.1 Die Bezugsberechtigte definiert ihren Bedarf im behördeninternen, bedarfsabhängigen und anbieterneutralen Pflichtenheft. Die Bezugsberechtigte erstellt es jeweils anlassbezogen (im Einzelfall).

2.2 Die Bezugsberechtigte nennt im behördeninternen, bedarfsabhängigen und anbieterneutralen Pflichtenheft die Auswahl sowie die abschliessende Definition der Abrufkriterien, deren Gewichtung sowie den Stichtag (mit Datum und Zeit), an dem die Bewertung vorgenommen werden soll. Diese Auswahl und Definition basiert auf dem folgenden Kriterienkatalog:

[redacted]

2.2.1 Erfüllungsgrad der technischen Anforderungen
2.2.2 Risikobeurteilung (Datenschutz, Informationssicherheit, organisatorische, technische und vertragliche Massnahmen)
2.2.3 Konformität zur Cloud-Strategie und zur bestehenden Ausgangslage bei der Bezugsberechtigten (insbesondere Architekturen, bei der Bezugsberechtigten vorhandenes Fachpersonal, bestehende Anwendungen bei einer der Zuschlagsempfängerinnen, die mit der neuen Anwendung interagieren sollen)
2.2.4 Preis (Kosten / Service-Kosten) (bezogen auf die geplante Bezugsmenge)
2.2.5 Allfällige Migrationskosten

2.3 Zur Deckung des Bedarfs kann die Bezugsberechtigte den ganzen oder teilweisen Bezug von Leistungen von mehr als einer Zuschlagsempfängerin vorsehen.

3 Evaluation, Entscheid und Leistungsbezug

3.1 Die Bezugsberechtigte vergleicht und bewertet die vorhandenen Leistungsangebote der Zuschlagsempfängerinnen basierend auf den Informationen, welche auf den Webseiten und Portalen der Zuschlagsempfängerinnen verfügbar sind (s.a. Ziff. 5); Ziff. 4 ist vorbehalten.

3.2 Die Bezugsberechtigte entscheidet nach Massgabe der von ihr im Einzelfall festgelegten Abrufkriterien (Ziff. 2.2), mit welchem bzw. mit welchen der vorhandenen Leistungsangebote sie den von ihr bestimmten Bedarf (Ziff. 2.1 ganz oder teilweise deckt. Entscheid im Sinne dieser Ziff. 3.2 meint die Festlegung einer Bezugsberechtigten, für einen bestimmten Zweck (wie z.B. eine Fachanwendung) und einen geplanten Zeitrahmen ein Portfolio von vorhandenen Leistungsangeboten von einer oder mehreren der Zuschlagsempfängerinnen zu beziehen. Die Bezugsberechtigte dokumentiert ihren Entscheid.

3.3 Die Bezugsberechtigte bezieht die Leistung(en) entsprechend dem Entscheid eigenständig auf den Webseiten und Portalen der ausgewählten Zuschlagsempfängerinnen.

4 Allfällige weitere Interaktionen mit Zuschlagsempfängerinnen

4.1 Die Bezugsberechtigte prüft nach Massgabe der von ihr im Einzelfall festgelegten Abrufkriterien (Ziff. 3.2), ob nach Durchlaufen der Prüfung gem. Ziff. 3.1 noch zusätzliche Informationen notwendig oder wünschenswert sind, um die beabsichtigte Nutzung zu beurteilen.

4.2 Im Rahmen von Ziff. 4.1 kann die Bezugsberechtigte einer oder mehreren Zuschlagsempfängerinnen Fragen zu deren vorhandenen Leistungsangeboten stellen. In Bezug auf eines oder mehrere der vorhandenen Leistungsangebote kann die Bezugsberechtigte auch Proof(s) of Concept durchführen.

4.3 Die Firma hat keinen Anspruch, gem. Ziff. 4.2 eingebunden zu werden.

4.4 Die Bezugsberechtigte dokumentiert die Gründe, die zu Fragen gem. Ziff. 4.2 Satz 1 geführt haben, ebenso die Resultate.

4.5 Zeigt sich, dass die Bezugsberechtigte darüber hinaus Bedarf zur Einholung von einzelfallbezogenen Angeboten hat, regelt sie die Einzelheiten im Einzelfall und informiert die Firma. Die Bedarfsstelle kann dazu auch einen neuen Anhang zum Rahmenvertrag vorsehen.

5 Dokumentation von Seiten der Firma

5.1 Die Firma unterhält auf ihren der Bedarfsstelle bekanntzugebenden Webseiten und Portalen die folgenden Standardinformationen:

5.1.1 Paket #01: Beschreibung des vorhandenen Leistungsangebots (z.B. Service Namen oder Service-ID's mit Hinweisen, wo die Bedarfsstelle und alle Bezugsberechtigten weitere Informationen beziehen können, genügen)

5.1.2 Paket #02: Preislisten

5.1.3 Paket #03: Weitere Dienstleistungen, die für den Leistungsbezug notwendig sind

5.1.4 Paket #04: Nicht-funktionale Eigenschaften (Sicherheitsdokumentationen, Prüfberichte, etc.)

5.1.5 Paket #05: Besonderes

5.2 Die Firma stellt sicher, dass die Bedarfsstelle und alle Bezugsberechtigten Zugriff auf die Informationen gem. Ziff. 5.1 erhalten.

5.3 Die Bezugsberechtigte darf im Rahmen der Prüfung gem. Ziff. 3.1 auf die Informationen gem. Ziff. 5.1 abstellen (weitere Recherchen sind nicht notwendig), muss sich aber nicht auf diese beschränken (die Bezugsberechtigte darf in guten Treuen weitere Informationsquellen für ihren Entscheid einbeziehen; sie beachtet das Sachlichkeitsgebot).

6 Kein Anspruch auf Berücksichtigung

Die Firma hat keinen Anspruch darauf, dass sie unter der Beschaffung WTO 20007 Leistungen an die Bundesverwaltung erbringen kann.

7 Mitteilung der Entscheide gem. Ziff. 3.2

7.1 Im Sinne der Transparenz teilt die Bezugsberechtigte Entscheide gem. Ziff. 3.2 allen Zuschlagsempfängerinnen zeitnah nach Bezugsentscheid mit. Diese Ziffer 7 nennt die Anforderungen.

7.2 Als Abruf im Sinne von Ziff. 7.1 gilt nicht jeder einzelne technische Leistungsbezug im Sinne von Ziff. 3.3 (z.B. "3.2 Gigabyte S3-Storage" für September 2022), sondern die Festlegung der Bezugsberechtigten gem. Ziff. 3.2.

7.3 Die Bezugsberechtigte teilt Folgendes mit:

7.3.1 die von ihr im Einzelfall festgelegten Abrufkriterien gem. internem anbieterneutralen Pflichtenheft für den konkreten Bedarf

7.3.2 den Entscheid (Ziff. 3.2), mit Nennung der zugewiesenen Abrufsumme, Zuschlagsperiode und Stichtag (mit Datum und Zeit), zu dem die Bewertung vorgenommen wurde

7.3.3 die summarische Begründung für den Entscheid. Diese Begründung erläutert den Entscheid auf der Basis der im Einzelfall festgelegten Abrufkriterien

7.4 Sofern die Bedarfsstelle kein zentrales Verzeichnis für die Mitteilung von Entscheiden bereithält, sorgt die Bezugsberechtigte dafür, dass sie die Informationen allen Zuschlagsempfängerinnen im Wesentlichen zeitgleich übermittelt.

8 Allgemeine Bestimmungen

Die Regeln des Rahmenvertrags kommen kraft Verweises zur Anwendung.

Mit Ausnahme der durch diese Zusatzvereinbarung eingetretenen Änderungen bleibt der oben genannte Beitritt oder Vertrag unverändert und in voller Rechtskraft. Wenn ein Konflikt zwischen einer Bestimmung in dieser Zusatzvereinbarung und einer Bestimmung im oben genannten Beitritt oder Vertrag besteht, so ist diese Zusatzvereinbarung maßgebend.

Diese Zusatzvereinbarung muss zu ihrer Rechtsgültigkeit einem Unterschriftsblatt beigefügt werden.

Microsoft Internal Use Only:

(CTM)AgrAmend(Rahmenvertrag WTO20007)(DE)Bund_June 2022_FINAL.docx	CTM	CTM-CTC-AGR-CTL-LOL-ENR	BD

Microsoft Volume Licensing

Formblatt für Unterschriften für das Programm

MBA-/MBSA-Nummer	U6714200
Nummer des Vertrages	54E61212

7-XR7BIUMGD

Hinweis: Geben Sie die entsprechenden aktiven Nummern an, die zu den unten stehenden Dokumenten gehören. Microsoft benötigt die hier angegebenen aktiven Nummern bzw. die nachfolgenden neuen Nummern.

Im Sinne dieses Formblatts kann „Kunde" die unterzeichnende Gesellschaft, das Beitrittsunternehmen, der Partner für die Verwaltung, die Einrichtung oder eine andere Partei sein, die einen Vertrag im Rahmen eines Volumenlizenzprogramms schließt.

Dieses Formblatt für Unterschriften und alle in der Tabelle unten aufgeführten Vertragsdokumente gelten ab dem unten angegebenen Wirksamkeitsdatum zwischen dem Kunden und der unterzeichnenden Microsoft-Gesellschaft.

Vertragsdokument	Nummer oder Code
<Vertrag auswählen>	
<Vertrag auswählen>	
<Vertrag auswählen>	
<Vertrag auswählen>	
<Vertrag auswählen>	
<Beitritt/Registrierung auswählen>	
<Beitritt/Registrierung auswählen>	
<Beitritt/Registrierung auswählen>	
<Beitritt/Registrierung auswählen>	
<Beitritt/Registrierung auswählen>	
Zusatzvereinbarung	CTM-CTC-AGR-CTL-LOL-ENR 7-XR7BIUMGD

Durch die nachfolgende Unterschrift erklären der Kunde und die Microsoft-Gesellschaft, dass beide Parteien (1) die oben genannten Vertragsdokumente einschließlich jeglicher Websites oder Dokumente, die durch Bezugnahme Bestandteil dieser Dokumente werden, und jeglicher Zusatzvereinbarungen zu diesen Dokumenten gelesen und verstanden haben und (2) sich damit einverstanden erklären, durch die Bestimmungen all dieser Dokumente gebunden zu sein.

Kunde	
Name der Gesellschaft (muss der rechtliche Name der Gesellschaft sein)*	Bundesamt für Bauten und Logistik BBL [redacted]
Unterschrift*	[redacted]
Vor- und Nachname in Druckbuchstaben*	[redacted]
Titel in Druckbuchstaben	[redacted]
Datum der Unterschrift*	16.09.2022

** bezeichnet Pflichtfelder*

Microsoft-Gesellschaft
Microsoft Ireland Operations Limited
Umsatzsteuer-Identifikationsnummer (USt-IdNr.) IE8256706U
Unterschrift _____
Vor- und Nachname in Druckbuchstaben
Titel in Druckbuchstaben
Datum der Unterschrift* (Datum der Gegenzeichnung durch die Microsoft-Gesellschaft)
Wirksamkeitsdatum des Vertrages* (kann vom Datum der Unterschrift von Microsoft abweichen)

Microsoft
Microsoft Ireland Operations Ltd.
22 SEP 2022
[redacted]
Duly Authorised on behalf of
Microsoft Ireland Operations Ltd.

Wahlweise 2. Unterschrift des Kunden oder Unterschrift des Outsourcers (sofern zutreffend)

Kunde
Name der Gesellschaft (muss der rechtliche Name der Gesellschaft sein)* Bundeskanzlei
Unterschrift* [redacted]
Datum der Unterschrift* 20.9.2022

** bezeichnet Pflichtfelder*

Outsourcer
Name der Gesellschaft (muss der rechtliche Name der Gesellschaft sein)*
Unterschrift* _____
Vor- und Nachname in Druckbuchstaben*
Titel in Druckbuchstaben
Datum der Unterschrift*

** bezeichnet Pflichtfelder*

Wenn der Kunde zusätzliche Kontakte benötigt oder mehrere frühere Beitritte meldet, fügen Sie diesem Unterschriftsblatt das/die entsprechende(n) Formular(e) bei.

Nach der Unterzeichnung dieses Formblatts für Unterschriften durch den Kunden senden Sie das Formblatt und die Vertragsdokumente an den Vertriebspartner oder Microsoft-Kundenbetreuer des Kunden, der sie unter folgender Adresse einreichen muss. Wenn das Formblatt für Unterschriften von Microsoft ordnungsgemäß ausgefertigt wurde, erhält der Kunde eine Kopie der Annahmebestätigung.

Microsoft Ireland Operations Limited
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18
D18 P521
Ireland

10

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Bauten und Logistik
Bereich Logistik
Abteilung Beschaffung

Vertragswerke der Firma:

13

15

Volumenlizenz

Datenschutznachtrag zu den Produkten und Services von Microsoft

Letzte Aktualisierung: 15. September 2021

Microsoft

Inhaltsverzeichnis

Einleitung

Die Parteien stimmen überein, dass dieser Datenschutznachtrag zu den Produkten und Services von Microsoft (Data Protection Addendum, „DPA") ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten, Professional Services-Daten und personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. Das DPA wird durch Bezugnahme in die Produktbestimmungen und andere Microsoft-Verträge aufgenommen. Wenn kein separater Vertrag über Professional Services besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung und Sicherheit der Professional Services-Daten ebenfalls diesem DPA 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 DPA-Bestimmungen und anderen Bestimmungen des Volumenlizenzvertrags des Kunden hat dieses DPA Vorrang. Die DPA-Bestimmungen haben Vorrang vor anderslautenden Bestimmungen in der Datenschutzerklärung von Microsoft, die ansonsten möglicherweise für die Verarbeitung von Kundendaten, personenbezogenen Daten oder Professional Services-Daten (Begriffe gemäß den Definitionen in diesem DPA) gelten. Der Klarheit halber wird darauf hingewiesen, dass, entsprechend Klausel 10 der Standardvertragsklauseln von 2010 in Anhang 1, wenn die Standardvertragsklauseln von 2010 gelten, die Standardvertragsklauseln von 2010 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 Produktbestimmungen, die ansonsten für ein bestimmtes Produktabonnement oder eine Lizenz gelten, und (2) von anderen Verträgen, die auf die Produktbestimmungen verweisen.

wendbare DPA-Bestimmungen und -Aktualisierungen

Beschränkungen für Aktualisierungen

Wenn der Kunde ein Produktabonnement verlängert oder ein neues Abonnement kauft oder einen Arbeitsauftrag für Professional Services eingeht, gelten die jeweils aktuellen DPA-Bestimmungen bleiben während des Abonnements des Kunden für dieses Produkt oder die Laufzeit für diesen Professional Services unverändert. Wenn der Kunde eine zeitlich unbeschränkte Lizenz für die Software erwirbt, gelten die jeweils aktuellen DPA-Bestimmungen (nach den gleichen Bestimmungen zur Festlegung der jeweils geltenden Produktbestimmungen für diese Software in der Volumenlizenz des Kunden) und bleiben während der Laufzeit der Lizenz des Kunden für diese Software unverändert.

Neue Features, Ergänzungen oder zugehörige Software

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

Behördliche Vorschriften und Verpflichtungen

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

Elektronische Benachrichtigungen

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

Frühere Versionen

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

Definitionen

Definierte Begriffe, die in diesem DPA verwendet, jedoch nicht in diesem DPA selbst definiert werden, besitzen die im 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 Professional Services-Daten 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 produktspezifischen Bestimmungen in den Produktbestimmungen, die speziell die Datenschutz- und Sicherheitsbestimmungen in dem DPA für ein spezifisches Produkt (oder ein Feature eines Produkts) ergänzen oder ändern. Bei Konflikten oder Widersprüchen zwischen dem DPA und solchen produktspezifischen Bedingungen sind die produktspezifischen Bedingungen für das jeweilige Produkt (oder das Feature des jeweiligen Produkts) vorrangig.

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

kale EU-/EWR-Datenschutzgesetze" bezeichnet alle untergeordneten Gesetze und Vorschriften zur Umsetzung der DSGVO.

„DSGVO-Bestimmungen" bezieht sich auf die Bestimmungen in Anlage 2, 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.

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

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

„Professional Services" bezeichnet die folgenden Dienstleistungen: (a) Beratungsdienste von Microsoft, bestehend aus der Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und aus Lösungs-/Softwareentwicklungsdiensten, die im Rahmen eines Enterprise Services-Arbeitsauftrags bereitgestellt werden, in den dieser DPA durch Verweis aufgenommen wird; und (b) technische Support-Services, die von Microsoft bereitgestellt werden und dem Kunden helfen, Produkte betreffende Probleme zu identifizieren und zu beheben, einschließlich technischen Supports, der als Teil der Microsoft Unified Support oder Premier Support Services bereitgestellt wird (wie in der Beschreibung der Services Consulting und Support bzw. der Beschreibung der Services dargelegt), sowie alle anderen technischen Support-Services. Die Professional vices umfassen weder die Produkte noch, für die Zwecke des DPA, Zusätzliche Professional Services.

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

„Standardvertragsklauseln von 2010" 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 von 2010 befinden sich in Anlage 1.

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

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

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

In diesem DPA verwendete Begriffe, die nicht definiert werden, wie „Verletzung des Schutzes personenbezogener Daten", „Verarbeitung", „Verantwortlicher", „Profiling", „personenbezogene Daten" und „betroffene Person" haben die Bedeutung gemäß Artikel 4 DSGVO, unabhängig davon, ob die DSGVO anwendbar ist.

Inhaltsverzeichnis / Allgemeine Bestimmungen

Allgemeine Bestimmungen

Einhaltung von gesetzlichen Regelungen

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

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

Datenschutzbestimmungen

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
- Kalifornisches Datenschutzgesetz (California Consumer Privacy Act, CCPA)
- Biometrische Daten
- Zusätzliche Professional Services
- Kontaktaufnahme mit Microsoft
- Anhang A – Sicherheitsmaßnahmen
- Anhang B – Betroffene Personen und Kategorien personenbezogener Daten
- Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen.

Umfang

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

Die DPA-Bestimmungen gelten nicht für Produkte, die oder soweit sie in den Produktbestimmungen ausdrücklich als ausgeschlossen gekennzeichnet werden, die den Datenschutz- und Sicherheitsbestimmungen in den jeweiligen produktspezifischen Bedingungen unterliegen.

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

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

Previews werden unter Umständen weniger oder andere Datenschutz- und Sicherheitsmaßnahmen vorsehen als dies normalerweise bei Produkten und Services 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 von Produkten: Verarbeitung personenbezogener Daten; DSGVO, Datensicherheit und HIPAA Business Associate. Für Professional Services gilt, dass die Angebote, die als Previews oder Limited Release bezeichnet werden, nur die Bedingungen der Zusätzlichen Professional Services erfüllen.

Art der Datenverarbeitung; Eigentumsverhältnisse

Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig verarbeiten, (a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zur Verfügung zu stellen, und (b) für die Geschäftstätigkeiten von Microsoft, die mit der Bereitstellung der Produkte und Services an den Kunden verbunden sind. Unter den Parteien behält sich der Kunde alle Rechte, Ansprüche und Eigentum an und für Kundendaten und Professional Services-Daten vor. Microsoft erwirbt keine Rechte an den Kundendaten oder Professional Services-Daten, mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt. Dieser Absatz berührt nicht die Rechte von Microsoft an Software oder Services, für die Microsoft dem Kunden eine Lizenz gewährt.

Verarbeitung zur Bereitstellung der Produkte und Services für Kunden

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

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

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

- der Bereitstellung der Professional Services, einschließlich technischem Support, professioneller Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und Lösungs-/Softwareentwicklung.
- Die Fehlerbehebung (Verhindern, Erkennen, Untersuchen, Abschwächen und Beheben von Problemen, einschließlich Sicherheitsvorfällen und Problemen, die bei der Bereitstellung von Professional Services in den Professional Services oder relevanten Produkten festgestellt wurden); und
- Die kontinuierliche Verbesserung (Verbesserung der Bereitstellung, Wirksamkeit, Qualität und Sicherheit von Professional Services und den zugrunde liegenden Produkten basierend auf Problemen, die bei der Bereitstellung von Professional Services festgestellt wurden, einschließlich der Installation der neuesten Updates und der Behebung von Softwarefehlern).

Bei der Bereitstellung von Produkten und Services wird Microsoft Kundendaten, Professional Services-Daten 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 Geschäftstätigkeiten

Für die Zwecke dieses DPA umfassen „Geschäftstätigkeiten" die folgenden Aktivitäten, jeweils mit der Bereitstellung der Produkte und Services für den Kunden verbunden: (1) Abrechnungs- und Kontoverwaltung; (2) Vergütung (z. B. Berechnung von Mitarbeiter-provisionen 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 diese Geschäftstätigkeiten wendet Microsoft die Grundsätze der Datenminimierung an und verwendet oder verarbeitet keine Kundendaten, Professional Services-Daten oder personenbezogenen Daten für: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke.

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) Professional Services-Daten, (c) personenbezogene Daten und (d) alle weiteren Daten, die von Microsoft im Zusammenhang mit den Produkten und Services 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 dem Volumenlizenzvertrag.

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 personenbezogenen Daten, die von Microsoft im Zusammenhang mit der Bereitstellung der Produkte und Services verarbeitet werden, werden entweder als Teil von (a) Kundendaten, (b) Professional Services-Daten oder (c) von Microsoft generierten, abgeleiteten oder gesammelten Daten erhoben, einschließlich Daten, die an Microsoft als Ergebnis der Nutzung dienstbasierter Funktionen durch einen Kunden gesendet werden oder die von Microsoft von lokal installierter Software bezogen wurden. Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung des Onlinediensts zur Verfügung gestellt werden, sind ebenfalls Kundendaten. Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung der Professional Services zur Verfügung gestellt werden, sind ebenfalls Professional Services-Daten. Pseudonymisierte Kennungen können in Daten enthalten sein, die von Microsoft im Zusammenhang mit der Bereitstellung der Produkte verarbeitet werden, und sind ebenfalls personenbezogene Daten. Bei personenbezogenen Daten, die zwar pseudonymisiert wurden oder keine direkte Identifizierung mehr ermöglichen, jedoch nicht anonymisiert wurden, sowie bei aus personenbezogenen Daten abgeleiteten personenbezogenen Daten handelt es sich ebenfalls um personenbezogene Daten.

Soweit Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter personenbezogener Daten ist, die der DSGVO unterliegen, regeln die DSGVO-Bestimmungen in Anlage 2 die Verarbeitung. Die Parteien vereinbaren außerdem die folgenden Bestimmungen in diesem Unterabschnitt („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 produktspezifischen Bedingungen oder in diesem DPA wird etwas anderes bestimmt. Wenn Microsoft als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, verarbeitet Microsoft personenbezogene Daten nur nach den dokumentierten Weisungen des Kunden. Der Kunde stimmt zu, dass sein Volumenlizenzvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Features der Produkte durch den Kunden die vollständigen und dokumentierten Weisungen des Kunden gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten darstellen, oder die Dokumentation der Professional Services und die Nutzung der Professional Services durch den Kunden. Informationen zur Verwendung und Konfiguration der Produkte sind unter https://docs.microsoft.com/de-de/ (oder einer entsprechenden, dieser nachfolgenden Stelle) oder in einem anderen Vertrag, der dieses DPA einbezieht, zu finden. Zusätzliche oder andere Weisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Vertrages des Kunden. In allen Fällen, in denen die DSGVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Weisungen des Kunden einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden.

Soweit Microsoft personenbezogene Daten, die der DSGVO unterliegen, für Geschäftstätigkeiten im Zusammenhang mit der Bereitstellung der Produkte und Services an den Kunden nutzt oder anderweitig verarbeitet, wird Microsoft für diese Nutzung die Pflichten eines unabhängigen Datenverantwortlichen gemäß der DSGVO erfüllen. Microsoft übernimmt die zusätzlichen Pflichten eines „für die Datenverarbeitung Verantwortlichen" gemäß DSGVO für die Verarbeitung im Zusammenhang mit ihren Geschäftstätigkeiten zum: (a) Handeln in Einklang mit den regulatorischen Anforderungen, insoweit dies von der DSGVO gefordert wird; und (b) Schaffung einer erhöhten Transparenz für Kunden und Bestätigung der Verantwortlichkeit von Microsoft für eine solche Verarbeitung. Microsoft nutzt Sicherheitsmaßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten während der Verarbeitung zu schützen, einschließlich der in diesem DPA aufgeführten sowie der in Artikel 6(4) der DSGVO vorgesehenen Maßnahmen. In Bezug auf die Verarbeitung personenbezogener Daten gemäß diesem Absatz übernimmt Microsoft die im Abschnitt „Zusätzliche Sicherheitsvorkehrungen" aufgeführten Verpflichtungen. Für diese Zwecke (i) gilt jede Offenlegung personenbezogener Daten, wie im Abschnitt „Zusätzliche Schutzmaßnahmen" beschrieben, durch Microsoft, die im Zusammenhang mit Geschäftstätigkeiten übertragen wurden, als „Relevante Offenlegung" und (ii) finden die im Abschnitt „Zusätzliche Schutzmaßnahmen" beschriebenen Verpflichtungen Anwendung auf diese personenbezogenen Daten.

Verarbeitungsdetails

Die Parteien bestätigen und vereinbaren Folgendes:

- **Gegenstand.** Der Gegenstand der Verarbeitung ist auf personenbezogene Daten innerhalb des Geltungsbereichs des Abschnitts dieses DPA mit dem Titel „Art der Verarbeitung; Eigentumsverhältnisse" weiter oben sowie der DSGVO eingeschränkt.

- **Dauer der Verarbeitung.** Die Dauer der Verarbeitung richtet sich nach den Weisungen des Kunden sowie den Bestimmungen des DPA.
- **Art und Zweck der Verarbeitung.** Art und Zweck der Verarbeitung ist die Bereitstellung der Produkte und Services gemäß dem Volumenlizenzvertrag des Kunden und für die Geschäftstätigkeiten in Verbindung mit der Bereitstellung der Produkte und Services für den Kunden (wie ausführlicher im Abschnitt dieses DPA mit dem Titel „Art der Verarbeitung; Eigentumsverhältnisse" weiter oben beschrieben).
- **Kategorien von Daten.** Zu den Arten von personenbezogenen Daten, die von Microsoft bei der Bereitstellung der Produkte und Services verarbeitet werden, gehören: (i) Personenbezogene Daten, die der Kunde in Kundendaten und Professional Services-Daten aufnehmen möchte; und (ii) diejenigen, die ausdrücklich in Artikel 4 DSGVO genannt sind, die von Microsoft generiert, abgeleitet oder gesammelt werden können, einschließlich Daten, die aufgrund der Nutzung dienstbasierter Funktionen durch einen Kunden an Microsoft gesendet oder von Microsoft aus lokal installierter Software bezogen werden. Bei den Arten von personenbezogenen Daten, die der Kunde in die Kundendaten und Professional Services-Daten aufnehmen möchte, kann es sich um alle Kategorien von personenbezogenen Daten handeln, die in Aufzeichnungen genannt werden, die vom Kunden als Verantwortlicher gemäß Artikel 30 DSGVO handelnd gepflegt werden, einschließlich der in Anhang B aufgeführten Kategorien personenbezogener Daten.
- **Betroffene Personen.** Die Kategorien betroffener Personen sind Vertreter und Endnutzer des Kunden, wie Mitarbeiter, Auftragnehmer, Partner und Kunden. Dies kann auch andere Kategorien betroffener Personen umfassen, die in Verzeichnissen genannt werden, welche vom Kunden als Verantwortlicher gemäß Artikel 30 DSGVO geführt werden, einschließlich der in Anhang B aufgeführten Kategorien betroffener Personen.

Rechte der betroffenen Personen; Unterstützung bei Anfragen

Microsoft ermöglicht dem Kunden, Anfragen betroffener Personen zur Ausübung ihrer Rechte nach der DSGVO auf eine mit der Funktion der Produkte und Services und der Rolle von Microsoft als Auftragsverarbeiter personenbezogener Daten betroffener Personen konsistente Art und Weise nachzukommen. Wenn Microsoft eine Anfrage der betroffenen Person des Kunden erhält, mindestens eines ihrer Rechte nach der DSGVO in Verbindung mit den Produkten und Services, für die Microsoft Auftragsverarbeiter oder Unterauftragsverarbeiter ist, auszuüben, verweist Microsoft die betroffene Person, damit sie ihre Anfrage direkt an den Kunden richtet. Der Kunde ist für die Beantwortung einer solchen Anfrage verantwortlich, einschließlich, falls erforderlich, durch Nutzung der Funktionalität der Produkte und Services. Microsoft kommt angemessenen Anfragen des Kunden nach Unterstützung bei der Bearbeitung von Anfragen betroffener Personen nach.

Verzeichnis von Verarbeitungstätigkeiten

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

Datensicherheit

Sicherheitsverfahren und Sicherheitsrichtlinien

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

Darüber hinaus erfüllen diese Maßnahmen die Anforderungen von ISO 27001, ISO 27002 und ISO 27018. Eine Beschreibung der Sicherheitskontrollen für diese Anforderungen steht den Kunden zur Verfügung.

Jeder Core-Onlinedienst entspricht auch den Kontrollstandards und -bestimmungen, die in der Tabelle in den Produktbestimmungen aufgeführt sind. Jeder Core-Onlinedienst und Professional Service implementiert und unterhält die in Anhang A dargelegten Sicherheitsmaßnahmen zum Schutz von Kundendaten und Professional Services-Daten.

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

Datenverschlüsselung

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

Microsoft verschlüsselt auch ruhende Kundendaten in Onlinediensten und ruhende Professional Services-Daten. Im Fall von Onlinediensten, in denen der Kunde oder ein Dritter, der im Namen des Kunden handelt, Anwendungen erstellen kann (z. B. bestimmte Azure-Dienste), kann die Verschlüsselung der in diesen Anwendungen gespeicherten Daten nach Ermessen des Kunden erfolgen, unter Verwendung von Funktionen, die von Microsoft 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 und Professional Services-Daten (einschließlich darin enthaltener personenbezogener Daten) zu kontrollieren. Eine rollenbasierte Zugriffssteuerung wird eingesetzt, um sicherzustellen, dass der für den Servicebetrieb erforderliche Zugriff auf Kundendaten und Professional Services-Daten einem angemessenen Zweck dient und unter Aufsicht des Vorgesetzten genehmigt ist. Für Core-Onlinedienste und Professional Services unterhält Microsoft Zugriffskontrollmechanismen, die in der Tabelle mit dem Titel „Sicherheitsmaßnahmen" in Anhang A beschrieben sind. Für Core-Onlinedienste gibt es keinen ständigen Zugriff von Microsoft-Mitarbeitern auf Kundendaten und jeder erforderliche Zugriff ist zeitlich begrenzt.

Pflichten des Kunden

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

Prüfung der Einhaltung

Microsoft wird Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft zur Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten nutzt, wie folgt durchführen:

- Sieht eine Norm oder ein Rahmenkonzept Prüfungen vor, so wird mindestens einmal jährlich eine Prüfung dieser Kontrollnorm oder dieses Rahmenkonzepts veranlasst.
- Jede Prüfung wird entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder Rahmenbestimmungen durchgeführt.
- Jede Prüfung wird von qualifizierten, unabhängigen dritten Sicherheitsprüfern durchgeführt, die von Microsoft ausgewählt werden und für die Microsoft die Kosten trägt.

Jede Prüfung führt zur Erstellung eines Prüfungsberichts („Microsoft-Prüfungsbericht"), den Microsoft unter https://servicetrust.microsoft.com/ oder an einem anderen von Microsoft angegebenen Ort zur Verfügung stellt. Der Microsoft-Prüfungsbericht ist eine Vertrauliche Information von Microsoft und legt alle wesentlichen Feststellungen des Prüfers eindeutig offen. Microsoft behebt umgehend alle in einem Microsoft-Prüfbericht festgestellten Probleme zur Zufriedenheit des Prüfers. Auf Verlangen des Kunden stellt Microsoft dem Kunden jeden Microsoft-Prüfbericht zur Verfügung. Der Microsoft-Prüfbericht unterliegt den Vertraulichkeits- und Verteilungseinschränkungen, 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. Soweit für die Durchführung der Prüfung erforderlich stellt Microsoft die relevanten Verarbeitungssysteme, Einrichtungen und unterstützende Unterlagen zur Verfügung, die für die Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten durch Microsoft, die mit Microsoft verbundenen Unternehmen und Unterauftragsverarbeiter relevant sind. Eine solche Prüfung wird von einer unabhängigen, akkreditierten und externen Prüfungsgesellschaft während der normalen Geschäftszeiten mit angemessener Vorankündigung für Microsoft sowie unter Einhaltung angemessener Vertraulichkeitsverfahren durchgeführt. Weder der Kunde noch der Prüfer haben Zugriff auf die Daten anderer Kunden von Microsoft oder auf Microsoft-Systeme oder Einrichtungen, die nicht an der Bereitstellung der jeweiligen Produkte und Services beteiligt sind. Der Kunde ist für sämtliche Kosten und Gebühren im Zusammenhang mit dieser Prüfung verantwortlich, einschließlich aller angemessenen Kosten und Gebühren, die Microsoft für eine solche Prüfung aufwendet, zusätzlich zu den Gebühren für von Microsoft erbrachte Dienstleistungen. Wenn der als Ergebnis der Prüfung des Kunden erstellte Prüfbericht Erkenntnisse zu wesentlichen Fällen fehlender Einhaltung dokumentiert, leitet der Kunde diesen Prüfbericht an Microsoft weiter. Microsoft muss jede wesentliche fehlende Einhaltung unverzüglich beheben.

Wenn die Standardvertragsklauseln von 2010 gelten, findet dieser Absatz zusätzlich zu Klausel 5, Absatz f und Klausel 12, Absatz 2 der Standardvertragsklauseln von 2010 Anwendung. Keine Bestimmung in diesem Abschnitt des DPA ändert die Standardvertragsklauseln von 2010 oder die DSGVO-Bestimmungen oder beeinträchtigt die Rechte einer Aufsichtsbehörde oder einer betroffenen Person gemäß den Standardvertragsklauseln von 2010 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, Professional Services-Daten oder personenbezogene Daten während der Verarbeitung durch Microsoft führt (jeweils ein „Sicherheitsvorfall"), wird Microsoft den Kunden unverzüglich und ohne schuldhaftes Zögern (1) vom Sicherheitsvorfall benachrichtigen; (2) den Sicherheitsvorfall untersuchen und den Kunden mit detaillierten Informationen über den Sicherheitsvorfall versorgen; (3) angemessene Maßnahmen ergreifen, um die Auswirkungen zu mildern und den Schaden, der sich aus dem Sicherheitsvorfall ergibt, so gering wie möglich zu halten.

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

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

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

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

Datenübermittlungen und Speicherstelle

Datenübermittlungen

Kundendaten, Professional Services-Daten und personenbezogene Daten, die Microsoft im Auftrag des Kunden verarbeitet, dürfen nur gemäß den DPA-Bestimmungen und den nachstehend in diesem Abschnitt vorgesehenen Sicherheitsmaßnahmen an einen bestimmten geografischen Standort übermittelt und dort gespeichert und verarbeitet werden. Unter Berücksichtigung solcher Sicherheitsmaßnahmen beauftragt der Kunde Microsoft, Kundendaten, Professional Services-Daten und 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 Produkte zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den DPA-Bestimmungen beschrieben.

Für sämtliche Übermittlungen von Kundendaten, Professional Services-Daten und personenbezogenen Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Produkte und Services gelten die von Microsoft implementierten Standardvertragsklauseln von 2021. Darüber hinaus unterliegen Übertragungen aus dem Vereinigten Königreich und der Schweiz den Standardvertragsklauseln von 2010. Im Falle einer Inkonsistenz zwischen den Standardvertragsklauseln von 2021 und den Standardvertragsklauseln von 2010 wird die Inkonsistenz so behoben, dass ein angemessenes Datenschutzniveau für die Kundendaten, Professional Services-Daten und personenbezogenen Daten nach geltendem Recht gewährleistet ist. 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 den Produktbestimmungen beschrieben.

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

Speicherung und Löschung von Daten

Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu löschen.

Mit Ausnahme von kostenlosen Testversionen und LinkedIn-Diensten wird Microsoft Kundendaten, die in den Onlinediensten gespeichert bleiben, 90 Tage lang nach Ablauf oder Beendigung des Abonnements des Kunden in einem eingeschränkten Funktionskonto aufbewahren, damit der Kunde die Daten extrahieren kann. Nach Ablauf der 90-tägigen Aufbewahrungsfrist deaktiviert Microsoft das Konto des Kunden und löscht die in den Onlinediensten gespeicherten Kundendaten und personenbezogenen Daten innerhalb weiterer 90 Tage; es sei denn, Microsoft ist durch dieses DPA zur Aufbewahrung autorisiert.

Für personenbezogene Daten in Verbindung mit der Software sowie für Professional Services-Daten gilt, dass Microsoft alle Kopien löschen wird, nachdem die geschäftlichen Zwecke erfüllt wurden, zu denen die Daten erhoben oder übermittelt wurden (auf Kundenwunsch auch früher); es sei denn, Microsoft ist durch diesen DPA zur Aufbewahrung dieser Daten autorisiert.

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

Vertraulichkeitsverpflichtung des Auftragsverarbeiters

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

Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern

Microsoft kann Unterauftragsverarbeiter beauftragen, bestimmte eingeschränkte oder unterstützende Dienstleistungen für Microsoft zu erbringen. Der Kunde erklärt sich einverstanden, dass eine solche Beauftragung erfolgt und dass Microsoft-Gesellschaften als Unterauftragsverarbeiter eingesetzt werden. Die oben genannten Autorisierungen stellen die vorherige schriftliche Zustimmung des Kunden zur Untervergabe der Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten durch Microsoft dar, wenn eine solche Zustimmung nach den Standardvertragsklauseln oder den Bestimmungen der 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, Professional Services-Daten oder personenbezogene Daten nur zugreifen und diese nur dazu nutzen darf, um die Dienstleistungen zu erbringen, für die Microsoft ihn beauftragt hat; und dass es ist ihm untersagt ist, Kundendaten, Professional Services-Daten oder personenbezogene Daten für andere Zwecke zu nutzen. Microsoft wird sicherstellen, dass Unterauftragsverarbeiter durch schriftliche Vereinbarungen gebunden sind, die von ihnen verlangen, dass sie mindestens das Datenschutzniveau bieten, das dieses DPA von Microsoft verlangt, einschließlich der Beschränkungen für die Offenlegung verarbeiteter Daten. Microsoft verpflichtet sich, die Unterauftragsverarbeiter zu beaufsichtigen, um sicherzustellen, dass diese vertraglichen Verpflichtungen erfüllt werden.

Microsoft beauftragt gelegentlich möglicherweise neue Unterauftragsverarbeiter. Microsoft informiert den Kunden mindestens 6 Monate, bevor dieser Zugriff auf Kundendaten erhält über jeden neuen Unterauftragsverarbeiter (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 Professional Services-Daten oder personenbezogene Daten erhält, die nicht in den Kundendaten enthalten sind. Wenn Microsoft einen neuen Unterauftragsverarbeiter für ein neues Produkt oder einen Professional Service beauftragt, der Kundendaten, Professional Services-Daten oder personenbezogene Daten verarbeitet, wird Microsoft den Kunden vor der Verfügbarkeit dieses Produkts oder Professional Services benachrichtigen.

Wenn der Kunde einem neuen Unterauftragsverarbeiter für einen Onlinedienst oder für Professional Services nicht zustimmt, kann er ein etwaiges Abonnement für den betroffenen Onlinedienst oder die zutreffenden Leistungsbeschreibungen, wie z. B. einen Enterprise Services-Arbeitsauftrag, für den betreffenden Professional Services, jeweils ohne Strafe oder Kündigungsgebühr beenden, indem er vor dem Ablauf der entsprechenden Kündigungsfrist eine schriftliche Kündigung einreicht. Wenn der Kunde einem neuen Unterauftragsverarbeiter für Software nicht zustimmt und der Kunde die Nutzung des Unterauftragsverarbeiters nicht vernünftigerweise vermeiden kann, indem er Microsoft daran hindert, Daten wie in der Dokumentation oder dieser DPA beschrieben zu verarbeiten, kann der Kunde jede Lizenz für das betroffene Softwareprodukt durch schriftliche Kündigung vor Ablauf der jeweiligen Kündigungsfrist ohne Strafe kündigen. Der Kunde kann zusammen mit der Kündigung auch eine Erklärung der Gründe für seine Ablehnung beifügen, damit Microsoft die Möglichkeit hat, diesen neuen Unterauftragsverarbeiter anhand der vorgebrachten Bedenken neu zu bewerten. Wenn das betroffene Produkt Teil einer Suite (oder eines ähnlichen einzelnen Kaufs von Diensten) ist, gilt die Kündigung für die gesamte Suite. Nach der Kündigung entfernt Microsoft die Zahlungsverpflichtungen für jedwedes Abonnement oder sonstige entsprechende nicht bezahlte Arbeiten für die gekündigten Produkte oder Services aus den nachfolgenden Rechnungen an den Kunden oder seinen Handelspartner.

Bildungseinrichtungen

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

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

CJIS-Kundenvertrag

Microsoft stellt bestimmte Verwaltungs-Cloud-Services („abgedeckte Services") in Übereinstimmung mit der Sicherheitsrichtlinie der FBI Criminal Justice Information Services („CJIS-Richtlinie") zur Verfügung. Die CJIS-Richtlinie regelt die Nutzung und Übertragung von Strafjustizinformationen. Alle abgedeckten CJIS-Services von Microsoft unterliegen den Bestimmungen des CJIS-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 „geschützte Gesundheitsinformationen („protected health information")" in Kundendaten oder Professional Services-Daten enthält, wie diese Begriffe im Health Insurance Portability and Accountability Act von 1996 in der jeweils geltenden Fassung und in den darunter veröffentlichten Vorschriften (zusammen „HIPAA") definiert sind, umfasst die Ausfertigung des Volumenlizenzvertrags des Kunden die Ausfertigung des HIPAA Vertrags für Geschäftspartner (HIPAA Business Associate Agreement „BAA"). Der vollständige Text des BAA identifiziert die Onlinedienste oder Professional Services, für die er gilt, und ist verfügbar unter http://aka.ms/BAA. Der Kunde kann 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, Professional Services-Daten und personenbezogene Daten im Namen des Kunden und wird diese Daten nicht für andere als die in diesen DPA-Bestimmungen genannten und nach dem CCPA zulässigen Zwecke aufbewahren, verwenden oder offenlegen, einschließlich Ausnahmeregelungen für den „Verkauf". Unter keinen Umständen verkauft Microsoft solche Daten. Diese CCPA-Bestimmungen begrenzen oder verringern nicht die Datenschutzverpflichtungen, die Microsoft gegenüber dem Kunden in den DPA-Bestimmungen, den Produktbestimmungen oder in anderen Vereinbarungen zwischen Microsoft und dem Kunden eingegangen ist.

Biometrische Daten

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

Zusätzliche Professional Services

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

[redacted]

Für Zusätzliche Professional Services gelten die folgenden Abschnitte des DPA in gleicher Weise wie für Professional Services: „Einleitung", „Einhaltung von Gesetzen", „Art der Datenverarbeitung; Eigentumsverhältnisse", „Offenlegung verarbeiteter Daten", „Verarbeitung personenbezogener Daten; DSGVO", erster Absatz von „Sicherheitspraktiken und -richtlinien", „Pflichten des Kunden", „Benachrichtigung über Sicherheitsvorfälle", „Datenübertragung" (einschließlich der Bestimmungen zu den Standardvertragsklauseln 2010 und Standardvertragsklauseln 2021), der dritte Absatz von „Datenaufbewahrung und -löschung", „Vertraulichkeitsverpflichtung des Verarbeiters", „Hinweise und Kontrollen bei der Verwendung von Unterauftragsverarbeitern", „HIPAA Business Associate" (soweit im BAA anwendbar), „California Consumer Privacy Act (CCPA)", „Biometrische Daten", „Kontaktaufnahme mit Microsoft", „Anhang B – Betroffene Personen und Kategorien personenbezogener Daten" und „Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen".

Kontaktaufnahme mit Microsoft

Wenn der Kunde der Ansicht ist, dass Microsoft seinen Datenschutz- und Sicherheitsverpflichtungen nicht nachkommt, kann der Kunde Microsoft über den Kundensupport oder über das Datenschutzformular über http://go.microsoft.com/?linkid=9846224 kontaktieren. Postanschrift von Microsoft:

Microsoft Enterprise Service-Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052, USA

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

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

Inhaltsverzeichnis / Allgemeine Bestimmungen

Anhang A – Sicherheitsmaßnahmen

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

Domäne	Praktiken
Organisation der IT-Sicherheit	**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, die Zugang zu Kundendaten oder Professional Services-Daten haben, sind zur Vertraulichkeit verpflichtet. **Risikomanagementprogramm.** Microsoft hat vor der Verarbeitung der Kundendaten oder dem Start des Onlinedienstes und vor der Verarbeitung von Professional Services-Daten oder dem Start der Professional Services eine Risikobewertung durchgeführt. 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 oder Professional Services-Daten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf Microsoft-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind. **Asset-Handling** - Microsoft klassifiziert Kundendaten Professional Services-Daten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs darauf zu ermöglichen. - Microsoft legt Einschränkungen für das Drucken von Kundendaten und Professional Services-Daten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die solche Daten enthalten. - Mitarbeiter von Microsoft müssen eine Genehmigung von Microsoft einholen, bevor sie Kundendaten oder Professional Services-Daten auf tragbaren Geräten speichern, remote auf solche Daten zugreifen oder solche Daten außerhalb der Einrichtungen von Microsoft verarbeiten.
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 Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen. **Physischer Zugriff auf Komponenten.** Microsoft führt Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten. **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 Kundendaten und Professional Services-Daten 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 oder Professional Services-Daten haben. **Datenwiederherstellungsverfahren** - Microsoft erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es haben im betreffenden Zeitraum keine Aktualisierungen stattgefunden) mehrere Kopien von Kundendaten und Professional Services-Daten, aus denen solche Daten wiederhergestellt werden können. - Microsoft bewahrt Kopien von Kundendaten und Professional Services-Daten und Datenwiederherstellungsverfahren an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die die Kundendaten und Professional Services-Datenverarbeitet werden. - Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten und Professional Services-Daten regeln.

Domäne	Praktiken
	- Microsoft prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. Ausgenommen hiervon sind Verfahren für Professional Services und für Azure Government Services, die alle zwölf Monate geprüft werden. - 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. **Malware.** Microsoft nimmt Anti-Malware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Kundendaten und Professional Services-Daten erhält, einschließlich bösartiger Software aus öffentlichen Netzwerken. **Daten außerhalb von Landesgrenzen** - Microsoft verschlüsselt Kundendaten und Professional Services-Daten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung. - Microsoft schränkt den Zugriff auf Kundendaten und Professional Services-Daten in Medien ein, die die Einrichtungen von Microsoft verlassen. **Ereignisprotokollierung.** Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten oder Professional Services-Daten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.
Zugriffskontrolle	**Zugriffsrichtlinie.** Microsoft führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu Kundendaten oder Professional Services-Daten haben. **Zugriffsberechtigung** - Microsoft führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf Microsoft-Systeme autorisiert sind, die Kundendaten oder 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. - Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten oder Professional Services-Daten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen. **Geringste Rechte** - Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten und Professional Services-Daten nur gestattet, wenn dies erforderlich ist. - Microsoft schränkt den Zugriff auf Kundendaten und 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 dem Kunden eine solche Überwachung. - Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden.

Domäne	Praktiken
	- 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 Kundendaten oder Professional Services-Daten zu erhalten, auf die sie nicht zugreifen dürfen.
Handhabung eines Informationssicherheitsvorfalls	**Vorfallreaktionsablauf** - Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens für die Wiederherstellung von Daten. - Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (wie im Abschnitt „Meldung von Sicherheitsvorfällen" weiter oben beschrieben) unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens Microsoft. - Microsoft untersucht Offenlegungen von Kundendaten und Professional Services-Daten einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage. **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 oder Professional Services-Daten verarbeiten. - Bei Microsoft sind redundante Speicherung und ihre Verfahren zur Datenwiederherstellung so konzipiert, dass versucht wird, Kundendaten und Professional Services-Daten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.

Inhaltsverzeichnis / Allgemeine Bestimmungen

Anhang B – Betroffene Personen und Kategorien personenbezogener Daten

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

- Mitarbeiter, Auftragnehmer und Zeitarbeitnehmer des Datenexporteurs (derzeitige, ehemalige, zukünftige);
- Angehörige der oben genannten Personen;
- Partner/Kontaktpersonen des Datenexporteurs (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeiter von Partnern/Kontaktpersonen (juristische Personen) (derzeitige, ehemalige, zukünftige),
- Benutzer (z. B. Kunden, Klienten, Patienten, Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen des 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
- Berufsgeheimnisträger (z. B. Ärzte, Anwälte, Notare, Kirchenmitarbeiter usw.).

Kategorien von Daten: Die übermittelten personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Produkte und Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte und Services die Möglichkeit hat, personenbezogene Daten aus 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-Protokoll);
- Kontaktinformationen (z. B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten);
- Eindeutige Identifikationsnummern und Signaturen (z. B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentennummer, Patientennummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien);
- Pseudonymisierte Kennungen;
- Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartenname und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität);
- Geschäftsinformationen (z. B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf);
- Biometrische Informationen (z. B. DNA, Fingerabdrücke und Iris-Erfassungen);
- Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden);
- Fotos, Videos und Audio;
- Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören);
- Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartennummer, MAC-Adresse);

- Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen);
- Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen);
- Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung);
- Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis);
- Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird;
- Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Anklagen); oder
- Alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten.

[redacted]

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 Anwendungsbereich der DSGVO durch Microsoft im Auftrag des Kunden und zusätzliche Rechtsbehelfe für die betroffenen Personen, auf die sich personenbezogene Daten beziehen.

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

1. **Anfechtung von Anordnungen.** Für den Fall, dass Microsoft von einem Dritten eine Anordnung zur zwingenden Offenlegung von personenbezogenen Daten erhält, die im Rahmen dieses DPA verarbeitet werden, wird Microsoft:

   a. alle angemessenen Anstrengungen unternehmen, um den Dritten bezüglich der Anforderung von Daten direkt an den Kunden zu verweisen;

   b. den Kunden unverzüglich 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

   c. alle rechtmäßigen Anstrengungen unternehmen, um die Aufforderung zur Offenlegung auf der Grundlage von Rechtsmängeln nach dem Recht der anfragenden Partei oder von relevanten Konflikten mit dem anwendbaren Recht der Europäischen Union oder dem anwendbaren Recht der Mitgliedstaaten anzufechten.

wenn Microsoft oder eines seiner verbundenen Unternehmen nach den unter a. bis c. oben beschriebenen 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.

2. **Entschädigung von betroffener Personen.** Vorbehaltlich der Abschnitte 3 und 4 hat Microsoft einer betroffene Person jeglichen materiellen oder immateriellen Schäden zu ersetzen, der der betroffenen Person dadurch entstehen, dass Microsoft personenbezogene Daten der betroffenen Person offenlegt, indem diese als Reaktion auf eine Aufforderung einer öffentlichen Stelle oder einer Strafverfolgungsbehörde außerhalb der EU/des EWR unter Verletzung der Verpflichtungen von Microsoft gemäß Kapitel V der DSGVO übermittelt wurden (eine „Relevante Offenlegung"). Ungeachtet des Vorstehenden ist Microsoft nicht verpflichtet, die betroffene Person gemäß dieses Abschnitt 2 zu entschädigen, soweit die betroffene Person bereits eine Entschädigung für denselben Schaden erhalten hat, sei es von Microsoft oder anderweitig.

3. **Bedingungen für die Entschädigung.** Die Entschädigung nach Abschnitt 2 setzt voraus, dass die betroffene Person zur angemessenen Zufriedenheit von Microsoft Folgendes nachweist:

   a. Microsoft hat eine Relevante Offenlegung vorgenommen;

   b. Die Relevante Offenlegung war die Grundlage eines offiziellen Verfahrens der öffentlichen Stelle oder Strafverfolgungsbehörde in einem Land außerhalb der EU/des EWR gegen die betroffene Person und

   c. die Relevante Offenlegung führte direkt zu materiellen oder immateriellen Schäden für die betroffene Person.

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.

4. **Umfang des Schadensersatzes.** Die Freistellung nach Abschnitt 2 ist auf materielle und immaterielle Schäden gemäß DSGVO beschränkt und schließt Folgeschäden und alle anderen Schäden aus, die nicht das Ergebnis eines Verstoßes von Microsoft gegen die DSGVO sind.

5. **Ausübung von Rechten.** Rechte, die betroffenen Personen in diesem Nachtrag gewährt werden, können von den betroffenen Personen unabhängig von den Beschränkungen in den Abschnitten 3 oder 6 der Standardvertragsklauseln Microsoft gegenüber durchgesetzt werden. Die betroffene Person darf einen Anspruch nach diesem Nachtrag nur auf individueller Basis erheben und nicht als Teil einer Muster-, Sammel-, Gruppen- oder Verbandsklage. Rechte, die betroffenen Personen im Rahmen dieses Nachtrags gewährt werden, sind nur für die betroffene Person bestimmt und nicht abtretbar.

6. **Änderungsmitteilung.** Microsoft stimmt zu und gewährleistet, dass Microsoft keinen Grund zu der Annahme hat, dass die für Microsoft oder ihre Unterauftragsverarbeiter geltenden Gesetze, einschließlich in jedem Land, in das Microsoft oder ihre Unterauftragsverarbeiter personenbezogene Daten übermitteln, Microsoft daran hindern, die vom Datenexporteur erhaltenen Weisungen und ihre Verpflichtungen aus diesem Nachtrag, den Standardvertragsklauseln von 2010 oder aus den Standardvertragsklauseln von 2021 zu erfüllen, und dass Microsoft im Fall einer Änderung dieser Gesetze, die wahrscheinlich erhebliche nachteilige Auswirkungen auf die in diesem Nachtrag 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.

7. **Beendigung.** Dieser Nachtrag endet automatisch, wenn die Europäische Kommission, eine zuständige Aufsichtsbehörde eines Mitgliedstaats oder ein Gericht der EU oder eines zuständigen Mitgliedstaats einen anderen gesetzlichen Übermittlungsmechanismus genehmigt, der auf die personenbezogenen Daten in den Kundendaten, Professional Services-Daten oder sonstigen personenbezogenen Daten, die unter dem DPA verarbeitet werden, anwendbar wäre (und falls ein solcher Mechanismus nur auf einige der Datenübermittlungen anwendbar ist, endet dieser Nachtrag nur in Bezug auf solche Daten) und der die in diesem Nachtrag festgelegten zusätzlichen Schutzmaßnahmen nicht erfordert.

Anhang 1 – Die Standardvertragsklauseln von 2010 (Auftragsverarbeiter)

Die Ausführung des Volumenlizenzvertrags durch den Kunden umfasst die Ausführung dieses Anhangs 1, der von der Microsoft Corporation gegengezeichnet ist. Dieser Anhang 1 gilt zusätzlich zur Ausführung der Standardvertragsklauseln von 2021 durch Microsoft. Im Falle einer Inkonsistenz zwischen diesem Anhang 1 und den Standardvertragsklauseln von 2021 wird die Inkonsistenz so behoben, dass ein angemessenes Datenschutzniveau für die Kundendaten, Professional Services-Daten und personenbezogenen Daten nach geltendem Recht gewährleistet 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 emessene 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

(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;

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

Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere geschäftsbezogene ...auseln 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 ... 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 Produktbestimmungen definierten Produkte 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, wie in Anhang B zum DPA angegeben.

Kategorien von Daten: Die übermittelten personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Produkte oder Professional Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte oder Professional Services die Möglichkeit hat, personenbezogene Daten aus einer der folgenden, in Anhang B des DPA angegebenen Kategorien aufzunehmen:

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 Bereitstellung der Produkte und 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 Produkte und 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 Produkte 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 -richtlinien" 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, Anhang 1 und Anhang 2 im Namen des Datenimporteurs:

Signature [redacted] .....

Rajesh Jha, Executive Vice President

Microsoft Corporation

One Microsoft Way, Redmond, WA 98052, USA

[redacted]

Anlage 2 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union

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

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

Relevante DSGVO-Verpflichtungen: Artikel 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 Bestimmungen

[redacted]