1

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – 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)

[redacted]

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:

a) Erfüllungsgrad der technischen Anforderungen
b) Risikobeurteilung (Datenschutz, Informationssicherheit, organisatorische, technische und vertragliche Massnahmen)
c) 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)
d) Preis (Kosten / Service-Kosten) (bezogen auf die geplante Bezugsmenge)
e) 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. 2.2), 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:

a) 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)
b) Paket #02: Preislisten
c) Paket #03: Weitere Dienstleistungen, die für den Leistungsbezug notwendig sind
d) Paket #04: Nicht-funktionale Eigenschaften (Sicherheitsdokumentationen, Prüfberichte, etc.)
e) 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:

a) die von ihr im Einzelfall festgelegten Abrufkriterien gem. internem anbieterneutralen Pflichtenheft für den konkreten Bedarf
b) den Entscheid (Ziff. 3.2), mit Nennung der zugewiesenen Abrufsumme, Zuschlagsperiode und Stichtag (mit Datum und Zeit), zu dem die Bewertung vorgenommen wurde
c) 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.

* * *

2

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Audit

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)

[redacted]

1. Begriffsdefinitionen

1.1 Für die Zwecke des vorliegenden Vertragsanhangs sind die folgenden Begriffe wie folgt definiert:

a) **«Auditberechtigte Stellen»** sind: die Vergabestelle und die jeweils Bezugsberechtigten sowie jeweils deren interne und externe Revisionsstellen, deren Aufsichtsbehörden und –stellen, vorausgesetzt diese haben ein selbständiges Auditrecht gegen die Firma als Clouddienstleister unter entsprechend anwendbarem Recht. Die Firma anerkennt ausdrücklich, dass auch die folgenden Stellen als Auditberechtigte Stellen gelten, vorausgesetzt diese haben ein entsprechendes Auditrecht unter der Datenschutz-/Finanzkontrollgesetzgebung:

- der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB);
- die Eidgenössische Finanzkontrolle (EFK).

b) **Audit** meint (austauschbar) Revision, Audit, Prüfung, Analyse oder Inspektion und steht zusammenfassend für alle Rechte unter diesem Anhang.

1.2 Ansonsten gelten die Begriffe gemäss Rahmenvertrag.

2. Kontrollrechte (Audit)

2.1 Die Firma räumt jeder Auditberechtigten Stelle hiermit das Recht ein, (i) Audit Reports von der Firma gemäss Ziff. 3.1 einzuholen und (ii) soweit gemäss Ziff. 3.2 notwendig, die Leistungserbringung an die Auditberechtigte Stelle, die Grundlagen der Rechnungsstellung hierfür und die dazu gehörenden Unterlagen, vorbehaltlich der Bestimmungen dieses Anhangs, maximal einmal jährlich einzusehen und zu prüfen.

2.2 Jede Auditberechtigte Stelle kann sich unabhängig von anderen Auditberechtigten Stellen auf das Recht gemäss Ziff. 2.1 berufen.

2.3 Die Vergabestelle kann sich auf das Recht gemäss Ziff. 2.1 gesamthaft und losgelöst vom Bedarf einer Bezugsberechtigten berufen und somit Audits auch mit einer Gesamtperspektive anlegen. Sie bedarf dazu der Mitwirkung der Bezugsberechtigten nicht.

3. Mitwirkungspflichten der Firma

3.1 Die Firma verschafft der Auditberechtigten Stelle auf Anfrage Auditberichte, die von unabhängigen, qualifizierten Drittprüfern erstellt wurden und die Erbringung von Dienstleistungen unter einem Einzelabruf unter dem Rahmenvertrag abdecken.

3.2 Für den Fall, dass:

(i) eine Sicherheitsverletzung aufgetreten ist oder eine Auditberechtigte Stelle dokumentierte Hinweise hat, dass die Firma kein ausreichendes Qualitäts- und/oder Sicherheitsniveau aufrechterhält, um die Anforderungen des Rahmenvertrags zu erfüllen;

(ii) die in Ziff. 3.1 erwähnten Auditberichte sich nicht auf die Einhaltung der Qualitäts- und/oder Sicherheitsanforderungen durch die Firma gemäss anwendbarem Recht oder Rahmenvertrag erstrecken und bescheinigen können; oder

(iii) eine zwingende Vorschrift einer Auditberechtigten Stelle ein unmittelbares Recht gibt, die Firma zu prüfen;

kann die Auditberechtigte Stelle die Firma mit einer Frist von mindestens fünfzehn Arbeitstagen schriftlich auffordern, ihr zum Zwecke der Durchführung eines Audits folgenden Zugang und folgende Unterstützung zu gewähren:

a) Physischen Zugang zu den Standorten, von denen aus die Dienstleistungen erbracht werden;

b) Physischen und logischen Zugriff auf alle die Dienstleistungen betreffenden Daten und Unterlagen;

Zugang und Zugriffsmöglichkeiten müssen den Zweck des beantragten Audits, der Prüfung oder Inspektionen ermöglichen (dazu Ziff. 4).

Die Firma hat solche Prüfungen angemessen zu begleiten, zu unterstützen und an ihnen mitzuwirken.

3.3 Die Firma verpflichtet sich, alle Informationen und Erläuterungen bereitzustellen, welche die Prüfer der Auditberechtigten Stellen für notwendig oder hilfreich erachten.

4. Zweck des Audits

4.1 Das Audit kann insbesondere die folgenden Ziele und Zwecke verfolgen:

a) öffentlich-rechtliche Anforderungen nachzuweisen bzw. deren Erfüllungsgrad zu prüfen;

b) Anfragen von Aufsichtsbehörden zu erfüllen;

c) festzustellen, ob die Dienstleistungen mit den Bedingungen des Rahmenvertrags und den geltenden Leistungsbeschreibungen übereinstimmen;

d) die Durchführung von Abläufen und Verfahren einschliesslich Datenbearbeitungsaktivitäten und -kontrollen der Firma zu prüfen; und

e) die Richtigkeit der Vergütung festzustellen.

5. Prüfer der Auditberechtigten Stelle

Ein Audit kann (i) von internen Mitarbeitenden einer Auditberechtigten Stelle, (ii) von unabhängigen, von der Auditberechtigten Stelle beauftragten Dritten (Ziffern (i) und (ii) nachfolgend zusammengefasst als "**Prüfer der Auditberechtigten Stelle**" bezeichnet) sowie (iii) von Aufsichtsbehörden und den von diesen bezeichneten Vertreter/innen durchgeführt werden.

6. Kosten des Audits

6.1 Die Firma trägt die eigenen internen Kosten (inklusive Kosten für Auditberichte gem. Ziff. 3.1), die ihr bei der Durchführung des Audits anfallen. Ziff. 6.5 ist vorbehalten.

6.2 Die Auditberechtigte Stelle, die einen Audit auslöst, trägt ihre eigenen intern und extern entstehenden Kosten (beispielsweise indem sie eine Drittprüferin beauftragt) selber.

6.3 Die weiteren Kosten für die Durchführung eines Audits trägt die Stelle, welche die Durchführung des Audits bei der Firma auslöst, sofern das Audit keinen erheblichen Verstoss gegen den Rahmenvertrag und/oder die anwendbaren gesetzlichen Verpflichtungen ergibt.

6.4 Ergibt das Audit einen erheblichen Verstoss gegen den Rahmenvertrag und/oder anwendbare gesetzliche Verpflichtungen durch die Firma, trägt die Firma die Kosten des betreffenden Audits (d.h. Kosten gem. Ziff. 6.3, aber nicht interne Aufwendungen der Auditberechtigten Stelle gem. Ziff. 6.2).

6.5 Übersteigt der interne Aufwand der Firma zur Unterstützung der Prüfer der Auditberechtigten Stelle 10 Personentage pro Vertragsjahr, ist der darüberhinausgehende Aufwand von der Auditberechtigten Stelle zu vergüten. Der Tagessatz pro Person beträgt 1'500 Schweizer Franken.

7. Festgestellte Unregelmässigkeiten in Bezug auf Vergütungen

7.1 Ergibt eine Prüfung, dass die Firma Vergütungen unter Verstoss gegen den Rahmenvertrag in Rechnung gestellt hat, hat sie den zu Unrecht in Rechnung gestellten Betrag unverzüglich zurückzuerstatten, sofern dieser Teil bereits bezahlt wurde.

7.2 Ergibt eine solche Prüfung ferner, dass mehr als fünf Prozent (5%) des effektiv zu belastenden Betrags zu viel berechnet wurden, hat die Firma zudem die Kosten der Prüfung (Kosten gem. Ziff. 6.3) zu erstatten und ihre internen Kosten selber zu tragen.

8. Festgestellte Unregelmässigkeiten in Bezug auf andere Vorgaben

8.1 Ergibt eine Prüfung, dass die Firma andere wesentliche Vorgaben des Rahmenvertrags nicht eingehalten hat, hat sie umgehend den vertragsgemässen Zustand herzustellen oder, falls eine Wiederherstellung aufgrund der Art des Verstosses nicht möglich ist, die Auswirkungen des Verstosses unverzüglich zu beheben.

8.2 Sollte sie nicht in der Lage sein, den vertragsgemässen Zustand innert einer Frist von fünf (5) Arbeitstagen seit Mitteilung der Unregelmässigkeit an die Firma wieder herzustellen oder entsprechende Auswirkungen zu beheben, ist die Firma auf eigene Kosten zu den folgenden Schritten verpflichtet:

a) Umgehende Information an die Bezugsberechtigte und immer auch an die Vergabestelle, dass sie zur sofortigen Herstellung des rechtmässigen Zustands oder Behebung der entsprechenden Auswirkungen nicht in der Lage ist.

b) Unterbreitung eines Lösungskonzepts an die Bezugsberechtigte und immer auch an die Vergabestelle, das den Weg und die zeitlichen Aspekte bis zur Wiederherstellung des rechtmässigen Zustands oder Behebung der entsprechenden Auswirkungen aufzeigt.

c) Darlegung der Massnahmen, die bis zu einer definitiven Lösung vorzukehren sind, damit die nachteiligen Folgen der Situation von der Bezugsberechtigten, der Vergabestelle und der Bundesverwaltung insgesamt abgewendet werden können.

* * *

[redacted]

3

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Datenschutz

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)

[redacted]

Inhaltsübersicht:

[redacted]

I. ALLGEMEINE BESTIMMUNGEN

1. Anwendbares Recht

1.1 Die einschlägigen Bestimmungen des Bundes zur Vertraulichkeit, Geheimhaltung, Informatiksicherheit und zum Datenschutz finden sich insbesondere in den folgenden Erlassen:

a) Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1)

b) Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11)

c) Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (ISG; BBl 2020 9975; in Kraft ab 1. April 2023).

d) Verordnung über den Schutz von Informationen des Bundes (ISchV; SR 510.411). Diese Verordnung wird mit Inkrafttreten des ISG ausser Kraft gesetzt.

e) Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG; SR 235.3) (namentlich für Strafverfolgungsbehörden; solange das SDSG noch in Kraft ist)

f) in sämtlichen Folgeerlassen zu den vorstehenden Erlassen.

g) weitere Schweizer Erlasse mit Spezialbestimmungen und Anwendbarkeit für eine oder mehrere Bezugsberechtigte.

1.2 Die Firma nimmt zur Kenntnis, dass die Vergabestelle sowie die Bezugsberechtigten – im Sinne des Datenschutzgesetzes (DSG; SR 235.1) – als Bundesorgan gelten.

1.3 Die Firma unternimmt zumutbare Anstrengungen ihre Leistungen so zu erbringen, dass die Vergabestelle sowie Bezugsberechtigte die im Bereich des Datenschutzes für die Bezugsberechtigte massgebenden Schweizer Bestimmungen, welche sie der Firma zur Kenntniss bringen, einhalten können.

2. Zu diesem Vertragsanhang

2.1 Dieser Vertragsanhang Datenschutz («Vertragsanhang») regelt die Rollen, Zuständigkeiten und Verantwortlichkeiten sowie die Rechte und Pflichten in Bezug auf die Bearbeitung von Personendaten im Rahmen der Leistungserbringung der Firma im Auftrag der Bezugsberechtigten.

2.2 Dieser Vertragsanhang soll dazu dienen, dass jede Partei die sich aus dem für sie anwendbaren Datenschutzrecht ergebenden Pflichten erfüllen kann.

2.3 Dieser Vertragsanhang stellt massgeblich ab auf die Standardvertragsklauseln der Europäischen Kommission betreffend die Auftragsverarbeitung gemäss Artikel 28(7) EU-DSGVO[1] (dazu Abschnitt II) und die Standardvertragsklauseln der Europäischen Kommission betreffend die grenzüberschreitende Übermittlung von Personendaten in Drittstaaten (dazu Abschnitt III).[2]

---

1 Anhang zum Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäss Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Euopäischen Parlaments und des Rates, ABl. L 199 vom 7. Juni 2021, S. 18–30.

2 Anhang zum Durchführungsbeschluss der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Eupäischen Parlaments und des Rates, Abl L 199 vom 7. Juni 2021, S. 31–61.

II. KLAUSELN FÜR DIE DATENBEARBEITUNG IM AUFTRAG

A. Allgemeine Bestimmungen

3. Zweck und Anwendungsbereich

3.1 Mit diesen Klauseln soll die Einhaltung von Artikel 10a DSG (resp. Art. 9 revidiertes DSG, in der Folge "nDSG") beziehungsweise (wenn Firma eine in der EU niedergelassene Anbieterin ist) von Artikel 28 EU-DSGVO sichergestellt werden.

3.2 Diese Klauseln gelten für die Bearbeitung sämtlicher Personendaten, welche die Firma (in diesem Abschnitt II deshalb auch "Auftragsbearbeiterin" genannt) als Auftragsbearbeiterin im Auftrag der Bezugsberechtigten (in diesen diesem Abschnitt II deshalb auch "Verantwortliche" genannt) bearbeitet.

3.3 Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit Datenübermittlungen von der Schweiz ins Ausland gemäss Art. 6 DSG (resp. Art. 16 nDSG) bzw. von EU/EWR-Mitgliesstaaten in Drittstaaten gemäss Art. 44 ff. EU-DSGVO erfüllt werden. Diesbezüglich gelten zusätzlich die Bestimmungen in Abschnitt III (Ziff. 20 ff.).

4. Auslegung

4.1 Werden in diesen Klauseln die im DSG (resp. nDSG) definierten Begriffe verwendet, so haben diese Begriffe die ihnen dort zugeschriebene Bedeutung.

4.2 Diese Klauseln sind im Lichte der Bestimmungen des DSG (resp. nDSG) auszulegen.

4.3 Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den im DSG (resp. nDSG) vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

5. Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen des Rahmenvertrags, diesbezüglicher Vertragsnachträge oder Leistungsabrufe, haben diese Klauseln Vorrang.

6. Beschreibung der Auftragsbearbeitung

6.1 Gegenstand und Zweck der Auftragsbearbeitung ist die Bereitstellung der Cloud-Services der Auftragsbearbeiterin für die Verantwortliche.

6.2 Die Auftragsbearbeitung umfasst jede Bearbeitung von Personendaten, welche die Auftragsbearbeiterin im Auftrag der Verantwortlichen im Rahmen der Bereitstellung der Cloud-Services vornimmt, insbesondere jeder so erfolgte und instruierte Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Personendaten.

6.3 Die Art der Personendaten und der Kreis (Kategorien) betroffener Personen ergeben sich aus der Nutzung der Cloud-Services durch die Verantwortliche, den von der Verantwortlichen vorgenommenen Einstellungen sowie aus den öffentlich-verfügbaren Dienstleistungsbeschreibungen der Auftragsbearbeiterin. Zu den bei der Nutzung der Cloud-Services bearbeiteten Personendaten gehören die von der Verantwortlichen bei der Nutzung der Cloud-Services hochgeladenen, eingegebenen, bereitgestellten, gespeicherten oder bearbeiteten Arten von Personendaten.

B. Pflichten der Parteien

7. Weisungen

7.1 Die Auftragsbearbeiterin bearbeitet Personendaten wie folgt:

a) Die Auftragsbearbeiterin bearbeitet Personendaten nur auf dokumentierte Weisung der Verantwortlichen, es sei denn, sie ist nach Schweizer Recht oder nach einem fremden Recht, dem sie unterliegt, zur weitergehenden Bearbeitung verpflichtet.

b) Die Auftragsbearbeiterin teilt der Verantwortlichen mit, wenn ihre Weisungen gegen rechtliche Anforderungen verstossen, sofern das betreffende Recht dies nicht verbietet.

c) Die Verantwortliche kann während der gesamten Dauer der Bearbeitung von Personendaten weitere Weisungen erteilen.

7.2 Die Parteien sind sich einig, dass sich die dokumentierten Weisungen der Verantwortlichen gemäss Ziffer a)7.1 aus dem Rahmenvertrag inkl. Anhänge, anderweitige Vereinbarungen zwischen den Verantwortlichen und der Auftragsbearbeiterin, den durch die Verantwortliche vorgenommenen Einstellungen, der Nutzung der Cloud-Services durch die Verantwortliche sowie den öffentlich-verfügbaren Dienstleistungsbeschreibungen der Auftragsbearbeiterin ergeben.

8. Zweckbindung

Die Auftragsbearbeiterin bearbeitet die Personendaten nur für die spezifischen Zweck(e) der Auftragsbearbeitung, sofern sie keine weiteren Weisungen der Verantwortlichen erhält.

9. Dauer der Bearbeitung von Personendaten

Die Dauer der Bearbeitung der Personendaten ergibt sich aus der Nutzung des Cloud-Services durch die Verantwortliche und aus dem Anhang Migration und Löschung.

10. Sicherheit der Bearbeitung

10.1 Die Auftragsbearbeiterin ergreift angemessene technische und organisatorische Massnahmen, um die Sicherheit der Personendaten zu gewährleisten. Dies umfasst den Schutz der Personendaten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmässig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „**Verletzung der Datensicherheit**").

10.2 Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Bearbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

11. Dokumentation und Einhaltung der Klauseln

11.1 Die Auftragsbearbeiterin muss die Einhaltung dieser Klauseln nachweisen können.

11.2 Die Auftragsbearbeiterin bearbeitet Anfragen der Verantwortlichen bezüglich der Bearbeitung von Personendaten gemäss diesen Klauseln zeitnah und in angemessener Weise.

[redacted]

11.3 Die Auftragsbearbeiterin stellt der Verantwortlichen alle verfügbaren Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus dem DSG (resp. nDSG) hervorgehenden Pflichten erforderlich sind. Dazu gehören auch Informationen zu abgeschlossenen Vereinbarungen betreffend Unterauftragsbearbeitung und Datentransfers ausserhalb des EWR, des Vereinigten Königreichs und der Schweiz.

12. Audit

Auf Verlangen der Verantwortlichen gestattet die Auftragsbearbeiterin ebenfalls die Prüfung der unter diese Klauseln fallenden Bearbeitungstätigkeiten wie im Anhang Audit geregelt. Bei der Entscheidung über eine Überprüfung oder Prüfung kann die Verantwortliche einschlägige Zertifizierungen der Auftragsbearbeiterin berücksichtigen.

13. Einsatz von Unterauftragsbearbeitern

13.1 Die Auftragsbearbeiterin besitzt die allgemeine Genehmigung der Verantwortlichen für die Beauftragung von Unterauftragsbearbeitern, die in der auf dem Portal zur Verfügung gestellten Liste aufgeführt sind, welche von Zeit zu Zeit gemäss Ziffer 13.2 aktualisiert werden kann. Per Zeitpunkt der Vertragsunterzeichnung können die Unterauftragsverhältnisse gemäss Beilage Alibaba Cloud Subsidiaries/Affiliates Sub-processors zu diesem Anhang für die unter einem Einzelabruf bezogenen Dienstleistungen relevant sein, abhängig von der Wahl der Bezugsberechtigten betreffend Datenlokalisation.

13.2 Die Auftragsbearbeiterin unterrichtet die Verantwortliche mindestens drei Monate im Voraus ausdrücklich in schriftlicher Form, wenn die Firma beabsichtigt, eine Unterauftragsbearbeiterin auszutauschen, welche Data-Center-Dienstleistungen an eine Bezugsberechtigte erbringt. Über beabsichtigte Änderungen der Liste gemäss Ziffer 13.1 im Bereich anderer Dienstleistungen (z.B. Support) informiert die Auftragsbearbeiterin die Verantwortliche 10 Tage im Voraus. Die Verantwortliche hat das Recht, Einwände gegen die angekündigten Änderungen zu erheben. Die Auftragsbearbeiterin stellt der Verantwortlichen die erforderlichen Informationen zur Verfügung, damit diese ihr Widerspruchsrecht ausüben kann. Die Verantwortliche hat einen allfälligen Widerspruch gegen einen neuen Unterauffragsbearbeiter zu begründen. Hält die Auftragsbearbeiterin trotz Widerspruchs am Beizug des neuen Unterauftragsbearbeiters fest, so initiiert sie einen Einigungsversuch mit der Verantwortlichen, zu dem die Auftragsbearbeiterin weitere Parteien (namentlich den Unterauftragsbearbeiter) beiziehen kann. Scheitert der Einigungsversuch, steht es der Verantwortlichen frei, auf die Nutzung der Dienstleistungen zu verzichten und den entsprechenden Leistungsabruf ausserordentlich zu kündigen auf den Zeitpunkt auf welchen der entsprechend wiedersprochener Auftragsbearbeiter beigezogen wird.

13.3 Beauftragt die Auftragsbearbeiterin einen Unterauftragsbearbeiter mit der Durchführung bestimmter Bearbeitungstätigkeiten (im Auftrag der Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsbearbeiter materiell dieselben Datenschutzpflichten auferlegt wie diejenigen, die für die Auftragsbearbeiterin gemäss diesen Klauseln gelten. Die Auftragsbearbeiterin stellt sicher, dass der Unterauftragsbearbeiter die Pflichten erfüllt, denen die Auftragsbearbeiterin entsprechend diesen Klauseln und gemäss anwendbarem Datenschutzrecht unterliegt.

13.4 Die Auftragsbearbeiterin haftet unter Anwendung der unter dem Rahmenvertrag geltenden Haftungsbeschränkungen gegenüber der Verantwortlichen dafür, dass der Unterauftragsbearbeiter seinen Pflichten gemäss dem mit der Auftragsbearbeiterin geschlossenen Vertrag nachkommt. Die Auftragsbearbeiterin benachrichtigt die Verantwortliche unverzüglich, wenn der Unterauftragsbearbeiter seine vertraglichen

[redacted]

Pflichten nicht erfüllt. Die Auftragsbearbeiterin ist verpflichtet, den Unterauftragsbearbeiter zur Erfüllung seiner Pflichten anzuhalten.

14. Internationale Datenübermittlungen

14.1 Jede Übermittlung von Personendaten durch die Auftragsbearbeiterin ausserhalb des EWR, des Vereinigten Königreichs und der Schweiz oder an eine internationale Organisation erfolgt ausschliesslich auf der Grundlage dokumentierter Weisungen der Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Recht eines Staates, dem die Auftragsbearbeiterin unterliegt oder wie unter den öffentlich verfügbaren Dienstleistungsbeschreibungen vorgesehen, und muss mit Art. 6 DSG (resp. Art. 16 nDSG) im Einklang stehen.

14.2 Die Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen die Auftragsbearbeiterin einen Unterauftragsbearbeiter gemäss Klausel 13 für die Durchführung bestimmter Bearbeitungstätigkeiten (im Auftrag der Verantwortlichen) in Anspruch nimmt und diese Bearbeitungstätigkeiten eine Übermittlung von Personendaten im Sinne von Art. 6 DSG (resp. Art. 16 nDSG) beinhalten, die Auftragsbearbeiterin und der Unterauftragsbearbeiter die Einhaltung von Art. 6 DSG (resp. Art. 16 nDSG) sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäss Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden.

14.3 Im Übrigen gelten die Bestimmungen gemäss Abschnitt III (Ziff. 20 ff.).

C. Koordination und Compliance

15. Unterstützung der Verantwortlichen

15.1 Die Auftragsbearbeiterin unterrichtet die Verantwortliche zeitnah über jeden Antrag auf Anfrage der Bearbeitung von Personendaten von betroffenen Personen. Sie beantwortet den Antrag inhaltlich nicht selbst, es sei denn, sie wurde von der Verantwortlichen dazu ermächtigt

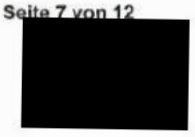
15.2 Unter Berücksichtigung der Art der Bearbeitung unterstützt die Auftragsbearbeiterin die Verantwortliche bei der Erfüllung von deren Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung ihrer Pflichten gemäss diesem und dem vorangehenden Absatz befolgt die Auftragsbearbeiterin die Weisungen der Verantwortlichen.

15.3 Abgesehen von der Pflicht der Auftragsbearbeiterin, die Verantwortliche gemäss dem vorangehenden Absatz zu unterstützen, unterstützt die Auftragsbearbeiterin unter Berücksichtigung der Art der Datenbearbeitung und der ihr zur Verfügung stehenden Informationen die Verantwortliche zudem bei der Einhaltung der folgenden Pflichten:

a) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Bearbeitungsvorgänge für den Schutz von Personendaten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Bearbeitung voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte betroffener Personen zur Folge hat;

b) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Bearbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Bearbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Massnahmen zur Eindämmung des Risikos trifft;

c) Verpflichtungen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes bearbeiten zu schützen.



15.4 Sofern die Unterstützung gemäss Ziffern 15.115.3–15.3 den vertraglich vereinbarten Leistungsumfang erweitert, übernimmt die Verantwortliche die Mehrkosten.

15.5 Die Parteien legen die geeigneten technischen und organisatorischen Massnahmen zur Unterstützung der Verantwortlichen durch die Auftragsbearbeiterin sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest. Falls keine entsprechende gemeinsame Festlegung vor Dienstleistungsabruf erfolgt, gelten die durch die Auftragsbearbeiterin jeweils implementierten technischen und organisatorischen Massnahmen als genügend.

16. Meldung von Verletzungen der Datensicherheit, allgemeine Bestimmungen

Im Falle einer Verletzung der Datensicherheit arbeitet die Auftragsbearbeiterin mit der Verantwortlichen zusammen und unterstützt sie entsprechend, damit die Verantwortliche ihren Verpflichtungen gemäss dem anwendbaren Datenschutzrecht nachkommen kann, wobei die Auftragsbearbeiterin die Art der Bearbeitung und die ihr zur Verfügung stehenden Informationen berücksichtigt.

17. Meldung einer Verletzung der Datensicherheit durch die Auftragsbearbeiterin an die Verantwortliche

17.1 Im Falle einer Verletzung der Datensicherheit im Zusammenhang mit den von der Auftragsbearbeiterin im Auftrag der Verantwortlichen bearbeiteten Personendaten meldet die Auftragsbearbeiterin diese der Verantwortlichen unverzüglich, nachdem ihr die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung der Datensicherheit eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung der Datensicherheit, einschliesslich Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

17.2 Falls nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen. Weitere Informationen werden ab Verfügbarkeit ohne unangemessene Verzögerung bereitgestellt. Die Parteien legen alle sonstigen Angaben fest, die die Auftragsbearbeiterin zur Verfügung zu stellen hat, um der Verantwortlichen bei der Erfüllung von deren Pflichten gemäss anwendbarem Datenschutzrecht zu unterstützen.

18. Meldung einer Verletzung der Datensicherheit durch die Verantwortliche an Aufsichtsbehörden oder betroffene Personen

Im Falle einer Verletzung der Datensicherheit im Zusammenhang mit den von der Verantwortlichen bearbeiteten Personendaten unterstützt die Auftragsbearbeiterin die Verantwortliche, unter Kostenfolgen zu Lasten der Verantwortlichen, wie folgt:

a) bei der unverzüglichen Meldung der Verletzung der Datensicherheit an die zuständige(n) Aufsichtsbehörde(n), nachdem der Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung der Datensicherheit führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit oder die Grundrechte betroffener Personen);

[redacted]

b) bei der Einholung der Informationen, die gemäss dem anwendbaren Datenschutzrecht in der Meldung der Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   i. die Art der Personendaten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen Datensätze;

   ii. die wahrscheinlichen Folgen der Verletzung der Datensicherheit;

   iii. die von der Verantwortlichen ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung der Datensicherheit und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschliessend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäss anwendbarem Datenschutzrecht, die betroffene Person unverzüglich von der Verletzung der Datensicherheit zu benachrichtigen (namentlich dann, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hat).

19. Verstösse gegen die Klauseln und Beendigung

19.1 Falls die Auftragsbearbeiterin ihren Pflichten gemäss diesen Klauseln nicht nachkommt, kann die Verantwortliche – unbeschadet der Bestimmungen des DSG – die Auftragsbearbeiterin anweisen, die Bearbeitung von Personendaten auszusetzen, bis sie diese Klauseln einhält oder der betroffene Leistungsabruf unter dem Rahmenvertrag beendet ist, was auch immer früher erfolgt. Die Auftragsbearbeiterin unterrichtet die Verantwortliche unverzüglich, wenn sie aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

19.2 Die Verantwortliche ist berechtigt, den betroffenen Leistungsabruf zu kündigen, soweit er die Bearbeitung von Personendaten gemäss diesen Klauseln betrifft, wenn

a) die Verantwortliche die Bearbeitung von Personendaten durch die Auftragsbearbeiterin gemäss dem ersten Absatz ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

b) die Auftragsbearbeiterin in erheblichem Umfang gegen diese Klauseln verstösst;

c) die Auftragsbearbeiterin einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die ihre Pflichten gemäss diesen Klauseln, dem DSG oder (wo anwendbar) der EU-DSGVO zum Gegenstand hat, nicht nachkommt.

19.3 Die Auftragsbearbeiterin ist berechtigt, den betroffenen Leistungsabruf mit unmittelbarer Wirkung zu kündigen, soweit sie die Bearbeitung von Personendaten gemäss diesen Klauseln betrifft, wenn die Verantwortliche auf der Erfüllung ihrer Anweisungen besteht, nachdem sie von der Auftragsbearbeiterin darüber in Kenntnis gesetzt wurde, dass ihre Anweisungen gegen geltende rechtliche Anforderungen gemäss Ziffer 7.1 b) verstossen. Die Verantwortliche hat bereits erbrachte Leistungen zu vergüten. Allfällige Vorauszahlungen für künftige Leistungen unter dem Leistungsabruf werden nicht zurückerstattet.

19.4 Nach Beendigung des betroffenen Leistungsabrufs löscht die Auftragsbearbeiterin nach Wahl der Verantwortlichen alle im Auftrag der Verantwortlichen bearbeiteten Personendaten und bescheinigt der Verantwortlichen, dass dies erfolgt ist, oder sie gibt alle Personendaten an die Verantwortliche zurück und löscht bestehende Kopien, sofern

[redacted]

nicht nach geltendem Recht eine Verpflichtung zur Speicherung der Personendaten besteht. Bis zur Löschung oder Rückgabe der Daten gemäss Anhang Migration und Löschung gewährleistet die Auftragsbearbeiterin weiterhin die Einhaltung dieser Klauseln.

III. KLAUSELN BETREFFEND DIE ÜBERMITTLUNG VON PERSONENDATEN INS AUSLAND

20. Übermittlung von Personendaten ins Ausland durch die Bezugsberechtigte

20.1 Werden im Rahmen der Cloud-Services von der Bezugsberechtigten Personendaten aus der Schweiz heraus direkt in Cloud-Services der Firma im Ausland übermittelt, und liegt für den betreffenden Staat kein Entscheid des Bundesrates vor, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet[3], so verpflichtet sich die Firma auf schriftliche Aufforderung der Vergabestelle oder der Bezugsberechtigten zur Umsetzung bzw. Dokumentierung einer der folgenden Garantien Hand zu bieten:

a) Spezifische Datenschutzklauseln in einem Vertrag zwischen der Bezugsberechtigten und der Firma, die dem EDÖB vorgängig mitgeteilt werden (siehe Art. 16 Abs. 2 lit. b. nDSG);

b) Umsetzung spezifischer Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat (siehe Art. 16 Abs. 2 lit. c. nDSG);

c) Unterzeichnung von Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat (siehe Art. 16 Abs. 2 lit. d. nDSG); oder

d) Vorlage verbindlicher unternehmensinterner Datenschutzvorschriften bei Firma, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

20.2 Zudem gelten die Ausnahmen gemäss Art. 17 nDSG.

20.3 Werden im Falle von lit. c) die Standarddatenschutzklauseln der EU-Kommission vom 4. Juni 2021 verwendet[4], verpflichtet sich die Firma zur Umsetzung der für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[5].

21. Übermittlung von Personendaten ins Ausland im Rahmen der Leistungserbringung

21.1 Die Parteien halten fest, dass unter der Auftragsbearbeitung im Rahmen von Cloud-Services Folgendes gilt:

---

3 Resp. bis zum Inkrafttreten des nDSG: befindet sich der betreffende Staat nicht auf der Liste des EDÖBs derjenigen Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet.

4 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

5 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB – Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge, 27. August 2021; https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Paper%20SCC%20def.%20D%2024082021.pdf.download.pdf/Paper%20SCC%20def.%20D%2024082021.pdf

Regionale Bindung:

(1) Der Ort der Datenhaltung kann nach Regionen festgelegt werden.

(2) Insbesondere kann festgelegt werden, dass die Daten in einem Land, in dem ein «Angemessener Schutz für natürliche Personen» gemäss der Staatenliste vom EDÖB gewährleistet ist, gehalten werden. (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/staatenliste.pdf.download.pdf/20181213_Staatenliste_d.pdf).

21.2 Die Firma sorgt dafür, dass die Datenhaltung gemäss Festlegung durch die Bezugsberechtigte oder die Vergabestelle gemäss Absatz (1) in Ziff. 21.1 umgesetzt wird. Sollte die Firma davon abweichen wollen oder müssen, wird sie die Vergabestelle vorgängig informieren. Die Firma sorgt dafür, dass diese Information mindestens 20 Arbeitstage vor Umsetzung der Anpassung bei der Vergabestelle eingeht. Ausnahmen sind möglich (i) aus absolut zwingenden Gründen, die jedoch so rasch wie möglich der Vergabestelle zur Kenntnis gebracht werden müssen, sobald der Hinderungsgrund für die Information an die Vergabestelle weggefallen ist; oder (ii) wenn die Verantwortliche dies wünscht.

21.3 Die Firma bestätigt, dass Bezugsberechtigte die Möglichkeit haben, Datenstandorte in mindestens einem Land zu wählen, das die Anforderungen gem. Ziff. 21.1 Absatz (2) erfüllt.

21.4 Liegt keine Instruktion der Bezugsberechtigten oder der Vergabestelle vor, gilt folgendes:

Personenbezogene Daten dürfen im Rahmen der Erbringung der Cloud-Services durch die Firma von der Schweiz ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 nDSG) [6]. Liegt kein Entscheid des Bundesrates vor, so dürfen personenbezogene Daten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

a) Datenschutzklauseln in einem Vertrag zwischen der Firma und ihrer Vertragspartnerin im Ausland, die dem EDÖB vorgängig mitgeteilt wurden;

b) spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat;

c) Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder

d) verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

Zudem gelten die Ausnahmen gemäss Art. 17 nDSG.

21.5 Werden im Falle von lit. c) die Standarddatenschutzklauseln der EU-Kommission vom 4. Juni 2021 verwendet[7], verpflichtet sich die Firma zur Umsetzung der für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[8].

---

6 Resp. bis zum Inkrafttreten des nDSG: Wenn sich der betreffende Staat auf der Liste des EDÖBs derjenigen Staaten befindet, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet.

7 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

8 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB – Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge, 27. August

[redacted]

21.6 Werden Personendaten im Rahmen der Erbringung der Cloud-Services durch die Firma im Ausland zwischen Staaten übermittelt, hält sich die Firma jederzeit an das einschlägige Recht des Exportstaates, dem die Firma unterliegt, insbesondere – falls es sich beim Exportstaat um einen EU-/EWR- Mitgliedsstaat handelt – an die Bestimmungen des Kapitel 5 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO).

Beilage

- Alibaba Cloud Subsidiaries/Affiliates Sub-processors

* * *

2021; https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Paper%20SCC%20def.%20D%2024082021.pdf.download.pdf/Paper%20SCC%20def.%20D%2024082021.pdf

[redacted]

4

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – IT- und Datensicherheit

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)

[redacted]

Präambel

Datensicherheit ist aus Sicht der Bundesverwaltung zentral. Dies bedingt IT-Sicherheit. Der vorliegende Vertragsanhang ist Bezugspunkt für die zwischen der Firma und der Bezugsberechtigten abgestimmten Massnahmen zur IT- und Datensicherheit.

Für die Zwecke dieses Anhangs bezieht sich der Begriff "Daten" nur auf Daten, die eine Bezugsberechtigte (i) auf den Cloud-Diensten der Firma erfasst, (ii) mit den Cloud-Diensten der Firma verbindet, oder (iii) unter dem bei der Firma eröffneten Benutzerkonto an die Cloud-Dienste der Firma übermittelt oder in diese hochlädt.

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Rolle der Bezugsberechtigten

1.1 Die Bezugsberechtigte wählt nach dem Konzept der "Shared Responsibility" einen Dienst aus, der einen im Verhältnis zu den bearbeiteten Daten angemessenen Schutz gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen sowie Massnahmen zur Sicherstellung der Portabilität der zu schützenden Daten bewirkt.

1.2 Die Bezugsberechtigte muss namentlich beurteilen, ob die dokumentierten Standards ausreichend sind zur Erstellung eines Sicherheitsniveaus, das unter den folgenden Kriterien angemessen ist:

a) Inhalt der zu schützenden Daten;

b) Bedeutung der zu schützenden Daten für die Eidgenossenschaft, für deren Bevölkerung oder für konkrete Einzelpersonen;

c) Risiken der Informationssicherheit;

d) Gewährleistung des sicheren Einsatzes von IT-Infrastrukturen und weiterer Informatikmittel.

1.3 Die Bezugsberechtigte muss gegebenenfalls dafür sorgen, dass ein den Mindestschutzstandard gem. Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.**2 übersteigendes Schutzniveau eingerichtet wird, wenn der Inhalt der zu schützenden Daten, deren Bedeutung (namentlich, falls sie zu kritischen Infrastrukturen gehören) oder die Risiken der Informationssicherheit einen höheren Schutzstandard indizieren.

1.4 Für die Firma ergeben sich keine Verpflichtungen direkt aus dieser Ziffer 1.

2. Sicherheit auf IT-Infrastrukturen der Firma

2.1 Die Firma verpflichtet sich, für die Leistungserbringung unter dem Rahmenvertrag nur IT-Infrastrukturen einzusetzen, die mit Blick auf die der Bezugsberechtigten angebotenen Leistung das Schutzniveau gemäss Ziff. 2.2 (Mindestschutz) erreichen.

2.2 Der Mindestschutz entspricht mindestens den Vorgaben, die sich aus den Standards bzw. Zertifizierungen ergeben, welche die Firma mit ihrer Antwort in der Ausschreibung WTO 20007 zu EK04 («Zertifizierungen») als massgeblich bezeichnet hat. Dies gilt, soweit der aktuelle Stand der Technik sich nicht darüber hinaus entwickelt hat (es gilt der strengere Standard).

2.3 Sofern die Firma einen höheren Standard anbietet, geht sie nicht ohne Not hinter den bei Unterzeichnung des Rahmenvertrags bestehenden Sicherheitsstandard zurück.

2.4 Die Vorgaben gemäss Ziff. 2.2 bilden in jedem Fall die untere Mindestschutzgrenze. Diese ist von der Firma mit allen Leistungsangeboten, die sie für eine Bezugsberechtigte abrufbar macht, mindestens einzuhalten.

2.5 Die Firma verpflichtet sich zur kontinuierlichen Weiterentwicklung der von ihr eingesetzten Schutzmassnahmen und setzt diese um.

3. Schutzziele

Die Sicherheitsmassnahmen müssen geeignet sein, um davor zu schützen, dass nicht, ob unbeabsichtigt oder unrechtmässig, eine Vernichtung, ein Verlust, eine Veränderung oder eine unbefugte Offenlegung von beziehungsweise ein unbefugter Zugang zu den zu schützenden Daten resultiert (im Folgenden „Verletzung des Schutzes von Daten").

4. Dokumentation «IT- und Datensicherheit»

Die Firma stellt der Vergabestelle auf ihren Webseiten und Portalen sowie auf Anfrage konsolidierte Informationen bereit, welche über die Sicherheitssituation des Leistungsangebots informiert.

5. Mindestanforderungen an die Dokumente betr. Zertifizierungen und weitere Pflichten in Bezug auf Zertifizierungen

5.1 Die Firma muss ausdrücklich angeben, inwiefern die Leistungen, die sie unter dem Rahmenvertrag an Bezugsberechtigte zum Abruf anbietet, die folgenden Standards einhalten und inwiefern für diese (sofern überhaupt möglich) eine Zertifizierung eingeholt wurde:

a) ISO 27001 (ISMS)

b) ISO 27002

c) ISO 27017 (Cloud Security)

d) ISO 27018 (Cloud Privacy)

5.2 Die Firma informiert die Vergabestelle mindestens 12 Monate im Voraus, wenn sie sich entscheidet, ein Zertifikat gemäss Ziff. 5.1 nicht weiter aufrechtzuerhalten.

5.3 Sollte die Firma eine der Zertifizierungen gemäss Ziff. 5.1 ungewollt verlieren, informiert sie umgehend die Vergabestelle darüber.

5.4 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die gemäss Ziff 5.1 eingeholten Zertifikate zu.

6. Mindestanforderungen an die Dokumente betr. Audits und weitere Pflichten in Bezug auf Audits

6.1 Die Firma muss ausdrücklich angeben, inwiefern für die Leistungen, die sie unter dem Rahmenvertrag an Bezugsberechtigte zum Abruf anbietet, (sofern überhaupt möglich) einer der folgenden Audit-Berichte eingeholt wurde:

a) SOC 1

b) SOC 2

6.2 Die Firma informiert, ob sie SOC-Berichte gemäss Ziff. 6.1 als Type I (Type a) oder als Type II (oder Type b) eingerichtet hat.

6.3 Sollte der Firma eine Attestierung einer Audit-Unternehmung gemäss Ziff. 6.1 aberkannt worden sein, informiert sie umgehend die Vergabestelle darüber.

6.4 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die gemäss Ziff. 6.1 eingeholten Audit-Berichte zu.

6.5 Wenn eine auditierende Stelle ein Problem anspricht, wird die Firma das Problem adressieren und Massnahmen treffen, um das Problem zu beheben. Die Firma wird die Vergabestelle über solche Probleme, welche sich auf die durch Bezugsberechtigten bezogenen Leistungen auswirken können, über die Umsetzung der Mitigierungsmassnahmen sowie die über die Re-Evaluierung der Attestierungssituation bzw. des Problems durch die auditierende Stelle informieren.

7. Verschlüsselte Datenhaltung

7.1 Die Firma muss die technischen Voraussetzungen dafür schaffen, dass die Daten der Bezugsberechtigten auf den Systemen der Firma stets in verschlüsselter Form gespeichert werden können. Darüber hinaus sind die physischen Systeme der Firma (Racks etc.) standardmässig verschlüsselt.

7.2 Die Firma lässt zu, dass die Bezugsberechtigte ihre Daten verschlüsseln kann. Sie lässt insbesondere Verschlüsselungsmethoden zu, bei denen ausschliesslich die Bezugsberechtigte den Masterkey besitzt bzw. diesen Masterkey kennt.

7.3 Die Firma identifiziert welche Leistungen der Firma welche Verschlüsselungsmöglichkeiten vorsehen, um einer Bezugsberechtigten, die Leistungen von Firma beziehen will, den Entscheid zu ermöglichen, ob sie die Datenhaltung innerhalb eines Tenants besonders verschlüsseln will und, wenn ja, welche Form der Verschlüsselung sie einsetzen will.

8. Verschlüsselte Datenübermittlungen

8.1 Die Firma muss die technischen Voraussetzungen dafür schaffen, dass elektronische Übermittlungen von Daten bei der Verwendung von Cloud Diensten nur über verschlüsselte Kanäle erfolgen. Dies betrifft namentlich:

a) Datenübermittlung innerhalb eines Tenants

b) Datenübermittlung innerhalb der Systeme der Firma (tenantübergreifend)

c) «händische» Systemaufrufe von aussen (Abfragen über Webschnittstelle)

d) Systemaufrufe über maschinelle Programmierschnittstellen (API) oder sonstige Abfragemethoden (REST Calls oder dergleichen)

Darüber hinaus ist jede elektronische Übermittlung von Daten über das öffentliche Internet aus der Cloud heraus oder in die Cloud hinein standardmässig mit gängigen Verschlüsselungsprotokollen (wie TLS und https) verschlüsselt.

8.2 Alle Verschlüsselungen bei Übermittlung und Speicherung der Daten erfolgen jeweils mindestens nach dem Standard gem. Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.**.

9. Beizug von eigenem Personal (durch Firma oder Subunternehmen)

9.1 Die Firma gewährt ihrem Personal nur angemessenen Zugang zu ihren Systemen, die sich auf die für die Bezugsberechtigten erbrachten Dienstleistungen auswirken können.

9.2 Die Firma legt den Genehmigungsprozess und die entsprechenden Verfahren fest, damit die Bezugsberechtigten dem Personal der Firma Zugang zu Daten der Bezugsberechtigten gewähren können (bspw. im Falle einer von der Bezugsberechtigten beantragten Fehlerbehebung).

9.3 Sofern die Bezugsberechtigte keinen Zugang gewährt, gewährt die Firma ihrem Personal nur insoweit Zugang zu diesen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Einzelabrufs oder des Rahmenvertrags unbedingt erforderlich ist.

9.4 Sofern Personal der Firma Klartextzugriff auf Daten der Bezugsberechtigten erhält, trifft die Firma Massnahmen, die es der Bezugsberechtigten erlauben, das Ereignis des Klartextzugriffs zu protokollieren (Zugriffsprotokolle).

9.5 Die Firma schafft die technischen Voraussetzungen dafür, dass die Bezugsberechtigte solche Zugriffsprotokolle gemäss den Bedürfnissen der Bezugsberechtigten aufbewahren kann.

9.6 Die Firma gewährleistet, dass sich die zur Bearbeitung der erhaltenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

10.1 Wo eine Pflicht unter diesem Vertragsanhang die Firma trifft oder eine Rechtsfolge sich auf die Firma bezieht, sind Hilfspersonen und Subunternehmen der Firma jeweils mit verpflichtet.

10.2 Die Firma steht dafür ein, dass ihre Hilfspersonen und Subunternehmen die Pflichten der Firma unter diesem Vertragsanhang einhalten.

* * *

5

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Migration und Löschung der Daten

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)

[redacted]

Präambel

Dieser Vertragsanhang dient der Umsetzung der Anforderungen aus der Ausschreibung (EK05: «Der Anbieter ermöglicht dem Dateneigner den Export (aus der Cloud heraus) und die unwiderrufliche Löschung seiner Daten.»)

Auf dieser Grundlage vereinbaren die Parteien Folgendes:

Im Einzelnen:

I. Datenmigration

1. Datenmigration in die IT-Infrastrukturen der Firma

1.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch, gemäss separater Vereinbarung und gegen separate Vergütung, bei der Migration von Daten in die IT-Infrastrukturen der Firma.

1.2 Die Firma gibt Auskunft über:

a) bestehende Import- und Exportroutinen, welche für die Migration der Daten nützlich sind;

b) bestehende APIs, welche für die Migration der Daten benutzt werden können;

c) weitere notwendige oder nützliche Massnahmen.

2. Anspruch auf Herausgabe

2.1 Die Bezugsberechtigte hat einen Anspruch auf Herausgabe ihrer Daten in einem strukturierten, gängigen, maschinenlesbaren und elektronischen Format.

2.2 Der Anspruch gemäss Ziff. 2.1 bezieht sich auf:

a) Daten, welche die Bezugsberechtigte im Rahmen der Cloud-Services auf IT-Infrastrukturen der Firma speichert, bekannt gibt oder bearbeitet.

b) Daten, die von Daten gemäss Ziff. 2.2 a) abgeleitet sind (z.B. gespeicherte Nutzungsprofile; Metadaten; Randdaten; Parametrisierungsdaten; Nutzungsdaten etc.).

2.3 Die Firma stellt der Bezugsberechtigten die technischen Mittel oder Prozesse zur Verfügung, um die Herausgabe entweder an die Bezugsberechtigte oder an eine von der Bezugsberechtigten bezeichnete Dritte auszuführen. Ziff. 2.4 gilt ergänzend.

2.4 Die Firma erfüllt Ziff. 2.3, wenn sie die herausverlangten Daten zum Download im Cloud Account bereitstellt.

2.5 Die Datenherausgabe kann bis zum Ablauf der maximalen Datenhaltedauer (Ziff. 8.1) und wiederholt ausgeführt werden.

2.6 Herausgabe im Sinne von Ziff. 2.1 bedeutet Folgendes:

a) Transformation des herauszugebenden Datenbestands in ein Datenformat, das den Anforderungen gemäss Ziff. 2.1 genügt.

b) Bereitstellung der Daten gemäss Ziff. 2.3 und Ziff. 2.4.

3. Unterstützungsleistungen von Firma betreffend Datenmigration aus den IT-Infrastrukturen der Firma heraus

3.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch, gemäss separater Vereinbarung und gegen separate Vergütung, bei der Migration von Daten aus den IT-Infrastrukturen der Firma heraus.

3.2 Die Firma wird Unterstützungsleistungen an die Bezugsberechtigte nicht unsachlich verweigern.

II. Datenhaltung während der Nutzung

4. Sicherung von Daten

4.1 Die Firma garantiert, dass Daten der Bezugsberechtigten mindestens entsprechend dem Stand der Technik gesichert werden können.

4.2 Die Firma stellt die technischen Mittel zur Verfügung um der Bezugsberechtigten die Sicherung ihrer Daten gemäss ihren Bedürfnissen und im Rahmen von der Firma angebotenen Optionen zu ermöglichen. Die Bezugsberechtigte ist selber besorgt dafür, ihr Datensicherungskonzept umzusetzen.

4.3 Unter Vorbehalt von Ziff. 4.4 gelten die Service Levels der Firma.

4.4 Zusätzlich gelten die folgenden Mindestanforderungen:

a) Möglichkeit regelmässiger Sicherungen in durch die Bezugsberechtige zu definierender Frequenz. Jede dieser Sicherungen kann mindestens 30 Tage lang von der Bezugsberechtigten aufbewahrt werden.

b) Zusätzlich können Monatssicherungen und Jahressicherungen erstellt werden. Diese werden für die von der Bezugsberechtigten eingestellten Dauern aufbewahrt.

5. Wiederherstellung

5.1 Die Firma garantiert, dass die Bezugsberechtigte auf Methoden zur Wiederherstellung ihrer Daten zurückgreifen kann, die mindestens dem Stand der Technik entsprechen.

5.2 Die Sicherung und Wiederherstellungs-Funktionalität ist von der Firma mindestens zwei Mal pro Jahr zu testen. Der Vergabestelle ist das Testresultat mitzuteilen.

5.3 Unter Vorbehalt von Ziff. 5.4 gelten die Service Levels der Firma.

5.4 Ein Recovery Time Objective kann von der Bezugsberechtigten realisiert werden, sofern die dafür notwendigen Einstellungen durch die Bezugsberechtigte vorgenommen wurde.

6. Allgemeine Regeln betreffend Datenhaltung

6.1 Jede Bezugsberechtigte kann den Standort der Datenhaltung im Rahmen des Leistungsangebots der Firma auf ein bestimmtes Land oder auf mehrere bestimmte Länder beschränken.

6.2 Der Datenhaltungsstandort für bezogene Leistungen wird durch die Bezugsberechtigte beim Bezug der Leistung erstmalig gewählt und kann während der Erbringung der Dienstleistung auf Wunsch erweitert werden. Sofern die Bezugsberechtigte den Standort der Datenhaltung nicht ändert, greift der ursprünglich gewählte Datenhaltungsort. Insbesondere wird die Firma nicht ohne Zustimmung oder Anweisung durch eine Bezugsberechtigte eine Änderung des Datenhaltungsorts oder Replizierung an einen anderen Datenhaltungsort vornehmen.

6.3 Die Firma informiert die Vergabestelle und auf Wunsch der Stelle gemäss Ziff. 6.5 auch diese in einer durch Text nachweisbaren Form über die Methoden, den Datenhaltungsstandort zweifelsfrei feststellen zu können.

6.4 Die Firma beantwortet Rückfragen über den Datenhaltungsstandort innert längstens 3 Arbeitstagen. Solche Rückfragen können sowohl die Bezugsberechtigte, die Vergabestelle als auch die Stelle gemäss Ziff. 6.5 stellen.

6.5 Die Bedarfsstelle und ein oder mehrere von ihr bezeichnete Stellen, die in der Bundesverwaltung als Intermediäre handeln, haben jederzeit das Recht, die Information gemäss Ziff. 6.3 und Ziff. 6.4 anzufragen und zu erhalten.

III. Datenhaltung nach Beendigung des Leistungsbezugs

7. Definition «Vertragsbeendigung»

7.1 Als Vertragsbeendigung im Sinne dieses Abschnitts III. gilt der Zeitpunkt, auf welchen der Leistungsbezug durch eine Bezugsberechtigte endet. Ergänzend gilt Folgendes:

a) Die Firma stellt sicher, dass in jedem Fall klar dokumentiert ist, welches Datum als Zeitpunkt der Vertragsbeendigung gilt.

b) Die Firma informiert die Vergabestelle und auf Wunsch der Stelle gemäss Ziff. 7.2 auch diese in einer durch Text nachweisbaren Form über die Methoden, diesen Zeitpunkt zweifelsfrei feststellen zu können.

c) Die Firma beantwortet Rückfragen über den Zeitpunkt der Vertragsbeendigung innert längstens 3 Arbeitstagen. Solche Rückfragen können sowohl die Vergabestelle als auch die Stelle gemäss Ziff. 7.2 stellen.

7.2 Die Bedarfsstelle und ein oder mehrere von ihr bezeichnete Stellen, die in der Bundesverwaltung als Intermediäre handeln, haben jederzeit das Recht, die Information gemäss Ziff. 7.1 b) und Ziff. 7.1 c) anzufragen und zu erhalten.

8. Maximale Datenhaltedauer

8.1 Die Firma darf den Datenbestand der Bezugsberechtigten während maximal **60 Kalendertagen** nach Vertragsbeendigung gemäss Ziff. 7.1 (**maximale Datenhaltedauer**) speichern.

8.2 Ziff. 8.1 gilt nicht in den folgenden Fällen:

a) falls die Bezugsberechtigte den Leistungsbezug nach Vertragskündigung reaktiviert (sofern die Firma dies überhaupt zulässt): Die maximale Datenhaltedauer beginnt in diesen Fällen ab dem Zeitpunkt der definitiven Vertragsbeendigung).

b) in Bezug auf Nutzungsdaten (gemäss Ziff. 2.2 b)a), nur soweit sie für Zwecke der Abrechnung massgeblich sind: Solche Daten dürfen 10 Jahre ab deren Erstellung aufbewahrt werden.

c) in Bezug auf Löschprotokolle: es gilt Ziff. 12.3.

d) falls die Bezugsberechtigte eine längere Datenhaltungsdauer einstellt.

e) soweit regulatorische Vorschriften oder zuständige Datenschutzbehörden oder Gerichte eine längere Datenhaltungsdauer verlangen oder anordnen.

8.3 Die Firma sorgt dafür, dass der Datenbestand der Bezugsberechtigten nach Ablauf des Löschverbots (Ziff. 9.2) und vor Ablauf der maximalen Datenhaltedauer (Ziff. 8.1) gelöscht wird (**Löschpflicht**). Die Anforderungen der Datenlöschung ergeben sich aus Abschnitt IV.

9. Koordinationsregeln im Umfeld der Vertragsbeendigung

9.1 Ab dem Zeitpunkt der Vertragsbeendigung gemäss Ziff. 7.1 gelten zeitlich gestaffelt das Löschverbot (gemäss Ziff. 9.2) und dann die Löschpflicht der Firma (gemäss Ziff. 8.3).

9.2 Während einer Dauer von 30 Kalendertagen ab Vertragsbeendigung gemäss Ziff. 7.1 (soweit keine länger Dauer gemäss Portal vorgesehen ist oder zwischen der Bezugsberechtigten und der Firma vereinbart wurde) hat die Bezugsberechtigte das Recht, ihren Anspruch auf Herausgabe gemäss Ziff. 2 dieses Vertragsanhangs auszuüben, jedoch kein Recht auf ständigen Zugang oder Nutzung. Während dieser Dauer ist es der Firma verboten, die Daten gemäss Ziff. 2.2 zu löschen (**Löschverbot**). Das Löschverbot steht unter dem Vorbehalt von Anordnungen der Bezugsberechtigten, von Dritten oder von zuständigen Datenschutzbehörden oder Gerichten, aufgrund welcher die Firma bzw. die Bezugsberechtigte zur früheren Löschung der gespeicherten Daten verpflichtet wurde; solche Anordnungen gehen dem Löschverbot in jedem Fall vor.

IV. Datenlöschung

10. Vorbemerkungen

10.1 Dieser Abschnitt gilt sowohl für Datenlöschungen während noch laufender Nutzung als auch für Datenlöschungen nach Beendigung der Nutzung.

10.2 Dieser Abschnitt präzisiert, wie die Firma Instruktionen betreffend Löschung von Daten mindestens umzusetzen hat.

10.3 Instruktionen betreffend Löschung von Daten können sich aus verschiedenen Quellen[1] ergeben:

a) Instruktionen im Einzelfall

b) Vertragsanhang Vertraulichkeit der Daten

c) Vertragsanhang Zugriff auf Daten durch Unberechtigte

---

[1] **Hinweis**: Hier nicht genannt sind Löschungen während der Nutzung (z.B. Bildschirmeingaben). Diese ergeben sich aus der Funktionalität der Cloud-Lösung der Firma einerseits und andererseits aus den Regeln betreffend Datensicherung (Ziff. 4 in diesem Vertragsanhang).

11. Unwiderrufliche Löschung

11.1 Die Verfahren der Firma zur Datenlöschung stellen die Einhaltung der vertraglichen Vereinbarungen sicher.

11.2 Anforderungen an das Löschverfahren:

a) Die Firma verwendet Verfahren der «Best Practice» und eine Wipinglösung, die den Anforderungen des Standards NIST SP 800-88 entspricht.

b) Die Firma stellt überdies sicher, dass für das Löschverfahren Abläufe gemäss den Standards ISO 27001 und ISO 27018 bestehen.

c) Die Datenlöschung läuft in Stufen ab. Zunächst wird sichergestellt, dass der betreffende Datensatz auf dem System nicht mehr zur Verfügung steht, so dass auch ein Datenbankadministrator ihn nicht mehr aufrufen könnte[2]. Ein daran anknüpfendes Folgeverfahren beseitigt die Daten dauerhaft (inklusive durch mehrfaches Überschreiben)[3]. Daran können gemäss den Verfahren der Firma zu einem späteren Zeitpunkt physikalische Verfahren zur Vernichtung der Speichermedien anknüpfen (dazu Ziff. 11.2 d) und Ziff. 11.2 e)).

d) In Bezug auf Speichermedien (Festplatten, etc.) verwendet die Firma einen Vernichtungsprozess, der für unwiederbringliche Zerstörung des Datenträgers und der darauf gespeicherten Daten sorgt. Dies bedingt, dass die Wiederherstellung (Lesbarmachen) von Daten unmöglich ist. Die physische Zerstörung von Speichermedien kann z.B. gemäss den Standards NIST SP 800-88 oder äquivalenten Standards erfolgen. Der Klarheit halber wird festgehalten, dass die physische Vernichtung von Speichermedien nur dann erfolgt, wenn die Firma beschliesst, solche Speichermedien nicht mehr für ihre Kunden zu verwenden (d.h. wenn sich die Speichermedien als fehlerhaft erwiesen haben oder wenn sie gemäss den Richtlinien der Firma ihr *End of Life* erreicht haben). Auf der Grundlage einer separaten Vereinbarung und gegen eine separate Vergütung kann die Bezugsberechtigte ausnahmsweise die physische Vernichtung von Speichermedien verlangen (z.B. wenn darauf klassifizierte Informationen der Bezugsberechtigten gespeichert waren).

e) Betreffend die physische Vernichtung von Speichermedien gemäss Ziff. 11.2 d) spezifiziert die Firma, inwiefern Verfahren nach NIST SP 800-88 der Stufe DESTROY (z.B. Zerkleinern/Shreddern, Zersetzen, Pulverisieren oder Schmelzen) eingesetzt werden. Sofern die physische Vernichtung ausnahmsweise mit einer Bezugsberechtigten vereinbart wurde, hält die Firma die vereinbarten Verfahren ein.

f) Das Folgeverfahren gemäss Ziff. 11.2 c) verhindert eine Wiederherstellung mit forensischen Mitteln.

g) Papierdokumente (sofern solche überhaupt erstellt werden) werden im Rahmen von geregelten Prozessen vernichtet, wobei dafür ein prozessgesteuerter und im Voraus festgelegter Vernichtungszeitpunkt festgelegt ist.

h) Die Firma setzt für das Entsorgen von Hardware standardisierte Entsorgungsverfahren ein.

11.3 Die Löschung umfasst:

a) alles, was gemäss Anhang Vertraulichkeit der Daten als **Vertrauliches** gilt;

b) Daten in aktiven Umgebungen;

11.4 Die Firma überprüft die Wirksamkeit der Löschung und ihrer Löschmethoden (namentlich in Bezug auf Ziff. 11.2) regelmässig, mindestens einmal jährlich.

---

[2] «CLEAR» gemäss NIST SP 800-88, d.h. Löschung mit rein logischen Verfahren.

[3] «PURGE» gemäss NIST SP 800-88, d.h. Löschung mit physikalischen oder logischen Verfahren. Purge verlangt auch die Löschung von versteckten Speichern, wie Host Protected Areas (HPA) oder Device Configuration Overlays (DCO).

12. Dokumentation der Löschung

12.1 Die Firma zeichnet die Vornahme der Löschung bzw. Vernichtung (Löschprotokolle; als solche gelten auch System-Logs) auf.

12.2 Anforderungen an die Löschprotokolle:

a) Löschprotokolle müssen genügend aussagekräftig sein, um die Nachvollziehbarkeit der Löschung zu ermöglichen (z.B. in Bezug auf die Frage, ob die Anforderung gemäss Ziff. 11.3 eingehalten sind).

b) Ein durch die Firma beauftragter Drittprüfer muss die Löschprotokolle anschliessend überprüfen können. Zudem muss der Prüfer den Systemstatus des Verfahrens zur Löschung der Daten überprüfen können.

12.3 Die Firma bewahrt Löschprotokolle für die Zeit auf, welche gemäss lokal anwendbaren gesetzlichen Anforderungen verlangt wird.

13. Vernichtungspflichten von Unterlagen oder Datenträgern

13.1 Soweit die vorstehenden Bestimmungen die Löschung von Unterlagen oder Datenträgern noch nicht regeln, gilt folgendes:

13.2 Die Firma verpflichtet sich, allfällige Unterlagen oder Datenträger im Eigentum der Bezugsberechtigten zu vernichten oder vernichten zu lassen, nachdem die Bezugsberechtigte zur Vernichtung der Unterlagen / Datenträger aufgefordert hat.

13.3 Die Firma bestätigt die Vernichtung von Unterlagen / Datenträgern bzw. die Löschung von Daten unaufgefordert in einer durch Text nachweisbaren Form.

* * *

6

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

[redacted]

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)

[redacted]

7

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Technische Anforderungen

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)

[redacted]

Präambel

In Ergänzung zu den ansonsten geltenden oder vereinbarten technischen Anforderungen gilt Folgendes:

[redacted]

5. Technische Spezifikationen

Des Weiteren gelten die in der WTO-20007 beschriebenen Kriterien TS 01-05 («Katalog der Technischen Spezifikationen»).

[redacted]

[redacted]

8

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Vertraulichkeit der Daten

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)

[redacted]

Präambel

Der vorliegende Vertragsanhang beschreibt die Vertraulichkeitspflichten der Firma.

Schutzziel des vorliegenden Vertragsanhangs ist das Verhindern von unbefugten Klartextzugriffen und das Verhindern der Verwendung von Vertraulichem (wie in Ziff. 1.4, unten, definiert) zu Zwecken der Firma, ihrer Subunternehmen oder zu Zwecken von Dritten.

Im Verhältnis der Parteien gelten auch andere Bundesstellen als Dritte.

Vertraulich im Sinne von Ziff. 1.4 meint nicht dasselbe wie vertraulich im Sinne der geltenden ISchV oder Ersatzregelung.

Der Umgang mit vertraulichen Informationen der Firma ist im Vertragswerk der Firma geregelt, ergänzend gilt Ziff. 18 des Rahmenvertrags (Offenlegungspflicht).

Der Vertragsanhang Zugriff auf Daten durch Unberechtigte enthält ergänzende Regeln zum Erreichen des Bestimmungsrechts der Bundesverwaltung über ihren Datenbestand.

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Vertraulichkeit im Allgemeinen

1.1 Die Firma ist verpflichtet, die Vertraulichkeit von Vertraulichem (wie in Ziff. 1.4 definiert) gemäss dem Rahmenvertrag und dessen Anhängen zu gewährleisten. Die Firma darf somit Vertrauliches nicht anderweitig offenbaren, die Firma muss Vertrauliches gegen unbefugte Klartextzugriffe schützen und darf Vertrauliches nicht zu Zwecken von Firma, ihrer Subunternehmen oder zu Zwecken Dritter verwenden. Für die Zwecke dieses Anhangs beziehen sich die Begriffe "Daten" und "Informationen" nur auf Daten und Informationen, die eine Bezugsberechtigte (i) auf den Cloud-Diensten der Firma erfasst, (ii) mit den Cloud-Diensten der Firma verbindet, oder (iii) unter dem bei der Firma eröffneten Benutzerkonto an die Cloud-Dienste der Firma übermittelt oder in diese hochlädt.

1.2 Der Begriff **Information** im Sinne des vorliegenden Vertragsanhangs meint den Bedeutungsgehalt von Daten. Als Information werden in diesem Vertragsanhang Aufzeichnungen bezeichnet, die etwas oder jemanden beschreiben. Dies gilt unabhängig von ihrer Darstellungsform und ihrem Informationsträger.

1.3 Der Begriff der **Daten** im Sinne des vorliegenden Vertragsanhangs meint konkrete Speicherobjekte in einem bestimmten Speicherformat (PDF-Dateien; png-Dateien; SQL-Datenbanken-Speicherformate etc.). In Abgrenzung zu Information sind Daten gleichsam die «Behälter» für Informationen.

1.4 Daten und Information der Bezugsberechtigten, egal ob fassbar oder nicht, egal in welcher Speicherform (d.h. Kenntnisse, Daten, etc.) und egal auf welchem Datenträger (Dokumente wie Unterlagen, Speichermedien, etc.), gelten als **Vertrauliches.** Eine öffentlich zugängliche Information wird nicht nur deshalb in anderen Kontexten zu Vertraulichem, weil sie auch auf den Clouddiensten der Firma erfasst, übermittelt oder hochgeladen wurde.

1.5 Wenn Bezüge zur Bundesverwaltung, zu den bei ihr tätigen Personen oder über Dritte (Angaben zur Bevölkerung, zu Unternehmen, die mit der Bundesverwaltung im Austausch stehen) nicht entfernt wurden, gehört auch Folgendes zu Vertraulichem (andernfalls gehören die folgenden Kategorien nicht zu Vertraulichem):

a) Information, die von Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.** abgeleitet ist (z.B. Nutzungsprofile; Metadaten; Randdaten; Parametrisierungsdaten; Nutzungsdaten, etc.).

b) Information, die unter Beobachtung der Angaben gemäss Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.** bei der Firma entstanden ist.

2. Verschwiegenheitspflicht und Schutzpflichten

2.1 Die Firma verpflichtet sich, über Vertrauliches Stillschweigen zu bewahren.

2.2 Die Firma verpflichtet sich, technische und organisatorische Massnahmen zu implementieren, die geeignet sind, Klartextzugriffe auf Vertrauliches durch Unbefugte zu verhindern.

2.3 Die Firma wird Vertrauliches, das ihr im Rahmen ihrer Tätigkeit unter diesem Rahmenvertrag zukommt, sorgfältig aufbewahren und vor Klartextzugriffen Dritter schützen.

3. Datenherausgabeverbot (Einwilligungsvorbehalt)

3.1 Die Firma verpflichtet sich, Vertrauliches nur mit vorgängiger schriftlicher Zustimmung der Bezugsberechtigten an Dritte herauszugeben (Datenherausgabe). Als Datenherausgabe gilt auch das Gewähren von Klartextzugriff auf Vertrauliches in anderer Form als durch Herausgabe von Daten, Unterlagen oder dergleichen. Der Anhang Zugriff auf Daten durch Unberechtigte bleibt vorbehalten.

3.2 Die Firma sorgt dafür, dass dieser Einwilligungsvorbehalt auch von ihren Subunternehmen beachtet wird.

3.3 Eine Vertragshaftung für Verstösse gegen diese Ziff. 3 entfällt nur im Umfang, wie Firma im Rahmen ihrer Informations- und Schutzpflichten unter dem Vertragsanhang Zugriff auf Daten durch Unberechtigte (namentlich dessen Ziff. 4, 5 und 6) alles ihr Zumutbare unternommen hat, Vertrauliches vor einer Offenlegung an Dritte zu schützen.

4. Verwendungsverbot

4.1 Die Firma verpflichtet sich, Vertrauliches ausschliesslich zum Zwecke einer ordnungsgemässen Abwicklung und Erfüllung dieses Vertrags oder eines Vertrags mit einer Bezugsberechtigten zu verwenden.

4.2 Auch nach Ende des Vertrags wird die Firma Vertrauliches nicht für eigene Zwecke, zum eigenen Vorteil oder für Zwecke oder zum Vorteil Dritter verwenden.

5. Amtsgeheimnisse, Berufsgeheimnisse, Datengeheimnisse

5.1 Die Firma nimmt zur Kenntnis, dass die Vergabestelle sowie die Bezugsberechtigten bzw. deren Mitarbeitende dem Amtsgeheimnis (Art. 320 StGB), dem Berufsgeheimnis (Art. 321 StGB) und / oder dem Datengeheimnis (Art. 35 DSG / Art. 62 nDSG) unterstehen oder unterstehen könnten.

5.2 Die Firma muss davon ausgehen, dass die für die Bezugsberechtigten bearbeiteten Daten und Informationen mindestens einer der in Ziff. 5.1 genannten Geheimnispflichten unterstehen können.

5.3 Die Firma verpflichtet sich weiter zur Einhaltung aller Pflichten unter diesem Anhang.

5.4 Die Firma stellt sicher, dass sämtliche mit der Leistungserbringung befassten Hilfspersonen, Subunternehmer und deren Hilfspersonen, die Zugang zu Vertraulichem erhalten:

a) über die Ausgangslage gem. Ziff. 5.1 von Ziff. 5.2 informiert wurden

b) die Pflichten gem. Ziff. 5.2 und Ziff. 5.3 ebenso einhalten wie die Firma

c) eine entsprechende Geheimhaltungserklärung unterschrieben haben und einhalten.

6. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

6.1 Wo eine Pflicht unter diesem Anhang die Firma trifft oder eine Rechtsfolge sich auf die Firma bezieht, sind Hilfspersonen und Subunternehmen der Firma jeweils mit verpflichtet.

6.2 Die Firma steht dafür ein, dass ihre Hilfspersonen und Subunternehmen die Pflichten der Firma unter diesem Vertragsanhang einhalten.

7. Allgemeine Regeln

7.1 Dauer der Vertraulichkeitsvorschriften: Die Pflichten gemäss diesem Vertragsanhang gelten über die Beendigung des Vertragsverhältnisses hinaus.

7.2 Die Vertraulichkeitspflichten der Firma in diesem Vertragsanhang ergänzen die Vertraulichkeitspflichten der Firma gemäss ihren eigenen Vertragsunterlagen. Soweit Abweichungen bestehen, gehen die Regeln im vorliegenden Vertragsanhang vor.

* * *

[redacted]

9

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Zugriff auf Daten durch Unberechtigte

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

Dieser Vertragsanhang präzisiert die Pflichten der Firma zur Wahrung der Vertraulichkeit der vertraulichen Daten der Bezugsberechtigten gemäss dem Anhang Vertraulichkeit der Daten. Für den Umfang und die Definition von "Vertraulichem"/ "Vertrauliches" gilt entsprechend der Anhang Vertraulichkeit der Daten. Er dient der Umsetzung der Anforderungen aus der Ausschreibung (Mindestbedingungen gem. Ziff. 8.1 des Pflichtenhefts: «Der Anbieter ist verpflichtet, die Vertraulichkeit der Daten des Auftraggebers zu gewährleisten.» Mit Vertraulichkeit ist nicht die Vertraulichkeit gemäss IschV gemeint.

Entsprechend vereinbaren die Parteien was folgt:

1. Zweck des vorliegenden Vertragsanhangs

1.1 Die unter diesem Vertragsanhang definierten Massnahmen bezwecken, dass (i) Vertrauliches nicht gegenüber unbefugten Personen bekannt wird (keine Klartextzugriffe); (ii) dass Vertrauliches nicht von unbefugten Personen verwendet wird; (iii) dass Vertrauliches mittels technischer, organisatorischer und vertraglicher Massnahmen vor unbefugten Klartextzugriffen geschützt wird; (iv) dass Vertrauliches für die Bezugsberechtigte verfügbar ist und bleibt; (v) dass Vertrauliches nicht unberechtigt oder unbeabsichtigt verändert wird (Integrität) und (vi) dass die IT-Infrastrukturen, auf denen Vertrauliches bearbeitet werden, vor Missbrauch und Störung geschützt sind.

1.2 Die Bezugsberechtigte will damit erreichen, dass sie über den Umgang mit Vertraulichem bestimmen kann, namentlich, dass sie

a) bestimmen kann, wer wann und in welchem Ausmass auf Vertrauliches Zugriff erhält und/oder Vertrauliches verwenden darf bzw. verwendet (Nachvollziehbarkeit von Zugriff/Verwendung).

b) bestimmen kann, ob eine bestimmte Person oder Stelle Vertrauliches löschen muss (oder die Löschung davon bei einem Dritten durchsetzen muss).

c) informiert ist darüber, ob andere auf Vertrauliches Zugriff erhalten, Vertrauliches gelöscht bzw. Vertrauliches verwendet haben (Nachvollziehbarkeit).

2. Informations- und Dokumentationspflichten allgemeiner Art

2.1 Die Firma stellt der Bezugsberechtigten und der Bedarfsstelle auf Verlangen alle nötigen Informationen für den Schutz ihrer IT-Infrastruktur in geeigneter Form zu.

2.2 Die Firma unterstützt die Bezugsberechtigte in angemessenem Umfang darin Vorsorgeplanungen für allfällige schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben der Bezugsberechtigten gefährden können, zu erstellen.

2.3 Die Firma informiert die Bezugsberechtigte auf schriftliche Anfrage in abstrakter und anonymisierter Form darüber, wie oft und in Bezug auf welche Art von Anlassfällen eine Behörde oder eine Amtsstelle eines ausländischen Staats auf IT-Infrastrukturen der Firma oder ihrer Subunternehmer zugegriffen hat. Solche Information bezieht sich namentlich auf Berichtsperioden während der Laufzeit des Rahmenvertrags und während einem Jahr zuvor. Sofern die Firma solche Berichte öffentlich zugänglich macht, verweist sie auf solche Information im Format, das der Anhang Abrufverfahren regelt.

2.4 Die Firma informiert hiermit die Vergabestelle nach bestem Wissen und Gewissen über bestehende Datenherausgabepflichten gegenüber ausländischen Behörden, namentlich für die folgenden Rechtsordnungen:

a) USA
Die Firma adressiert Datenanfragen sowohl im zivil- als auch im strafrechtlichen Kontext, welche über die richtigen juristischen und/oder diplomatischen Kanäle und unter strikter Einhaltung der einschlägigen Ermächtigungs- und Blockierungsgesetze in den USA, im Vereinigten Königreich (wo es seinen Sitz hat) und gegebenenfalls in den/m Staat(en), in denen sich das/die betroffene(n) Datenzentrum(e) befindet/befinden, zugestellt werden. Dazu gehört auch die gebührende Berücksichtigung von Jurisdiktions- und anderen Fragen, einschliesslich der Frage, ob das Unternehmen den betreffenden Ermächtigungsgesetzen unterliegt, ob ein bilaterales Abkommen zwischen den USA und dem betreffenden Staat im Rahmen des Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") geschlossen wurde und soweit angemessen, die vollständige Nutzung der formalen rechtlichen Verfahren zur Anfechtung von Forderungen, die im Rahmen des CLOUD Act oder anderer Ermächtigungsgesetze gestellt werden.

b) China
Die Firma adressiert Datenanfragen sowohl im zivil- als auch im strafrechtlichen Kontext, welche über die richtigen juristischen und/oder diplomatischen Kanäle und unter strikter Einhaltung der einschlägigen Ermächtigungs- und Blockierungsgesetze in China und gegebenenfalls in den/m Staat(en), in denen sich das/die betroffene(n) Datenzentrum(e) befindet/befinden, zugestellt werden. Dazu gehört auch die gebührende Berücksichtigung des Chinesischen Datensicherheitsgesetzes und des Chinesischen Datenschutzgesetzes.

c) Deutschland
Die Firma adressiert Datenanfragen sowohl im zivil- als auch im strafrechtlichen Kontext, welche über die richtigen juristischen und/oder diplomatischen Kanäle und unter strikter Einhaltung der einschlägigen Ermächtigungs- und Blockierungsgesetze in Deutschland und gegebenenfalls in dem/n Staat(en), in dem/nen sich das/die betroffene(n) Datenzentrum(en) befindet/n, zugestellt werden. Dazu gehört auch die gebührende Berücksichtigung des Deutschen Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien und der Ermächtigungs- und Beschränkungsregelungen in bilateralen Abkommen zur Datenherausgabe zwischen Deutschland und einem anderen Staat

d) Vereinigtes Königreich
Die Firma adressiert Datenanfragen sowohl im zivil- als auch im strafrechtlichen Kontext, welche über die richtigen juristischen und/oder diplomatischen Kanäle und unter strikter Einhaltung der einschlägigen Ermächtigungs- und Blockierungsgesetze im Vereinigten Königreich und gegebenenfalls in dem/n Staat(en), in dem/nen sich das/die betroffene(n) Datenzentrum(en) befindet/n, zugestellt werden. Dazu gehört auch die gebührende Berücksichtigung des Datenschutzgesetzes 2018 und der Ermächtigungs- und Beschränkungsregelungen in bilateralen Abkommen zur Datenherausgabe zwischen dem Vereinigten Königreich und einem anderen Staat, einschliesslich mit Bezug auf den CLOUD Act.

3. Cybervorfälle

3.1 Die Firma stellt sicher, dass sie über die nötigen Kapazitäten zur technischen Analyse und zur Bewältigung von Cybervorfällen verfügt, die ihr selber, ihre Subunternehmer oder die Bezugsberechtigte(n) betreffen. Sie sorgt dafür, dass Verletzungen der Informationssicherheit in ihrem Zuständigkeitsbereich rasch erkannt, deren Ursachen abgeklärt und allfällige Auswirkungen minimiert werden.

3.2 Die Firma sorgt in ihrem Zuständigkeitsbereich dafür, dass allfällige Risiken für die Informationssicherheit laufend beurteilt werden und informiert die Bezugsberechtigte bei etwaigen Sicherheitsvorfällen mit nachteiliger Auswirkung auf die Bezugsberechtigte.

3.3 Die Firma bietet auf schriftliche Aufforderung der Bezugsberechtigten Hand zur Definition eines Prozesses betreffend Cybervorfällen mit Bezug zu Vertraulichem.

3.4 Die Firma meldet der Bezugsberechtigten und den gesetzlich vorgeschriebenen Stellen (welche durch die Bezugsberechtigte vorgängig schriftlich mitgeteilt wurden) unverzüglich entdeckte Schwachstellen und Sicherheitsvorfälle, die deren Informatikschutzobjekte betreffen.

4. Koordination in Bezug auf die erzwungene Datenherausgabe an Dritte im Zusammenhang mit in- oder ausländischen Verfahren

4.1 Die Firma verpflichtet sich, die Bezugsberechtigte unverzüglich über das Auftreten eines oder mehrerer der folgenden Ereignisse zu informieren, soweit Vertrauliches betroffen ist und soweit die Firma unter anwendbarem Recht über solche Ereignisse informieren darf (Meldepflichten):

a) die Firma oder eines ihrer Subunternehmen werden in ein Verfahren verwickelt, in dem eine zuständige in- oder ausländische Behörde die Firma oder das Subunternehmen zur Herausgabe von Vertraulichem auffordert (der Erhalt einer *subpoena* oder eines *warrants* ist der Verfahrenseröffnung gleichgestellt).

b) Eine zuständige Behörde verlangt die Sicherung von Vertraulichem (Erstellen eines Legal Hold oder einer ähnlichen Zustandsaufnahme über Vertrauliches).

c) die Firma oder eines ihrer Subunternehmen wird gerichtlich oder behördlich verbindlich zur Herausgabe von Vertraulichem verpflichtet.

d) die Änderung von anwendbarem Recht, der Erlass verbindlicher Präzedenzfälle oder eine bevorstehende Übernahme der Firma, führt dazu, dass die Gefahr neuer Pflichten betreffend Herausgabe von Vertraulichem entsteht (z.B. bevorstehende Übernahme der Firma durch ein ausländisches Unternehmen mit der Wirkung, dass ausländische Behörden Datenherausgabemöglichkeiten erhalten; Begründung der Anwendbarkeit ausländischer Erlasse, welche einem ausländischen Staat Zugriff auf Vertrauliches ermöglichen, wie z.B. US CLOUD Act oder ähnliche Regeln der US-amerikanischen oder anderer Rechtsordnungen).

e) In jedem der vorgenannten Fälle informiert die Firma auch über die Umstände (inkl. Rechtsgrundlage) solcher Zugriffe und darüber, inwiefern die Firma Massnahmen zur Abwehr solcher Zugriffsanfragen getroffen hat und inwiefern diese Massnahmen erfolgreich waren. Wenn die Firma solche Zugriffe nicht abwehren konnte oder eine vorgängige Information an die Bezugsberechtigte nicht möglich gewesen sein sollte, informiert die Firma die betroffene Bezugsberechtigte so bald wie möglich darüber, dass ein Zugriff erfolgt ist. Sofern die Firma vom ausländischen Staat zum Stillschweigen über solche Vorgänge verpflichtet wurde, informiert sie die Bezugsberechtigte und die Bedarfsstelle so rasch wie möglich darüber, nachdem die Verpflichtung zum Stillschweigen dahingefallen ist.

Soweit ein Dritter, ausgenommen zuständige Gerichte und zuständige in- oder ausländische Behörden, die Herausgabe Vertraulicher Informationen verlangt, wird die Firma dieses Verlangen zurückweisen.

4.2 Die Firma trifft alle angemessenen in ihrer Macht stehenden *Abwehrmassnahmen*, insbesondere ergreift sie auch angemessene Rechtsbehelfe, damit Verpflichtungen zur erzwungenen Datenherausgabe (Ziff. 4) oder vorbereitende Massnahmen oder Schritte von Behörden zur Begründung solcher Verpflichtungen zu Lasten der Firma oder ihrer Subunternehmen verhindert werden oder ohne Wirkung bleiben. Die Firma wird sich generell jederzeit dafür einsetzen, dass Bestands- oder Verkehrs- und Inhaltsdaten wenn überhaupt nur unter Wahrung von Schutzmassnahmen in die Hände einer ausländischen Behörde oder Amtsstelle gelangen.

4.3 Wenn eine ausländische Behörde oder Amtsstelle von der Firma die Herausgabe von Vertraulichem fordert, informiert die Firma die ausländische Amtsstelle oder Behörde darüber, dass die Schweizerische Eidgenossenschaft als Staatswesen an den Daten ein Interesse hat und an diesen Daten berechtigt ist. Sie informiert die ausländische Amtsstelle oder Behörde über die der Firma bekannten Kontaktpersonen bei der Bedarfsstelle.[1]

4.4 Wenn eine ausländische Behörde oder Amtsstelle von der Firma die Herausgabe von Vertraulichem fordert, verlangt die Firma, dass die Behörde oder die Amtsstelle die Voraussetzungen für die von ihr/ihnen beantragte erzwungene Datenherausgabe in dokumentierter Weise substantiiert. Solche Forderungen sollten nur über die richtigen juristischen und/oder diplomatischen Kanäle und an die richtige juristische Person, die im Besitz dieser Informationen ist, gerichtet werden. Die Firma erwartet die Einhaltung ihres Alibaba Cloud International Law Enforcement User Information Request Guides (abrufbar unter: https://www.alibabagroup.com/en/contact/law_alibaba_cloud), wo immer dieser anwendbar ist.

4.5 Die Firma speichert die dokumentierten Informationen betreffend Aufforderungen gemäss Ziff. 4.4 und sendet diese an die Bezugsberechtigte und die Bedarfsstelle weiter, sofern dies der Firma unter anwendbarem Recht gestattet ist.

5. Koordination in Bezug auf die Datenherausgabe im Rahmen eines Konkurs- oder Nachlassstundungsverfahrens

5.1 Die Firma verpflichtet sich, die Bedarfsstelle unverzüglich über das Auftreten eines oder mehrere der folgenden Ereignisse zu informieren (Meldepflichten):

a) der Firma droht Zahlungsunfähigkeit.

b) einem Subunternehmen der Firma droht Zahlungsunfähigkeit, die die Vertraulichkeit oder Verfügbarkeit von Vertraulichem beeinträchtigen könnte.

c) ein Dritter leitet gegen die Firma ein Konkurs- oder Nachlassverfahren ein, das im Laufe der 6 folgenden Kalendermonate zu einer Beeinträchtigung der Vertraulichkeit von Vertraulichem oder zu einer Beeinträchtigung der Verfügbarkeit der Leistung oder der in den IT-Infrastrukturen der Firma verwalteten Daten führen könnte.

d) es wird über die Firma oder eines ihrer Subunternehmen, welches Zugriff auf Vertrauliches hat, der Konkurs oder eine Nachlassstundung (oder ein gleichwertiges Verfahren im Ausland) eröffnet, welches nicht innert 6 Monaten abgewendet wird.

5.2 Die Firma unternimmt alle zumutbaren Anstrengungen, dass Vertrauliches vollständig unter der Bestimmungsgewalt der Bezugsberechtigten verbleibt und trifft alle zumutbaren Massnahmen, damit Vertrauliches nicht in die Konkursmasse fällt.

5.3 Die Firma wird alle zumutbaren Anstrengungen unternehmen, dass Vertrauliches aus dem ausländischen Verfahren gemäss Ziff. 5.1d) ausgesondert und an die Bezugsberechtigte herausgegeben wird, so dass Vertrauliches nicht ohne Zustimmung der Bezugsberechtigten in die Hände Dritter gelangt. Eine Verwertung von Vertraulichem in einem solchen Verfahren muss mittels besonderer Massnahmen ausgeschlossen sein. Die Konkurs- und Nachlassbehörden im In- und Ausland gelten nicht als Dritte, wenn sichergestellt ist, dass sie wirksamen Geheimhaltungspflichten, Verwendungs- und Weitergabeverboten unterstehen.

5.4 Die Firma hat bereits zum Voraus alle angemessenen Massnahmen zu ergreifen, damit Daten der Bezugsberechtigten von der Verwertung in einem solchen Verfahren ausgenommen werden.

---

[1] Es ist dann Aufgabe der Bedarfsstelle, sicherzustellen, dass die botschafterliche / konsularischen Kanäle aktiviert werden, damit ein Austausch auf Regierungsebene möglich wird und die Daten aus den gewöhnlichen Abläufen der normalen Straf- und Geheimdiensttätigkeiten ausgenommen werden]

6. Milderungsmassnahmen betreffend Datenherausgaben und Gefahren betreffend Beeinträchtigung der Verfügbarkeit

6.1 Die Firma ergreift alle in ihrer Macht stehenden *Milderungsmassnahmen* für den Fall, dass die Abwehrmassnahmen gemäss Ziff. 5.4 keine vollständige Wirkung entfalten. Milderungsmassnahmen haben das Ziel, dass Verpflichtungen zur Datenherausgabe im Umfang oder sonst wie in ihrer Wirkung reduziert werden.

6.2 In Bezug auf die erzwungene Datenherausgabe im Rahmen von inländischen oder ausländischen Verfahren geht es um die folgenden Milderungsmassnahmen:

a) Beantragung der Siegelung der Daten der Bezugsberechtigten entsprechend Art. 248 ff. StPO bzw. einer entsprechenden ausländischen Regelung;

b) Geltendmachung der Tatsache, dass die Daten, welche vom Herausgabebegehren betroffen sind, einer gesetzlichen Geheimnispflicht unterstehen könnten (beispielsweise Amts- oder Berufsgeheimnis), die einer Verwendung von Vertraulichem in einem ausländischen Verfahren entgegenstehen (zwecks Comity-Analyse durch die ausländischen Behörde);

c) Geltendmachung von Argumenten der ausländischen Rechtsordnung, damit eine Comity-Analyse durch die ausländische Behörde (oder eine entsprechende Regel in der ausländischen Rechtsordnung) zu Gunsten der Bezugsberechtigten ausfallen und einer Verwendung von Vertraulichem durch ausländische Stellen entgegenstehen.

6.3 Wenn eine ausländische Behörde oder Amtsstelle von der Firma die Herausgabe von Vertraulichem fordert, informiert die Firma die ausländische Amtsstelle oder Behörde darüber, dass die Schweizerische Eidgenossenschaft als Staatswesen an den Daten ein Interesse hat und an diesen Daten berechtigt ist. Sie informiert die ausländische Amtsstelle oder Behörde über die der Firma bekannten Kontaktpersonen bei der Bedarfsstelle.

* * *

10

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vertragswerke der Firma:

11

CLOUD SERVICES PURCHASE AGREEMENT

This Cloud Services Purchase Agreement (the "**Agreement**") is entered into by and between:

1. **The Swiss Confederation**, acting through the Federal Office for Buildings and Logistics (*Bundesamt für Bauten und Logistik* – BBL) with its address at Fellerstrasse 21, CH-3003 Bern, Switzerland ("**Customer**").

2. **Alibaba.com (Europe) Limited,** a company incorporated under the laws of England and having its registered address at 8th floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP United Kingdom, registration number 6721521 ("**Alibaba Cloud**"); and

Each of Alibaba Cloud and Customer are each referred to herein individually as a "**Party**" and collectively as the "**Parties**".

In consideration of the mutual covenants set forth herein, the Parties hereby agree as follows:

1. PURCHASE CREDIT AND PRODUCT PURCHASES

1.1 Purchase Credit and Product Purchases. Subject to Alibaba Cloud's review of Customer's fulfillment of the purchase credit application terms and conditions (the "**Credit Application**") under the terms set forth in this Agreement, Alibaba Cloud will provide Customer a purchase credit limit (the "**Purchase Credit**") for making purchases of Alibaba Cloud's products and services on the Alibaba Cloud International Website (the "**Alibaba Cloud Products**"). Upon Alibaba Cloud's approval of Customer's Credit Application, the Customer's Purchase Credit will be displayed on Customer's membership account with the Alibaba Cloud International Website (URL: https://www.alibabacloud.com) and Customers may proceed to place purchase orders of Alibaba Cloud Products via the Alibaba Cloud International Website.

1.2 Credit Application and Approval.

(a) Customer shall, upon the instruction of Alibaba Cloud, file a written application to Alibaba Cloud for approval of a Purchase Credit limit. Alibaba Cloud shall have the right to request Customer to provide any information and documents as reasonably required by Alibaba Cloud to assess its financial status and capability for Alibaba Cloud to determine the appropriate Purchase Credit limit suitable for Customer.

(b) Alibaba Cloud shall have the right and sole discretion to decide on the amount of Purchase Credit limit to be provided to Customer. Alibaba Cloud's determination of the Purchase Credit limit to be approved and provided to Customer shall be final and conclusive. The amount of Purchase Credit limit granted to Customer will be notified to Customer in writing or will be displayed in the Customer account with the Alibaba Cloud International Website.

1.3 Use of Credit

(a) The Purchase Credit limit granted to Customer may be used to purchase any and all Alibaba Cloud Products by placing a purchase order online on the Alibaba Cloud International Website or offline using the form purchase order set forth in Schedule 1 (a "**Purchase Order**"), subject to the terms of use and pricing conditions as published on the Alibaba Cloud International Website.

(b) Used Purchase Credit will not be restored until Customer has settled payment for the used Purchase Credit in accordance with the payment settlement terms of this Agreement.

(c) If the payment arrangement for the Alibaba Cloud Product purchased is on a pay-per-use basis and Customer's Purchase Credit balance is insufficient for settling payment, Alibaba Cloud shall have the right, but not the obligation, to suspend Customer's subscription or use of the Alibaba Cloud Product until Customer's Purchase Credit balance is restored.

1.4 Restoration and Settlement of Credit

(a) Used Purchase Credit will be restored upon Customer's payment in accordance with the settlement terms of the Agreement.

(b) Alibaba Cloud shall have the right to adjust the amount Purchase Credit limit provided to Customer based on Customer's transaction history or financial status.

(c) Alibaba Cloud shall have the right, but not the obligation, to carry out any of the following in the event that Customer fails to make timely payment in accordance with the settlement terms in this Agreement:

(i) Reduce Customer's Purchase Credit limit;

(ii) Cancel Customer's Purchase Credit limit; or

(iii) Suspend or terminate Customer's subscription or use of the Alibaba Cloud Products purchased.

1.5 Term of Purchase Credit. Any Purchase Credit limit granted to Customer may be used until the expiry or termination of this Agreement for any reason whatsoever. Notwithstanding any of the foregoing, Customer's Purchase Credit will expire/cease to be available for use upon the occurrence of any of the following:

(i) Customer applies for cancellation of its Purchase Credit limit and Alibaba Cloud approves the application;

(ii) Customer has materially breached the terms of this Agreement;

(iii) Alibaba Cloud has reasons to believe that Customer is or may be unable to fulfill its payment obligations under this Agreement; or

(iv) Alibaba Cloud has reasons to believe that Customer has engaged in any unlawful activities.

1.6 Cancellation by Alibaba Cloud for Convenience. Unless otherwise provided in this Agreement, Alibaba Cloud has the right to cancel Customer's Purchase Credit limit at any time by providing a 30-day prior written notice to Customer.

2. SCOPE OF AGREEMENT

2.1 Scope of Agreement. This agreement including the Schedule(s) thereto ("**Agreement**"), Purchase Orders, Product Terms (as defined below), and the relevant SLA (as defined below), constitute the entire agreement between the Parties in relation to the sale and purchase of the Alibaba Cloud Products by Customer.

2.2 Inconsistency. In the event of any inconsistency between the terms of this Agreement, the Product Terms, the Purchase Order, and the SLA, the order of precedence shall be as follows (from top down):

[redacted]

(a) the body and Schedule(s) of this Agreement;

(b) Product Terms (as defined below);

(c) SLA; and

(d) Purchase Orders.

2.3 Product Terms. The use of Alibaba Cloud Products by Customer is at all times subject to any and all applicable product terms, terms of use, privacy policy, product SLA, payment and tax terms, membership agreement, rules and policies relating to the relevant Alibaba Cloud Products (together, the "**Product Terms**") as provided on the Alibaba Cloud International Website.

2.4 SLA. The purchase and use of certain Alibaba Cloud Products may come with service level guarantees by way of service level agreements (the "**SLA**"). Notwithstanding any of the foregoing, Customer acknowledges and agrees that not all Alibaba Cloud Products provide an SLA and only the latest version of the relevant SLAs as published on the Alibaba Cloud International Website during the time of Customer's use of the Alibaba Cloud Products shall be applicable to its purchase and use of the relevant Alibaba Cloud Products.

3. PRICES

3.1 Price. The price of the Alibaba Cloud Products (the "**Price**") shall be as stated on the Alibaba Cloud International Website from time to time.

3.2 Tax.

(a) Unless otherwise agreed, all amounts required to be paid hereunder do not include any taxes, duties or other assessments levied or based upon such amounts. If Customer is or may be required under any law or regulation of any governmental entity or authority, domestic or foreign, to withhold or deduct any withholding tax from an amount due to Alibaba Cloud pursuant to this Agreement, the amount payable to Alibaba Cloud shall be increased to the extent necessary to ensure that after making such deduction or withholding, Alibaba Cloud receives and retains a net sum equal to the sum it would have received but for such deduction or withholding being required. Customer shall promptly deliver to Alibaba Cloud all receipts and/or certificates or other proof evidencing the amounts (if any) paid in respect of any such deduction or withholding.

(b) Each Party shall be responsible for the direct tax liability imposed on its own net income. Customer shall be responsible for the payment of all other taxes including the local levies imposed by any relevant government authority in connection with the sale, promotion, and marketing of the Alibaba Cloud Products and provision of the Services under this Agreement.

4. PAYMENT

4.1 Payment. If the Customer is offered Purchase Credit by Alibaba Cloud, on or before the 10th day of each calendar month, the relevant Alibaba Cloud entity shall issue an invoice to Customer, setting out the amount due and payable for the previous month in connection with the amount of Purchase Credit used by Customer. Customer shall pay the invoiced amount in accordance with the payment schedule set forth on the invoice.

Otherwise, payments from the Customer to Alibaba Cloud should adhere to the provisions stipulated in the Payment and Tax Terms on Alibaba Cloud International Website.

[redacted]

4.2 Currency. Unless otherwise agreed, all payments to be made by Customer hereunder shall be denominated and made in US Dollars.

4.3 Bank Charges. Each Party shall be responsible for its own bank charges.

5. CONFIDENTIALITY

5.1 Definition. "**Confidential Information**" means business or technical information disclosed by either Party to the other Party that: (i) if disclosed in writing, is marked "confidential" or "proprietary" at the time of such disclosure; (ii) under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary; (iii) without limiting the foregoing, shall include the terms and conditions of this Agreement (including the Schedule) as the Confidential Information of both Parties.

5.2 Confidentiality Undertaking. Each Party will not use the other Party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its officers, directors, employees and agents that need to know such Confidential Information for the performance of this Agreement. The foregoing obligations will not restrict either Party from disclosing the other Party's Confidential Information, if pursuant to the order or request of a court, administrative agency, stock exchange, or other governmental body, provided that the Party required to make such a disclosure to the extent permitted by law gives reasonable written notice to the other Party to enable it to contest such order or request.

6. REPRESENTATIONS AND WARRANTIES OF THE PARTIES

6.1 Representation. Each Party represents and warrants to the other Party that:

(a) it has the authority and capacity to enter into this Agreement and it is not subject to any restrictive covenant or other legal obligation which prohibits it from performing its obligations hereunder; and

(b) it shall comply with all applicable laws and regulations and maintain any permits, licenses and approvals required to perform its obligations hereunder.

7. ANTI-BRIBERY

7.1 Each Party shall:

(a) comply with all applicable laws, regulations, codes, and sanctions relating to anti-bribery and anti-corruption;

(b) have and shall maintain in place throughout the term of this Agreement adequate anti-bribery policies and procedures and will enforce them where appropriate; and

(c) promptly report to the other party any request or demand for any undue financial or other advantage of any kind received in connection with the performance of this Agreement;

7.2 Material Breach. Breach of this Section 7 shall be deemed a material breach.

8. INDEMNITY

[redacted]

Each Party covenants and undertakes to indemnify, defend and hold harmless the other Party from and against any losses, claims, demands, actions, damages, penalties and costs or expenses ("**Loss**") resulting from any breach by the indemnifying Party of any of its representations, warranties and undertakings under the Agreement, provided that in no event shall an indemnifying Party, its successor or permitted assigns be liable to the Party being indemnified for any consequential, exemplary, punitive, reliance or special damages or loss of profits in connection with any Loss.

9. LIMITATION OF LIABILITY

9.1 Disclaimer. Except as expressly provided in this Agreement and to the maximum extent permitted by law, Alibaba Cloud makes no warranty, express or implied, with respect to the Alibaba Cloud Products in relation to it their merchantability and fitness for any particular purpose.

9.2 Exclusive Remedies. Notwithstanding any other terms of this Agreement to the contrary, Customer acknowledges and agrees that the remedies provided in the terms and conditions set forth in the Product Terms, including but not limited to the relevant SLA for the Alibaba Cloud Products, shall be the sole and exclusive remedies for Customer under this Agreement.

9.3 Limitation of Liability. Notwithstanding any other provisions of this Agreement, to the maximum extent permitted by law, and save as expressly stated in this Agreement, in no event shall either Party or its officers, directors, employees, or agents be liable to the other Party under any contract, tort (including negligence), strict liability or any other legal or equitable theory for any indirect, special, incidental, consequential, or exemplary damages, or loss of profits or data, even if such Party has been advised of the likelihood of such damages occurring. The total liability of Alibaba Cloud arising out of or relating to this Agreement, whether in contract, tort (including negligence) or otherwise, shall in no circumstances exceed the total aggregated sum of payment for Alibaba Cloud Products made by Customer and received by Alibaba Cloud under this Agreement as at the date the cause of action for such claim has arisen.

10. TERM AND TERMINATION

10.1 Term. This Agreement shall be effective from the date both Parties have executed this Agreement and shall remain valid until terminated by either Party pursuant to Clause 10.2 or 10.3 of this Agreement (the "**Term**").

10.2 Termination for Convenience. Either Party may terminate this Agreement without cause at any time by giving the other Party prior written notice of not less than one (1) month.

10.3 Termination for Cause. Either Party may terminate this Agreement with immediate effect on written notice to the other Party if:

(a) the other Party commits a material breach of this Agreement and fails to remedy the breach (if remediable) within thirty (30) days of receiving written notice to that effect specifying the breach and requiring it to be remedied;

(b) the other Party ceases to conduct its business operations;

(c) the other Party is unable to pay its debts due and payable; or

(d) the other Party enters into a composition with its creditors or goes into liquidation, or is dissolved, or adjudged insolvent or is otherwise rendered incapable of performing its obligations under this Agreement.

In such event, save in respect of any antecedent breaches, all rights and liabilities of the Parties shall cease and determine provided that (i) all amounts paid by Customer to Alibaba Cloud shall be non-refundable, (ii) all amounts due and owing by Customer to Alibaba Cloud shall continue to be due and owing and (iii) such termination shall be without prejudice to any rights or remedies of the Parties which have accrued prior to such termination.

10.4 Termination Due to Governmental Actions. If either Party is precluded by any applicable law, regulation or order of any Government Authority to provide or receive any Alibaba Cloud Products or fulfil its obligations under this Agreement, such Party may suspend or terminate the affected Alibaba Cloud Products or the Agreement upon providing [30] days prior written notice to the other Party or within timeline otherwise required by applicable law, regulation, order or Government Authority. Upon such suspension or termination, there shall be no further liabilities incurred by either Alibaba Cloud or Customer until any suspension is ended and Alibaba Cloud can continue to provide the affected Alibaba Cloud Products again. "Government Authority" means: (i) the government of any state, province (autonomous region, city directly under the central government), city or local area, or any political branch of the above; or (ii) any other government, quasi-government, judicial, public, administrative, legislative, or statutory institution, organization, department, bureau or entity (including any district or similar institution).

11. GENERAL

11.1 Assignment and Novation. Save and except Alibaba Cloud may at its sole and absolute discretion novate, assign or otherwise transfer this Agreement and its obligations thereunder at any time to any of its affiliated entities by giving written notice to the Customer, neither Party shall assign or transfer this Agreement or any rights and obligations hereunder, in whole or in part, to any third party, without the other Party's prior written consent.

11.2 Waiver. No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

11.3 Force Majeure. Neither Party will be liable for any breach, or delay in performance, of its obligations under this Agreement if, and to the extent that the breach or delay is directly caused by epidemics, fire, flood, earthquake or act of God; act of government, war, riot, civil disorder, act of terrorism or revolution; strikes, lock-outs or labor disputes; or other cause similar to the above beyond its reasonable control (a "**Force Majeure Event**"). The Party delayed or unable to perform will give prompt written notice, including the length of the expected delay, to the other Party. If a Force Majeure Event occurs, then the Parties will promptly mutually review the expected delay and the delayed Party or Parties will take reasonable measures to minimize any disruption. If the Force Majeure Event continues for thirty (30) consecutive days, then either Party may terminate this Agreement upon written notice to the other Party.

11.4 Independent Parties. The relationship between the Parties is that of independent contracting parties. Nothing in this Agreement shall constitute or be deemed to constitute a relationship of joint venture, partnership, franchise or similar arrangement between the Parties.

11.5 Governing Law. This Agreement will be governed by and construed in accordance with the laws of Singapore, without regard to or application of conflicts of law rules or principles. Any dispute, controversy, or claim shall be resolved through negotiation to the extent possible. In the event the parties fail to resolve any dispute arising hereunder through mutual negotiation, such dispute, controversy, difference or claim arising out of or relating to this Agreement,

including the existence, validity, interpretation, performance, breach or termination thereof or any dispute regarding non-contractual obligations arising out of or relating to it, shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre ("**SIAC**") under the arbitration rules of SIAC in force when the notice of arbitration is submitted, which rules are deemed to be incorporated by reference in this clause. The seat of arbitration shall be Singapore. The number of arbitrators shall be one. The arbitration proceedings shall be conducted in English.

11.6 Counterparts. This Agreement may be executed by the Parties in counterparts, each of which will be deemed an original, but all of which taken together will constitute one and the same instrument. Signatures executing this Agreement may be delivered by facsimile transmission or in an emailed PDF file or by other reliable means.

- The remainder of this page intentionally left blank -

[redacted]

IN WITNESS WHEREOF, the Parties below have caused this Agreement to be executed by their duly authorized representatives.

For and on behalf of

THE SWISS CONFEDERATION

acting through the *Bundesamt für Bauten und Logistik*

[redacted]

Date: 04.07.2022

[redacted]

Date: 4.7.2022

the *Bundeskanzlei*

[redacted]

Date: 5.7.2022

[redacted]

Date: 5.7.2022

For and on behalf of

ALIBABA.COM (EUROPE) LIMITED

Authorized Signatory:

[redacted] 24.08.2022

[redacted]telligence

Date:

[redacted]

Schedule 1

Form of Purchase Order

Alibaba Cloud:	**Customer:**
Name: **Alibaba.com (Europe) Limited** Contact Address: c/o 26/F, Tower One, Times Square, 1 Matheson Street, Causeway Bay, Hong Kong Telephone: Email: Contact Person:	Name: **The Swiss Confederation** Address: Fellerstrasse 21, CH-3003 Bern, Switzerland Telephone: Email: Contact Person:

PO No.		**Issue date**	
Alibaba Cloud's bank account details		**Currency**	USD
Beneficiary Name:		**Payment term**	Net 30
Account Number:			
Bank Name:			
Swift Number: Bank Address:			

Customer is to place an order with Alibaba Cloud for the following Alibaba Cloud Products on the terms and conditions set out in the Cloud Services Purchase Agreement entered into by and between Customer and Alibaba Cloud dated [•] (the "**Agreement**"). Unless otherwise provided herein, capitalized terms used in this Purchase Order shall have the same meaning as those defined in the Agreement.

DESCRIPTION (PRODUCT NAME/MODEL/SPECIFICATION)	**QTY**	**UNIT PRICE**	**TOTAL PRICE**
TOTAL VALUE (tax excluded)			

Other Terms:	

Approved by:

For and on behalf of Alibaba Cloud

Signature: _____
Name: _____
Title: _____
Date: _____

For and on behalf of Customer

Signature: _____
Name: _____
Title: _____
Date: _____

[redacted]

12

Alibaba Cloud Subsidiaries/Affiliates Sub-processors

As of the date 5 May, 2022

The subsidiary/affiliate entities of Alibaba Cloud listed in below table may participate in delivering, operating, maintaining and supporting the cloud services provided to our customers. Their participation depends on the type of products/services purchased and regions chosen and activated by the customers. These entities may, in the course of their participation, store, transfer or otherwise process customers' data as sub-processors. Such data will only be stored/processed on Alibaba Cloud facilities with the consistent standard of technical and organisational data protection measures.

Subsidiaries/Affiliates	Location
AliCloud (Germany) GmbH	Germany
Alibaba (Australia) Company Pty Ltd.	Australia
Alibaba Cloud (India) LLP	India
Alibaba Cloud (Malaysia) Sdn. Bhd.	Malaysia
Alibaba Cloud (Singapore) Private Limited	Singapore
Alibaba Cloud (Thailand) Limited	Thailand
Alibaba Cloud Computing Ltd.	China
Alibaba Cloud Japan Services Corporation	Japan
Alibaba Cloud Philippines, Inc.	Philippines
Alibaba Cloud US LLC	United States
Alibaba Korea Limited	Korea
Alibaba.com LLC	United States
PT. Alibaba Cloud Indonesia	Indonesia
Taobao Hong Kong Limited	Hong Kong

[redacted]

13

Composition of Contracts of the Company as Referred to under Clause 4.2 e)

1. Offline Contract (Cloud Service Purchase Agreement)
   - Europe (non-EEA) Alibaba Cloud - Offline Purchase Agreement
2. Online Available Terms (available at https://www.alibabacloud.com/help/en/legal)

   2a. Besucher Ebene
   - Alibaba Cloud International Website Terms of Use
   - Datenschutzerklärung der Alibaba Cloud International Website

   2b. Registrierte Benutzer-Ebene
   - EEA Data Processing Addendum
   - UK Data Processing Addendum and Standard Contractual Clauses
   - Membership Agreement
   - Alibaba Cloud International Website Beta Testing Terms
   - Payment and Tax Terms

   2c. Spezifische Benutzerebene

   2c 1) Product SLA
   - API Gateway Service Level Agreement
   - ApsaraDB Dedicated Cluster Service Level Agreement
   - DNS PrivateZone Service Level Agreement
   - Quotation Service Level Agreement
   - Monitor Service Level Agreement
   - ApsaraDB for RDS Service Level Agreement
   - Mail Service Level Agreement
   - Data Encryption Service Level Agreement
   - Elastic Compute Service (ECS) Service Level Agreement
   - Express Connect Service Level Agreement
   - Data Transmission Service Level Agreement
   - Table Store Service Level Agreement
   - Object Storage Service (OSS) Service Level Agreement
   - AnalyticDB for PostgreSQL Service Level Agreement
   - AnalyticDB for MySQL Service Level Agreement
   - Content Delivery Network (CDN) Service Level Agreement
   - ApsaraDB for MongoDB Service Level Agreement
   - E-MapReduce Service (EMR) Service Level Agreement
   - ApsaraDB HybridDB Service Level Agreement
   - Cloud Enterprise Network Service Level Agreement
   - Log Service Service Level Agreement
   - Anti-DDoS Premium Service Level Agreement
   - Anti-DDoS Pro Service Level Agreement
   - ApsaraDB for Cassandra Service Level Agreement
   - ApsaraVideo Live Service Level Agreement
   - ApsaraVideo Media Processing Service Level Agreement
   - Bastionhost Service Level Agreement
   - ApsaraDB for HBase Service Level Agreement
   - ApsaraDB for cache Service Level Agreement
   - ApsaraVideo VOD Service Level Agreement
   - ApsaraDB for Redis Service Level Agreement
   - Application Real-Time Monitoring Service Service Level Agreement

- Blockchain as a Service (BaaS) Service Level Agreement
- Container Registry Enterprise Edition Service Level Agreement
- Cloud Security Scanner Service Level Agreement
- Cloud Firewall Service Level Agreement
- Cloud Storage Gateway Service Level Agreement
- Batch Compute Service Level Agreement
- Content Moderation Service Level Agreement
- DataWorks Service Level Agreement
- Data Lake Analytics (DLA) Service Level Agreement
- E-HPC Service Level Agreement
- Enterprise Distributed Application Service (EDAS) Service Level Agreement
- Elastic Container Instance Service Level Agreement
- Hybrid Backup Service (HBR) Service Level Agreement
- DCDN Service Level Agreement
- Image Search Service Level Agreement
- Intelligent Speech Interaction Service Level Agreement
- Container Service for Kubernetes Service Level Agreement
- MaxCompute Service Level Agreement
- Network Attached Storage Service Level Agreement
- DAS Service Level Agreement
- Realtime Compute Service Level Agreement
- Distributed Relational Database Service Level Agreement
- Direct Mail Service Level Agreement
- Server Load Balancer Service Level Agreement
- Smart Access Gateway Service Level Agreement
- Elastic IP Service Level Agreement
- Hologres Service Level Agreement
- Global Accelerator Service Level Agreement
- Function Compute Service Level Agreement
- Database Backup Service Level Agreement
- Web Application Firewall (WAF) Service Level Agreement
- Website Threat Inspector Service Level Agreement
- Database Management Service Level Agreement
- DataV Service Level Agreement
- DNS Service Level Agreement
- Message Queue for Apache Kafka Service Level Agreement
- Key Management Service (KMS) Service Level Agreement
- IoT-Edge Service Level Agreement
- Machine Translation Service Level Agreement
- Elasticsearch Service Level Agreement
- Sensitive Data Discovery and Protection Service Level Agreement
- Fraud Detection Service Level Agreement
- Realtime Compute Fully Managed Flink Service Level Agreement
- AIRec Service Level Agreement
- mPaaS Service Level Agreement
- IoT Platform Service Level Agreement
- Alibaba Cloud Public DNS Service Level Agreement
- Message Service Service Level Agreement

- DataHub Service Level Agreement
- Elastic Desktop Service (EDS) Service Level Agreement
- Message Queue for Apache RocketMQ Service Level Agreement
- Machine Learning Platform for AI Service Level Agreement
- Security Center Service Level Agreement
- PolarDB Service Level Agreement
- Web Hosting Service Level Agreement
- Simple Application Server Service Level Agreement
- VPN Gateway Service Level Agreement
- NAT Gateway Service Level Agreement
- Short Message Service (SMS) Service Level Agreement
- Message Queue for RabbitMQ Service Level Agreement
- Quick BI Service Level Agreement
- Time Series Database Service Level Agreement
- Tracing Analysis Service Level Agreement
- Mobile Testing Service Level Agreement
- Real-Time Communication Service Level Agreement
- Service Mesh Service Level Agreement
- Historical SLAs - Not Currently In Effect

2c 2) Product Terms

- Product Terms of Service
- Smart Access Gateway Addendum to the Alibaba Cloud International Website Product Terms of Service

2c 3) Other Rules

- Alibaba Cloud - Domain Services - ICANN Supplemental Notice
- Alibaba Cloud International Website Domain Name Service Agreement
- API Term of Use
- The Third Party Software Manual

Further technical supporting documentation are available at:
https://www.alibabacloud.com/help/en/

[redacted]