



Rahmenvertrag (20007) 608 Public Clouds Bund

Firma: Amazon Web Services EMEA SARL

Inhaltsverzeichnis

Nr.	Bezeichnung	Unterzeichnung
0	Rahmenvertrag	A
1	Anhang Abrufverfahren	
2	Anhang Audit	
3	Anhang Datenschutz	
4	Anhang IT- und Datensicherheit	
5	Anhang Migration und Löschung der Daten	
6	Anhang Technische Anforderungen	
7	Anhang Vertraulichkeit der Daten	
8	Anhang Zugriff auf Daten durch Unberechtigte	
9	Vertragswerke der Firma:	
10	BBL_AWS Enterprise Agreement	B
11	BBL_AWS GDPR Data Processing Addendum_Switzerland	B
12	BBL_Supplementary Addendum to AWS GDPR Data Processing Addendum	B
13	BBL_Professional Secrecy Addendum	B
14	[REDACTED]	B
15	Mutual Non Disclosure Agreement vom 24.06.2020 (effective as of 01.01.2019)	

Unterzeichnung:

A

B



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Eidgenössisches Finanz-
departement EFD
Bundesamt für Bauten und Logistik
Bereich Logistik
Abteilung Beschaffung

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)

Abgeschlossen zwischen der Schweizerischen Eidgenossenschaft handelnd durch:

Bundesamt für Bauten und Logistik – BBL
Bereich Logistik
Fellerstrasse 21
3003 Bern

Nachstehend bezeichnet mit "Beschaffungsstelle"

für die

Bundeskanzlei
Bereich Digitale Transformation und IKT-Lenkung - DTI
Schwarztorstrasse 53
3003 Bern

Nachstehend bezeichnet mit "Bedarfsstelle", gemeinsam nachstehend je einzeln oder zusammen
„Vergabestelle“

und der Unternehmung

Amazon Web Services EMEA SARL
38 avenue John F. Kennedy
L-1855 Luxembourg

Nachstehend bezeichnet mit "Firma"

Inhaltsverzeichnis

Ausgangslage, Projektbeschreibung und Ziele	3
1 Rahmenvertrag als Abrufrahmen	3
2 Bezugsberechtigung.....	3
3 Vertragsgegenstand	3
4 Vertragsbestandteile.....	3
5 Bezugsregelung	4
6 Schlüsselpersonen	4
7 Eskalationsverfahren.....	4
8 Vergütung	5
9 Rechnungsstellung.....	5
10 Datenschutz und Datensicherheit	6
11 Vertraulichkeit der Daten.....	6
12 Migration und Löschung der Daten.....	6
13 Informationspflichten	6
14 Kontrollrechte (Audit)	6
15 Zugriff auf Daten durch Unberechtigte	6
16 Technische Anforderungen	6
17 Integritätsklausel.....	6
18 Offenlegungspflicht	6
19 Veränderung der rechtlichen Rahmenbedingungen	7
20 Weitere Bestimmungen	7
21 Anwendbares Recht / Gerichtsstand	9
22 Inkrafttreten / Rahmenvertragsdauer / Rahmenvertragsänderungen	9
23 Kündigung aus wichtigem Grund.....	9
24 Ausfertigung / Unterzeichnung durch die Parteien	10

Ausgangslage, Projektbeschreibung und Ziele

Auf Grundlage der öffentlichen Ausschreibung sowie der dazugehörigen Unterlagen vom 07.12.2020 auf der Publikationsplattform www.simap.ch hat die Firma ein Angebot zu den von der Vergabestelle nachgefragten Leistungen eingereicht. Der Firma wurde mit Publikation Nr. 12029371202937 auf www.simap.ch am 24.06.2021 der Zuschlag erteilt. Die diesbezüglichen vertraglichen Bedingungen werden in der vorliegenden Vertragsurkunde sowie den dazugehörigen Bestandteilen geregelt.

1 Rahmenvertrag als Abrufrahmen

- 1.1 Die zu beziehenden Cloud-Services können zum Zeitpunkt des Vertragsabschlusses nicht bestimmt werden. Infolge dieser Ausgangslage vereinbaren die Parteien einen Rahmenvertrag.
- 1.2 Gestützt auf den vorliegenden Rahmenvertrag werden mit Bezug auf die Realisierung einzelner Projekte jeweils Abrufe bei der Firma getätigt. Die Modalitäten der Abrufe ergeben sich aus dem Anhang Abrufverfahren. Verbindliche Leistungen ergeben sich jeweils erst aus den einzelnen Abrufen; aus diesem Rahmenvertrag ergibt sich weder eine Bezugspflicht der Vergabestelle noch eine diesbezügliche Leistungspflicht der Firma.

2 Bezugsberechtigung

- 2.1 Bezugsberechtigt sind die Verwaltungseinheiten der Bundesverwaltung gemäss Art. 8 der Regierungs- und Verwaltungsorganisationsverordnung (RVOV; SR 172.010.1), wie in Anhang 1 zur RVOV (https://www.fedlex.admin.ch/eli/cc/1999/170/de#annex_1/vl_d4e138) aufgelistet. Zusätzlich gelten als Bezugsberechtigte: die Parlamentsdienste, die Bundesanwaltschaft, das Bundesgericht, das Bundesverwaltungsgericht, das Bundespatentgericht und das Bundesstrafgericht.
- 2.2 Im Folgenden wird der Begriff «Bezugsberechtigte» eingesetzt für sowohl grundsätzlich bezugsberechtigte Verwaltungseinheiten der Bundesverwaltung als auch für Verwaltungseinheiten der Bundesverwaltung die tatsächlich Leistungen von der Firma beziehen. Im Innenverhältnis entscheidet die Bedarfsstelle (BK-DTI) darüber, welche Bezugsberechtigten tatsächlich Leistungen beziehen dürfen.
- 2.3 Es gelten ergänzend die Voraussetzungen der Ziff. 1.4 des AWS Enterprise Agreement.

3 Vertragsgegenstand

- 3.1 Der vorliegende Rahmenvertrag einschliesslich aller Vertragsbestandteile regelt grundsätzlich die Rechte und Pflichten der Parteien für die Erbringung von Leistungen im Umfeld Public Cloud Services.
- 3.2 Er bezweckt insbesondere die Herstellung eines koordinierten Prozesses im Rahmen der Realisierung von Einzelabrufen sowie die Harmonisierung der Abläufe.

4 Vertragsbestandteile

- 4.1 Die Bestimmungen der vorliegenden Vertragsurkunde gehen im Fall von Widersprüchen sämtlichen anderen Verträgen und Nachträgen vor, sofern die Parteien darin nicht ausdrücklich und unter Hinweis auf eine Abweichung der vorliegenden Vertragsurkunde eine andere Regelung vorsehen.
- 4.2 Im Übrigen sind integrierende Bestandteile des vorliegenden Rahmenvertrages in nachstehender Rangfolge:
 - a) Die vorliegende Rahmenvertragsurkunde inkl. allfälliger Nachträge dazu.
 - b) Die Anhänge zu diesem Rahmenvertrag inkl. allfälliger Nachträge dazu.
 - c) Die unterzeichneten Vertragswerke der Firma und im Vertragswerk einbezogene Dokumente.
 - d) Das Angebot der Firma vom 28.01.2021 sowie deren Nachofferte vom 31.03.2021.

- e) Die Ausschreibung sowie die dazugehörigen Unterlagen für das Projekt (20007) 608 Public Clouds Bund

- 4.3 Im Falle von Widersprüchen zwischen einzelnen Vertragsbestandteilen gilt die vorstehend genannte Rangfolge. Allfällige abweichende Regeln zur Rangfolge in den Vertragswerken der Firma sind bezüglich der Abrufe unter diesem Rahmenvertrag unbeachtlich. Bei Widersprüchen zwischen den Anhängen innerhalb derselben Hierarchiestufe gilt, dass jüngere Bestimmungen älteren Bestimmungen vorgehen.
- 4.4 Das Standard Leistungsangebot der Firma darf die Vertragsbestandteile nicht modifizieren. Es dient vor allem der Konkretisierung von Punkten, welche in den anderen Vertragsbestandteilen nicht hinreichend geregelt sind.
- 4.5 Die Parteien bestätigen mit der Unterzeichnung der vorliegenden Rahmenvertragsurkunde, dass sie im Besitze der obgenannten Vertragsbestandteile sind und diese auch in der genannten Rangfolge anerkennen.

5 Bezugsregelung

- 5.1 Verbindliche Leistungen ergeben sich jeweils erst aus einem Abruf.
- 5.2 Bevor zu einem konkreten Bedarfsfall Leistungen bezogen werden, wird in der Bundesverwaltung ein bestimmter Prozess durchlaufen (Abrufverfahren). Das Abrufverfahren richtet sich nach den Regeln im Anhang Abrufverfahren.
- 5.3 Da nicht absehbar ist, welcher der fünf (5) Zuschlagsempfänger der Ausschreibung (20007) 608 Public Clouds Bund für die einzelnen Leistungen berücksichtigt wird, gilt für jeden der fünf Zuschlagsempfänger das Kostendach von CHF 110'000'000.00 (exkl. MwSt.). Sobald die Summe sämtlicher bezogenen Leistungen über alle 5 Zuschlagsempfänger gerechnet das Kostendach erreicht, werden die Zuschlagsempfänger über die vollständige Ausschöpfung informiert.

6 Schlüsselpersonen

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

Funktion	Team Lead Government, Public Sector Switzerland
----------	---

Namensliste der Schlüsselperson bei der Firma

- 6.2 Auf Seite der Bedarfsstelle liegt die Gesamtverantwortung bei:

Funktion	Bundeskanzlei Bereich DTI
----------	---------------------------

Namensliste der Schlüsselperson bei der Bedarfsstelle

7 Eskalationsverfahren

- 7.1 Im Falle von Uneinigkeiten erfolgt die Bereinigung gemäss dem nachstehenden Eskalationsverfahren.
- 7.2 Eskalationsstufen auf Seiten der Vergabestelle:

Eskalationsstufe	Beteiligte
1	Auftraggeberin Transformation und Interoperabilität
2	Direktion

Eskalationsstufen seitens Vergabestelle

7.3 Eskalationsstufen auf Seiten der Firma:

Eskalationsstufe	Beteiligte
1	Team Lead Government, Public Sector Switzerland
2	Head Public Sector Switzerland

Eskalationsstufen seitens Firma

- 7.4 Das Eskalationsverfahren hat keinen Einfluss auf die geltende Unterschriftenregelung. Sobald eine Einigung erzielt werden konnte, ist für allfällige Vertragsanpassungen oder rechtsverbindliche Vertragsauslegungen in der Regel innert 10 Arbeitstagen die Zustimmung der jeweilszeichnungsberechtigten Personen einzuholen.
- 7.5 Die Parteien wenden das Eskalationsverfahren nach Treu und Glauben mit dem gemeinsamen Ziel der einvernehmlichen Bereinigung von Meinungsdivergenzen an. Jede Partei trägt dabei ihren eigenen Aufwand.
- 7.6 Sollte binnen 30 Tagen innerhalb einer Stufe keine Einigung erzielt werden können, so ist jede Partei berechtigt, die Meinungsdivergenz der nächsthöheren Ebene schriftlich zu unterbreiten. Dabei sind mindestens zu nennen: Inhalt der Meinungsdivergenz, Ursache aus Sicht der betreffenden Partei, Auswirkungen auf das Preis- und Leistungsverhältnis, Lösungsvorschlag bzw. -ansätze.
- 7.7 Jede Partei verpflichtet sich, eine allfällige Streitigkeit erst dann dem zuständigen Gericht zu unterbreiten, wenn innerhalb der höchsten Eskalationsstufe keine Einigung erzielt werden konnte.
- 7.8 Das Eskalationsverfahren muss nicht durchlaufen werden, sofern es offensichtlich sinnlos bzw. zwecklos ist (namentlich Konkursfall der Firma, Vertrauensverhältnis zwischen den Parteien tief erschüttert etc.). Soweit die Firma gemäss Vertragswerk der Firma berechtigt ist, den Zugang zu den Leistungen vorübergehend einzuschränken oder zu beenden oder Inhalte der Bezugsberechtigten zu entfernen, ist das Eskalationsverfahren keine zwingende Voraussetzung für diese Massnahmen.
- 7.9 Bei Streitigkeiten in Bezug auf «Service Fees» im Sinne von Ziffer 5.1 des AWS Enterprise Agreement gilt das dort geregelte Eskalationsverfahren.

8 Vergütung

Die Firma führt eine allgemein gültige und öffentlich zugängliche Preisliste.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10 Datenschutz und Datensicherheit

Die Firma verpflichtet sich zur Einhaltung der Bestimmungen zu Datenschutz und Datensicherheit in den Anhängen Datenschutz und IT- und Datensicherheit.

11 Vertraulichkeit der Daten

Die Firma ist verpflichtet, die Vertraulichkeit der Daten der Bezugsberechtigten zu gewährleisten. Anhang Vertraulichkeit der Daten regelt die Einzelheiten.

12 Migration und Löschung der Daten

Die Firma ermöglicht der Vergabestelle den Export (aus der Cloud heraus) und die unwiderrufliche Löschung ihrer Daten. Anhang Migration und Löschung der Daten regelt die Einzelheiten.

13 Informationspflichten

Die Firma informiert die Vergabestelle umgehend bei Vorkommnissen, die den angebotenen Leistungsumfang betreffen oder die die Integrität oder Vertraulichkeit der Daten der Vergabestelle oder der Bezugsberechtigten beeinträchtigen, entsprechend Ziffern 3.6 und 3.7 des AWS Enterprise Agreement sowie Ziffer 9 des AWS Data Processing Addendums.

14 Kontrollrechte (Audit)

Die Firma gewährt der Bedarfsstelle und von ihr beauftragten Verwaltungseinheiten der Bundesverwaltung Kontrollrechte. Anhang Audit regelt die Einzelheiten.

15 Zugriff auf Daten durch Unberechtigte

Die Firma verpflichtet sich auf Massnahmen zur Aufrechterhaltung der Kontrollbefugnisse über den Datenbestand der Bezugsberechtigten, soweit die Leistungserbringung der Firma einen Bezug zu diesem Datenbestand der Bezugsberechtigten aufweist. Anhang Zugriff auf Daten durch Unberechtigte regelt die Einzelheiten.

16 Technische Anforderungen

Die Firma verpflichtet sich zur Einhaltung der Bestimmungen zu den technischen Anforderungen im Anhang Technische Anforderungen.

17 Integritätsklausel

17.1 Die Parteien verpflichten sich, alle erforderlichen Massnahmen zur Vermeidung von Korruption zu ergreifen, so dass insbesondere keine Zuwendungen oder andere Vorteile angeboten oder angenommen werden. Einzelheiten regelt Ziffer 12.17 des AWS Enterprise Agreement.

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

18 Offenlegungspflicht

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

18.2 Die Vergabestelle konsultiert in der Regel die Firma, wenn es die Gewährung des Zugangs in Betracht zieht, und gibt ihr Gelegenheit zur Stellungnahme innert zehn Tagen.

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

19 Veränderung der rechtlichen Rahmenbedingungen

- 19.1 Die Firma anerkennt, dass es während der Vertragsdauer zu Änderungen der rechtlichen Rahmenbedingungen zum Schutz wichtiger Schutzziele der Bezugsberechtigten kommen kann.
- 19.2 Anpassungen in Regeln zu den folgenden Themen lösen die Pflichten gemäss Ziff. 19.3 aus:
- Regeln zum Amts- oder Berufsgeheimnis (Vorgaben in der Schweiz)
 - Regeln betreffend IT-Sicherheit
 - Regeln betreffend den Datenschutz
- 19.3 Die Firma unternimmt in einem solchen Fall von sich aus notwendige technisch und wirtschaftlich verhältnismässigen Massnahmen, welche die Bezugsberechtigten vernünftigerweise erwarten dürfen, damit diese weiterhin die Leistungen der Firma beziehen können.

20 Weitere Bestimmungen

- 20.1 Arbeitsschutzbestimmungen, Arbeitsbedingungen, Lohngleichheit und Umweltrecht

Für die im Rahmen der Vertragserfüllung in der Schweiz zu erbringenden Leistungen hält die Firma die am Ort der Leistung massgeblichen Arbeitsschutzbestimmungen und Arbeitsbedingungen, die Melde- und Bewilligungspflichten nach dem Bundesgesetz vom 17. Juni 2005 gegen Schwarzarbeit (BGSA)¹ sowie die Bestimmungen über die Gleichbehandlung von Frau und Mann in Bezug auf die Lohngleichheit ein. Als Arbeitsbedingungen gelten die Gesamt- und die Normalarbeitsverträge oder, wo diese fehlen, die tatsächlichen orts- und berufsüblichen Arbeitsbedingungen.

Für die im Rahmen der Vertragserfüllung im Ausland zu erbringenden Leistungen hält die Firma die entsprechenden Bestimmungen, die am Ort der Leistungserbringung gelten, mindestens aber die Kernübereinkommen der Internationalen Arbeitsorganisation (ILO)² ein.

Entsendet die Firma Arbeitnehmende aus dem Ausland in die Schweiz, um die Leistung auszuführen, so sind die Bestimmungen des Entsendegesetzes vom 8. Oktober 1999³ einzuhalten.

Für die im Rahmen der Vertragserfüllung in der Schweiz zu erbringenden Leistungen hält die Firma die am Ort der Leistung massgeblichen Bestimmungen des schweizerischen Umweltrechts ein; namentlich das Bundesgesetz über den Umweltschutz (USG)⁴, das Bundesgesetz über den Schutz der Gewässer (GSchG)⁵, das Bundesgesetz über den Natur- und Heimatschutz (NHG)⁶,

¹ SR 822.41

² ILO-Übereinkommen: Nr. 29 vom 28. Juni 1930 über Zwangs- oder Pflichtarbeit (SR 0.822.713.9), Nr. 87 vom 9. Juli 1948 über die Vereinigungsfreiheit und den Schutz des Vereinigungsrechtes (SR 0.822.719.7), Nr. 98 vom 1. Juli 1949 über die Anwendung der Grundsätze des Vereinigungsrechtes und des Rechtes zu Kollektivverhandlungen (SR 0.822.719.9), Nr. 100 vom 29. Juni 1951 über die Gleichheit des Entgelts männlicher und weiblicher Arbeitskräfte für gleichwertige Arbeit (SR 0.822.720.0), Nr. 105 vom 25. Juni 1957 über die Abschaffung der Zwangsarbeit (SR 0.822.720.5), Nr. 111 vom 25. Juni 1958 über die Diskriminierung in Beschäftigung und Beruf (SR 0.822.721.1), Nr. 138 vom 26. Juni 1973 über das Mindestalter für die Zulassung zur Beschäftigung (SR 0.822.723.8), Nr. 182 vom 17. Juni 1999 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit (SR 0.822.728.2).

³ SR 823.20

⁴ SR 814.01

⁵ SR 814.20

⁶ SR 451

das Waldgesetz (WaG)⁷ und das Chemikaliengesetz (ChemG)⁸ sowie die darauf basierenden Verordnungen.

Für Leistungen, die im Rahmen der Vertragserfüllung im Ausland erbracht werden, hält die Firma die am Ort der Leistung geltenden Umweltschutzbestimmungen ein, mindestens aber die für ihre Leistung relevanten Umweltabkommen gemäss Anhang 2 VöB⁹.

Die Firma ist verpflichtet, die Anforderungen gemäss den vorstehenden Absätzen dieser Ziffer 20.1 vertraglich auf ihre Subunternehmerinnen zu überbinden.

[REDACTED]

20.2 Sozialversicherungen

Ist die Firma eine juristische Person, so nimmt sie als selbstständiges Unternehmen die notwendigen Anmeldungen für sich und ihre Mitarbeitenden bei den Sozialversicherungen vor. Ist sie keine juristische Person, so muss sie mit Einreichung des Angebotes nachweisen, dass sie als Selbstständigerwerbende einer Ausgleichskasse angeschlossen ist.

Die Vergabestelle schuldet keine Sozialleistungen (AHV, IV, ALV, usw.) oder andere Entschädigungsleistungen, insbesondere bei Unfall, Krankheit, Invalidität und Tod.

20.3 Ausführung und Information

Die Firma verpflichtet sich zu einer sorgfältigen, getreuen und sachkundigen Vertragserfüllung und gewährleistet, dass alle erbrachten Leistungen den vertraglichen Bedingungen entsprechend und im Wesentlichen gemäss der unter <http://aws.amazon.com/documentation> (und Unterseiten dazu oder dort verlinkten Seiten) jeweils aktuellen Dokumentation (Nutzerleitfäden und Administratorenleitfäden) erbracht werden und dem aktuellen Stand der Technik sowie den auf die Firma anwendbaren gesetzlichen Vorgaben entsprechen.

Die Vergabestelle gibt der Firma rechtzeitig alle für die Vertragserfüllung erforderlichen Vorgaben bekannt. Allfällige weitere Mitwirkungspflichten der Vergabestelle werden in der Vertragsurkunde abschliessend vereinbart.

20.4 Dokumentation und Instruktion

Die Firma stellt im Self-Service Center oder auf der Firmenwebsite elektronisch, zusammen mit der vereinbarten Leistung, eine vollständige, kopierbare Dokumentation zur Verfügung.

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

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

20.5 Gewährleistung

Die Firma gewährleistet, dass die erbrachten Leistungen die vereinbarten und im Wesentlichen in der Dokumentation zugesicherten Eigenschaften aufweisen sowie diejenigen Eigenschaften, welche die Vergabestelle in guten Treuen auch ohne besondere Vereinbarung voraussetzen dürfte.

Die Firma gewährleistet, dass sie und von ihr beigezogene Dritte über alle Rechte verfügen, um ihre Leistungen vertragsgemäss zu erbringen. Sie ist insbesondere berechtigt, der Vergabestelle die Rechte an den Arbeitsergebnissen im vertraglich vereinbarten Umfang einzuräumen.

Sämtliche Unterlagen, die die Vergabestelle der Firma zur Verfügung stellt, auch solche in elektronischer Form, dürfen ausschliesslich für die Leistungserbringung genutzt und kopiert werden. Insofern gewährleistet die Vergabestelle, dass die Verwendung der Unterlagen durch die Firma keine Schutzrechte Dritter verletzt.

⁷ SR 921.0

⁸ SR 813.1

⁹ SR 172.056.11

20.6 Geheimhaltung

Es gelten das zwischen den Parteien vereinbarte Mutual Non Disclosure Agreement vom 24.06.2020 (effective as of 01.01.2019; "NDA") für vertrauliche Informationen im Sinne des NDA, die keinen Customer Content darstellen. Für Customer Content oder Customer Data gelten die Geheimhaltungs- und Vertraulichkeitspflichten gemäss (i) Anhängen Datenschutz, Zugriff auf Daten durch Unberechtigte und Vertraulichkeit und (ii) Vertragswerk der Firma.

Die Parteien ergänzen hiermit die in Ziffer 1 des NDA vom 24.06.2020 enthaltene Definition von "Affiliate" dahingehend, dass fortan alle Bezugsberechtigten gemäss Ziff. 2 "Affiliates" der "Company" (Schweizerischen Eidgenossenschaft, vertreten durch BBL) sind.

[REDACTED]

20.7 Schutzrechte

Ziffer 8 des AWS Enterprise Agreement regelt das Eigentum und die Nutzungsrechte in Bezug auf alle Schutzrechte (Immaterialgüter- und Leistungsschutzrechte sowie Anwartschaften an solchen) an den vereinbarten Leistungen und/oder im Rahmen der Vertragserfüllung entstandenen Arbeitsergebnissen.

20.8 Verletzung von Schutzrechten

Die Pflichten der Parteien zur Freistellung und Verteidigung der anderen Partei im Fall von Schutzrechtsverletzungen ergeben sich aus Ziffer 9.2. und 9.3 des AWS Enterprise Agreement.

20.9 Haftung

Die Haftung der Parteien ergibt sich aus Ziffer 11 des AWS Enterprise Agreement.

21 Anwendbares Recht / Gerichtsstand

21.1 Auf Streitigkeiten aus diesem Vertragsverhältnis ist ausschliesslich schweizerisches Recht anwendbar unter Ausschluss des Kollisionsrechts und des Übereinkommens der Vereinten Nationen vom 11. April 1980 über Verträge über den internationalen Warenkauf (Wiener Kaufrecht, CISG, SR 0.221.211.1).

21.2 Ausschliesslicher Gerichtsstand ist Bern, Schweiz.

22 Inkrafttreten / Rahmenvertragsdauer / Rahmenvertragsänderungen

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

22.2 Er ist gültig bis zum 31.08.2026.

22.3 Änderungen und Ergänzungen dieses Rahmenvertrages, des AWS Enterprise Agreements sowie des AWS Data Processing Addendums sind nur gültig, wenn sie von den Parteien schriftlich vereinbart werden. Dies gilt auch für die Aufhebung dieses Schriftlichkeitsvorbehaltes. Diese Ziffer 22.3 gilt nicht für Änderungen der AWS Service Terms, der Documentation, der Acceptable Use Policy, der AWS Privacy Notice, der Service Level Agreements und der Trademark Guidelines.

23 Kündigung aus wichtigem Grund

23.1 Jede Partei ist berechtigt, den Rahmenvertrag und/oder die Einzelverträge bei schwerwiegender Verletzung durch die andere Partei aus wichtigem Grund aufzulösen. Vor der Kündigung wird die kündigungswillige Partei der anderen Partei vorgängig eine angemessene Frist setzen, innerhalb welcher sie dieselbe zu vertragskonformer Leistung auffordert.

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

- über die Firma der Konkurs eröffnet wird oder sie ein Gesuch um Nachlassstundung einreicht oder in Liquidation tritt;
- die Firma die Liquidation (ausgenommen der Fall einer freiwilligen Liquidation zum Zweck der Fusion oder einer Reorganisation) erklärt;
- die Firma mit der Beschlagnahme ihres Vermögens konfrontiert wird;
- die Firma ihren vertraglichen Pflichten trotz schriftlicher Rüge und dem Setzen einer angemessenen Nachfrist nicht nachkommt.

23.3 Im Falle einer Kündigung aus wichtigem Grund bleiben sonstige Ansprüche der Parteien, einschliesslich Gewährleistungs- und Schadenersatzansprüche sowie Konventionalstrafen und die Geheimhaltungspflichten, unberührt.

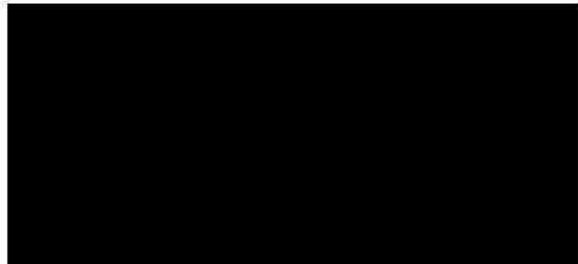
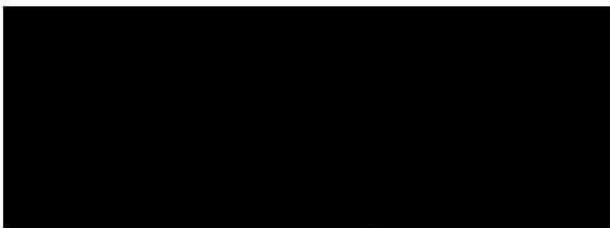
24 Ausfertigung / Unterzeichnung durch die Parteien

Die vorliegende Vertragsurkunde wird 3-fach ausgefertigt. Jede beteiligte Partei erhält ein unterzeichnetes Exemplar.

Für die Beschaffungsstelle

Bundesamt für Bauten und Logistik - BBL

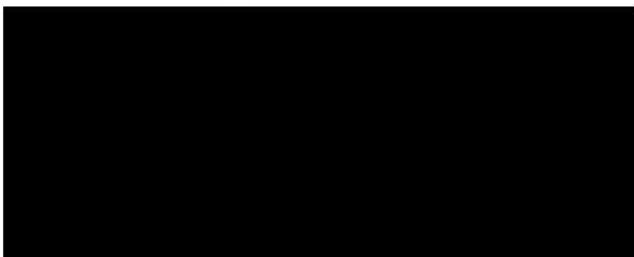
Ort und Datum: *Bern, 04.07.2022*



Für die Bedarfsstelle

Bundeskanzlei - BK

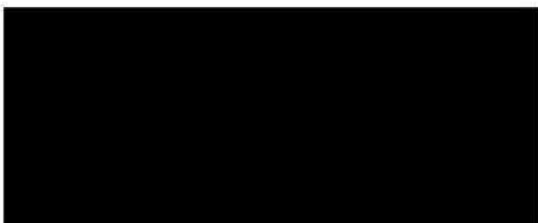
Ort und Datum: *Bern, 6.7.2022*



Für die Firma

Amazon Web Services EMEA SARL

Ort und Datum: *Zürich, 16.08.2022*



Anhänge:

Nr.	Bezeichnung
10	Anhang Abrufverfahren
20	Anhang Audit
30	Anhang Datenschutz
40	Anhang IT- und Datensicherheit
50	Anhang Migration und Löschung der Daten
60	Anhang Technische Anforderungen
70	Anhang Vertraulichkeit der Daten
80	Anhang Zugriff auf Daten durch Unberechtigte
90	Vertragswerke der Firma:
100	BBL_AWS Enterprise Agreement
110	BBL_AWS GDPR Data Processing Addendum_Switzerland
120	BBL_Supplementary Addendum to AWS GDPR Data Processing Addendum
130	BBL_Professional Secrecy Addendum
140	
150	



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)

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. 3.2), ob nach Durchlaufen der Prüfung gem. Ziff. 3.1 noch zusätzliche Informationen notwendig oder wünschenswert sind, um die beabsichtigte Nutzung zu beurteilen.
- 4.2 Im Rahmen von Ziff. 4.1 kann die Bezugsberechtigte einer oder mehreren Zuschlagsempfängerinnen Fragen zu deren vorhandenen Leistungsangeboten stellen. In Bezug auf eines oder mehrere der vorhandenen Leistungsangebote kann die Bezugsberechtigte auch Proof(s) of Concept durchführen.
- 4.3 Die Firma hat keinen Anspruch, gem. Ziff. 4.2 eingebunden zu werden.
- 4.4 Die Bezugsberechtigte dokumentiert die Gründe, die zu Fragen gem. Ziff. 4.2 Satz 1 geführt haben, ebenso die Resultate.
- 4.5 Zeigt sich, dass die Bezugsberechtigte darüber hinaus Bedarf zur Einholung von einzel-fallbezogenen Angeboten hat, regelt sie die Einzelheiten im Einzelfall und informiert die Firma. Die Bedarfsstelle kann dazu auch einen neuen Anhang zum Rahmenvertrag vor-sehen.

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 Na-men oder Service-ID's mit Hinweisen, wo die Bedarfsstelle und alle Be-zugsberechtigten 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, Prüf-be-richte, 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 Informati-onsquellen 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 Leis-tungen 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.

* * *



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Kontrollrechte (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)

1. Begriffsdefinitionen

- 1.1 Für die Zwecke des vorliegenden Vertragsanhangs sind die folgenden Begriffe wie folgt definiert:
- a) **Auditberechtigte Stellen** sind – nach den jeweils für sie geltenden Regelungen im AWS Enterprise Agreement und im AWS DPA – die Vergabestelle(n) und die jeweils Bezugsberechtigten (soweit ein eigener AWS Account genutzt wird) sowie jeweils deren interne und externe Revisionsstellen, deren Aufsichtsbehörden und -stellen. Die Firma anerkennt ausdrücklich, dass auch die folgenden Stellen als Auditberechtigte Stellen gelten:
 - der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB);
 - die Eidgenössische Finanzkontrolle (EFK).
 - b) **Audit** steht zusammenfassend für alle Rechte unter diesem Anhang, Ziffer 11 des DPA sowie Ziffer 3.8 des Enterprise Agreement.
- 1.2 Ansonsten gelten die Begriffe gemäss Rahmenvertrag, AWS Enterprise Agreement und AWS DPA.

2. Kontrollrechte (Audit)

Die Firma räumt jeder Auditberechtigten Stelle hiermit die folgenden Audit-Rechte ein:

- a) Ziffer 11 des DPA für die Vergabestelle und Bezugsberechtigte.
- b) Ziffer 3.8 des Enterprise Agreement für Aufsichtsbehörden.

3. Zweck des Audits

Das Audit kann insbesondere die folgenden Ziele und Zwecke der Auditberechtigten Stelle 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 Vertragswerks und den geltenden Leistungsbeschreibungen übereinstimmen;
- d) die Durchführung von Abläufen und Verfahren einschliesslich Datenbearbeitungsaktivitäten und -kontrollen der Firma zu prüfen.

* * *



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)

Inhaltsübersicht:

I.	Allgemeine Bestimmungen	3
1.	Anwendbares Recht.....	3
2.	Zu diesem Vertragsanhang	3
II.	Klauseln für die Datenbearbeitung im Auftrag.....	4
A.	Allgemeine Bestimmungen.....	4
3.	Zweck und Anwendungsbereich	4
4.	Auslegung.....	4
5.	Vorrang.....	4
6.	Beschreibung der Auftragsbearbeitung.....	4
B.	Pflichten der Parteien.....	5
7.	Weisungen.....	5
8.	Zweckbindung	5
9.	Dauer der Bearbeitung von Personendaten.....	5
10.	Sicherheit der Bearbeitung.....	5
11.	Dokumentation und Einhaltung der Klauseln	5
12.	Audit	6
13.	Einsatz von Unterauftragsbearbeitern.....	6
14.	Internationale Datenübermittlungen	6
C.	Koordination und Compliance	6
15.	Unterstützung der Verantwortlichen	6
16.	Meldung von Verletzungen der Datensicherheit, allgemeine Bestimmungen	7
17.	Meldung einer Verletzung der Datensicherheit durch die Auftragsbearbeiterin an die Verantwortliche.....	7
18.	Meldung einer Verletzung der Datensicherheit durch die Verantwortliche an Aufsichtsbehörden oder betroffene Personen.....	7
19.	Verstöße gegen die Klauseln und Beendigung	7
III.	Klauseln betreffend die Übermittlung von Personendaten ins Ausland	8
20.	Übermittlung von Personendaten ins Ausland	8

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 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 erbringt ihre Leistungen so, dass die Vergabestelle sowie Bezugsberechtigte die im Bereich des Datenschutzes für die Bezugsberechtigte massgebenden Bestimmungen einhalten können. Für die Nutzung der Leistungen gilt Ziffer 8 des AWS DPA.

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 orientiert sich für die Zwecke von Art. 10a DSG an den Regelungspunkten gemäss Art. 28(3) EU-DSGVO (dazu Abschnitt II) und stellt für die Zwecke von Art. 6 DSG ab auf die Standardvertragsklauseln der Europäischen Kommission betreffend die grenzüberschreitende Übermittlung von Personendaten in Drittstaaten (dazu Abschnitt III).¹
- 2.4 Dieser Vertragsanhang verweist auf Bestimmungen aus dem AWS GDPR Data Processing Addendum (wie für die Vergabestelle und die Bezugsberechtigten angepasst, das «AWS DPA»), dem AWS Supplementary Addendum to AWS GDPR Data Processing Addendum («Supplementary Addendum») und den AWS Standard Contractual Clauses (Controller-to-Processor sowie Processor-to-Processor; wie in Bezug auf den Geltungsbereich des Schweizer DSG durch das AWS DPA (Ziff. 12.4) angepasst, die «SCC»). Die Bestimmungen in AWS DPA, Supplementary Addendum

¹ 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 Europäischen Parlaments und des Rates, Abl L 199 vom 7. Juni 2021, S. 31–61.

und in den SCC gelten (i) unmittelbar als Bestandteil dieses Vertragsanhangs; und (ii) subsidiär, falls der vorliegende Vertragsanhang keinen solchen Verweis auf eine spezifische Bestimmung im AWS DPA, Supplementary Addendum oder in den SCC enthält.

II. KLAUSELN FÜR DIE DATENBEARBEITUNG IM AUFTRAG

A. Allgemeine Bestimmungen

3. Zweck und Anwendungsbereich

- 3.1 Mit den Klauseln dieser Ziffer II. soll die Einhaltung von Artikel 10a DSG (resp. Art. 9 revidiertes DSG, in der Folge "nDSG") beziehungsweise (soweit anwendbar) 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 diesem Abschnitt II deshalb auch "Verantwortliche" genannt) bearbeitet, soweit von der Bezugsberechtigten bei der Nutzung der Cloud-Services hochgeladenen, eingegebenen, gespeicherten oder bearbeiteten Arten von Personendaten (d.h. «Customer Data» nach dem AWS DPA).
- 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-Mitgliedstaaten in Drittstaaten gemäss Art. 44 ff. EU-DSGVO erfüllt werden. Diesbezüglich gelten zusätzlich die Bestimmungen in Abschnitt III (Ziff. 20 ff.).
- 3.4 Hinsichtlich der Kontrolle der Bezugsberechtigten über die Datenbearbeitung gilt Ziffer 1.2. des AWS DPA.

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. Soweit dieser Anhang auf das AWS DPA verweist, gelten die dort verwendeten Definitionen.
- 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

In Abweichung der Ziff. 4.2 des Rahmenvertrags gilt folgendes: Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen des Rahmenvertrags, diesbezüglicher Vertragsnachträge oder Leistungsabrufe, haben diese Klauseln, ihren Regelungsgegenstand betreffend, Vorrang.

6. Beschreibung der Auftragsbearbeitung

- 6.1 Der Gegenstand der Auftragsbearbeitung ist in Ziffer 1.3.1 des AWS DPA beschrieben.

- 6.2 Art und Zweck der Auftragsbearbeitung sind in Ziffern 1.3.3 und 1.3.4 des AWS DPA beschrieben.
- 6.3 Die Art der Personendaten und der Kreis (Kategorien) betroffener Personen sind in Ziffern 1.3.5 und 1.3.6 des AWS DPA beschrieben.

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 diejenigen rechtlichen Anforderungen, die von den Weisungen der Verantwortlichen abweichen, vor der Bearbeitung nach Möglichkeit mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
 - c) Die Verantwortliche kann während der gesamten Dauer der Bearbeitung von Personendaten weitere Weisungen erteilen.
- 7.2 Die Parteien sind sich einig, dass die Einzelheiten der Weisungen in Ziffer 2 des AWS DPA geregelt sind.

8. Zweckbindung

Die Auftragsbearbeiterin bearbeitet die Personendaten nur für die spezifischen Zweck(e) der Auftragsbearbeitung, sofern sie keine weiteren Weisungen der Verantwortlichen erhält oder einer der Fälle der Ziffer 3 des AWS DPA vorliegt.

9. Dauer der Bearbeitung von Personendaten

Die Daten werden von der Auftragsbearbeiterin nur für die vereinbarte Dauer bearbeitet.

10. Sicherheit der Bearbeitung

- 10.1 Die Auftragsbearbeiterin ergreift angemessene technische und organisatorische Massnahmen, um das AWS Netzwerk zu sichern, wie in Ziffer 5.1. des AWS DPA geregelt.
- 10.2 Der Verantwortliche kann gemäss Ziffer 5.2. des AWS DPA technische und organisatorische Massnahmen ergreifen, um die Sicherheit der Personendaten zu gewährleisten.

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 Daten gemäss diesen Klauseln umgehend und in angemessener Weise entsprechend der angebotenen Leistungen der Auftragsbearbeiterin.
- 11.3 Die Auftragsbearbeiterin stellt der Verantwortlichen alle 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.

- 11.4 Zur Erfüllung der Pflichten unter 11.1. und 11.3 stellt die Auftragsbearbeiterin Zertifizierungen und Berichte, wie in Ziffer 10 des AWS DPA beschrieben, zur Verfügung.

12. Audit

Auf Verlangen der Verantwortlichen gestattet die Auftragsbearbeiterin ebenfalls die Prüfung der unter diese Klauseln fallenden Bearbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Prüfung kann die Verantwortliche einschlägige Zertifizierungen der Auftragsbearbeiterin berücksichtigen. Die Einzelheiten des Auditrechts und der Durchführung regelt Ziffer 11 des AWS DPA.

13. Einsatz von Unterauftragsbearbeitern

Die Auftragsbearbeiterin besitzt die allgemeine Genehmigung der Verantwortlichen für die Beauftragung von Unterauftragsbearbeitern, die in einer durch die Auftragsbearbeiterin geführten Liste aufgeführt sind. Einzelheiten zur Änderung, Hinzufügung oder Ersetzung von Unterauftragsbearbeitern, Widerspruchsrechte und Weitergabe der Auftragsbearbeitungspflichten regelt Ziffer 6 des AWS DPA. Soweit die Nutzung der Leistungen nicht ohne den Einsatz eines Unterauftragsbearbeiters möglich ist, mit dem die Verantwortliche nicht einverstanden ist, ist der Verantwortliche berechtigt, die Nutzung der betroffenen Leistung einzustellen oder den Vertrag zu kündigen.

14. Internationale Datenübermittlungen

Für die Übermittlung von Personendaten ausserhalb des EWR oder der Schweiz oder an eine internationale Organisation gelten die Bestimmungen gemäss Abschnitt III (Ziff. 20).

C. Koordination und Compliance

15. Unterstützung der Verantwortlichen

- 15.1 Die Auftragsbearbeiterin unterstützt die Verantwortliche gemäss Ziffer 7 des AWS DPA hinsichtlich der Erfüllung von Rechten von betroffenen Personen.
- 15.2 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“) gemäss Ziffer 10.4 des AWS DPA;
 - b) Gemäss Ziffer 10.4 des AWS DPA: 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;

16. Meldung von Verletzungen der Datensicherheit, allgemeine Bestimmungen

Im Falle einer Verletzung der Datensicherheit (wie im AWS DPA als Security Incident definiert) arbeitet die Auftragsbearbeiterin mit der Verantwortlichen entsprechend Ziffer 9 des AWS DPA zusammen.

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

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 gemäss Ziffer 9 des AWS DPA.

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 gemäss Ziffer 9 des AWS DPA.

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. 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 beenden bzw. einzustellen, 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 oder fortdauernd gegen diese Klauseln verstösst oder ihre Verpflichtungen gemäss DSG oder (bei Auftragsbearbeiterinnen mit Niederlassung in EU/EWR) EU-DSGVO nicht erfüllt;
- 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 zu kündigen bzw. einzustellen, soweit er 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 7.1b) verstossen.

19.4 Nach Beendigung des betroffenen Leistungsabrufs kann die Verantwortliche nach ihrer Wahl alle im Auftrag der Verantwortlichen bearbeiteten Personendaten löschen oder herunterladen, sofern nicht nach geltendem Recht eine Verpflichtung zur Speicherung

der Personendaten durch die Auftragsbearbeiterin besteht oder die Herausgabe nach geltendem Recht nicht erlaubt ist. Die Einzelheiten werden im Anhang Migration und Löschung geregelt. Bis zur Löschung oder Rückgabe der Daten gewährleistet die Auftragsbearbeiterin weiterhin die Einhaltung dieser Klauseln.

III. KLAUSELN BETREFFEND DIE ÜBERMITTLUNG VON PERSONENDATEN INS AUSLAND

20. Übermittlung von Personendaten ins Ausland

20.1 Die Parteien halten fest, dass unter dem Rahmenvertrag Folgendes gilt:

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).

20.2 Für die Übermittlung von Personendaten ausserhalb des EWR oder der Schweiz oder an eine internationale Organisation gelten im Übrigen die Ziffer 12 des AWS DPA, das Supplementary Addendum, die SCC und das Professional Secrecy Addendum.

* * *



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)



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.

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Zur 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 bewirken kann.
- 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.** 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.

2. Sicherheit auf IT-Infrastrukturen der Firma

- 2.1 Die Firma verpflichtet sich, für das AWS Netzwerk das Schutzniveau gemäss Ziff. 2.2 (Mindestschutz) zu 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 Vertragsunterzeichnung 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. Dokumentation «IT- und Datensicherheit»

Die Firma stellt der Vergabestelle auf ihren Portalen und Webseiten konsolidierte Informationen bereit, welche über die Sicherheitsaspekte des Leistungsangebots informieren.

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

- 4.1 Die Firma muss auf ihren Portalen und Webseiten ausdrücklich angeben, inwiefern die Leistungen, die sie unter dem Rahmenvertrag anbietet, die folgenden Standards einhalten und inwiefern für diese (sofern überhaupt möglich) eine Zertifizierung eingeholt wurde:
- a) ISO 27001 (ISMS) einschliesslich ISO 27002
 - b) ISO 27017 (Cloud Security)
 - c) ISO 27018 (Cloud Privacy)
- 4.2 Soweit die Vergabestelle den AWS Enterprise Support bezieht, informiert die Firma die Vergabestelle über den Technical Account Manager nach Möglichkeit über Verzögerungen und Verlust/Aufgabe einer Zertifizierung.
- 4.3 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Zertifikate im Self-Service zur Verfügung.

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

- 5.1 Die Firma muss ausdrücklich angeben, inwiefern für die Leistungen, die sie unter dem Rahmenvertrag anbietet, (sofern überhaupt möglich) einer der folgenden Audit-Berichte eingeholt wurde:
- a) SOC 1 (Type II)
 - b) SOC 2 (Type II)
- 5.2 Soweit die Vergabestelle den AWS Enterprise Support bezieht, informiert die Firma die Vergabestelle über den Technical Account Manager nach Möglichkeit über Verzögerungen und Verlust/Aufgabe eines Auditberichts.
- 5.3 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Audit-Berichte im Self-Service zur Verfügung.
- 5.4 Wenn eine auditierende Stelle eine Beanstandung ausspricht, wird die Firma die Beanstandung adressieren und Massnahmen treffen, um die Beanstandung obsolet zu machen.

6. Verschlüsselte Datenhaltung

- 6.1 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.
- 6.2 Der Bezugsberechtigten stehen Informationen zur Verfügung 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.

7. Verschlüsselte Datenübermittlungen

- 7.1 Die Firma stellt Verschlüsselungstechnologien für elektronische Übermittlung von Daten zur Verfügung, der Kunde ist verantwortlich, dass auch verschlüsselt wird. 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)
- 7.2 Alle Verschlüsselungen bei Übermittlung und Speicherung der Daten erfolgen jeweils mindestens nach dem Standard gem. Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.**

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

- 8.1 Hinsichtlich des Zugriffs und der Nutzung von Daten gelten Ziffern 3.2 des AWS Enterprise Agreements und Ziffer 3 des AWS DPA. Die Firma gewährt ihrem Personal nur insoweit Zugang zum AWS Netzwerk der Bezugsberechtigten die Gegenstand der Bearbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist wie in Ziffer 1.1. der AWS Security Standards beschrieben.
- 8.2 Sofern eine Person Klartextzugriff auf Daten erhält, trifft die Firma Massnahmen, die erlauben, das Ereignis des Klartextzugriffs und den Namen der Person(en), von welchen die Klartextzugriffe ausgegangen sind, namentlich (in Bezug auf die Personen) und konkret (in Bezug auf Datenbestand, Datum etc.) zu protokollieren (Zugriffsprotokolle).
- 8.3 Die Firma gewährleistet, dass sich die zur Bearbeitung der erhaltenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

9. Pflicht zur Überbindung innerhalb der gesamten Organisation und auf Unterauftragsbearbeiter

Hinsichtlich des Einsatzes und der Weitergabe von Pflichten auf Mitarbeiter und Unterverarbeitern gelten Ziffern 4 und 6 des AWS DPA.

* * *



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)

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:

I.	Datenmigration	2
1.	Datenmigration in die IT-Infrastrukturen der Firma.....	2
2.	Anspruch auf Herausgabe	2
3.	Unterstützungsleistungen von Firma betreffend Datenmigration aus den IT-Infrastrukturen der Firma heraus	3
II.	Datenhaltung während der Nutzung	3
4.	Sicherung von Daten.....	3
5.	Wiederherstellung.....	3
6.	Allgemeine Regeln betreffend Datenhaltung.....	3
III.	Datenhaltung nach Beendigung des Leistungsbezugs	3
7.	Definition «Vertragsbeendigung».....	3
8.	Maximale Datenhaltungsdauer.....	3
9.	Koordinationsregeln im Umfeld der Vertragsbeendigung	4
IV.	Datenlöschung.....	4
10.	Unwiderrufliche Löschung	4

Im Einzelnen:

I. Datenmigration

1. Datenmigration in die IT-Infrastrukturen der Firma

- 1.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch bei der Migration von Daten in die IT-Infrastrukturen der Firma auf Grundlage der allgemein durch die Firma verfügbar gemachten Leistungen.
- 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 kann die Kundendaten (Customer Content gemäss Ziffer 13 des AWS Enterprise Agreements) in einem strukturierten, gängigen, maschinenlesbaren und elektronischen Format herunterladen.

- 2.2 Die Kundendaten können während der gesamten Vertragslaufzeit des AWS Enterprise Agreements heruntergeladen werden. Die Einzelheiten regelt Ziffer 7.3. des AWS Enterprise Agreements.

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

- 3.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch bei der Migration von Daten aus den IT-Infrastrukturen der Firma heraus auf Grundlage der allgemein durch die Firma verfügbar gemachten Leistungen.
- 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 ist verpflichtet, dass Kundendaten der Bezugsberechtigten mindestens entsprechend dem Stand der Technik durch die Bezugsberechtigten gesichert werden können.
- 4.2 Es gelten die Service Level Agreements der Firma.

5. Wiederherstellung

- 5.1 Die Firma stellt Methoden zur Wiederherstellung ihrer Daten zur Verfügung, die mindestens dem Stand der Technik entsprechen.
- 5.2 Es gelten die Service Level Agreements der Firma.

6. Allgemeine Regeln betreffend Datenhaltung

- 6.1 Jede Bezugsberechtigte kann den Standort der Datenhaltung im Rahmen des Leistungsangebots der Firma auf eine oder mehrere von der Firma angebotene AWS Region(en) beschränken. Einzelheiten hierzu regelt Ziff. 12.1 des AWS DPA.
- 6.2 Der Datenhaltungsstandort für bezogene Leistungen ist über die AWS Management Console ersichtlich.

III. Datenhaltung nach Beendigung des Leistungsbezugs

7. Definition «Vertragsbeendigung»

Als Vertragsbeendigung im Sinne dieses Abschnitts III. gilt der Zeitpunkt, auf welchen eine Partei den Nutzungsvertrag rechtmässig gekündigt hat oder auf welchen die Bezugsberechtigte den Leistungsbezug eingestellt hat. Einzelheiten hierzu ergeben sich aus Ziffer 7 des AWS Enterprise Agreements.

8. Maximale Datenhaltedauer

- 8.1 Die Firma speichert den Datenbestand der Bezugsberechtigten während **90 Kalendertagen** nach Vertragsbeendigung gemäss Ziff. 7 (maximale Datenhaltedauer; Post-Termination Period)
- 8.2 Die Firma sorgt dafür, dass der Datenbestand der Bezugsberechtigten anschliessend gelöscht wird, und zwar nach Ablauf der maximalen Datenhaltedauer (Ziff. 8.1) nachdem der Kunde die entsprechenden Kundenaccounts geschlossen hat (vgl. Ziff. 7.3. des

AWS Enterprise Agreements und Ziff. 14 des AWS DPA). Die Anforderungen der Datenlöschung ergeben sich aus Abschnitt IV.

9. Koordinationsregeln im Umfeld der Vertragsbeendigung

- 9.1 Ab dem Zeitpunkt der Vertragsbeendigung gemäss Ziff. 8.1 gelten zeitlich gestaffelt das Löschesverbot (gemäss Ziff. 9.2) und dann die Löschpflicht der Firma (gemäss Ziff. 9.3).
- 9.2 Während einer Dauer von 90 Kalendertagen ab Vertragsbeendigung hat die Bezugsberechtigte das Recht, die Kundendaten gemäss Ziff. 2 dieses Vertragsanhangs herunterzuladen. Während dieser Dauer ist es der Firma verboten, die Daten zu löschen (**Löschesverbot**).
- 9.3 Nach Ablauf des Löschesverbots gemäss Ziff. 9.2 ist die Firma verpflichtet, ihrer Pflicht gemäss Ziff. 8.2 nachzukommen (**Löschpflicht**) sofern nicht nach geltendem Recht eine Verpflichtung zur Speicherung der Personendaten durch die Auftragsbearbeiterin besteht. Die Bezugsberechtigte kann die Kundendaten auch früher löschen. Eine frühere Löschung kann sich auch aus Anordnungen von Dritten oder von zuständigen Gerichten ergeben, aufgrund welcher die Bezugsberechtigte zur früheren Löschung der gespeicherten Daten verpflichtet wurde.

IV. Datenlöschung

10. Unwiderrufliche Löschung

- 10.1 Die Verfahren der Firma zur Datenlöschung stellen die Einhaltung der vertraglichen Vereinbarungen sicher.
- 10.2 Die Bezugsberechtigte ist für das Lösches von Daten auf Stufe Applikation und Betriebssystem verantwortlich.
- 10.3 Die Daten der Bezugsberechtigten sind in unterschiedlichen Formen auf Speichermedien der Firma abgelegt. Sie üblichsten Formen sind logische Volumes und Object Storage.
- 10.4 Wird ein logisches Volume von einer Bezugsberechtigten gelöscht, sind die Daten unwiderruflich gelöscht.
- 10.5 Für Speichermedien, die das Ende ihrer Nutzungsdauer erreicht haben, sieht die Firma ein Ausserbetriebnahmeverfahren vor, mit dem verhindert werden soll, dass Unbefugte auf die Kundendaten zugreifen können.
- 10.6 Die Firma entscheidet über das Ende der Nutzungsdauer von Speichermedien.
- 10.7 Die Firma verwendet im Rahmen des Ausserbetriebnahmeverfahrens Prozesse, die in den NIST 800-88 Guidelines for Media Sanitization („Leitlinien für die Lösches von Medien“) festgelegt sind. Sämtliche Produktionsmedien werden in Übereinstimmung mit den Branchenstandards sicher ausser Betrieb genommen. Die Produktionsmedien werden erst dann aus der Firmen-Kontrollumgebung entfernt, nachdem sie sicher ausser Betrieb genommen wurden.
- 10.8 Die Firma überprüft die Wirksamkeit der Lösches und ihrer Löschmethoden regelmässig.
- 10.9 Die entsprechenden Kontrollen und ihre Wirksamkeit werden im ISAE 3000 (Revised) Type 2 Report on Management's Description of the Amazon Web Services, Inc.'s System on German Federal Office for Information Security BSI Cloud Computing Compliance Controls Catalogue (C5) dokumentiert.

* * *



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)



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

- [illegible]

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

* * *



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Vertraulichkeit

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

Der vorliegende Vertragsanhang beschreibt die Vertraulichkeitspflichten der Firma.

Schutzziel des vorliegenden Vertragsanhangs ist das Verhindern von unbefugten Klartextzugriffen und das Verhindern der unbefugten Verwendung von Vertraulichem.

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Vertraulichkeit im Allgemeinen

- 1.1 Die Firma ist verpflichtet, Vertraulichkeit zu gewährleisten.
- 1.2 Die Vertraulichkeitsregelungen bezüglich «Confidential Information» ergeben sich aus dem NDA.
- 1.3 Die Vertraulichkeits- und Sicherheitsregeln bezüglich «Customer Content» ergeben sich aus Ziffer 3 des AWS Enterprise Agreements.
- 1.4 Die Vertraulichkeitsregeln in Bezug auf die Verarbeitung von «Customer Data» ergeben sich aus dem AWS DPA, insbesondere aus Ziffer 3 und 4 des AWS DPA.
- 1.5 Der Vertragsanhang Zugriff auf Daten durch Unberechtigte sowie das AWS Supplementary Addendum enthalten ergänzende Regeln für den Fall von Anfragen von Regierungsstellen.
- 1.6 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. Vertraulichkeitsregeln in Bezug auf diese Regelungen finden sich im AWS Professional Secrecy Addendum.

* * *



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

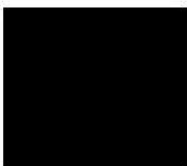
Anhang – Zugriff auf Daten durch Unberechtigte

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 Daten der Bezugsberechtigten. 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. Informations- und Dokumentationspflichten allgemeiner Art

- 1.1 Die Firma stellt der Bezugsberechtigten und der Bedarfsstelle alle nötigen Informationen für den Schutz ihrer IT-Infrastruktur über die AWS Konsole im Self-Service zur Verfügung.
- 1.2 Die Firma unterstützt die Bezugsberechtigte – im Rahmen des «Shared Responsibility» Modells – in angemessenem Umfang darin, Vorsorgeplanungen für allfällige schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben der Bezugsberechtigten gefährden können, zu erstellen.
- 1.3 Die Firma stellt Informationen darüber zur Verfügung, wie oft eine Behörde oder eine Amtsstelle eines ausländischen Staats ein Auskunftersuchen an die Firma gerichtet hat. Solche Information bezieht sich namentlich auf Berichtsperioden wie z.B. «vorangegangenes Jahr» / «vorangegangenes Halbjahr» / «vorangegangenes Quartal».

2. Cybervorfälle (Security Incidents)

- 2.1 Die Firma stellt sicher, dass sie über die nötigen Kapazitäten zur technischen Analyse und zur Bewältigung von Cybervorfällen verfügt, die sie 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.
- 2.2 Die Firma sorgt in ihrem Zuständigkeitsbereich dafür, dass allfällige Risiken für die Informationssicherheit laufend beurteilt werden und informiert die Bezugsberechtigten entsprechend der Regelung in Ziffer 9 des AWS DPA.
- 2.3 Die Firma meldet, soweit sie eine gesetzliche Pflicht trifft, den gesetzlich vorgeschriebenen Stellen unverzüglich Sicherheitsvorfälle, die deren Informatikschutzobjekte betreffen. Im Übrigen hält sich die Firma an die für sie anwendbaren gesetzlichen Meldepflichten in Bezug auf Cybervorfälle.
- 2.4 Die Berichtspflichten für Cybervorfälle (Security Incidents) werden durch Ziffer 9 des AWS DPA konkretisiert.

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

Die Firma verpflichtet sich, den im AWS Supplementary Addendum dargestellten Prozess zu befolgen.

4. Information bei drohender Zahlungsunfähigkeit

Die Firma verpflichtet sich, die Bedarfsstelle bei drohender Zahlungsunfähigkeit unverzüglich zu informieren.

* * *



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vertragswerke der Firma:

AWS Enterprise Agreement

This AWS Enterprise Agreement (this "**Agreement**") is made and entered into by and among Amazon Web Services, EMEA SARL ("**AWS**") and the customer specified on this Cover Page ("**Customer**").

In consideration of the mutual promises contained in this Agreement, AWS and Customer agree to all terms of the Agreement effective as of 1 July 2022 (the "**Effective Date**").

Defined terms used in this Agreement with initial letters capitalized have the meanings given in Section 13 below.

AWS Contracting Party:

Amazon Web Services EMEA SARL

Signature Date: 16.08.2023

Address:

**38 avenue John F. Kennedy,
L-1855 Luxembourg
Attention: AWS General Counsel
Fax: 352 2789 0057**

Customer Name:

The Swiss Confederation, acting through the Federal Office for Buildings and Logistics (Bundesamt für Bauten und Logistik – BBL) for Digital Transformation and ICT Steering (DTI) (hereafter "Customer" or

Address:

**BK-DTI
Bundeskanzlei
Bereich Digitale Transformation und IKT-Lenkung -
DTI
Schwarztörstrasse 53
3003 Bern**

1. Use of the Service Offerings.

1.1 Generally. Customer may access and use the Service Offerings in accordance with this Agreement. Service Level Agreements apply to certain Services. Customer's use of the Service Offerings will comply with the terms of this Agreement.

1.2 AWS Account. To access the Services, Customer must create one or more AWS Enterprise Accounts. Unless explicitly permitted by the Service Terms, Customer will only create one AWS Enterprise Account per email address. All AWS Enterprise Accounts will be covered by this Agreement. For all AWS Enterprise Accounts, this Agreement supersedes any acceptance of the AWS Customer Agreement by Customer or any of its employees acting on behalf of Customer. If any of Customer's AWS accounts do not meet the definition of an "AWS Enterprise Account," those accounts will be governed by the AWS Customer Agreement.

1.3 Third-Party Content. Third-Party Content may be used by Customer at Customer's election. Third-Party Content is governed by this Agreement unless accompanied by separate terms and conditions, which may include separate fees and charges.

1.4 Customer Affiliates. Any Customer Affiliate may use the Service Offerings under its own AWS Enterprise Account(s) under the terms of this Agreement by executing an addendum to this Agreement with AWS substantially in the form of Attachment C to this Agreement. In addition, any other Customer Affiliate covered as described below in this Section 1.4 (each a "Covered Affiliate"), may also use the Service Offerings under its own AWS Enterprise Account(s) under the terms of this Agreement. The AWS Enterprise Accounts of a Covered Affiliate that are governed by this Agreement, as described in this Section 1.4, are AWS accounts that: (a) are opened by the Covered Affiliate using an email address issued by the Covered Affiliate (with an email domain name that is owned by the Covered Affiliate); (b) are joined in an Organization for which a Customer's AWS Enterprise Account is the Management Account for purposes of AWS Organizations (or any successor Service offered by AWS); and (c) include the Covered Affiliate's full legal name in the "Company Name" field associated with the AWS account. Customer represents and warrants that it has the full power and authority to enter into this Agreement and legally bind each Covered Affiliate to the terms of this Agreement. Each Covered Affiliate will be deemed to have entered into a separate agreement with AWS under the same terms and conditions as this Agreement and, for purposes of this separate agreement (other than this Section 1.4 and the last sentence of Section 9.1), will be considered "Customer." If at any time during the Term, a Covered Affiliate no longer meets the definition of an "Affiliate" of Customer, then (i) it will no longer be a Covered Affiliate, and (ii) that former Covered Affiliate and its AWS accounts will no longer be covered under this Agreement (and in the absence of any other agreement between the former Covered Affiliate and AWS, all AWS accounts of such former Customer Affiliate will be governed by the AWS Customer Agreement).

2. Changes.

2.1 To the Service Offerings. AWS may change or discontinue any of the Service Offerings, from time to time. For any AWS Enterprise Accounts enrolled in AWS Support at the Developer-level tier or above (or any successor service providing such communications alerts), AWS will provide at least 12 months prior Notice to Customer if AWS decides to discontinue a Service that it makes generally available to its customers and that Customer is using. AWS will not be obligated to provide Notice under this Section 2.1 if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity.

2.2 To the Service Level Agreements. AWS may change Service Level Agreements from time to time, but will provide 180 days' prior Notice to Customer before materially reducing the benefits offered to Customer under any Service Level Agreement(s) that are available as of the Effective Date.

3. Privacy and Security.

3.1 AWS Security. AWS will implement reasonable and appropriate measures for the AWS Network (as determined by AWS) designed to help Customer secure Customer Content against accidental or unlawful loss, access or disclosure (the "Security Objectives") in accordance with the AWS Security Standards. AWS may modify

the AWS Security Standards from time to time, but will continue to provide at least the same level of security as is described in the AWS Security Standards on the Effective Date.

3.2 Data Privacy. Customer may specify the AWS regions in which Customer Content will be stored. Customer consents to the storage of Customer Content in, and transfer of Customer Content into, the AWS regions Customer selects. AWS will not access or use Customer Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. AWS will not (a) disclose Customer Content to any government or third party, or (b) subject to Section 3.3, move Customer Content from the AWS regions selected by Customer; except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, AWS will give Customer reasonable Notice of any legal requirement or order referred to in this Section 3.2, to enable Customer to seek a protective order or other appropriate remedy. AWS will only use Account Information in accordance with the Privacy Notice, and Customer consents to such usage. The Privacy Notice does not apply to Customer Content.

3.3 Service Attributes. To provide billing and administration services, AWS may process Service Attributes in the AWS region(s) where Customer uses the Service Offerings and the AWS regions in the United States. To provide Customer with support services initiated by Customer and investigate fraud, abuse or violations of this Agreement, AWS may process Service Attributes where AWS maintains its support and investigation personnel.

3.4 AWS Information Security Program. As of the Effective Date, the AWS Information Security Management System (ISMS) is ISO 27001 certified. AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by that certification under ISO 27001 on the Effective Date.

3.5 Audits of Technical and Organizational Measures. Upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will provide to Customer a copy of the AWS System and Organization Controls 1, Type 2 report or such alternative industry standard reports or certifications that are substantially equivalent as reasonably determined by AWS. AWS will make this documentation available to Customer via AWS Artifact (or an alternative means accessible via the AWS Site) and this documentation will be treated as Confidential Information of AWS under the NDA.

3.6 Performance Monitoring and Information. AWS publishes current information on service availability on its Service Health Dashboard on the AWS Site, located at <http://status.aws.amazon.com>, or any successor or related locations designated by AWS; Customer may also personalize the information they receive via the Personal Health Dashboard service. Amazon CloudWatch is a Service that allows Customer to monitor their AWS cloud resources and the applications they run on AWS. Customer may use these resources, as well as other information made available by AWS to obtain information of developments that might impair the proper performance of the outsourced activities and processes.

3.7 Disclosure of Events with Material Adverse Impact. In order to assist Customer with providing notice to a Regulator of developments which may have a material adverse impact on its ability to use the AWS Services ("Adverse Events") AWS will make available the information as set out in this Addendum and the Agreement, including by providing information and support by a technical account manager in case of unplanned Adverse Events as set out in the AWS Support Guidelines, provided Customer is enrolled in AWS Enterprise Support. For the purpose of this Section, "AWS Enterprise Support" means the AWS Support at the Enterprise-level tier (or any successor service providing such communications alerts), and "AWS Support Guidelines" means the guidelines currently available at <https://aws.amazon.com/premiumsupport/plans/enterprise/> (or any successor or related locations designated by AWS), as such guidelines may be updated by AWS from time to time.

3.8 Regulatory Supervision. If a Regulator requires Customer to verify its compliance with applicable laws administered by the Regulator in connection with Customer's use of the Services (a "Request"), then AWS will assist Customer to address the Request as described in this Section.

(a) Information Requests. If Customer cannot satisfy a Request after using commercially reasonable efforts to do so (including by providing available information and documentation and access to the relevant AWS Enterprise



Accounts) and notifies AWS of this condition, AWS will use commercially reasonable efforts to assist Customer to respond to the Request by providing (i) relevant information and documentation regarding the technical and organizational measures of AWS or its Affiliates and about this Agreement, and (ii) for those questions that cannot be satisfied by such information and documentation, if any, a security and compliance briefing by personnel of AWS or its Affiliates.

(b) **On-Site Visit.** Following a notice to AWS by a Regulator confirming its regulatory authority and that the Request cannot be satisfied by means that are less burdensome for AWS including pursuant to Section 3.8(a), AWS will permit a reasonable number of Regulator's compliance personnel or auditors to visit the premises of AWS or its Affiliates (a "Visit") for the purpose of assisting Customer to satisfy the Request. The Visit will be conducted in a manner that reasonably minimizes the disruption on the operations of AWS and its Affiliates.

(c) **Confidentiality and Costs.** Any assistance AWS provides under this Section 3.8 will be subject to AWS's applicable policies and reasonable limits related to safety, security, confidentiality, and maintaining the integrity of the AWS Network. Customer will undertake to obtain confidential treatment or similar protection for any information disclosed to, or gathered by, Regulator under this Section. Customer will reimburse AWS and its Affiliates for their costs and expenses related to a Request.

4. Customer Responsibilities.

4.1 Customer Content. Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Content. Customer agrees that Customer Content will not violate any of the Policies or any applicable law.

4.2 Customer's Security and Redundancy. Customers have a variety of options to choose from when configuring their accounts, and for all sensitive or otherwise valuable content AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings in a manner that provides security and redundancy of its AWS Enterprise Accounts and Customer Content, such as, for example, using enhanced access controls to prevent unauthorized access to AWS Enterprise Accounts and Customer Content, using encryption technology to prevent unauthorized access to Customer Content, and ensuring the appropriate level of backup to prevent loss of Customer Content.

4.3 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for Customer's internal use only and Customer may not sell, transfer or sublicense them to any other entity or person, except that Customer may disclose its private key to its agents and subcontractors (including any of its Affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer. Except to the extent caused by AWS's breach of this Agreement, as between the parties, Customer is responsible for all activities that occur under its AWS Enterprise Accounts.

4.4 End Users. If Customer uses the Services to provide services to, or otherwise interact with, End Users, then Customer, and not AWS, will have the relationships (e.g., via executed contracts between Customer and End Users or via online terms of service) with End Users. Therefore Customer, and not AWS, is responsible for End Users' use of Customer Content and the Service Offerings. To the extent that Customer enables End Users to access the Services or Customer Content, Customer will ensure that all End Users comply with any applicable obligations of Customer under this Agreement and that any terms of any agreement with each End User are not inconsistent with this Agreement. AWS does not provide any support or services to End Users unless AWS has a separate agreement with Customer or an End User obligating AWS to provide support or services to End Users. Customer is responsible for providing customer service (if any) to End Users.

5. Fees and Payment.

5.1 Service Fees. Unless otherwise stated on the AWS Site, AWS will invoice Customer at the end of each month for all applicable fees and charges accrued for use of the Service Offerings, as described on the AWS Site, during the month. The AWS Site lists the prices for the Services applicable to Customer except as otherwise expressly agreed by the Parties. Customer will pay AWS all invoiced amounts within 30 days of the date of the



invoice (other than Disputed Amounts). For any Disputed Amounts, Customer will provide Notice to AWS, including the basis for the dispute (including any supporting documentation), and the parties will meet within 30 days of the date of the Notice to resolve the dispute. If the parties fail to resolve the dispute within such 30 day period, AWS may, at its option, limit (in full or in part) Customer's or any End User's right to access or use the Service Offerings until the dispute is resolved. All amounts payable by Customer under this Agreement will be paid to AWS without setoff or counterclaim and without deduction or withholding, provided that Disputed Amounts will be handled as set forth above. Fees and charges for any new Service or new feature of a Service will be effective when AWS posts updated fees and charges on the AWS Site, unless expressly stated otherwise in a Notice. AWS may increase or add new fees and charges for any existing Service by giving Customer at least 60 days' prior Notice.

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under this Agreement. All fees payable by Customer are exclusive of Indirect Taxes, except where applicable law requires otherwise. AWS may charge and Customer will pay applicable Indirect Taxes that AWS is legally obligated or authorized to collect from Customer. Customer will provide such information to AWS as reasonably required to determine whether AWS is obligated to collect Indirect Taxes from Customer. AWS will not collect, and Customer will not pay, any Indirect Tax for which Customer furnishes AWS a properly completed exemption certificate or a direct payment permit certificate for which AWS may claim an available exemption from such Indirect Tax. All payments made by Customer to AWS under this Agreement will be made free and clear of any deduction or withholding, as may be required by law. If any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, Customer will pay such additional amounts as are necessary so that the net amount received by AWS is equal to the amount then due and payable under this Agreement. AWS will provide Customer with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Agreement.

6. Temporary Limitation of Access and Use Rights. AWS may temporarily limit (in full or in part, as set forth in this Section 6) Customer's or any End User's right to access or use the Service Offerings upon Notice to Customer (which will be reasonable prior notice unless AWS reasonably believes immediate limitation is necessary) if AWS reasonably determines that Customer's or an End User's use of the Service Offerings poses a security risk or threat to the function of the Service Offerings, or poses a security or liability risk or threat to AWS, its Affiliates or any third party. AWS will only limit Customer's right to access or use the instances, data or portions of the Service Offerings that caused the security or liability risk or threat. AWS will restore Customer's access and use rights promptly after Customer has resolved the issue giving rise to the limitation. Customer remains responsible for all fees and charges for the Service Offerings during the period of limitation.

7. Term; Termination.

7.1 Term. The term of this Agreement will commence on the Effective Date and will remain in effect until terminated pursuant to this Agreement. Any Notice of termination of this Agreement must include a Termination Date.

7.2 Termination.

(a) Termination for Convenience. Customer may terminate this Agreement for any reason by providing AWS Notice. AWS may terminate this Agreement for any reason by providing Customer at least two years' Notice.

(b) Termination for Cause.

(i) By Customer or AWS. Either Customer or AWS may terminate this Agreement for cause if the other is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of Notice by the breaching party.

(ii) By AWS. AWS may terminate this Agreement for cause (a) upon 90 days' Notice to Customer if AWS has the right to limit Customer's or any End User's right to access or use the Service Offerings under

Section 6 and Customer has not cured the condition giving rise to that right to limit within such 90 day period, or (b) upon 30 days' Notice to Customer in order to comply with applicable law or requirements of governmental entities.

7.3 Effect of Termination.

(a) Generally. Upon the Termination Date:

- (i) except as provided in Section 7.3(b), all of Customer's rights under this Agreement immediately terminate;
- (ii) Customer remains responsible for all fees and charges Customer has incurred through the Termination Date;
- (iii) Customer will immediately return or, if instructed by AWS, destroy all AWS Content in Customer's possession (except for AWS Content that is publicly available on the AWS Site); and
- (iv) Sections 4, 5, 7.3, 8.1, 8.3, 8.4, 9, 10.3, 11, 12 and 13 will continue to apply in accordance with their terms.

(b) Post-Termination Retrieval of Customer Content. During the 90 days following the Termination Date, AWS will not take action to remove any Customer Content as a result of the termination from any AWS Enterprise Account that is open on the Termination Date. In addition, during such period, AWS will allow Customer to retrieve any remaining Customer Content from the Services, unless (i) prohibited by law or the order of a governmental or regulatory body or it could subject AWS or its Affiliates to liability, or (ii) Customer has not paid all amounts due under this Agreement, other than Disputed Amounts. For any use of the Services during such period, the terms of this Agreement will apply and Customer will pay the applicable fees at the rates under Section 5 (including, without limitation, applicable fees for storage). No later than the end of this 90 day period, Customer will close all AWS Enterprise Accounts.

8. Proprietary Rights.

8.1 Customer Content. As between Customer and AWS, Customer (or Customer's licensors) own all right, title, and interest in and to Customer Content. Except as provided in this Agreement, AWS obtains no rights under this Agreement from Customer (or Customer's licensors) to Customer Content.

8.2 Service Offerings License. AWS or its licensors own all right, title, and interest in and to the Service Offerings, and all related technology and intellectual property rights. Subject to the terms of this Agreement, AWS grants Customer a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to do the following: (a) access and use the Services solely in accordance with this Agreement; and (b) copy and use the AWS Content solely for Customer's permitted use of the Services. Except as provided in this Section 8.2, Customer obtains no rights under this Agreement from AWS, its Affiliates, or their licensors to the Service Offerings, including without limitation any related intellectual property rights. Some AWS Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, which will be identified to Customer in the notice file or on the download page, in which case that license will govern Customer's use of that AWS Content.

8.3 License Restrictions. Neither Customer nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither Customer nor any End User may, or may attempt to (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content included in the Service Offerings (except to the extent Content included in the Service Offerings is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the Service Offerings or apply any other process or procedure to derive the source code of any software included in the Service Offerings, (c) access or use the Service Offerings in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the Service Offerings. Customer may only use the AWS Marks in accordance with the Trademark Use Guidelines. Customer will not misrepresent or embellish the relationship between AWS and Customer (including by expressing or implying that AWS supports, sponsors, endorses, or contributes to Customer or Customer's business endeavors). Customer will not imply any relationship or affiliation between AWS and Customer except as expressly permitted by this Agreement.



8.4 Suggestions. If Customer elects to provide any Suggestions to AWS or its Affiliates, AWS and its Affiliates will be entitled to use the Suggestions without restriction.

9. Third-Party Claims.

9.1 Policies and End User Disputes. Customer will defend, indemnify and hold harmless AWS, its Affiliates, and their respective employees, officers, directors, and representatives against any Losses arising from or related to any third-party claim that arises from a violation of the Policies by Customer or any End User, or that arises from any dispute between Customer and any End User. Customer will also defend, indemnify and hold harmless AWS, its Affiliates, and their respective employees, officers, directors, and representatives against any Losses arising from or related to any third-party claim that arises from any breach by Customer of the representation and warranty in Section 1.4.

9.2 Intellectual Property.

(a) Subject to the limitations in this Section 9, AWS will defend Customer, its Affiliates and its respective employees, officers, and directors against any third-party claim alleging that the Services infringe or misappropriate that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(b) Subject to the limitations in this Section 9, Customer will defend AWS, its Affiliates, and their respective employees, officers, and directors against any third-party claim alleging that any Customer Content infringes or misappropriates that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(c) No party will have obligations or liability under this Section 9.2 arising from infringement by combinations of the Services or Customer Content, as applicable, with any other product, service, software, data, content, or method. In addition, AWS will have no obligations or liability arising from Customer's or any End User's use of the Services after AWS has notified Customer to discontinue such use. The remedies provided in this Section 9.2 are the sole and exclusive remedies for any third-party claims of infringement or misappropriation of intellectual property rights by the Services or by Customer Content.

(d) For any claim covered by Section 9.2(a), AWS will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or this Agreement.

9.3 Process. The obligations under this Section 9 will apply only if the party seeking defense, payment or indemnity from another party: (a) gives that party prompt Notice of the claim; (b) permits that party to control the defense and settlement of the claim; and (c) reasonably cooperates with that party (at that party's expense) in the defense and settlement of the claim. In no event will AWS or Customer agree to any settlement of any claim that involves any commitment, other than the payment of money, without the written consent of the other.

10. AWS Warranties and Warranty Disclaimers.

10.1 AWS Warranties. AWS represents and warrants to Customer that the Services will perform substantially in accordance with the Documentation.

10.2 Mutual Warranties. Customer and AWS each represents and warrants to the other that (a) it has full power and authority to enter into and perform this Agreement, (b) the execution and delivery of this Agreement has been duly authorized, (c) it will comply with all applicable laws, rules, regulations and ordinances in the performance of this Agreement (and, in the case of Customer, the use of the Service Offerings), and (d) its performance hereunder does not breach any other agreement to which it is bound.

10.3 Warranty Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 10.1 AND SECTION 10.2, AND EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS, ITS AFFILIATES AND ITS LICENSORS MAKE NO



REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND DISCLAIM ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (A) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (B) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (C) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (D) THAT ANY CONTENT, INCLUDING CUSTOMER CONTENT OR THIRD-PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

11. Limitations of Liability.

11.1 Liability Disclaimers. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9.1, OR DAMAGES FOR GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, NEITHER PARTY NOR ANY OF THEIR AFFILIATES OR LICENSORS WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, (B) THE VALUE OF CUSTOMER CONTENT, (C) LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, OR (D) UNAVAILABILITY OF THE SERVICE OFFERINGS (THIS DOES NOT LIMIT ANY SERVICE CREDITS THAT MAY BE AVAILABLE UNDER SERVICE LEVEL AGREEMENTS).

11.2 Damages Cap. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9, OR DAMAGES FOR GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, THE AGGREGATE LIABILITY UNDER THIS AGREEMENT OF EITHER AWS OR CUSTOMER, AND ANY OF THEIR RESPECTIVE AFFILIATES OR LICENSORS, WILL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO AWS UNDER THIS AGREEMENT FOR THE SERVICES THAT GAVE RISE TO THE LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE; PROVIDED, HOWEVER THAT NOTHING IN THIS SECTION 11 WILL LIMIT CUSTOMER'S OBLIGATION TO PAY AWS FOR CUSTOMER'S USE OF THE SERVICE OFFERINGS PURSUANT TO SECTION 5, OR ANY OTHER PAYMENT OBLIGATIONS UNDER THIS AGREEMENT.

12. Miscellaneous.

12.1 Assignment. Neither Customer nor AWS may assign or otherwise transfer this Agreement or any of its rights and obligations under this Agreement without the prior written approval of the other; except that either Customer or AWS may assign or otherwise transfer this Agreement without the consent of the other (a) in connection with a merger, acquisition or sale of all or substantially all of its assets, or (b) to any Affiliate or as part of a corporate reorganization, or (c) in the case of AWS, with respect to specific AWS Enterprise Accounts, to an Affiliate. Effective upon such assignment or transfer, subject to the assignee/transferee's consent, the assignee/transferee is deemed substituted for the assignor/transferor as a party to this Agreement and the assignor/transferor is fully released from all of its obligations and duties to perform under this Agreement. Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective permitted successors and assigns.

12.2 Counterparts; Facsimile. This Agreement may be executed by facsimile or by electronic signature in a format approved by AWS, and in counterparts, each of which (including signature pages) will be deemed an original, but all of which together will constitute one and the same instrument.

12.3 Entire Agreement. This Agreement incorporates the Policies and the AWS Contracting Party Site by reference and is the entire agreement between Customer and AWS regarding the subject matter of this Agreement. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS, whether written or verbal, regarding the subject matter of this Agreement (including, as set forth in Section 1.2, any acceptance of the AWS Customer Agreement by Customer or any of its employees acting on behalf of Customer). AWS will not be bound by any term, condition or other provision which is different from or in addition to the provisions of this Agreement (whether or not it would materially alter this Agreement) including for example, any term, condition or other provision (a) submitted by Customer in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other questionnaire, or (c) related to any invoicing process that Customer submits or requires AWS to complete except for the General Terms and Conditions for IT Services of the Swiss Confederation (Allgemeine Geschäftsbedingungen des Bundes (AGB) für Informatikdienstleistungen (Ausgabe Oktober 2010, Stand Juni 2019) (the "GTC" Attachment



C). If the terms of this document are inconsistent with the terms contained in any Policy, the GTC or the AWS Contracting Party Site, the terms contained in this document will control, except that (i) the Service Terms will control over this document and (ii) the AWS Contracting Party Site will control over this document with respect to any AWS Enterprise Accounts associated with an AWS Contracting Party that is added to this Agreement pursuant to Section 12.14. No modification or amendment of any portion of this Agreement will be effective unless in writing and signed by the parties to this Agreement.

12.4 Force Majeure. Except for payment obligations, no party will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond its reasonable control, including acts of God, labor disputes or other industrial disturbances, electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

12.5 Governing Law; Venue. The laws of Switzerland, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between the parties. Any dispute relating in any way to the Service Offerings or this Agreement (including a breach of Section 9) will only be adjudicated in the courts of the City of Bern. Each party consents to exclusive jurisdiction and venue in these courts. Notwithstanding the foregoing, either party may seek injunctive relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of such party's, its Affiliates' or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

12.6 Trade Compliance. In connection with this Agreement, each party will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. Customer is solely responsible for compliance with applicable laws related to the manner in which Customer chooses to use the Service Offerings, including (i) Customer's transfer and processing of Customer Content, (ii) the provision of Customer Content to End Users, and (iii) specifying the AWS region in which any of the foregoing occur. Customer represents that Customer and the entities that own or control Customer, and the financial institutions used to pay AWS under this Agreement, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the U.S. Department of Treasury's Specially Designated Nationals list and Foreign Sanctions Evaders list, and the U.S. Department of Commerce's Entity List), the European Union or its member states, or other applicable government authority.

12.7 Independent Contractors. AWS and Customer are independent contractors, and this Agreement will not be construed to create a partnership, joint venture, agency, or employment relationship. Neither Customer nor AWS, nor any of their respective Affiliates, is an agent of the other for any purpose or has the authority to bind the other.

12.8 Language. All communications and Notices made or given pursuant to this Agreement must be in the English language. If AWS provides a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

12.9 Nondisclosure; Publicity. If the parties have an NDA, then the NDA is incorporated by reference into this Agreement, except that the security provisions in Section 3, not the NDA, apply to Customer Content. Except to the extent permitted by applicable law, neither Customer nor AWS will issue any press release or make any other public communication with respect to this Agreement or Customer's use of the Service Offerings. AWS and Customer agree that the contents of this Agreement are not publicly known and will not be disclosed by them.

12.10 Notice.

(a) General. Except as otherwise set forth in Section 12.10(b), to give notice to a party under this Agreement, each party must contact that other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the fax number of the other party listed on the Cover Page to this Agreement or addressed to the address of the other party listed on the Cover



Page to this Agreement (or in the case of any AWS Contracting Party that is added to this Agreement pursuant to Section 12.14, to such fax number or address provided on the AWS Contracting Party Site), or such other fax number or address as a party may subsequently provide in writing to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.

(b) Electronic Notice. AWS may provide notice to Customer (i) under Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Attachment A by sending a message to the email address then associated with Customer's applicable AWS Enterprise Account, and (iii) under Section 2.1 by sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.

12.11 No Third-Party Beneficiaries. Except as set forth in Section 9, this Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to this Agreement.

12.12 No Waivers. The failure by a party to enforce any provision of this Agreement will not constitute a present or future waiver of such provision nor limit such party's right to enforce such provision at a later time. All waivers by a party must be provided in a Notice to be effective.

12.13 Severability. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect. Any invalid or unenforceable portions will be interpreted to give effect to the intent of the original portion. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement but the rest of the Agreement will remain in full force and effect.

12.14 Account Servicing; Addition of AWS Contracting Parties. The AWS Contracting Party for each AWS Enterprise Account is identified on the AWS Contracting Party Site and is determined based on the geographic location associated with each such account. The AWS Contracting Party for each AWS Enterprise Account is solely responsible for providing the Service Offerings and for all of AWS's obligations under this Agreement for each such account. If the geographic location associated with a new or existing AWS Enterprise Account is set or changed to a location that corresponds to a party on the AWS Contracting Party Site that is not yet a party to this Agreement, then such party independently offers the terms of this Agreement (including any applicable terms that may be specified on the AWS Contracting Party Site) to Customer. Unless Customer is notified otherwise by AWS, such party will be added to this Agreement as an AWS Contracting Party as of the date of the setting or change, without any further action required by the parties.

12.15 Dispute Resolution. The following process applies when there is a dispute between the parties relating to this Agreement:

- (a) Either party can, by giving written Notice to the other party (an "Escalation Notice"), request a meeting of the Executive Sponsors to resolve a dispute between the parties. For purposes of this Section 12.15, "Executive Sponsors" means an AWS Head of Germany, Austria, Switzerland Public Sector and the Customer Head of COGIS (Vice Director of Bundesamt für Bauten und Logistik (*Vizedirektion (BBL)*)).
- (b) The Escalation Notice will describe the nature of the dispute, the initiating party's position, and a summary of the information supporting the position and will reference this Agreement and the dispute resolution process in this Section. The party receiving the Escalation Notice will send the other party a response to the Escalation Notice within 30 days of receipt of the Escalation Notice.
- (c) The Executive Sponsors will meet within 30 days of receipt of the Escalation Notice (or such longer period as may be agreed between them) to discuss and attempt to resolve the dispute. Such meeting will be conducted at a reasonable time to be agreed between the parties and may be carried out by telephone.

Neither party may commence proceedings with respect to a dispute escalated under this Section until after the Executive Sponsors have met to attempt to resolve the dispute. Notwithstanding the foregoing, this Section 12.15 will not prevent either party from seeking urgent interlocutory relief or exercising any of its rights under this

Agreement (including without limitation any right to suspend Customer's access to the Services or terminate the Agreement) at any time

12.16 International Labour Organisation Core Conventions. AWS will respect the Core Conventions of the International Labour Organisation set out in Attachment C of the Agreement ("**ILO Core Conventions**"), provided that Customer's sole and exclusive remedy for AWS's failure to comply with the ILO Core Conventions is termination of this Agreement. This Section 12.16 will not survive termination of the Agreement for any reason.

12.17 Bribery and Corruption. Compliance with applicable laws in relation to bribery and corruption is a matter of fundamental importance for Customer. AWS's Code of Business Conduct and Ethics (as of the Effective Date, located at <http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-govConduct>) prohibits the paying of bribes to anyone for any reason, whether in dealings with governments or the private sector. Each of the parties therefore agrees to act in accordance with all laws applicable to it relating to bribery and corruption during the Term.

13. Definitions. Defined terms used in this Agreement with initial letters capitalized have the meanings given below:

"Acceptable Use Policy" means the policy located at <http://aws.amazon.com/aup> (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.

"Account Information" means information about Customer that Customer provides to AWS in the creation or administration of an AWS Enterprise Account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with an AWS Enterprise Account.

"Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with that party.

"API" means an application program interface.

"AWS Content" means Content that AWS or any of its Affiliates makes available related to the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept, templates, and other related technology (including but not limited to any of the foregoing that are provided by any AWS personnel). AWS Content does not include the Services or Third-Party Content.

"AWS Contracting Party" means each party identified on the AWS Contracting Party Site that is or becomes a party to this Agreement.

"AWS Contracting Party Site" means <https://aws.amazon.com/legal/aws-contracting-party> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"AWS Customer Agreement" means AWS's standard user agreement located on the AWS Site at <http://aws.amazon.com/agreement> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"AWS Enterprise Account" means any AWS account that (a) is opened by Customer using a Customer-issued email address (with an email domain name that is owned by Customer), (b) includes Customer's full legal name in the "Company Name" field associated with the AWS account, and (c) is associated with a location in Europe, the Middle East, or Africa. AWS determines the location associated with each AWS Enterprise Account in the manner described on the AWS Site. A list of the countries and territories located in Europe, the Middle East, or Africa for purposes of this definition is available on the AWS Site."

"AWS Marks" means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its Affiliates that AWS may make available to Customer in connection with this Agreement.

"AWS Network" means AWS's data center facilities, servers, networking equipment, storage media, and host software systems (e.g., virtual firewalls) that are within AWS's control and are used to provide the Services.

"AWS Security Standards" means the security standards attached to this Agreement as Attachment B.



"AWS Site" means <http://aws.amazon.com> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Content" means software (including machine images), data, text, audio, video, or images.

"Customer Content" means Content that Customer or any End User transfers to AWS for processing, storage or hosting by the Services in connection with an AWS Enterprise Account and any computational results that Customer or any End User derive from the foregoing through its use of the Services. For example, Customer Content includes Content that Customer or any End User stores in Amazon Simple Storage Service. Customer Content does not include Account Information.

"Disputed Amounts" means amounts disputed by Customer in a Notice and in good faith as billing errors.

"Documentation" means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at <http://aws.amazon.com/documentation> (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time.

"End User" means any individual or entity that directly or indirectly through another user (a) accesses or uses Customer Content, or (b) otherwise accesses or uses the Service Offerings under an AWS Enterprise Account. The term "End User" does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than under an AWS Enterprise Account.

"Indirect Taxes" means applicable taxes and duties, including, without limitation, VAT, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

"Losses" means any damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees).

"NDA" means the Mutual Nondisclosure Agreement between Customer and Amazon Web Services EMEA SARL, dated 1 January 2019.

"Notice" means any notice provided in accordance with Section 12.10.

"Policies" means the Acceptable Use Policy, Privacy Notice, and the Service Terms.

"Privacy Notice" means the privacy notice located at <http://aws.amazon.com/privacy> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Regulator" means a government or regulatory body with binding authority to regulate Customer's services activities; provided, that the term Regulator does not include any regulatory body or instrumentality of Iran, North Korea, the People's Republic of China or of any country that is subject to embargo or sanction by the United States as administered by the Office of Foreign Assets Control (OFAC).

"Service" means each of the services made available by AWS or its Affiliates for which Customer registers via the AWS Site (or by such other means made available by AWS), including those web services described in the Service Terms. Services do not include Third-Party Content.

"Service Attributes" means Service usage data related to an AWS Enterprise Account, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics.

"Service Level Agreement" means all service level agreements that AWS offers with respect to the Services and post on the AWS Site, as they may be updated by AWS from time to time. The service level agreements that AWS offers with respect to the Services are located at <https://aws.amazon.com/legal/service-level-agreements> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Service Offerings" means the Services, the AWS Content, the AWS Marks, and any other product or service provided by AWS under this Agreement. Service Offerings do not include Third-Party Content.

"Service Terms" means the rights and restrictions for particular Services located at <http://aws.amazon.com/serviceterms> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Suggestions" means all suggested improvements to the Service Offerings that Customer provides to AWS.



"Term" means the term of this Agreement described in Section 7.1.

"Termination Date" means the effective date of termination provided in a Notice in accordance with Section 7.

"Third-Party Content" means Content of a third party made available on the AWS Marketplace or on developer forums, sample code repositories, public data repositories, community-focused areas of the AWS Site, or any other part of the AWS Site that allows third parties to make available software, products, or data.

"Trademark Use Guidelines" means the guidelines and trademark license located at <http://aws.amazon.com/trademark-guidelines/> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.



Attachment A

AWS Account ID(s):

The list above includes any Master Account or Member Accounts joined to such accounts via AWS Organizations, as described in the Service Terms.

Customer may add AWS accounts to the list above or remove AWS accounts from the list above by providing notice to AWS via email to enterprise-accounts@amazon.com, that includes (1) Customer's full name, (2) the Enterprise Agreement number (which begins with "CC" and is found on the upper right corner of each page of this Agreement), and (3) the AWS Account ID of each added or removed AWS account. Upon Notice, AWS may replace the notification process or make available another means of adding and removing AWS accounts to the list above.



Attachment B
AWS Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable AWS Enterprise Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Affiliate Addendum to the AWS Enterprise Agreement

This Affiliate Addendum (this "**Addendum**") by and among ("Customer Affiliate"), ("Customer"), the AWS Contracting Parties identified in the signature blocks below, and any other AWS Contracting Party that is added to the Agreement pursuant to Section 2 of this Addendum (the "**Amazon Parties**"), is an addendum to the AWS Enterprise Agreement or AWS Enterprise Customer Agreement, as applicable, dated_, between Customer and the applicable Amazon Parties (the "**Agreement**"). This Addendum is effective as of the date the last party signs below (the "**Addendum Effective Date**"). Unless otherwise defined in this Addendum, all capitalized terms in this Addendum have the meanings set forth in the Agreement.

As of the Addendum Effective Date, the terms of the Agreement will apply to AWS Enterprise Accounts opened by Customer Affiliate, subject to the following:

1. **Customer Affiliate.** With respect to Customer Affiliate's AWS Enterprise Accounts, Customer Affiliate (a) is responsible for Customer's obligations and liabilities under the Agreement, and (b) assumes Customer's rights under the Agreement.
2. **Affiliate Status.** Customer Affiliate represents and warrants that it is an Affiliate of Customer. If Customer Affiliate ceases to be an Affiliate of Customer, Customer Affiliate will promptly provide written notice to AWS, and AWS may terminate this Addendum upon written notice to Customer Affiliate. Following such termination, continued use of Customer Affiliate's AWS Enterprise Accounts will be governed by the AWS Customer Agreement (located at <https://aws.amazon.com/agreement/>) unless Customer Affiliate and AWS have entered into another written agreement that applies to that usage.
3. **Account Servicing; Addition of AWS Contracting Parties.** The AWS Contracting Party for each of Customer Affiliate's AWS Enterprise Accounts is identified on the AWS Contracting Party Site and is determined based on the geographic location associated with each such account. The AWS Contracting Party for each of Customer Affiliate's AWS Enterprise Accounts is solely responsible for providing the Service Offerings and for all of AWS's obligations under the Agreement for each such account. If the geographic location associated with any of Customer Affiliate's new or existing AWS Enterprise Accounts is set or changed to a location that corresponds to a party on the AWS Contracting Party Site that is not yet a party to this Addendum, then such party independently offers the terms of the Agreement (including any applicable terms that may be specified on the AWS Contracting Party Site) to Customer Affiliate. Unless Customer Affiliate is notified otherwise by AWS, such party will be added to this Addendum as an AWS Contracting Party as of the date of the setting or change, without any further action required by the parties. With respect to specific AWS Enterprise Accounts, AWS may transfer the Agreement to AWS's Affiliates, without the consent of Customer or Customer Affiliate.
4. **AWS Enterprise Account.** For purposes of this Addendum, "**AWS Enterprise Account**" means any AWS account that (1) is listed on Attachment 1 to this Addendum, as that list may be updated from time to time as described in Attachment 1, (2) is opened by Customer Affiliate using a Customer Affiliate-issued email address (with an email domain name that is owned by Customer Affiliate), and (3) includes Customer Affiliate's full legal name in the "Company Name" field associated with the AWS



account, and (d) is associated with a geographic location that corresponds to an AWS Contracting Party that is party to the Agreement.

5. **Nondisclosure.** The existence and terms of this Addendum are not publicly known and will not be disclosed by the parties.

6. **Entire Agreement.** As between Customer Affiliate and the Amazon Parties, this Addendum, together with the Agreement (a) is the final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between them, with respect to the subject matter hereof. If there is a conflict between the provisions of the Agreement and this Addendum, the terms of this Addendum will control with respect to Customer Affiliate. Except as expressly provided herein, nothing in this Addendum will be deemed to waive or modify any of the provisions of the Agreement, or any amendment or addendum thereto.

7. **Counterparts and Facsimile Delivery.** This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this Addendum by facsimile or by electronic signature in a format approved by AWS.

[Remainder of Page Intentionally Left Blank]



Attachment 1

AWS Account ID(s):

The list above include any Master Account or Member Accounts joined to such accounts via AWS Organizations, as described in the Service Terms.

Customer Affiliate may add AWS accounts to the list above or remove AWS accounts from the list above by providing notice to AWS via email to enterprise-accounts@amazon.com, that includes (1) Customer Affiliate's full name, (2) the Affiliate Addendum number (which begins with "CC" and is found on the upper right corner of each page of this Addendum), and (3) the AWS Account ID of each added or removed AWS account. Upon Notice, AWS may replace the notification process or make available another means of adding and removing AWS accounts to the list above.



Attachment D
Core Conventions of the
International Labour Organisation

- Convention No. 29 of 28 June 1930 on forced or compulsory labour (SR 0.822.713.9);
- Convention No. 87 of 9 July 1948 on the freedom of association and protection of the right to organise (SR 0.822.719.7);
- Convention No. 98 of 1 July 1949 on the application of the principles of the right to organise and the right to collective bargaining (SR 0.822.719.9);
- Convention No. 100 of 29 June 1951 on equal remuneration between men and women for equal work (SR 0.822.720.0);
- Convention No. 105 of 25 June 1957 on the abolition of forced labour (SR 0.822.720.5);
- Convention No. 111 of 25 June 1958 on discrimination in employment and occupation (SR 0.822.721.1);
- Convention No. 138 of 26 June 1973 on the minimum age for employment (SR 0.822.723.8);
- Convention No. 182 of 17 June 1999 on the prohibition of and immediate measures to abolish the worst forms of child labour (SR 0.822.728.2).



AWS GDPR DATA PROCESSING ADDENDUM: SWITZERLAND

This Data Processing Addendum (this "Addendum") is effective as of 1 July 2022 (the "Addendum Effective Date") and is entered into by and among Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together "AWS") and the customer specified on the signature page ("Customer"). This Addendum supplements the AWS Enterprise Agreement between Customer and AWS, dated of 1 July 2022, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "Agreement"). Unless otherwise defined in this Addendum or in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them in Section 19 of this Addendum.

1. Data Processing.

- 1.1 Scope and Roles.** This Addendum applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.
- 1.2 Customer Controls.** Customer can use the Service Controls to assist it with its obligations under the GDPR and the DSG, as applicable, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.
- 1.3 Details of Data Processing.**
 - 1.3.1 Subject matter.** The subject matter of the data processing under this Addendum is Customer Data.
 - 1.3.2 Duration.** As between AWS and Customer, the duration of the data processing under this Addendum is determined by Customer.
 - 1.3.3 Purpose.** The purpose of the data processing under this Addendum is the provision of the Services initiated by Customer from time to time.
 - 1.3.4 Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
 - 1.3.5 Type of Customer Data.** Customer Data uploaded to the Services under Customer's AWS accounts.
 - 1.3.6 Categories of data subjects.** The data subjects could include Customer's customers, employees, suppliers and End Users.
- 1.4 Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including the GDPR and the DSG.



- 5.2 Customer can elect to implement technical and organisational measures to protect Customer Data. Such technical and organisational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third party supplier:
- (a) pseudonymisation and encryption to ensure an appropriate level of security;
 - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;
 - (c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by Customer. .
- 5.3 Taking into account the nature of the processing and the information available to AWS, AWS assists Customer in complying with its obligations pursuant to Article 32 of the GDPR by:
- (a) implementing and maintaining the AWS Security Standards in accordance with Section 5.1; and
 - (b) making the technical and organisational measures described in Section 5.2 available to Customer.

6. Sub-processing.

- 6.1 **Authorised Sub-processors.** Customer provides general authorisation to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("Sub-processors") in accordance with this Section. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another AWS Region where AWS has not engaged the Sub-processor.
- 6.2 **Sub-processor Obligations.** Where AWS authorises a Sub-processor as described in Section 6.1:
- (i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;
 - (ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this Addendum, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this Addendum; and



service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

- (ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

10. AWS Certifications and Audits.

10.1 AWS ISO-Certification and SOC Reports. In addition to the information contained in this Addendum, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

- (i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and
- (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 AWS Audits. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be AWS's Confidential Information.

10.3 Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this Addendum.

10.4 Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.

11. Customer Audits. Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR, the DSG or the Standard Contractual Clauses, by instructing



controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.

- 12.3 Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Data Transfers.
- 12.4 Transfers from Switzerland to a Third Country.** The following is deemed added to Annex 3 of the Standard Contractual Clauses where Customer Data is transferred from Switzerland to a Third Country:
- (i) Where the Clauses refer to Member States, they shall be read to refer to Switzerland.
 - (ii) Where the Clauses refer to applicable data protection law or the GDPR, they shall be read to refer to the Swiss Federal Act on Data Protection (as revised from time to time).
 - (iii) The reference to the courts of the Member State in Clause 18 (c) shall be read to refer to the Swiss courts for the place where the data subject has his/her habitual residence.
 - (iv) In accordance with Clause 13, the reference to the competent supervisory authority in Annex I.C. shall be read to refer to the Swiss Federal Data Protection and Information Commissioner.
- 13. Termination of the Addendum.** This Addendum will continue in force until the termination of the Agreement (the "Termination Date").
- 14. Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.
- 15. Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.
- 16. Nondisclosure.** Customer agrees that the details of this Addendum are not publicly known and constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting AWS Confidential Information and Customer and AWS or its Affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.
- 17. Entire Agreement; Conflict.** This Addendum incorporates the Standard Contractual Clauses by reference. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS,



"Security Incident" means a breach of AWS's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

"Third Country" means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

[Remainder of page intentionally left blank]



Annex 1

AWS Security Standards

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and



AWS GDPR DATA PROCESSING ADDENDUM: SWITZERLAND

This Data Processing Addendum (this “**Addendum**”) is effective as of 1 July 2022 (the “**Addendum Effective Date**”) and is entered into by and among Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together “**AWS**”) and the customer specified on the signature page (“**Customer**”). This Addendum supplements the AWS Enterprise Agreement between Customer and AWS, dated of 1 July 2022, or other agreement between Customer and AWS governing Customer’s use of the Service Offerings (the “**Agreement**”). Unless otherwise defined in this Addendum or in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them in Section 19 of this Addendum.

1. **Data Processing.**

- 1.1 **Scope and Roles.** This Addendum applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.
- 1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under the GDPR and the DSG, as applicable, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.
- 1.3 **Details of Data Processing.**
 - 1.3.1 **Subject matter.** The subject matter of the data processing under this Addendum is Customer Data.
 - 1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this Addendum is determined by Customer.
 - 1.3.3 **Purpose.** The purpose of the data processing under this Addendum is the provision of the Services initiated by Customer from time to time.
 - 1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
 - 1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer’s AWS accounts.
 - 1.3.6 **Categories of data subjects.** The data subjects could include Customer’s customers, employees, suppliers and End Users.
- 1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including the GDPR and the DSG.



2. **Customer Instructions.** The parties agree that this Addendum and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Data ("**Documented Instructions**"). AWS will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this Addendum and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this Addendum. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe the GDPR. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.
3. **Confidentiality of Customer Data.** AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will ask the governmental body to request that data directly from Customer, unless AWS is legally prohibited from doing so. As part of this effort, AWS may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.
4. **Confidentiality Obligations of AWS Personnel.** AWS restricts its personnel from processing Customer Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
5. **Security of Data Processing**
 - 5.1 AWS has implemented and will maintain the technical and organisational measures for the AWS Network as described in the AWS Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organisational measures:
 - (a) security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;
 - (b) physical security of the facilities as set out in Section 1.2 of the AWS Security Standards;
 - (c) measures to control access rights for AWS employees and contractors for to the AWS Network as set out in Section 1.1 of the AWS Security Standards; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by AWS as described in Section 2 of the AWS Security Standards.



- 5.2 Customer can elect to implement technical and organisational measures to protect Customer Data. Such technical and organisational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third party supplier:
- (a) pseudonymisation and encryption to ensure an appropriate level of security;
 - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;
 - (c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by Customer. .
- 5.3 Taking into account the nature of the processing and the information available to AWS, AWS assists Customer in complying with its obligations pursuant to Article 32 of the GDPR by:
- (a) implementing and maintaining the AWS Security Standards in accordance with Section 5.1; and
 - (b) making the technical and organisational measures described in Section 5.2 available to Customer.

6. Sub-processing.

- 6.1 **Authorised Sub-processors.** Customer provides general authorisation to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("Sub-processors") in accordance with this Section. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another AWS Region where AWS has not engaged the Sub-processor.
- 6.2 **Sub-processor Obligations.** Where AWS authorises a Sub-processor as described in Section 6.1:
- (i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;
 - (ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this Addendum, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this Addendum; and



- (iii) AWS will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this Addendum.

7. AWS Assistance with Data Subject Requests. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR and DSG, as applicable. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorises on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. Optional Security Features. AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorised access and measures to control access rights to Customer Data.

9. Security Incident Notification.

9.1 Security Incident. AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 AWS Assistance. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 Unsuccessful Security Incidents. Customer agrees that:

- (i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of



service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

- (ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

10. AWS Certifications and Audits.

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this Addendum, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

- (i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and
- (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be AWS's Confidential Information.

10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this Addendum.

10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.

11. **Customer Audits.** Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR, the DSG or the Standard Contractual Clauses, by instructing



AWS to carry out the audit described in Section 10. The parties acknowledge that under certain circumstances it might be legally mandatory for Customer to demonstrate compliance with the GDPR by means other than reviewing the Report, including for example being provided with additional information, being briefed on specific security issues, or visiting AWS's premises. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement and change the instruction as follows:

- (i) Customer will submit a request for additional information in writing to AWS, specifying such details as may be needed to enable AWS to review this request effectively, including what information is being requested, in what form Customer needs to obtain it and what is the underlying legal requirement for the request (the "Request").
- (ii) (Within a reasonable time after AWS has received and reviewed the Request, the parties will discuss and work in good faith towards agreeing on a plan to determine the details of how the Request can be addressed. The parties agree to use the least intrusive means for AWS to verify AWS's compliance with its obligations under this Addendum, taking into account the applicable legal requirements and the urgency of the matter as well as the need for AWS to maintain the security of its facilities, maintain uninterrupted business operation, protect itself and its customers from risk and to prevent disclosure of information that would jeopardise the confidentiality of AWS information. The parties agree that this Section 11 does not restrict any statutory rights a competent supervisory authority may have under applicable law to perform audits based on a valid and binding order.
- (iii) Any information and documentation provided by AWS or its auditors in relation to this Section will be provided at Customer's cost and will constitute AWS's Confidential Information under the confidentiality provisions of the Agreement.

If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

12. Transfers of Personal Data.

- 12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "Region"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.
- 12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, from the EEA to any Third Country, (each a "Data Transfer").
 - 12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
 - 12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's



controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.

- 12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Data Transfers.
- 12.4 **Transfers from Switzerland to a Third Country.** The following is deemed added to Annex 3 of the Standard Contractual Clauses where Customer Data is transferred from Switzerland to a Third Country:
- (i) Where the Clauses refer to Member States, they shall be read to refer to Switzerland.
 - (ii) Where the Clauses refer to applicable data protection law or the GDPR, they shall be read to refer to the Swiss Federal Act on Data Protection (as revised from time to time).
 - (iii) The reference to the courts of the Member State in Clause 18 (c) shall be read to refer to the Swiss courts for the place where the data subject has his/her habitual residence.
 - (iv) In accordance with Clause 13, the reference to the competent supervisory authority in Annex I.C. shall be read to refer to the Swiss Federal Data Protection and Information Commissioner.
13. **Termination of the Addendum.** This Addendum will continue in force until the termination of the Agreement (the "Termination Date").
14. **Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.
15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.
16. **Nondisclosure.** Customer agrees that the details of this Addendum are not publicly known and constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting AWS Confidential Information and Customer and AWS or its Affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.
17. **Entire Agreement; Conflict.** This Addendum incorporates the Standard Contractual Clauses by reference. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS,



whether written or verbal, regarding the subject matter of this Addendum, including any data processing addenda entered into between Amazon Web Services, Inc. and Customer containing terms and conditions about Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control. Nothing in this document varies or modifies the Standard Contractual Clauses.

18. **Counterparts and Facsimile or Email Delivery.** This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties deliver this Addendum by facsimile or email transmission.

19. **Definitions.** Unless otherwise defined in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them below:

"AWS Network" means AWS's data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services.

"AWS Security Standards" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this Addendum as Annex 1.

"controller" has the meaning given to it in the GDPR.

"Controller-to-Processor Clauses" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Controller to Processor SCCs.pdf](https://d1.awsstatic.com/Controller%20to%20Processor%20SCCs.pdf).

"Customer Data" means the "personal data" (as defined in the GDPR and the DSG) that is uploaded to the Services under Customer's AWS accounts.

"DSG" means the Swiss Federal Act on Data Protection (Bundesgesetz über den Datenschutz) or any succeeding Swiss data protection law replacing the Swiss Federal Act on Data Protection.

"EEA" means the European Economic Area. For purposes of this Addendum, the EEA also includes Switzerland.

"GDPR" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"processing" has the meaning given to it in the GDPR and DSG "process", "processes" and "processed" will be interpreted accordingly.

"processor" has the meaning given to it in the GDPR.

"Processor-to-Processor Clauses" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Processor to Processor SCCs.pdf](https://d1.awsstatic.com/Processor%20to%20Processor%20SCCs.pdf).



"Security Incident" means a breach of AWS's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

"Third Country" means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

[Remainder of page intentionally left blank]



Amazon Web Services EMEA SARL [Redacted]	<u>Customer:</u> The Swiss Confederation, acting through the Federal Office for Buildings and Logistics (hereinafter "FOBL" or "Procurement agency") for Digital Transformation and ICT Steering (DTI) (hereafter "Customer" or [Redacted]
Date Signed: 16.08.2022	Date Signed: 04.07.2022
[Redacted]	[Redacted]
	Date Signed: 9.7.2022
	[Redacted]
	Date Signed: 5.7.2022
	[Redacted]
Address: 38 avenue John F. Kennedy L-1855 Luxembourg Attention: AWS General Counsel	Date Signed: 5.7.2022
	Address: BK-DTI, Bundeskanzlei, Bereich Digitale Transformation und IKT- Lenkung - DTI Schwarztorstrasse 53, 3003 Bern Attention:



Annex 1
AWS Security Standards

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the “Facilities”). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and



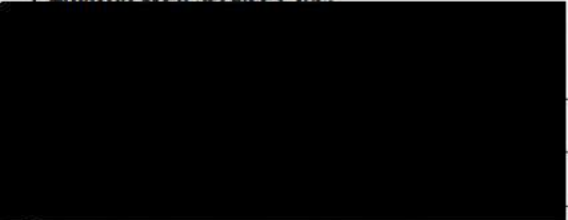
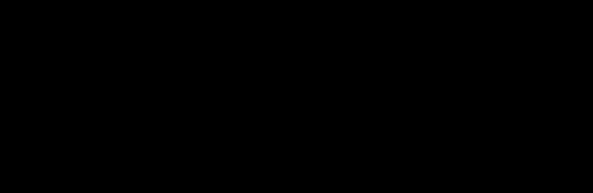
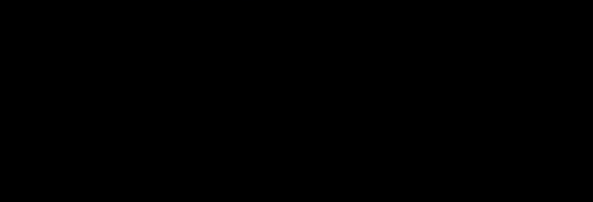
its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.



CC OTH 00462793 2022 TR

SUPPLEMENTARY ADDENDUM TO AWS GDPR DATA PROCESSING ADDENDUM

The purpose of this supplementary addendum (this "Addendum") is to outline supplemental measures that AWS takes to protect Customer Data. This Addendum is effective as of the day the last party signs this Addendum (the "Addendum Effective Date") and is entered into by and among Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties, as applicable (together "AWS") under the AWS GDPR DPA and the customer specified in the table below ("Customer").

Amazon Web Services, Inc. 	<u>Customer:</u> The Swiss Confederation, acting through the Federal Office for Buildings and Logistics (Bundesamt für Bauten und Logistik -BBL) for Digital transformation and ICT STEERING (DTI) 
Date Signed: August 17, 2022	Date Signed: 04.09.2022
Address: 410 Terry Ave North Seattle, WA 98109-5210	 Date Signed: 4.7.2022  Date Signed: 5.7.22  Date Signed: 5.7.2022
	BK-DTI Bundeskanzlei Bereich Digitale Transformation und IKT-Lenkung



1. Requests for Customer Data

1.1 If AWS receives a valid and binding order ("Request") from any governmental body ("Requesting Party") for disclosure of Customer Data, AWS will use every reasonable effort to redirect the Requesting Party to request Customer Data directly from Customer.

1.2 If compelled to disclose Customer Data to a Requesting Party, AWS will:

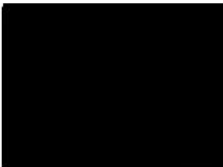
- (a) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so (including by asserting its sovereign immunity or other rights afforded to the Customer under international law). If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible;
- (b) (i) inform the Requesting Party that the Request seeks Customer Content from an AWS Enterprise Account that is owned by a foreign government and, therefore, may be protected by the sovereign immunity or other rights afforded to the Customer under international law and (ii) request that the Requesting Party grant Customer the opportunity to present Customer's positions regarding such Customer Content; and
- (c) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union, applicable Member State law, or the sovereign immunity or other rights afforded to the Customer under international law).

1.3 If, after exhausting the steps described in Section 1.2, AWS remains compelled to disclose Customer Data to a Requesting Party, AWS will disclose only the minimum amount of Customer Data necessary to satisfy the Request.

1.4 As of the Addendum Effective Date and upon the Parties' reasonable review, AWS and the Customer believe that the Customer's sovereign immunity is protected by the US Foreign Sovereign Immunities Act and that, therefore, the US CLOUD Act does not apply to Customer Data when the Services are used by Customer in its official government capacity.

2. Data Subject Rights. Nothing in this Addendum restricts Customer's data subjects from exercising their rights under the GDPR, including their rights to compensation from AWS for material or non-material damage under, and in accordance with, Article 82 of the GDPR.

3. Warranty. AWS agrees and warrants that it has no reason to believe that the legislation applicable to it, or its sub-processors, including in any country to which Customer Data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from Customer and its obligations under this Addendum and the AWS GDPR DPA and that in the event



SUPPLEMENTARY ADDENDUM TO AWS GDPR DATA PROCESSING ADDENDUM

The purpose of this supplementary addendum (this "Addendum") is to outline supplemental measures that AWS takes to protect Customer Data. This Addendum is effective as of the day the last party signs this Addendum (the "Addendum Effective Date") and is entered into by and among Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties, as applicable (together "AWS") under the AWS GDPR DPA and the customer specified in the table below ("Customer").

Amazon Web Services, Inc.	Customer: The Swiss Confederation, acting through the Federal Office for Buildings and Logistics (Bundesamt für Bauten und Logistik -BBL) for Digital transformation and ICT STEERING (DTI)
Signature:	[Redacted]
Name:	[Redacted]
Title:	[Redacted]
Date Signed:	Date Signed: 04.07.2022
Address: 410 Terry Ave North Seattle, WA 98109-5210	[Redacted]
	Date Signed: 4.7.2022
	[Redacted]
	Date Signed: 5.7.2022
	BK-DTI Bundeskanzlei Bereich Digitale Transformation und IKT-Lenkung



Amazon Web Services EMEA SARL

DTI
 Schwarztorstrasse 53
 3003 Bern

Date Signed: 16.08.2022

Address:
 38 avenue John F. Kennedy
 L-1855 Luxembourg

This Addendum supplements, but does not modify, the AWS GDPR Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf, or other agreement between Customer and AWS governing the processing of Customer Data pursuant to the GDPR (the "AWS GDPR DPA"). Unless otherwise defined in this Addendum, all capitalized terms used in this Addendum will have the meanings given to them in the AWS GDPR DPA.

1. Requests for Customer Data

- 1.1 If AWS receives a valid and binding order ("**Request**") from any governmental body ("**Requesting Party**") for disclosure of Customer Data, AWS will use every reasonable effort to redirect the Requesting Party to request Customer Data directly from Customer.
- 1.2 If compelled to disclose Customer Data to a Requesting Party, AWS will:
 - (a) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so (including by asserting its sovereign immunity or other rights afforded to the Customer under international law). If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible;
 - (b) (i) inform the Requesting Party that the Request seeks Customer Content from an AWS Enterprise Account that is owned by a foreign government and, therefore, may be protected by the sovereign immunity or other rights afforded to the Customer under international law and (ii) request that the Requesting Party grant Customer the opportunity to present Customer's positions regarding such Customer Content; and
 - (c) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union, applicable Member State law, or the sovereign immunity or other rights afforded to the Customer under international law).
- 1.3 If, after exhausting the steps described in Section 1.2, AWS remains compelled to disclose Customer Data to a Requesting Party, AWS will disclose only the minimum amount of Customer Data necessary to satisfy the Request.
- 1.4 As of the Addendum Effective Date and upon the Parties' reasonable review, AWS and the Customer believe that the Customer's sovereign immunity is protected by the US Foreign Sovereign Immunities Act and that, therefore, the US CLOUD Act does not apply to Customer Data when the Services are used by Customer in its official government capacity.

2. **Data Subject Rights.** Nothing in this Addendum restricts Customer's data subjects from exercising their rights under the GDPR, including their rights to compensation from AWS for material or non-material damage under, and in accordance with, Article 82 of the GDPR.

3. **Warranty.** AWS agrees and warrants that it has no reason to believe that the legislation applicable to it, or its sub-processors, including in any country to which Customer Data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from Customer and its obligations under this Addendum and the AWS GDPR DPA and that in the event

of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum and the AWS GDPR DPA, AWS will promptly notify the change to Customer as soon as AWS is aware, in which case Customer is entitled to suspend the transfer of Customer Data and/or terminate the Agreement.

4. **Expiry.** The term of this Addendum will commence on the Addendum Effective Date and will remain into effect until the earlier of (a) the termination of the AWS GDPR DPA, or (b) AWS's notification to Customer that AWS has made available a revised AWS GDPR DPA online, to reflect an alternative recognized compliance standard for the lawful transfer of Customer Data outside the EEA.
5. **Nondisclosure.** Customer agrees that the details of this Addendum are not publicly known and constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting AWS Confidential Information and Customer and AWS or its affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.
6. **Entire Agreement; Conflict.** Except as supplemented by this Addendum, the AWS GDPR DPA and the Agreement will remain in full force and effect. This Addendum, together with the AWS GDPR DPA and the Agreement: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. If there is a conflict between the AWS GDPR DPA and this Addendum, the terms of this Addendum will control.
7. **Counterparts and Facsimile or Email Delivery.** This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties deliver this Addendum by facsimile or email transmission.

[Remainder of Page Intentionally Left Blank]

PROFESSIONAL SECRECY ADDENDUM

This Addendum ("Addendum") is effective as of the date the last party signs this Addendum (the "Addendum Effective Date") and is entered into by and among The Swiss Confederation, acting through the Federal Office for Buildings and Logistics (Bundesamt für Bauten und Logistik – BBL) ("Customer") and the AWS Contracting Party or AWS Contracting Parties (as applicable) ("AWS") under the Agreement. This Addendum supplements the AWS Customer Agreement available at <http://aws.amazon.com/agreement> (as updated from time to time) between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "Agreement"). The parties agree as follows.

1. **Statutory Secrecy Obligations.** AWS is aware that there are specific professional secrecy provisions in Switzerland (the "Secrecy Provisions") that require Customer to impose strict confidentiality and secrecy obligations upon its service provider when using services that include the processing of information protected under the Secrecy Provisions by the service provider. AWS acknowledges that Customer Content may include information that is subject to these Secrecy Provisions. AWS agrees to use Customer Content only as necessary in accordance with the terms of this Addendum, the Agreement and the AWS GDPR Data Processing Addendum:Switzerland. AWS is aware that a violation of applicable Secrecy Provisions may result in criminal sanctions pursuant to Art. 320 and 321 of the Swiss Criminal Code (StGB) and Art. 35 Swiss Data Protection Act (DSG)/ Art. 62 new Swiss Data Protection Act (revDSG).
2. **AWS Personnel.** AWS restricts its personnel from processing Customer Content without authorisation as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection, security and secrecy and trains its personnel accordingly, as evidenced in the Service Organization Controls 2, Type 2 report. Amazon.com has a Code of Business Conduct and Ethics currently posted at <https://ir.aboutamazon.com/corporate-governance/documents-charters/code-business-conduct-and-ethics> (as updated from time to time, the "Code") that obligates employees to follow applicable laws, rules and regulations at all times.
3. **Subcontractors.** If AWS uses subcontractors in the performance of the Services under the Agreement, AWS will impose appropriate contractual obligations upon such subcontractors, including obligations regarding confidentiality and secrecy.
4. **Nondisclosure.** The existence and terms of this Addendum are not publicly known and will not be disclosed by Customer.
5. **Entire Agreement.** This Addendum supersedes all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS, whether written or verbal, regarding the subject matter of this Addendum. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.
6. **Counterparts and Facsimile Delivery.** This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this Addendum by facsimile transmission.



IN WITNESS WHEREOF, Customer and AWS have executed this Addendum as of the Addendum Effective Date.

Amazon Web Services EMEA SARI



Date: 16.08.2022

THE SWISS CONFEDERATION, ACTING THROUGH THE FEDERAL OFFICE FOR BUILDINGS AND LOGISTICS (BUNDESAMT FÜR BAUTEN UND LOGISTIK -BBL) FOR DIGITAL TRANSFORMATION AND ICT STEERING (DTI)



Date: 04.07.2022

Date: 4.7.2022



Date: 5.7.2022

Date: 5.7.2022



[REDACTED]

This Addendum supplements the Agreement and is entered into by and between the parties listed on this page.

Addendum Effective Date: The date the last party signs this Addendum.

AMAZON WEB SERVICES EMEA SARL [REDACTED]	THE SWISS CONFEDERATION, ACTING THROUGH THE FEDERAL OFFICE FOR BUILDINGS AND LOGISTICS (BUNDESAMT FÜR BAUTEN UND LOGISTIK -BBL) FOR DIGITAL TRANSFORMATION AND ICT STEERING (DTI) (hereafter "you") [REDACTED]
Date signed: <u>16.08.2022</u>	Date signed: <u>04.07.2022</u>
	[REDACTED]
	Date signed: <u>4.7.2022</u>
	[REDACTED]
	Date signed: <u>5.7.22</u>
	[REDACTED]
	Date signed: <u>5.7.2022</u>

MUTUAL NONDISCLOSURE AGREEMENT

The parties have executed this Agreement as of the Effective Date.

Amazon Web Services EMEA SARL

**Company: Swiss Confederation, represented by
Bundesamt für Bauten und Logistik**

Date Signed: 24/06/2020

Mail: 38 avenue John F. Kennedy, L-1855 Luxembourg

Email: [REDACTED]

Attention: General Counsel

Date Signed: 18.05.2020

Date Signed: 26.05.2020

By: _____

its _____

Print Name: _____

Date Signed: _____

By: _____

its _____

Print Name: _____

Date Signed: _____

Mail: _____

Email: _____

Attention: _____



This Mutual Nondisclosure Agreement (this "Agreement"), effective as of 1 January 2019 (the "Effective Date"), is made between Amazon Web Services EMEA SARL, a Luxembourg corporation ("Amazon"), and Swiss Confederation, represented by Bundesamt für Bauten und Logistik, a Swiss Government company ("Company"). In connection with the parties' commercial relationship or discussions about a possible relationship or transaction (the "Relationship"), each party may receive confidential information from the other party. Accordingly, Amazon and Company hereby agree as follows:

1. Affiliates; Confidential Information. The term "Affiliate" means, with respect to (i) Amazon, any entity that directly or indirectly controls, is controlled by or is under common control with Amazon, and (ii) the Swiss Confederation, consisting the administrative units as part of the central Federation Administration (*Verwaltungseinheiten der zentralen Bundesverwaltung*) in accordance with the relevant legal bases (cf. Swiss Government and Administration Organisation Act of 21 March 1997 [GAOA, cc – classified compilation of Acts & Ordinances - 172.010] and related Government and Administration Ordinance of 25 November 1998 [GAOO, Cc 172.010.1]) and the term "Confidential Information" means all nonpublic information concerning the Relationship disclosed by either party, its Affiliates, or their agents (as applicable, such entities collectively, the "Disclosing Party") to the other party, its Affiliates, or their agents (collectively, the "Receiving Party") that is designated as confidential or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered as confidential. Confidential Information includes, without limitation (i) nonpublic information relating to the Disclosing Party's technology, products, services, processes, data, customers, business plans and methods, promotional and marketing activities, finances and other business affairs, (ii) third-party information that the Disclosing Party is obligated to keep confidential, and (iii) the nature, content and existence of a Relationship, discussions or negotiations between the parties.

2. Exclusions. Confidential Information does not include any information that (i) is or becomes publicly available without breach of this Agreement (provided, however, information that is rumored or reported does not become public based only on such rumors or reports), (ii) was known by the Receiving Party prior to its receipt from the Disclosing Party, (iii) is disclosed to the Receiving Party from any third party, except where the Receiving Party knows, or reasonably should know, that such disclosure constitutes a wrongful or tortious act or (iv) is

independently developed by the Receiving Party without use of any Confidential Information.

3. Use and Disclosure of Confidential Information. The Receiving Party will use Confidential Information only in connection with the Relationship. Except as provided in this Agreement, the Receiving Party will not disclose Confidential Information to anyone without the Disclosing Party's prior written consent. The Receiving Party will take reasonable measures to avoid disclosure, dissemination or unauthorized use of Confidential Information.

4. Receiving Party Personnel; Affiliates. The Receiving Party will restrict the possession, knowledge and use of Confidential Information to its directors, officers, employees, contractors, agents, legal and accounting advisers, and entities controlled by the Receiving Party (collectively, "Personnel") who (i) have a need to know Confidential Information in connection with the Relationship, (ii) are informed of the confidential nature of the Confidential Information, and (iii) have obligations with respect to the Confidential Information that are consistent with this Agreement. Each of Amazon and the Company will ensure that its Affiliates comply with this Agreement.

5. Disclosures to Governmental Entities. The Receiving Party may disclose Confidential Information as required to comply with orders of governmental entities that have jurisdiction over it or as otherwise required by law.

6. Ownership of Confidential Information. All Confidential Information will remain the exclusive property of the Disclosing Party. The Disclosing Party's disclosure of Confidential Information will not constitute an express or implied grant to the Receiving Party of any rights to or under the Disclosing Party's patents, copyrights, trade secrets, trademarks or other intellectual property rights. Except to the extent permitted by applicable law in the absence of any express license or other grant of rights, neither party will use any trade name, trademark, logo or any other proprietary rights of the other party (or any of its Affiliates) in any manner without prior written authorization of such use by a Vice President of such other party.

7. Notice of Unauthorized Use. The Receiving Party will notify the Disclosing Party promptly upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this Agreement by the Receiving Party. The Receiving Party will cooperate with the Disclosing Party to help the Disclosing Party regain possession of such Confidential

Information and prevent its further unauthorized use and disclosure.

8. Return of Confidential Information. Subject to compliance with orders of governmental entities that have jurisdiction over it or as otherwise required by law, the Receiving Party will return or destroy all tangible materials or portions thereof constituting Confidential Information (including, without limitation, all summaries, copies and excerpts of Confidential Information) promptly following the Disclosing Party's written request.

9. Injunctive Relief. The Receiving Party acknowledges that a breach of its obligations under this Agreement could cause irreparable harm to the Disclosing Party as to which monetary damages may be difficult to ascertain or an inadequate remedy. The Receiving Party therefore agrees that the Disclosing Party will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

10. Scope; Termination. This Agreement covers Confidential Information disclosed by the Disclosing Party on and after the Effective Date. This Agreement automatically will terminate upon the earlier of (i) termination of all written agreements between the parties or their Affiliates regarding the Relationship, or (ii) if no agreements are executed, termination of discussions between the parties or their Affiliates regarding the Relationship or delivery of written notice terminating this Agreement; provided, however, that (a) each party's obligations with respect to the other party's Confidential Information will survive for three (3) years following termination, and (b) Sections 6, 9, 10, and 11 will survive indefinitely.

11. Miscellaneous.

11.1 This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes all prior communications and agreements between the parties with respect thereto. This Agreement may be amended, modified, or waived only with the mutual written consent of the parties hereto. This Agreement will not be assignable by either party without the prior written consent of the other party; provided that prior written consent will not be required for any assignment by a party to an Affiliate. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties and their respective successors and assigns.

11.2 The Disclosing Party acknowledges that the Receiving Party may now have, or in the future may develop or receive, information that is the same as, or similar to, Confidential Information without having

breached this Agreement. Nothing in this Agreement (a) prevents the Receiving Party from using, for any purpose and without compensating the Disclosing Party, information retained in the memory of the Receiving Party's Personnel who have had access to Confidential Information or (b) obligates the Receiving Party to restrict the scope of employment of the Receiving Party's Personnel provided, however, that this section does not create a license under any copyright or patent of the Disclosing Party.

11.3 If a provision of this Agreement is held invalid under any applicable law, such invalidity will not affect any other provision of this Agreement that can be given effect without the invalid provision. Further, all terms and conditions of this Agreement will be deemed enforceable to the fullest extent permissible under applicable law, and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.

11.4 This Agreement will be governed by the laws of the Switzerland, without reference to its choice of law rules. Exclusive jurisdiction over and venue of any suit arising out of or relating to this Agreement will be in the state and federal courts located in the City of Bern, and each of the parties hereto consents to the personal jurisdiction of, and venue in, those courts.

11.5 All notices hereunder will be given in writing, will refer to this Agreement and will be personally delivered or sent by overnight courier, electronic mail, or registered or certified mail (return receipt requested) to the address set forth below the parties' signatures on the first page of this Agreement.

