Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 10 – Abrufverfahren

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

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

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

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Vorgehen im Überblick

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

2. Bestimmung des Bedarfs und der Abrufkriterien

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

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

[redacted]

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), soweit möglich, entsprechend dem Entscheid eigenständig auf den Webseiten und Portalen der ausgewählten Zuschlagsempfängerinnen.

4. Allfällige weitere Interaktionen mit Zuschlagsempfängerinnen

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

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

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

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

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

5. Dokumentation von Seiten der Firma

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

a) Paket #01: Beschreibung des vorhandenen Leistungsangebots (z.B. Service Namen oder Service-ID's mit Hinweisen, wo die Bedarfsstelle und alle Bezugsberechtigten weitere Informationen beziehen können, genügen)
b) Paket #02: Preislisten
c) Paket #03: Weitere Dienstleistungen, die für den Leistungsbezug notwendig sind
d) Paket #04: Nicht-funktionale Eigenschaften (Sicherheitsdokumentationen, Prüfberichte, etc.)
e) Paket #05: Besonderes

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

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

[redacted]

6. Kein Anspruch auf Berücksichtigung

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

7. Mitteilung der Entscheide gem. Ziff. 3.2

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

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

7.3 Die Bezugsberechtigte teilt Folgendes mit:

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

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

8. Allgemeine Bestimmungen

Die Regeln des Rahmenvertrags kommen kraft Verweises zur Anwendung.

* * *

[redacted]

2

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 20 – 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)

[redacted]

1. Begriffsdefinitionen

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

a) **Auditberechtigte Stellen** sind: die jeweils Bezugsberechtigten, deren Aufsichtsbehörden und -stellen. Die Firma anerkennt ausdrücklich, dass auch die folgenden Stellen als Auditberechtigte Stellen gelten Aufsichtsbehörden wie:

- die Eidgenössische Finanzkontrolle (EFK);
- die vorgesetzten Amts- oder Aufsichtsstellen;
- die parlamentarischen Kontrollorgane oder ad hoc bestellte Kommissionen.

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

c) **Eidgenössische Finanzkontrolle (EFK)**

Die Firma ist verpflichtet, ordnungsgemässe Bücher und Aufzeichnungen in Bezug auf Gebühren, Zahlungen und Rechnungen, die für die Services im Rahmen dieses Rahmenvertrags der Bezugsberechtigten in Rechnung gestellt wurden, in Übereinstimmung mit den gesetzlichen oder archivarischen Anforderungen der Firma, externen Rechnungslegungsstandards und aufsichtsrechtlichen Anforderungen zu führen. Die EFK kann diese Unterlagen nach zeitlich angemessener schriftlicher Mitteilung an die Firma, höchstens jedoch einmal alle 12 Monate auf eigene Kosten prüfen, sofern eine solche Prüfung den normalen Geschäftsbetrieb der Firma nicht unangemessen beeinträchtigt. Der Antrag der EFK auf eine Prüfung solcher Unterlagen muss der Firma innerhalb von zwei Jahren nach dem Datum der betreffenden Zahlung oder Rechnung zugehen.

Diese unter Ziff. 1.1 a) und 1.1 c) genannten Auditberechtigten Stellen müssen eine für die Firma annehmbare schriftliche Vertraulichkeitsvereinbarung abschliessen oder auf andere Weise durch eine gesetzliche oder rechtliche Vertraulichkeitsverpflichtung gebunden sein.

1.2 Ansonsten gelten die Begriffe gemäss Ziff. 4.2 des Rahmenvertrags.

2. Kontrollrechte (Audit)

2.1 Die Firma gewährt der Bezugsberechtigten Einsichtnahme- und Prüfungsrechte, damit die Bezugsberechtigte beurteilen kann, inwieweit die von der Bezugsberechtigten bestellten Cloud Services der Firma mit dem Rahmenvertrag und/oder den geltenden Gesetzen und Vorschriften übereinstimmen. Diese Einsichtnahme- und Prüfungsrechte umfassen den Zugriff auf Informationen oder Berichten und/oder eine Einsichtnahme in die Einrichtungen der Firma, die zur Erbringung der bestellten Cloud Services genutzt werden, wie im Folgenden näher beschrieben.

2.2 Sofern die Bezugsberechtigte feststellt, dass es ausreicht, die aufsichtsrechtlichen Anforderungen der Bezugsberechtigten einzuhalten und soweit sich eine Prüfung gemäss diesem Rahmenvertrag auf dieselben Kontrollen bezieht wie die Prüfung der Bezugsberechtigten gemäss dem Anhang Datenschutz, wird die Bezugsberechtigte diese Prüfungen so koordinieren, dass unnötige Doppelarbeit vermieden wird.

2.3 Wenn ein Dritter die Prüfung durchführt, wird dieser Dritte von der Bezugsberechtigten und der Firma gemeinsam vereinbart (es sei denn, ein solcher Dritter ist in der von der Firma veröffentlichten Liste der zugelassenen Prüfer zum Zeitpunkt der Prüfungsanfrage enthalten). Die Firma wird ihre Zustimmung zu einem von der Bezugsberechtigten

angeforderten externen Prüfer nicht unangemessen verweigern. Der Dritte muss vor Durchführung der Prüfung eine für die Firma annehmbare schriftliche Vertraulichkeitsvereinbarung abschliessen oder anderweitig durch eine gesetzliche oder rechtliche Geheimhaltungsverpflichtung gebunden sein.

2.4 Um eine Prüfung anzufordern, wird die Bezugsberechtigte der Firma mindestens dreissig Arbeitstage vor dem geplanten Prüfungsdatum einen Vorschlag für einen detaillierten Prüfungsplan vorlegen. Der vorgeschlagene Prüfungsplan sollte den vorgeschlagenen Umfang, die Dauer und das Anfangsdatum der Prüfung nennen. Die Firma wird den vorgeschlagenen Prüfungsplan überprüfen und der Bezugsberechtigten alle Bedenken und Fragen mitteilen, wobei verstanden wird, dass diese Bedenken und Fragen die effektive Ausführung der Zugriffs- und Prüfungsrechte der Bezugsberechtigten, wie diese unter der geltenden Gesetzgebung und diesem Rahmenvertrag erforderlich sind, weder erschweren noch einschränken werden. Die Firma wird mit der Bezugsberechtigten zusammenarbeiten, um einen endgültigen Prüfungsplan zu vereinbaren, um die Prüfungsrechte der Bezugsberechtigten gemäss dieser Ziff. 2 zu erleichtern, aber die Ausübung die Prüfungsrechte der Bezugsberechtigten in Übereinstimmung mit diesem Anhang ist nicht von der Zustimmung zu dem Plan abhängig.

2.5 In Bezug auf eine in dieser Ziff. 2 vorgesehene Prüfung wird die Firma kooperieren und jede angemessene Unterstützung und sämtliche Informationen zur Verfügung stellen, die aufgrund von Gesetzen oder Vorschriften, die für die Bezugsberechtigte gelten und erforderlich sind, einschliesslich vollständiger Zugang zu allen relevanten Geschäftsräumen (z. B. Hauptgeschäftsstellen und Betriebszentren), einschliesslich aller relevanten Geräte, Systeme, Netzwerke, Informationen und Daten, die für die Erbringung der Cloud Services verwendet werden, unter der Voraussetzung, dass kein Zugriff auf Daten oder Serviceumgebungen gewährt wird, die einem anderen Kunden von der Firma gehören, noch zu Informationen, deren Offenlegung Oracle-Netzwerke oder -Systeme oder die Serviceumgebungen anderer Kunden von der Firma gefährden könnte.

2.6 Jegliche Einsichtnahme/Prüfung vor Ort muss während der regulären Geschäftszeiten in der betreffenden Einrichtung unter Aufsicht von der Firma und unter Einhaltung der Gesundheits- und Sicherheitsrichtlinien und -verfahren von der Firma durchgeführt werden und darf die geschäftlichen Tätigkeiten von der Firma nicht unangemessen beeinträchtigen. Das Recht der Bezugsberechtigten auf Einsichtnahme/Prüfung sollte in einer Weise ausgeübt werden, die dem Grundsatz der Verhältnismässigkeit entspricht, auch im Hinblick auf die Art und Komplexität der betreffenden Cloud Services und darauf, ob die Cloud Services für kritische oder wichtige Funktionen des Betriebs der Bezugsberechtigten genutzt werden.

2.7 Sofern nicht gesetzlich verboten, stellt die Bezugsberechtigte der Firma eine Kopie der Ergebnisse des endgültigen Prüfungsberichts zur Verfügung, die mit den Cloud-Services von der Firma zusammenhängen. Die Bezugsberechtigte darf die Prüfungsberichte ausschliesslich zur Erfüllung der aufsichtsrechtlichen Prüfungspflichten der Bezugsberechtigten und/oder zur Bestätigung der Einhaltung der geltenden Gesetze und Verordnungen, des Rahmenvertrags, und des Auftrags der Bezugsberechtigten nutzen.

2.8 Ergänzend zu Ziff. 5.2 dieses Anhangs, kann die Firma für die Unterstützung im Zusammenhang mit einer Prüfung (sei es durch die Bezugsberechtigte oder die Aufsichtsbehörde), eine Gebühr zu den zu diesem Zeitpunkt gültigen Sätzen von der Firma oder wie anderweitig in einem von den Parteien abgeschlossenen Auftrag vereinbart) erheben, die die Mehraufwendungen deckt, die der Firma in angemessener Weise zur Unterstützung einer Prüfung entstanden sind.

2.9 Sofern die Bezugsberechtigte feststellt, dass dies ausreicht, um ihre aufsichtsrechtlichen Anforderungen zu erfüllen, wird die Bezugsberechtigte ihre Zugriffs- und Prüfungsrechte wahrnehmen, indem die Bezugsberechtigte von der Firma verlangt, ihr vertrauliche Kopien von Bescheinigungen und Prüfberichten bereitzustellen, oder, falls die Firma einen Prozess für gepoolte Prüfungen implementiert hat, durch eine gepoolte Prüfung, die in Zusammenarbeit mit anderen Kunden der Firma im Einklang mit einem derartigen Prozess durchgeführt wurde.

2.10 Die Parteien kommen überein, dass die Bezugsberechtigte im Falle von Auditprozeduren, die durch Aufsichtsbehörden angeordnet oder initiiert werden, die Bestimmungen in dieser Ziff. 2 nur so weit einhalten wird, wie dies im Rahmen der angeordneten Überprüfung vernünftigerweise möglich ist. Die Firma wird über solche Audits und ihre Modalitäten so früh vernünftigerweise möglich und im gesetzlich zulässigen Mass informiert werden.

3. Zweck des Audits

Das Audit kann die folgenden Ziele und Zwecke verfolgen:

a) Die Einhaltung gesetzlicher Anforderungen nachzuweisen bzw. deren Erfüllungsgrad zu prüfen nur insoweit, als sie sich auf die Erbringung der Services gemäss dem jeweiligen Auftrag beziehen;

b) Anfragen und Auskunfts- resp. Prüfungsbegehren von Aufsichtsbehörden, mit der Ausnahme der Datenschutzaufsichtsbehörden (z.B. EDÖB), der Bezugsberechtige zu erfüllen und zu entsprechen;

Die Durchführung von Audits, die die Verpflichtungen der Firma gemäss Anhang Datenschutz, beziehungsweise DPA zum Gegenstand haben, richten sich nach dem Anhang Datenschutz und wird von den Parteien ausdrücklich vom Anwendungsbereich dieses Anhangs ausgeschlossen.

4. Prüfer der Auditberechtigten Stelle

Ein Audit kann (i) von internen Mitarbeitenden einer Auditberechtigten Stelle, (ii) nach schriftlicher Zustimmung der Firma von unabhängigen, von der Auditberechtigten Stelle beauftragten Dritten gemäss der Ziff. 2.3 dieses Anhangs (Subziffern (i) und (ii) durchgeführt werden (nachfolgend zusammengefasst als "Prüfer der Auditberechtigten Stelle" bezeichnet).

5. Kosten des Audits

5.1 Jede Partei bzw. die Auditberechtigte Stelle, die einen Audit auslöst, trägt ihre eigenen entstehenden Kosten selbst, die ihr bei der Durchführung des Audits anfallen, sofern das Audit keinen erheblichen Verstoss gegen die vertraglichen Vereinbarungen und/oder die anwendbaren Gesetze ergibt.

5.2 Sofern das Audit keinen erheblichen Verstoss ergibt, trägt die Bezugsberechtigte, die die Durchführung des Audits bei der Firma auslöst, die weiteren Kosten für die Durchführung eines Audits, wenn die Firma den Bezugsberechtigten nach Prüfung des Auditplans des Bezugsberechtigten unverzüglich darüber informiert, dass sie bei der Durchführung des Audits mit zusätzlichen Kosten oder Gebühren rechnet, die nicht durch die im Rahmen des Rahmenvertrags respektive des massgeblichen Auftrags zu zahlenden Gebühren abgedeckt sind, vereinbaren die Parteien nach Treu und Glauben über solche Kosten oder Gebühren zu verhandeln.

5.3 Ergibt das Audit einen einzig durch Oracle verursachten erheblichen Verstoss gegen

die vertraglichen Vereinbarungenund/oder anwendbare Gesetze, trägt die Firma die angemessenen Kosten des betreffenden Audits (d.h. Kosten gem. Ziff. 5.2).

6. Festgestellte Unregelmässigkeiten in Bezug auf andere Vorgaben

6.1 Ergibt eine Prüfung nach Massgabe dieses Anhangs, dass die Firma materielle Pflichten gemäss Rahmenvertrag und des massgeblichen Auftrages, mit Ausnahme des Anhangs Datenschutz und des DPA, nicht eingehalten hat, wird die Auditberechtige Stelle resp. die Bezugsberechtigte die Firma unverzüglich schriftlich informieren. Die Firma wird sich nach Erhalt der schriftlichen Prüfungsfeststellungen bemühen, die Nichteinhaltung innerhalb einer angemessenen Frist zu korrigieren.

6.2 Sollte sie nicht in der Lage sein, den vertragsgemässen Zustand innert nützlicher Frist, wieder herzustellen, ist die Firma auf eigene Kosten zu den folgenden Schritten verpflichtet:

a) Information an die Bezugsberechtigte, dass die Firma an der Herstellung des rechtmässigen Zustands arbeitet.

b) Unterbreitung eines Lösungskonzepts an die Bezugsberechtigte, welches die sachlichen und zeitlichen Aspekte bis zur Wiederherstellung des rechtmässigen Zustands aufzeigt.

c) Darlegung der kurzfristigen Massnahmen, die bis zu einer definitiven Umsetzung des Lösungskonzepts zu treffen sind, damit die nachteiligen Folgen der Situation von der Bezugsberechtigten insgesamt abgewendet oder gemindert werden können.

* * *

3

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 30 – Datenschutz

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Inhaltsübersicht:

[redacted]

I. ALLGEMEINE BESTIMMUNGEN

1. Anwendbares Recht

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

a) Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1), das neue Bundesgesetz über den Datenschutz (nDSG), auf das im Folgenden Bezug genommen wird, ist erst ab seinem Inkrafttreten anwendbar.

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), ab dem Zeitpunkt ihres Inkrafttretens.

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; so lange das SDSG noch in Kraft ist)

f) in sämtlichen Folgeerlassen und -Versionen gemäss lit. a) bis e).

g) Im „einschlägigen Datenschutzrecht", einschliesslich des einschlägigen europäischen Datenschutzrechts verstanden als alle Datenschutzgesetze und -vorschriften weltweit, die für die Verarbeitung personenbezogener Daten im Rahmen dieses Anhangs. gelten.

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

1.3 Die Firma unterstützt in ihrer Rolle als Datenverarbeiterin die Verantwortliche die im Hinblick auf die Services auf sie anwendbaren einschlägigen gesetzlichen Bestimmungen betreffend Datenschutz einhalten zu können.

2. Zu diesem Vertragsanhang

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

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

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

---

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

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

2.4 Dieser Vertragsanhang verweist auf Bestimmungen aus (i) dem Data Processing Agreement for Oracle Services in der Version vom 26. Juni 2019 welches in Exhibit 1 das European Data Processing Addendum for Oracle Services («European DPA Addendum») enthält (kollektiv als «Oracle DPA» bezeichnet, siehe Beilage 1); (b) den Oracle EU Standard Contractual Clauses for Controller to Processor Transfers («Oracle SCC», siehe Beilage 2) welche die für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[3] enthalten,

Die Bestimmungen im Oracle DPA und in den Oracle SCC sind Beilagen zu diesem Vertragsanhang und gelten unmittelbar als dessen Bestandteil.

2.5 Die Parteien kommen überein, dass das Oracle DPA punkto allfälliger Abänderungen auf jedem Fall dem Vorbehalt einer bilateralen schriftlichen Anpassung gemäss Ziff. 21.3 Rahmenvertrag unterliegt. Hiervon explizit ausgenommen ist jedoch eine einseitige, durch die Firma initiierte Anpassung der im Oracle DPA in Ziff. 6 referenzierten Dokumentation (Oracle Security Practices) betreffend der von der Firma zum Schutze von personenbezogenen Daten zu treffenden technischen und organisatorischen Massnahmen.

Der Vorbehalt von Ziff. 21 Rahmenvertrag "Inkrafttreten / Rahmenvertragsdauer / Rahmenvertragsänderungen" gilt auch für die Oracle SCC. Beiden Parteien können im Falle von relevanten Gesetzesänderungen oder einschlägiger Judikatur eine entsprechende Anpassung der SCC verlangen.

II. KLAUSELN FÜR DIE DATENBEARBEITUNG IM AUFTRAG

A. Allgemeine Bestimmungen

3. Zweck und Anwendungsbereich

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

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

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

4. Auslegung

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

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

---

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

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.

4.4 Begriffe, die im Rahmenvertrag oder im Oracle DPA definiert sind, haben in diesem Dokument die gleiche Bedeutung. Begriffe die in den vorgenannten Dokumenten nicht definiert sind, haben die Bedeutung gemäss anwendbarer gDatenschutzgesetzgebung.

4.5 Als «Aufsichtsbehörde» im Sinne dieses Anhanges und seiner Beilagen gelten alle Aufsichtsstellen, denen die Vergabestelle respektive die Bezugsberechtigte bezüglich ihrer Tätigkeit und der Speicherung personenbezogener Daten Rechenschaft schuldig ist wie z.B. der Eidgenössische Datenschutz- und Öffentlichkeitsverantwortliche, die Eidgenössische Finanzkontrolle. die vorgesetzten Amts- oder Aufsichtsstellen und/oder die parlamentarischen Kontrollorgane oder ad hoc bestellte parlamentarische Kommissionen.

5. Vorrang

5.1 Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen des Rahmenvertrags, diesbezüglicher Vertragsnachträge oder Leistungsabrufe, haben diese Klauseln Vorrang. Die Klauseln dieses Anhanges sind in Verbindung mit den Bestimmungen des Oracle DPA und den Oracle SCC zu lesen und werden durch diese subsidiär ergänzt. Bei Inkonsistenzen und Wiedersprüchen geht jedoch dieser Anhang dem Oracle DPA vor.

6. Beschreibung der Auftragsbearbeitung

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

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

6.3 Art und Zweck der Auftragsbearbeitung sind die Speicherung und Bereitstellung der vertragsgegenständlichen Personendaten bei der Erbringung der Cloud-Services für die Verantwortliche.

6.4 Die Art der Personendaten und der Kreis (Kategorien) betroffener Personen ergeben sich aus der Nutzung der Cloud-Services durch die Verantwortliche (namentlich den von der Verantwortlichen vorgenommenen Einstellungen) sowie aus den öffentlich-verfügbaren Dienstleistungsbeschreibungen der Auftragsbearbeiterin.

6.5 Diese Klausel wird durch die Bestimmungen von Artikel 2 des European DPA Addendums ergänzt.

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 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.

d) Die Weisungen sind stets zu dokumentieren.

7.2 Die Parteien sind sich einig, dass sich die dokumentierten Weisungen der Verantwortlichen bei Cloud-Services aus den durch die Verantwortliche vorgenommenen Einstellungen sowie den öffentlich verfügbaren Dienstleistungsbeschreibungen der Auftragsbearbeiterin ergeben. Diese sind in den entsprechenden Security Practices für diese Dienste dargelegt:

- Für **Cloud Services**: Oracle's Hosting & Delivery Policies, abrufbar unter http://www.oracle.com/us/corporate/contracts/cloud-services/index.html.

8. Zweckbindung

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

9. Dauer der Bearbeitung von Personendaten

Die Daten werden von der Auftragsbearbeiterin nur für die vereinbarte Dauer bearbeitet und zur Erfüllung seiner Verpflichtungen zum Datenabruf oder zur Datenlöschung gemäss Ziff. 19.4 unten, sofern das geltende Recht nichts anderes vorschreibt.

10. Sicherheit der Bearbeitung

10.1 Die Auftragsbearbeiterin ergreift angemessene technische und organisatorische Massnahmen um die Sicherheit, Vertraulichkeit oder Integrität der Personendaten, welche übertragen, gespeichert oder anderweitig auf Oracle-Systemen oder in der Oracle Service-Umgebung verarbeitet werden, zu gewährleisten. Dies umfasst den Schutz der Personendaten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmässig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den einschlägigen Personendaten führt (im Folgenden "Verletzung der Datensicherheit").

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

11. Dokumentation und Einhaltung der Klauseln

11.1 Die Auftragsbearbeiterin muss die Einhaltung dieser Klauseln in Übereinstimmung mit ihren Dokumentationspflichten für Datenverarbeiter gemäss dem geltenden Datenschutzrecht und gemäss Ziff. 5 des European DPA Addendum nachweisen.

11.2 Die Auftragsbearbeiterin bearbeitet Anfragen der Verantwortlichen bezüglich der Bearbeitung von Daten gemäss diesen Klauseln in einem angemessenen Zeitrahmen welcher es dem jeweils Verantwortlichen erlaubt, die jeweils anwendbaren gesetzlichen Fristen einzuhalten.

[redacted]

11.3 Die Auftragsbearbeiterin stellt der Verantwortlichen die relevanten 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, indem sie die Verantwortliche elektronischen Zugriff auf eine Aufzeichnung der Verarbeitungstätigkeiten und alle verfügbaren Leitfäden für Datenschutz- und Sicherheitsfunktionen für die Dienste gewähren. Diese Informationen sind über (i) My Oracle Support, Document ID 111.1 oder ein anderes für die Services bereitgestelltes primäres Support-Tool, wie das NetSuite Support Portal, oder (ii) auf Anfrage verfügbar, wenn der Verantwortlichen ein solcher Zugang zu My Oracle Support (oder einem anderen primären Support-Tool) nicht zur Verfügung steht.

12. Audit

12.1 Die Verantwortliche kann (i) maximal einmal im Jahr vor Ort bei der Auftragsbearbeiterin; (ii) in angemessener, verhältnismässiger und regelmässiger Weise und durch Informations- und Dokumentationsanforderungen prüfen, ob die Auftragsbearbeiterin ihren Pflichten aus diesem Datenschutz Anhang erfüllt. Darüber hinaus darf die Verantwortliche oder die jeweils verantwortliche Aufsichtsbehörde des jeweiligen Verantwortlichen gemäss Ziff. 4.5, solche Überprüfungen unter (i) und (ii), soweit dies nach einschlägigem Datenschutzrecht und den in Ziff. 1.1 referenzierten Bestimmungen erforderlich ist, häufiger durchführen.

12.2 Wenn Dritte die Überprüfung durchführen, muss dieser Dritte von der Verantwortlichen und der Auftragsbearbeiterin einvernehmlich vereinbart werden (es sei denn, diese Drittpartei ist eine Aufsichtsbehörde). Die Auftragsbearbeiterin wird seine Zustimmung zu einem von der Verantwortlichen angeforderten unabhängigen Prüfer nicht unbillig verweigern. Die Drittpartei muss vor Durchführung der Prüfung eine für die Durchführung von IT-industrieübliche Audits schriftliche Vertraulichkeitsvereinbarung unterzeichnen oder anderweitig durch eine gesetzliche oder rechtliche Geheimhaltungsverpflichtung gebunden sein, die mindestens ebenso streng sind wie die zwischen den Parteien gemäss diesem Anhang vereinbarten Geheimhaltungs- und Vertraulichkeitsverpflichtungen.

12.3 Um eine Überprüfung anzufordern, muss die Verantwortliche der Auftragsbearbeiterin mindestens zwei Wochen vor dem vorgeschlagenen Prüfungsdatum einen Vorschlag für einen detaillierten Prüfungsplan vorlegen. Der vorgeschlagene Prüfungsplan muss den vorgeschlagenen Umfang, die Dauer und das Anfangsdatum der Überprüfung nennen. Die Auftragsbearbeiterin wird den vorgeschlagenen Prüfungsplan überprüfen und der Verantwortlichen alle Bedenken und Fragen mitteilen, wobei verstanden wird, dass diese Bedenken und Fragen objektiv angemessen sein müssen und die Auftragsbearbeiterin bemüht sein wird die effektive Ausführung der Zugriffs- und Prüfungsrechte der Verantwortlichen, wie diese unter der geltenden Gesetzgebung und dem Rahmenvertrag erforderlich sind, weder zu erschweren noch einzuschränkeneinschränken. . Die Auftragsbearbeiterin wird den vorgeschlagenen Prüfungsplan überprüfen und der Verantwortlichen alle Bedenken und Fragen mitteilen. Die Auftragsbearbeiterin wird mit der Verantwortlichen zusammenarbeiten, um einen endgültigen Prüfungsplan zu vereinbaren um die Prüfungsrechte der Bezugsberechtigten gemäss dieser Ziff. 12 zu erleichtern, aber die Ausübung die Prüfungsrechte der Verantwortlichen in Übereinstimmung mit dieser Ziff. 12 ist nicht von der Zustimmung der Auftragsbarbeiterin zu dem Plan abhängig.

12.4 Die Überprüfung muss in der betroffenen Einrichtung innerhalb der regulären Geschäftszeiten durchgeführt werden und sie wird entsprechend dem vereinbarten endgültigen Prüfungsplan sowie den Gesundheits- und Sicherheitsrichtlinien von der Auftragsbearbeiterin oder sonstigen relevanten Richtlinien durchgeführt und darf die Geschäftstätigkeiten von der Auftragsbearbeiterin nicht unangemessen beeinträchtigen.

[redacted]

12.5 Sofern nicht gesetzlich verboten, stellt die Verantwortliche nach Abschluss der Prüfung der Auftragsbearbeiterin eine Kopie des Prüfreports zur Verfügung, der den Vertraulichkeitsbedingungen des Services-Auftrags der Verantwortlichen unterliegt. Die Verantwortliche darf die Prüfungsberichte ausschliesslich zur Erfüllung Ihrer aufsichtsrechtlichen Prüfungspflichten und/oder zur Bestätigung der Einhaltung der Bedingungen dieses Datenverarbeitungsvertrags verwenden.

12.6 Jede Partei trägt ihre eigenen Kosten in Bezug auf die Überprüfung selbst, es sei denn die Auftragsbearbeiterin informiert die Verantwortliche unverzüglich nach Durchsicht des Prüfungsplans, dass die Auftragsbearbeiterin bei der Durchführung der Überprüfung zusätzliche Kosten oder Gebühren aufzuwenden erwartet, die nicht durch die im Rahmen des Rahmenvertrags respektive des massgeblichen Auftrags zu zahlenden Gebühren abgedeckt sind. Die Parteien werden nach Treu und Glauben über solche Kosten oder Gebühren verhandeln.

12.7 Unbeschadet der oben in Ziff. 12.1 eingeräumten Rechte, wenn der angeforderte Umfang der Überprüfung in einem SOC, ISO, NIST, PCI DSS, HIPAA oder einem ähnlichen Prüfreport behandelt wird, der innerhalb der letzten 12 Monate von einer qualifizierten Drittpartei als Prüfer erstellt wurde, und wenn die Auftragsbearbeiterinder Verantwortlichen einen solchen Prüfreport zur Verfügung mit der Bestätigung überlässt, dass es bei den geprüften Kontrollen keine wesentlichen bekannten Änderungen gegeben hat, dann wird die Verantwortliche in dem Prüfreport der Drittpartei dargestellten Ergebnisse anstelle einer Überprüfung derselben, in dem Report behandelten Kontrollen akzeptieren.

12.8 Die Parteien kommen überein, dass die Verantwortliche im Falle von Auditprozeduren, die durch Aufsichtsbehörden angeordnet oder initiiert werden, die Bestimmungen in den Ziff. 12.2, 12.3, 12.4, 12.5 und 12.7 nur soweit einhalten wird, wie dies im Rahmen der angeordneten Überprüfung vernünftigerweise möglich ist. Die Firma wird über solche Audits und ihre Modalitäten so früh vernünftigerweise möglich und im gesetzlich zulässigen Mass informiert werden.

12.9 Die jeweilige Bezugsberechtigte hat das Recht, gegenüber der Firma zu beantragen, dass Audit-spezifische zusätzliche Fragen in den Audit-Plan aufgenommen werden, wie z.B. eine Liste von aller Verarbeitungstätigkeiten in Verbindung mit Service-Monitoring und Service-Analyse von Daten und deren Protokollierung. Die Firma wird dafür sorgen, dass der Zugriff auf Daten und ihre Verarbeitung zur Überwachung und Analyse von Services durch die Firma angemessen überwacht, protokolliert und geprüft wird. Wenn die Firma Verbrauchsberichte («Consumtion Reports») erstellt, werden die darin enthaltenen Daten auf einer so hohen Ebene aggregiert, dass keine Informationen über die Nutzung oder die Nutzungsmuster individueller Benutzer bzw. von Bezugsberechtigten der Services an bestimmten Tagen oder zu bestimmten Zeiten abgeleitet werden können.

13. Einsatz von Unterauftragsbearbeitern

13.1 Die Auftragsbearbeiterin besitzt die allgemeine Genehmigung der Verantwortlichen für die Beauftragung von Unterauftragsbearbeitern, die in einer Liste aufgeführt sind, die von der Auftragsbearbeiterin geführt und gemäss Klausel 4.2. des European DPA Addendum veröffentlicht wird.

13.2 Für OCI Cloud Services unterrichtet die Auftragsbearbeiterin die Verantwortliche mindestens einen Monat im Voraus ausdrücklich in schriftlicher Form, nachdem sich die Verantwortliche gemäss den Anweisungen auf My Oracle Support, Document ID 2288528.1 angemeldet hat, über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsbearbeitern. Die Verantwortliche hat die Möglichkeit , innert eines Monat nach Empfang der Änderung der Liste gegen die Beauftragung des/der betreffenden

Unterauftragsbearbeiter/s Einwände zu erheben und ein Widerspruchsverfahren einzuleiten. Die Auftragsbearbeiterin stellt der Verantwortlichen die erforderlichen Informationen zur Verfügung, d.h. den Namen, den Ort und die Art der Datenverarbeitung, die von den Unterauftragsverarbeitern Dritter oder den verbundenen Unternehmen von Oracle durchgeführt wird, damit diese ihr Widerspruchsrecht ausüben kann. Die Verantwortliche hat einen allfälligen Widerspruch gegen einen neuen Unterauffragsbearbeiter objektiv zu begründen in Bezug auf die Fähigkeit des Unterauftragsverarbeiters oder des verbundenen Unternehmens von der Auftragsbearbeiterin, personenbezogene Daten in Übereinstimmung mit dem Datenschutz Anhang oder dem anwendbaren europäischen Datenschutzrecht angemessen zu schützen. Hält die Auftragsbearbeiterin trotz Widerspruchs am Beizug des neuen Unterauftragsbearbeiters fest, so initi ert sie einen Einigungsversuch mit der Verantwortlichen, zu dem die Auftragsbearbeiterin weitere Parteien (namentlich den Unterauftragsbearbeiter) beiziehen kann. Scheitert der Einigungsversuch in einem angemessenen Zeitrahmen, steht es der Verantwortlichen frei, auf die Nutzung der Dienstleistungen zu verzichten und den entsprechenden Leistungsabruf zu kündigen. (i) mit einer Vorankündigung von dreissig (30) Tagen; (ii) ohne Haftung der Verantwortlichen oder der Auftragsbearbeiterin gegenüber und (iii) ohne die Verantwortliche von den Zahlungsverpflichtungen der Verantwortlichen im Rahmen der Servicevereinbarung bis zum Datum der Kündigung zu entbinden. Bezieht sich die Kündigung gemäss diesem Abschnitt nur auf einen Teil der Services im Rahmen einer Bestellung, so schliesst die Auftragsbearbeiterin eine Änderungs- oder Ersatzbestellung ab, die diese teilweise Kündigung widerspiegelt.

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

13.4 Die Auftragsbearbeiterin stellt der Verantwortlichen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung, auf schriftlichen Antrag. Soweit es zum Schutz von Geschäftsgeheimnissen oder von anderen vertraulichen Informationen, einschliesslich von Personendaten, notwendig ist, kann die Auftragsbearbeiterin den betreffenden Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

Die Auftragsbearbeiterin haftet gegenüber der Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsbearbeiter seinen Pflichten gemäss dem mit der Auftragsbearbeiterin geschlossenen Vertrag nachkommt. Die Verantwortliche kann verlangen, dass die Auftragsbearbeiterin einen Unterauftragsverarbeiter eines Dritten prüft oder bestätigt, dass eine solche Prüfung stattgefunden hat (oder, sofern verfügbar, einen Prüfbericht eines Dritten über die Tätigkeit des Unterauftragsverarbeiters einholen oder der Verantwortlichen dabei helfen, einen solchen Bericht zu erhalten), um die Einhaltung der Verpflichtungen des Unterauftragsverarbeiters eines Dritten zu überprüfen.

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

[redacted]

14. Internationale Datenübermittlungen

14.1 Jede Übermittlung von Daten durch die Auftragsbearbeiterin an ein Drittland oder eine internationale Organisation erfolgt ausschliesslich auf der Grundlage dokumentierter Weisungen der Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Recht eines Staates, dem die Auftragsbearbeiterin unterliegt, und muss mit Art. 6 DSG (resp. Art. 16 nDSG) im Einklang stehen.

14.2 Die Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen die Auftragsbearbeiterin einen Unterauftragsbearbeiter gemäss Klausel 13 für die Durchführung bestimmter Bearbeitungstätigkeiten (im Auftrag der Verantwortlichen) in Anspruch nimmt und diese Bearbeitungstätigkeiten eine Übermittlung von Personendaten im Sinne von Art. 6 DSG (resp. Art. 16 nDSG) beinhalten, die Auftragsbearbeiterin und der Unterauftragsbearbeiter die Einhaltung von Art. 6 DSG (resp. Art. 16 nDSG) sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäss Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, oder, für bestehende Verträge mit Unterauftragsverarbeitern oder verbundenen Unternehmen, und das voraussichtlich bis Ende Dezember 2022,die im Rahmen der Datenschutzrichtlinie 95/46 angenommen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind. Die Firma bestätigt, dass diese Standardvertragsklauseln ab dem 01. Januar 2023 nicht mehr im Rahmen von Verträgen mit Unterauftragsbearbeitern angewendet werden.

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

C. Koordination und Compliance

15. Unterstützung der Verantwortlichen

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

15.2 Unter Berücksichtigung der Art der Bearbeitung unterstützt die Auftragsbearbeiterin die Verantwortliche durch geeignete technische und organisatorische Massnahmen,, bei der Erfüllung von deren Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten, d.h., dass der Verantwortlichen entweder (i) sicher auf seine Service-Umgebung zugreifen kann, in der sich die personenbezogenen Daten befinden, um die Anfrage zu bearbeiten, oder (ii), sofern der Verantwortlichen ein solcher Zugriff nicht möglich ist, eine "Service-Anfrage" über My Oracle Support (oder ein anderes primäres Support-Tool oder einen anderen Support-Kontakt, der für die Services zur Verfügung gestellt wird, wie z. B. Ihr Projektmanager) mit detaillierten schriftlichen Anweisungen an der Auftragsbearbeiterin übermitteln kann, wie dem Verantwortlichen bei dieser Anfrage geholfen werden kann.

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

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

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

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

Diese Verpflichtungen können von der Auftragsbearbeiterin erfüllt werden, indem der Verantwortlichen elektronischer Zugriff auf eine Aufzeichnung der Verarbeitungstätigkeiten und alle verfügbaren Leitfäden für Datenschutz- und Sicherheitsfunktionen für die Services gewährt wird. Diese Informationen sind verfügbar über (i) My Oracle Support, Document ID 111.1 oder ein anderes für die Services bereitgestelltes primäres Support-Tool, wie das Net-Suite Support Portal, oder (ii) auf Anfrage, wenn dem Verantwortlichen ein solcher Zugang zu My Oracle Support (oder einem anderen primären Support-Tool) nicht zur Verfügung steht.

16. Meldung von Verletzungen der Datensicherheit, allgemeine Bestimmungen

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

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

17.1 Im Falle einer bestätigten Verletzung der Datensicherheit im Zusammenhang mit den von der Auftragsbearbeiterin im Auftrag der Verantwortlichen bearbeiteten Personendaten meldet die Auftragsbearbeiterin diese der Verantwortlichen ohne unnötige Verzögerung (spätestens innerhalb 24 Stunden) nachdem ihr die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

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

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

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

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

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

Im Falle einer bestätigten Verletzung der Datensicherheit im Zusammenhang mit den von der Verantwortlichen bearbeiteten Personendaten unterstützt die Auftragsbearbeiterin die Verantwortliche : unter Berücksichtigung der Art der Verarbeitung und der der Auftragsverarbeiterin zur Verfügung stehenden Informationen,

indem sie Informationen zur Verfügung stellt, um auf die nachfolgenden Aktivitäten reagieren zu können:

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

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

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

   ii. die wahrscheinlichen Folgen der Verletzung der Datensicherheit;

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

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

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

19. Verstösse gegen die Klauseln und Beendigung

Nur bei grob fahrlässigen oder vorsätzlichen Verstössen in erheblichem Umfang oder fortlaufenden Verstössen gegen die Verpflichtungen aus dem Anhang Datenschutz oder dem DPA durch die Auftragsbearbeiterin ("wesentliche Verstösse") gilt das Folgende:

19.1 Falls die Auftragsbearbeiterin ihren Pflichten in materieller Weise, wie in Ziff. 16 der Oracle SCCs der Firma dargelegt, nicht nachkommt, kann die Verantwortliche – unbeschadet der Bestimmungen des DSG/nDSG – die Auftragsbearbeiterin anweisen, die Bearbeitung von Personendaten auszusetzen, bis sie diese Klauseln einhält oder der betroffene Leistungsabruf unter dem Rahmenvertrag beendet ist, je nachdem, welches Ereignis zuerst eintritt .

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

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

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

c) die Auftragsbearbeiterin einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die ihre Pflichten gemäss diesen Klauseln innerhalb der gesetzlich festgelegten Fristen nicht nachkommt.

19.3 Die Auftragsbearbeiterin ist berechtigt, den betroffenen Leistungsabruf zu kündigen, 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 verstossen.

19.4 Nach Beendigung des betroffenen Leistungsabrufs löscht die Auftragsbearbeiterin nach Wahl der Verantwortlichen alle im Auftrag der Verantwortlichen bearbeiteten Personendaten und, auf schriftlichen Antrag, bescheinigt der Verantwortlichen, dass dies erfolgt ist, oder sie gibt alle Personendaten an die Verantwortliche zurück und löscht bestehende Kopien, sofern nicht nach geltendem Recht eine Verpflichtung zur Speicherung der Personendaten besteht. 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 durch die Bezugsberechtigte

20.1 Werden im Rahmen der Cloud-Services von der Bezugsberechtigten Personendaten aus der Schweiz heraus direkt in Cloud-Services der Firma im Ausland übermittelt, und liegt für den betreffenden Staat kein Entscheid des Bundesrates vor, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet[4], so verpflichtet sich die Firma auf schriftliche Aufforderung der Vergabestelle oder der Bezugsberechtigten zur Umsetzung bzw. Dokumentierung einer der folgenden Garantien Hand zu bieten:

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

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

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

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

20.2 Zudem gelten die Ausnahmen gemäss Art. 17 nDSG.

20.3 Werden im Falle von lit. c) die Standarddatenschutzklauseln der EU-Kommission vom 4. Juni 2021 verwendet[5], verpflichtet sich die Firma zur Umsetzung der für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[6],die diesem Anhang als Beilage 2 (Oracle SCC) beigefügt sind.

---

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

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

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

21. Übermittlung von Personendaten ins Ausland im Rahmen der Leistungserbringung

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

Regionale Bindung:

(1) Der Ort der Datenspeicherung 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, gespeichert werden. (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/staatenliste.pdf.download.pdf/20181213_Staatenliste_d.pdf).

21.2 Ungeachtet anderslautender Bestimmungen in den Service-Spezifikationen vereinbaren die Parteien ausdrücklich, dass der Zugriff von der Firma verbundenen Unternehmen (wie in dem Datenschutz Anhang definiert) auf Ihre Inhalte bei der Erbringung der Services nur dann erfolgt, wenn (i) die Bezugsberechtigte der Firma aktiv Zugriff auf der Bezugsberechtigten Inhalte gewähren (z. B. in Verbindung mit einer Support-Anfrage) oder (ii) die Bezugsberechtigte Inhalte als Teil einer Service-Anfrage angeben. Dritte Unterauftragsverarbeiter kann auf der Bezugsberechtigten Inhalte für die Dienste zugreifen, die in der Liste der Unterauftragsverarbeiter aufgeführt sind, die in dem Oracle DPA enthalten ist. Die Firma sorgt dafür, dass die Datenspeicherung gemäss Festlegung durch die Bezugsberechtigte oder die Vergabestelle gemäss Absatz (1) in Ziff. 21.1 umgesetzt wird. Sollte die Firma davon abweichen wollen oder müssen, durch eine Datenmigration, wird sie die Vergabestelle vorgängig in Übereinstimmung mit den Oracle Cloud Hosting and Delivery Policies informieren. Die Firma ist berechtigt, der Bezugsberechtigten Oracle Cloud Services, die in von der Firma beibehaltenen Rechenzentren bereitgestellt werden, zwischen Produktionsrechenzentren in derselben Rechenzentrumsregion (die Rechenzentrumsregion diesie im massgeblichen Service Order festgehalten ist oder wie von der Bezugsberechtigten bei der Aktivierung der Produktionsinstanz des Service festgelegt worden ist), zu migrieren, wenn die Firma dies für erforderlich hält oder im Falle einer Notfallwiederherstellung. Bei Migrationen von Rechenzentren zu anderen Zwecken als der Wiederherstellung im Katastrophenfall wird die Bezugsberechtigte von der Firma mindestens 30 Tage im Voraus informiert -- Ausnahmen sind nur aus absolut zwingenden Gründen möglich, die jedoch so rasch wie möglich der Vergabestelle zur Kenntnis gebracht werden müssen, sobald der Hinderungsgrund für die Information an die Vergabestelle weggefallen ist.

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

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

Personenbezogene Daten dürfen im Rahmen der Erbringung der Cloud-Services durch die Firma von der Schweiz ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 nDSG) [7]. Liegt kein Entscheid des Bundesrates vor, so dürfen personenbezogene Daten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

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

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

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

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

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

Zudem gelten die Ausnahmen gemäss Art. 17 nDSG.

21.5 Werden im Falle von lit. c) die Standarddatenschutzklauseln der EU-Kommission vom 4. Juni 2021 verwendet[8], verpflichtet sich die Firma zur Umsetzung der für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[9], die diesem Anhang als Beilage 2 (Oracle SCC) beigefügt sind.

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

* * *

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

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

4

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 40 – IT- und Datensicherheit

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

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 bewirkt.

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

a) Inhalt der zu schützenden Daten;

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

c) Risiken der Informationssicherheit:

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

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

2. Sicherheit auf IT-Infrastrukturen der Firma

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

2.2 Der Mindestschutz entspricht mindestens den Vorgaben, die sich aus den Standards bzw. Zertifizierungen ergeben, welche die Firma mit ihrer Antwort in der Ausschreibung WTO 20007 zu EK04 («Zertifizierungen») als massgeblich bezeichnet hat. Dies gilt, soweit der aktuelle Stand der Technik sich nicht darüber hinaus entwickelt hat. Für den Fall, dass dieser sich weiterentwickelt hat, wird die Firma sich bemühen und in Betracht ziehen, diesen im Rahmen ihrer Sicherheits-Massnahmen zu berücksichtigen.

2.3 Sofern die Firma einen höheren Standard anbietet, geht sie nicht wesentlich 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. Schutzziele

Die von der Firma und den Bezugsberechtigten ergriffenen Sicherheitsmassregeln müssen davor schützen, dass nicht, ob unbeabsichtigt oder unrechtmässig, eine Vernichtung, ein Verlust, eine Veränderung oder eine unbefugte Offenlegung von beziehungsweise ein unbefugter Zugang zu den zu schützenden Daten resultiert.

4. Dokumentation «IT- und Datensicherheit»

Die Firma stellt der Vergabestelle an einem eindeutig identifizierten und über die Laufzeit des Rahmenvertrags nicht ohne Zustimmung der Vergabestelle zu verändernden Ablageort konsolidierte Informationen bereit, welche über die Sicherheitssituation des Leistungsangebots informiert, ist abrufbar unter dem folgenden Link:

- For **Cloud Services**: Oracle's Hosting & Delivery Policies, verfügbar unter http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- Für **Cloud Services**: Oracle Coporate Security Practices, verfügbar unter https://www.oracle.com/assets/corporate-security-practices-4490843.pdf.

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

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

a) ISO 27001 (ISMS)

b) ISO 27002

c) ISO 27017 (Cloud Security)

d) ISO 27018 (Cloud Privacy)

5.2 Die Firma informiert die Vergabestelle ohne unnötige Verzögerung im Voraus, wenn sie ein Zertifikat nicht weiter aufrechterhalten wird.

5.3 Sollte die Firma eine dieser Zertifizierungen ungewollt verlieren, informiert sie ohne unnötige Verzögerung die Vergabestelle darüber.

5.4 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Zertifikate gemäss Ziff. 5.1 zu. Die Bezugsberechtigte kann in der Cloud-Konsole unter dem Menü-Punkt «Compliance» die eingeholten Zertifikate jederzeit herunterladen.

5.5 Wenn eine zertifizierende Stelle eine Beanstandung für die jeweiligen bezogenen Services ausspricht, wird die Firma die Beanstandung adressieren.

5.6 Für den Fall, dass die Firma einer Benachrichtigungspflicht aus dieser Ziffer nicht nachkommt, hat die Vergabestelle einzig das Recht den/die jeweiligen Auftrag/Aufträge, welche(r) von der Nicht-Verlängerung der in dieser Ziffer genannten OCI-Cloud Services betroffen sind, zu kündigen und bereits bezahlte Vergütungen bzw. Gebühren werden der Vergabestelle anteilig gutgeschrieben.

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

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

a) SOC 1

b) SOC 2

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

6.3 Sollte der Firma eine Attestierung gem. Ziff. 6.1 aberkannt worden sein, informiert sie ohne unnötige Verzögerung die Vergabestelle darüber.

6.4 Die Firma stellt Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Audit-Berichte gemäss Ziff. 6.1 zu. Die Bezugsberechtigte kann in der Cloud-Konsole unter dem Menü-Punkt «Compliance» die eingeholten Audit-Berichte jederzeit herunterladen.

6.5 Wenn eine auditierende Stelle eine Beanstandung ausspricht, wird die Firma die Beanstandung adressieren.

6.6 Für den Fall, dass die Firma einer Benachrichtigungspflicht aus dieser Ziffer nicht nachkommt, hat die Vergabestelle einzig das Recht den/die jeweiligen Auftrag/Aufträge, welche(r) von der Nicht-Verlängerung der in dieser Ziffer genannten OCI-Cloud Services betroffen sind, zu kündigen und bereits bezahlte Vergütungen bzw. Gebühren werden der Vergabestelle anteilig gutgeschrieben.

7. Verschlüsselte Datenhaltung

7.1 Sollte die Bezugsberechtigte einen Verschlüsselungs-Mechanismus, welcher durch die Firma bereitgestellt wurde, nutzen, werden Daten der Bezugsberechtigten auf den Systemen der Firma stets in verschlüsselter Form gespeichert. Die Firma stellt klar, dass (i) Verschlüsslungs-Mechanismen grundsätzlich nur wie in den jeweils anwendbaren Service Specifications and Security Policies seitens der Firma zur Verfügung gestellt werden; und (ii) wo der Verschlüsselungs-Mechanismus verfügbar ist, nicht durch die Vergabestelle bzw. die Bezugsberechtigte abgeschaltet werden darf.

7.2 Für manche Services, (wie in den jeweiligen Services Beschreibungen beschrieben), lässt die Firma zu, dass die Bezugsberechtigte ihre Daten verschlüsseln kann. Sie lässt insbesondere Verschlüsselungsmethoden zu, bei denen ausschliesslich die Bezugsberechtigte den Masterkey besitzt bzw. diesen Masterkey kennt.

7.3 Die Firma identifiziert in ihren jeweiligen Services Beschreibungen und Dokumentationen welche Leistungen der Firma welche Verschlüsselungsmöglichkeiten vorsehen, um einer Bezugsberechtigten, die Leistungen von Firma beziehen will, den Entscheid zu ermöglichen, ob sie die Daten innerhalb eines Tenancys besonders verschlüsseln will (vorausgesetzt, Verschlüsselung ist ein konfigurierbares Feature für den jeweils beauftragten Service und, wenn ja, welche Form der Verschlüsselung sie einsetzen will für den Fall, dass verschiedene Verschlüsselungskontrollen oder Features für den jeweiligen Service verfügbar sind).

8. Verschlüsselte Datenübermittlungen

8.1 Unter dem Rahmenvertrag vorgenommene elektronische Übermittlungen von Daten erfolgen nur über verschlüsselte Kanäle, sofern dies für den gewählten Service gemäss der anwendbaren Service Specifications so vorgesehen ist. Dies betrifft namentlich:

a) Datenübermittlung innerhalb eines Tenants sofern die Bezugsberechtigte lediglich verschlüsselte Protokolle zulässt;

b) Datenübermittlung innerhalb der Systeme der Firma (tenantübergreifend) sofern die Bezugsberechtigte lediglich verschlüsselte Protokolle zulässt und die OCI Konsole / OCI REST API nutzt:

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

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

8.2 Alle Verschlüsselungen bei Übermittlung und Speicherung der Daten erfolgen jeweils mindestens nach dem Standard gem. Ziff. 2 dieses Anhangs.

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

9.1 Die Firma gewährt ihrem Personal nur insoweit Zugang zu Daten der Bezugsberechtigten die Gegenstand der Bearbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist.

9.2 Sofern Personal der Firma Klartextzugriff auf Daten erhält, wobei sich die Parteien darüber einig sind, dass aufgrund der technischen Konfigurationen von OCI ein solcher Klartextzugriff nicht vorgesehen ist, 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.) der Bezugsberechtigten mitzuteilen (Zugriffsprotokolle). Die Bezugsberechtigte hat auf Antrag und im Kontext eines Audits, das Recht, Zugang zu solchen Zugriffsprotokollen zu verlangen, soweit dies verhältnismässig und angemessen ist. In einem solchen Fall antwortet die Firma der Bezugsberechtigten innerhalb eines angemessenen Zeitrahmens unter Beilage der aktuellen Zugriffsprotokolle.

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

10. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

Der Anbieter steht dafür ein, dass seine Hilfspersonen und Subunternehmen die Pflichten des Anbieters unter diesem Vertragsanhang einhalten.

* * *

[redacted]

5

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 50 – 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 (EK06: «Der Anbieter ermöglicht dem Dateneigner den Export (aus der Cloud heraus) und die unwiderrufliche Löschung seiner Daten.»).

Auf dieser Grundlage vereinbaren die Parteien Folgendes:

Im Einzelnen:

I. Datenmigration

1. Datenmigration in die IT-Infrastrukturen der Firma

1.1 Während der Laufzeit des Rahmenvertrages unterstützt die Firma die Bezugsberechtigte auf Wunsch, gegen entsprechende Vergütung nach Abschluss eines entsprechenden separaten Vertrags, bei der Migration von Daten in die Cloud Infrastrukturen (Oracle Cloud Infrastructure «OCI») der Firma.

1.2 Für den Fall, dass die Parteien einen separaten Vertrag gemäss Ziff. 1.1 abgeschlossen haben, gibt die Firma Auskunft über:

a) bestehende Import- und Exportroutinen, welche für die Migration der Daten benutzt werden können;

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

c) weitere notwendige Massnahmen.

1.3 Während der Erbringung der Services kann die Bezugsberechtigte, vorbehaltlich der Verfügbarkeit der Cloud Service Umgebung, ihre Daten jederzeit auf Wunsch aus den Cloud Infrastrukturen (Oracle Cloud Infrastructure "OCI") der Firma abrufen.

1.4 Soll die Bezugsberechtigte angemessene Unterstützung bei der Nutzung der Datenexportfunktionalitäten der Dienste benötigen, kann die Bezugsberechtigte zu diesem Zweck eine Serviceanfrage in My Oracle Support stellen.

2. Anspruch auf Herausgabe

2.1 Während eines Zeitraums von 60 Tagen nach Beendigung der Oracle-Cloud-Services ermöglicht die Firma den Zugang zur OCI Serviceumgebung der Bezugsberechtigten über sichere Protokolle. Die Bezugsberechtigte kann in diesem Fall Daten in einem strukturierten, maschinenlesbaren Format die Inhalte der Bezugsberechtige, die sich in der Umgebung ihrer Oracle-Cloud-Services befinden, eigenständig herunterladen.

2.2 Der Anspruch gemäss Ziff. 2.1 bezieht sich auf Daten, welche die Bezugsberechtigte im Rahmen der Leistungen unter dem Rahmenvertrag auf der OCI Serviceumgebung der Firma speichert oder bearbeitet. Bezüglich Daten, die von vorstehenden Daten abgeleitet sind (wie z.B. gespeicherte Nutzungsprofile, Metadaten, Randdaten, Parametrisierungsdaten, Nutzungsdaten etc.) gelten die Bestimmungen und Rechte der Bezugsberechtigten gemäss Ziff. 12.9. Anhang Datenschutz.

2.3 Die Firma unterstützt die Bezugsberechtigten in angemessener Art und Weise bei der Herausgabe. Die OCI Serviceumgebung der Bezugsberechtigten wird während 60 Tagen erhalten, was es der Bezugsberechtigten ermöglicht auf die Daten zuzugreifen und diese herunterzuladen.

2.4 Die Bezugsberechtigte hat den Anspruch auf die Daten bis zum Ablauf der maximalen Datenspeicherungsdauer gemäss Ziff. 8.1 zuzugreifen und diese herunterzuladen. Dies kann in der in Ziff. 8.1 genannten Frist wiederholt geltend gemacht werden.

3. Unterstützungsleistungen von Firma betreffend Datenmigration aus der OCI der Firma heraus

3.1 Für den Fall, dass die Bezugsberechtige Unterstützung bei einem Übergang benötigt (sei es zu einem anderen Service-Anbieter oder zur Bezugsberechtigten), kann die Bezugsberechtigte zusätzliche professionelle Services von der Firma verlangen ("Transition Services"), und solange die Firma die Art der Transition Services seinen Kunden allgemein zur Verfügung stellt, wird die Firma mit der Bezugsberechtigte nach Treu und Glauben Verhandlungen über solche Transition Services eingehen. Gebühren und Umfang der von der Firma zu erbringenden Transition Services müssen von den Parteien in einem gesonderten Auftrag unter einem separaten Rahmenvertrag vereinbart werden, unter der Voraussetzung, dass die Bezugsberechtigte den Zugang auf ihre Daten ermöglicht.

3.2 Die Firma wird Transition Services gemäss Ziff. 3.1 an die Bezugsberechtigte nicht unbillig verweigern.

3.3 Sofern Firma solche Transition Services nicht standardmässig anbietet, wird sie nach Treu und Glauben Verhandlungen über solche kostenpflichtige Transition Services mit der Bezugsberechtigten eingehen.

II. Datenspeicherung während der Nutzung

4. Sicherung von Daten

Die Firma stellt der Bezugsberechtigten OCI-Services zur Verfügung, damit sie ihre Daten sichern kann, gemäss Anhang IT und Datensicherheit und Cloud Services Agreement

5. Wiederherstellung

Datenwiederherstellungsfunktionen sind in der OCI-Infrastruktur für gesicherte Daten gemäss Ziff. 4 verfügbar und können entsprechend den Oracle-Service-Spezifikationen und den für die Dienste geltenden Sicherheitsrichtlinien konfiguriert werden.

6. Allgemeine Regeln betreffend Datenspeicherung

6.1 Jede Bezugsberechtigte kann in Übereinstimmung mit dem Anhang IT- und Datensicherheit und dem Oracle Cloud Service Vertrag («CSA») den Standort der Datenspeicherung im Rahmen des Leistungsangebots der Firma auf eine bestimmte OCI-Region oder auf mehrere bestimmten OCI-Regionen beschränken.

"OCI-Region" bezieht sich auf die geografische Region, die in der Bestellung der Bezugsberechtigten für diese Services aufgeführt ist, oder, falls zutreffend, auf die geografische Region, die die Bezugsberechtigte bei der Aktivierung der Produktionsinstanz dieser Services ausgewählt hat.

6.2 Die Firma stellt sicher, dass der Datenspeicherungsstandort für bezogene Leistungen in jedem Fall klar (pro Instanz) in der OCI-Cloud-Konsole ersichtlich respektive dokumentiert ist, es kann im Rahmen der Notwendigkeit jede andere OCI-Region gewählt werden. Die OCI Regionen und ihre Standorte sind unter folgendem Link (zu dem Zeitpunkt der Unterzeichnung dieses Anhangs) spezifiziert https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm.

6.3 Die Firma stellt Schnittstellen zur Verfügung (OCI-Cloud-Konsole und OCI-API), die es den Bezugsberechtigten ermöglicht, den Datenspeicherungsstandort (OCI-Region) zweifelsfrei feststellen zu können.

III. Datenspeicherung nach Beendigung des Leistungsbezugs

7. Definition «Vertragsbeendigung»

Als Vertragsbeendigung im Sinne dieses Abschnitts III. gilt der Zeitpunkt, auf welchen eine Partei den Nutzungsvertrag («Auftrag» gemäss CSA) gekündigt hat.

8. Maximale Datenspeicherdauer

8.1 Die Firma erhält den Datenbestand der Bezugsberechtigten während maximal **60 Kalendertagen** nach Vertragsbeendigung gemäss Ziff. 7 (maximale Datenspeicherdauer) und gemäss Ziff. 9 vorgesehen ist.

8.2 Die Firma sorgt dafür, dass der Datenbestand der Bezugsberechtigten anschliessend gemäss Ziff. 9.5 CSA gelöscht wird. Die Anforderungen der Datenlöschung ergeben sich aus Abschnitt IV.

8.3 Ziff. 8.1 gilt nicht, falls die Bezugsberechtigte den Leistungsbezug nach Vertragskündigung und vor Ablauf der 60 Kalendertage Frist gemäss Ziff. 8.1 reaktiviert (sofern die Firma dies überhaupt zulässt): Die maximale Datenspeicherdauer beginnt ab dem Zeitpunkt der definitiven Vertragsbeendigung)

9. Koordinationsregeln im Umfeld der Vertragsbeendigung

9.1 Ab dem Zeitpunkt der Vertragsbeendigung gemäss Ziff. 7 gelten zeitlich gestaffelt das Löschverbot (gemäss Ziff. 9.2) und dann die Löschpflicht der Firma (gemäss Ziff. 9.3).

9.2 Während einer Dauer von 60 Kalendertagen ab Vertragsbeendigung hat die Bezugsberechtigte das Recht, ihren Anspruch gemäss Ziff. 2 dieses Vertragsanhangs auszuüben. Während dieser Dauer ist es der Firma verboten, die Daten (gemäss Ziff.

2.2) zu löschen (**Löschverbot**), es sei denn eine vorzeitige Löschung ist gesetzlich oder gerichtlich angeordnet.

9.3 Nach Ablauf des Löschverbots gemäss Ziff. 9.2 ist die Firma verpflichtet, ihrer Pflicht gemäss Ziff. 8.2 nachzukommen (**Löschpflicht**), es sei denn eine Löschung ist gesetzlich oder gerichtlich verboten.

IV. Datenlöschung

10. Vorbemerkungen

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

10.2 Dieser Abschnitt regelt, wie die Firma Datenlöschungen durchführt.

11. Unwiderrufliche Löschung

11.1 Anforderungen an das Löschverfahren:

a) Die Firma verwendet Verfahren der «Best Practice» und eine Wipinglösung, die den Anforderungen des Standards NIST 800-88 entspricht. Das derzeitige Vorgehen ist in folgenden Dokumenten beschrieben:

   a. https://www.oracle.com/a/ocom/docs/ncsc-cloud-security-principles.pdf

   b. https://www.oracle.com/assets/corporate-security-practices-4490843.pdf

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

c) Datenlöschung kann in Stufen ablaufen. Löschung muss zunächst mindestens bedeuten, dass der betreffende Datensatz auf dem System nicht mehr zur Verfügung steht, so dass auch ein Datenbankadministrator ihn nicht mehr aufrufen könnte[1]. Daran anknüpfende Verfahren (z.B. mehrfaches Überschreiben) beseitigen Daten dauerhaft[2].

d) Die Löschverfahren verhindern eine Wiederherstellung mit forensischen Mitteln.

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

f) Die Firma setzt für alle ihre Leistungen standardisierte Entsorgungsverfahren ein (Disposal Management Services).

11.2 Die Löschung liegt in der Verantwortung der Bezugsberechtigten.

11.3 Die Firma überprüft die Wirksamkeit der Löschung und ihrer Löschmethoden (namentlich in Bezug auf Ziff. 11.1) regelmässig.

11.4 Falls während der Erbringung der Services eine Löschfunktion von den Services in Übereinstimmung mit dem CSA und der anwendbaren Services-Dokumentationen bereitgestellt wird, kann die Bezugsberechtigte ihre in der OCI-Services-Umgebung gespeicherten Daten unwiederbringlich löschen, mit Ausnahme von (i) der Situation, in der die Bezugsberechtigte nach dem Löschen ihrer Daten erneut in die OCI-Services-Umgebung hochladen, und (ii) im Fall von routinemässigen Sicherungen, die im Rahmen

---

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

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

der normalen Geschäftstätigkeit, in Übereinstimmung mit den Cloud Hosting and Delivery Policies, durchgeführt werden.

12. Dokumentation der Löschung

12.1 Löschung von Daten in der OCI-Service-Umgebung der Bezugsberechtigten, die von dieser vorgenommen werden, erzeugen Log-Einträge, auf welche die Bezugsberechtige ausschliesslich Zugriff hat und die von der Bezugsberechtigten heruntergeladen werden können.

12.2 Die Bezugsberechtigte kann mittels automatisierter Auswertung die Log-Einträge auswerten und überprüfen.

12.3 Die Aufbewahrung der Log-Einträge liegt in der Verantwortung der Bezugsberechtigen.

13. Vernichtungspflichten von Unterlagen oder Datenträgern

Die Media Sanitation and Disposal Policy der Firma, welche sich an den NIST 800-88 Standard anlehnt, definiert die Anforderungen für die Vernichtung von Informationen von elektronischen Speichermedien (Sanitization) und die Vernichtung von Informationen, die nicht mehr benötigt werden, zum Schutz vor unberechtigtem Abruf und Rekonstruktion von Vertraulichem. Zu den elektronischen Speichermedien gehören Laptops, Festplatten, Speichergeräte und Wechselmedien.

* * *

[redacted]

6

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

[redacted]

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

7

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 70 – Technische Anforderungen

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

[redacted]

4. Technische Spezifikationen

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

* * *

8

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 80 – Vertraulichkeit der Daten

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

Der vorliegende Vertragsanhang beschreibt die Vertraulichkeitspflichten der Firma.

Schutzziel des vorliegenden Vertragsanhangs ist das Verhindern von unbefugten Klartextzugriffen, soweit dies im Zuständigkeitsbereich der Firma liegt, und das Verhindern der Verwendung von Vertraulichem (wie in Ziff. 1.2, unten, definiert) zu Zwecken der Firma, ihrer Subunternehmen oder zu Zwecken von Dritten.

Im Verhältnis der Parteien beziehungsweise der Firma und der jeweiligen Bezugsberechtigten gelten auch andere Bundesstellen als Dritte.

Vertraulich im Sinne von Ziff. 1.2 meint nicht dasselbe wie vertraulich im Sinne der geltenden ISchV oder Ersatzregelung. Die Parteien sind sich einig, dass die ISchV eine die Bundesverwaltung treffende interne Regelung darstellt.

Soweit die Firma gegenüber der Bundesverwaltung die Erwartung zum Schutz von Vertraulichem hat, regeln die eigenen Vertragsunterlagen der Firma (insbesondere Ziff. 4 des Oracle Cloud Services Vertrags, Ziff. 6 des Data Processing Agreements und Ziff. 5 dieses Anhangs) diese Pflichten; ergänzend gilt Ziff. 17 des Rahmenvertrags (Koordination in Bezug auf das Öffentlichkeitsprinzip).

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

Auf dieser Grundlage und soweit gesetzlich zulässig, vereinbaren die Parteien somit Folgendes:

1. Vertraulichkeit im Allgemeinen

1.1 Die Firma ist verpflichtet, Vertraulichkeit gemäss Ziff. 4.1 und 4.3 des Oracle Cloud Services Vertrags („CSA") «Geheimhaltung», zu gewährleisten. Die Firma darf somit Vertrauliches (wie in Ziff. 1.2 definiert) ohne Zustimmung der Bezugsberechtigten nicht offenbaren, und darf Vertrauliches nicht zu Zwecken der Firma, ihrer Subunternehmen oder zu Zwecken Dritter nutzen. Ziff. 11 des CSA wird durch diese Ziff. 1.1 nicht eingeschränkt.

1.2 Inhalte gemäss Ziff. 19.6 des CSA gelten als **Vertrauliches**. Ergänzend gilt Folgendes:

a) Wenn die Bezugsberechtigte Quelle des Vertraulichen ist oder wenn Vertrauliches für die Bezugsberechtigten bestimmt ist oder wenn die Firma das Vertrauliche im Rahmen der Vertragsbeziehung im Interesse der Bezugsberechtigten erstellt hat, liegt Vertrauliches vor.

b) Inhalte, welche die Bezugsberechtigte oder durch sie autorisierte oder angewiesene Dritte im Rahmen der Leistungen unter dem Rahmenvertrag auf OCI-Infrastrukturen der Firma speichert, bekanntgibt oder bearbeitet, gelten als Vertrauliches.

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

a) Vertrauliches, welches von Ziff. 1.2 a) oder b) abgeleitet ist (z.B. Nutzungsprofile; Metadaten; Randdaten; Parametrisierungsdaten; Nutzungsdaten, etc.).

b) Vertrauliches, welches unter Beobachtung der Angaben gemäss Ziff. 1.2 bei der Firma entstanden ist, gilt als Vertrauliches.

2. Verschwiegenheitspflicht und Schutzpflichten

2.1 Die Firma verpflichtet sich gemäss Ziff. 4.1 «Geheimhaltung» des CSA, über Vertrauliches Stillschweigen zu bewahren.

2.2 Die Firma wird Vertrauliches, welches sich auf der OCI-Infrastruktur befindet, gemäss Anhang IT und Datenschutz und den Oracle Cloud Hosting and Delivery Policies angemessen aufbewahren.

3. Datenherausgabeverbot (Einwilligungsvorbehalt)

Die Firma verpflichtet sich Vertrauliches gemäss Anhang Zugriff auf Daten durch Unbefugte zu behandeln.

4. Verwendungsverbot

4.1 Die Firma verpflichtet sich, Vertrauliches ausschliesslich zum Zwecke einer ordnungsgemässen Abwicklung und Erfüllung dieses Vertrags zu verwenden. Ziff. 11 des CSA wird durch diese Ziff. 4.1 dieses Anhangs nicht eingeschränkt.

4.2 Nach Beendigung des Rahmenvertrags wird die Firma Vertrauliches nicht für eigene Zwecke, zum eigenen Vorteil oder für Zwecke oder zum Vorteil Dritter verwenden, sofern im Anhang Zugriff auf Daten nicht anders angegeben ist.

5. Amtsgeheimnisse, Berufsgeheimnisse, Datengeheimnisse

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

5.2 Die Bezugsberechtigte bleibt verantwortlich für die Einhaltung spezifischer regulatorischer, gesetzlicher oder branchenspezifischer Datensicherheitsverpflichtungen, die für die Bezugsberechtigte in Bezug auf sensible oder spezielle Daten gelten.

5.3 Die Firma unterstützt die Bezugsberechtigten damit diese die Leistungen der Firma beziehen kann, ohne Ziff. 5.1 zu verletzen.

5.4 Die Firma ist verantwortlich für ihre Hilfspersonen und Subunternehmer gemäss Rahmenvertrag Ziff. 19.1.

6. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

Die Firma ist verantwortlich für ihre Hilfspersonen und Subunternehmer gemäss Ziff. 17.2 des CSA.

7. Allgemeine Regeln

7.1 Es gilt gemäss Ziff. 19.6.3 des Rahmenvertrags bezüglich der Dauer der Vertraulichkeitsverpflichtung. Die Vertraulichkeitspflichten der Firma in diesem Vertragsanhang ergänzen die Vertraulichkeitspflichten der Firma gemäss ihren eigenen Vertragsunterlagen. Soweit Abweichungen bestehen, gehen die Regeln im vorliegenden Vertragsanhang vor.

7.2 Keine Verletzung der Vertraulichkeitspflicht liegt bei der Weitergabe von Vertraulichem innerhalb des eigenen Konzerns oder an beigezogene Dritte vor. Die Firma sichert zu, dass ihre Mitarbeiter, Vertreter und Unterauftragnehmer, die Zugang zu Vertraulichem

erhalten, an Geheimhaltungsbestimmungen gebunden sind, die im Wesentlichen den in diesem Anhang festgelegten Bestimmungen entsprechen.

* * *

[redacted]

9

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang 90 – 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. 204859204859 am 07.12.202007.12.2020)

[redacted]

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. Zweck des vorliegenden Vertragsanhangs

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

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

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

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

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

2. Informations- und Dokumentationspflichten allgemeiner Art

2.1 Die Firma hat in Bezug auf die vertraglich vereinbarten Services adäquate technische und organisatorische Massnahmen zur Erreichung eines angemessenen Schutzniveaus ihrer Cloud Infrastrukturen (Oracle Cloud Infrastructure «OCI») implementiert. Die Bezugsberechtigte hat das Recht, diese, sich aus den Servicebeschreibungen ergebenden Massnahmen im Einklang mit dem Anhang Audit zu dokumentieren.

2.2 Unter Berücksichtigung der Art und Weise der Bearbeitung der Informationen, die der Firma zur Verfügung stehen, unterstützt die Firma die Bezugsberechtigte, gemäss Anhang IT- und Datensicherheit und analog den Bestimmungen des Anhangs Datenschutz, in angemessenem Umfang bei bestätigten Verstössen der Verletzungen der Informationssicherheit.

3. Cybervorfälle

3.1 Die Firma bestätigt, dass sie gemäss der jeweils aktuellen Oracle Cloud Hosting and Delivery Policies über Kapazitäten zur technischen Analyse und zur Bewältigung von Cybervorfällen (d.h. Sicherheitsverstösse, die zur widerrechtlichen Aneignung oder zufälligen oder unrechtmässigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum Zugriff auf Informationen führen, die auf Oracle-Systemen übertragen, gespeichert oder anderweitig verarbeitet werden und die die Sicherheit, Vertraulichkeit oder Integrität dieser Informationen beeinträchtigen) verfügt. Sie sorgt in diesem Zusammenhang dafür, dass Verletzungen der Informationssicherheit in ihrem Zuständigkeitsbereich rasch erkannt, deren Ursachen abgeklärt und allfällige Auswirkungen möglichst minimiert werden.

3.2 Die Firma sorgt in ihrem Zuständigkeitsbereich dafür, dass allfällige Risiken für die Informationssicherheit laufend beurteilt werden. Die Bezugsberechtigte kann sich für die entsprechende Benachrichtigung gemäss den Richtlinien für kritische Patch-Updates der Firma registrieren.

3.3 Die Firma unterstützt die Bezugsberechtigte, die Bedarfsstelle und die zuständige Stelle für Cybersicherheit darin, einen Prozess für die Bewältigung von Cybervorfällen zu definieren. Gebühren und Umfang der von der Firma zu erbringenden Unterstützung können von den Parteien in einem gesonderten Auftrag vereinbart werden, sofern die Firma dies aufgrund des Umfangs des Projektes für erforderlich hält.

3.4 Die Firma meldet der Bezugsberechtigten und den gesetzlich vorgeschriebenen Stellen, in Einklang mit den Oracle Corporate Security Practices (Information Security Incident Response), Vorfälle, die Inhalte der Bezugsberechtigten betreffen.

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

4.1 Sofern gesetzlich nicht anders vorgesehen, verpflichtet sich die Firma, die Bezugsberechtigte rechtzeitig über das Auftreten eines oder mehrerer der folgenden Ereignisse zu informieren, jedoch nur in Bezug auf Informationen, die bei der Bereitstellung der Services verarbeitet werden (Meldepflichten):

a) die Firma wird in ein Verfahren verwickelt, in dem ein Dritter (z.B. eine in- oder ausländische Behörde die Firma zur Herausgabe von Vertraulichem auffordert (der Erhalt einer *subpoena* oder eines *warrants* ist der Verfahrenseröffnung gleichgestellt);

b) ein Dritter (z.B. eine Behörde verlangt die Sicherung von Vertraulichem (Erstellen eines Legal Hold oder einer ähnlichen Zustandsaufnahme über Vertrauliches);

c) die Firma wird gerichtlich oder behördlich verbindlich zur Herausgabe von Vertraulichem verpflichtet;

d) es tritt eine Konstellation ein, welche begründeten Anlass zu der Annahme gibt, (i) dass die Firma Gegenstand eines Verfahrens ist (ii) oder neue Pflichten oder Verfahren, auch nach einer Änderung der Rechtsvorschriften des Drittlandes oder einer Massnahme (z. B. einer Aufforderung zur Offenlegung), betreffend Herausgabe von Vertraulichem entstehen lässt, die nicht mit ihren Verpflichtungen aus den EU-Standardvertragsklauseln übereinstimmen (z.B. bevorstehende Übernahme der Firma durch ein ausländisches Unternehmen mit der Wirkung, dass ausländische Behörden Datenherausgabemöglichkeiten erhalten oder Begründung der Anwendbarkeit ausländischer Erlasse, welche einem ausländischen Staat Zugriff auf Vertrauliches ermöglichen, wie z.B. US CLOUD Act oder ähnliche Regeln der US-amerikanischen oder anderer Rechtsordnungen);

e) In jedem der vorgenannten Fälle informiert die Firma auch über den rechtlichen Grund solcher Anfrage und die darüber vorgelegte Antwort. Wenn die Firma solche Zugriffe nicht abwehren konnte oder eine vorgängige Information an die Bezugsberechtigte nicht möglich gewesen sein sollte, informiert die Firma so bald wie möglich darüber, dass ein Zugriff erfolgt ist. Sofern die Firma vom ausländischen Staat zum Stillschweigen über solche Vorgänge verpflichtet wurde, soweit gesetzlich zulässig, informiert sie die Bezugsberechtigte so rasch wie möglich darüber, nachdem die Verpflichtung zum Stillschweigen dahingefallen ist.

4.2 Die Firma trifft die *Abwehrmassnahmen* nach dem anwendbaren Recht -, sie kann insbesondere auch Rechtsbehelfe ergreifen, damit (i) nicht rechtsgültige und bindende Verpflichtungen zur erzwungenen Datenherausgabe entstehen oder (ii) vorbereitende Massnahmen oder Schritte Dritter zur Begründung solcher Verpflichtungen zu Lasten der Firma oder ihrer Subunternehmen verhindert werden oder ohne Wirkung bleiben. Die Firma wird sich generell jederzeit dafür einsetzen, dass im Einklang mit dem geltenden Recht für nicht rechtsgültige und verbindliche Anfragen an die Firma, Bestands- oder Verkehrs- und Inhaltsdaten, wenn überhaupt nur unter Wahrung von Schutzmassnahmen in die Hände einer ausländischen Behörde oder Amtsstelle gelangen.

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

4.4 Wenn eine ausländische Behörde oder Amtsstelle von der Firma die Herausgabe von Vertraulichem fordert und dies gesetzlich zulässig ist, verlangt die Firma, dass die Behörde oder die Amtsstelle die Voraussetzungen, für die von ihr beantragte, erzwungene Datenherausgabe in dokumentierter Weise substantiiert.

4.5 Die Firma leitet die Informationen gemäss der EU-Standardvertragsklauseln an die Bezugsberechtigte weiter.

4.6 Erhält die Firma ein Ersuchen um Offenlegung personenbezogener Daten von einer Strafverfolgungsbehörde, einem staatlichen Sicherheitsorgan oder einer anderen staatlichen Behörde, wird die Firma zunächst im Einzelfall prüfen, ob dieses Offenlegungsersuchen rechtsgültig und für die Firma verbindlich ist. Jede Offenlegungsanfrage, die nicht rechtsgültig und für die Firma demensprechend nicht verbindlich ist, wird in Übereinstimmung mit dem anwendbaren Recht und, soweit gesetzlich zulässig, (i) unter Berufung auf die Privilegien der Bezugsberechtigten des öffentlichen Sektors und dem Statut der Bezugsberechtigten als souveräne(s) staatliche(s) Organ(e) und (ii) auch vor einem Schweizer Gericht oder mit der Bitte um Genehmigung durch eine Schweizer Behörde abgewehrt.

4.7 Vorbehaltlich der folgenden Absätze informiert die Firma die Bezugsberechtigten , die irische Aufsichtsbehörde (die federführende Aufsichtsbehörden der Firma) und die schweizerische Aufsichtsbehörde unverzüglich über rechtsgültige und verbindliche Offenlegungsanträge und bittet die Aufsichtsbehörde, solche Offenlegungsanträge für einen angemessenen Zeitraum zurückzustellen, um der irischen Aufsichtsbehörde die Möglichkeit zu geben, eine Stellungnahme zur Gültigkeit der betreffenden Offenlegung abzugeben.

---

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

4.8 Sofern gesetzlich zulässig, arbeitet die Firma mit der Bezugsberechtigten bei der inhaltlichen Beantwortung des Offenlegungsersuchens zusammen.

4.9 Bei der Beantwortung eines Offenlegungsersuchens hält sich die Firma an die technischen und betrieblichen Sicherheitsmassnahmen, die in der DSGVO und im Anhang zur IT-Sicherheit und zu den Daten vorgesehen sind.

4.10 Die Firma hat interne Richtlinien und Verfahren eingeführt und wird diese beibehalten, um die Einhaltung von Ziff. 15 der EU-Musterklauseln zu ermöglichen, einschliesslich der Rechtsaufsicht durch in der EU ansässige Rechtsteams, Verfahrensschritte und Schulungen zu den geltenden Grundsätzen des europäischen Datenschutzrechts.

4.11 Die Firma veröffentlicht in regelmässigen Abständen einen Transparenzbericht mit aggregierten Informationen über die Anzahl und die Art der rechtsverbindlichen Anfragen, die das Unternehmen in den vorangegangenen 12 Monaten erhalten hat, sowie über die Antwort von der Firma auf die Anfrage (z. B. "vollständige oder teilweise Antwort erteilt", "Antwort verweigert" oder "Bewertung der Antwort"). Die aktuelle Version des Berichts ist abrufbar unter: https://www.oracle.com/a/ocom/docs/cloud/oracle-law-enforcement-requests-report.pdf

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

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

a) der Firma droht Zahlungsunfähigkeit;

b) einem Subunternehmen der Firma droht Zahlungsunfähigkeit im Sinne von 5.1d), welche die Vertraulichkeit oder Verfügbarkeit von Vertraulichem beeinträchtigen könnte;

c) ein Dritter leitet ein Konkurs- oder Nachlassverfahren ein, das im Laufe der 12 folgenden Kalendermonate zu einer Beeinträchtigung der Vertraulichkeit von Vertraulichem oder zu einer Beeinträchtigung der Verfügbarkeit der Leistung oder der in den IT-Infrastrukturen der Firma verwalteten Daten führen könnte;

d) es wird über die Firma oder eines ihrer Subunternehmen der Konkurs oder eine Nachlassstundung (oder ein diesen Massnahmen gleichkommendes Verfahren im Ausland) eröffnet.

5.2 Die Firma stellt sicher, dass Vertrauliches vollständig unter der Bestimmungsgewalt der Bezugsberechtigten verbleibt und trifft Massnahmen, damit Vertrauliches nicht in die Konkursmasse oder in den Nachlass fällt.

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

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

6. Milderungsmassnahmen betreffend Datenherausgaben und Gefahren betreffend Beeinträchtigung der Verfügbarkeit

6.1 Die Firma ergreift nach Ihrem eigenen Ermessen *Milderungsmassnahmen,* wenn sie sich mit einem Ersuchen um Datenherausgabe oder Ähnlichem konfrontiert sieht. Milderungsmassnahmen haben das Ziel, dass Verpflichtungen zur Datenherausgabe im Umfang oder sonst wie in ihrer Wirkung reduziert werden.

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

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

b) Geltendmachung von Regeln des schweizerischen Rechts, die einer Verwendung von Vertraulichem in einem ausländischen Verfahren entgegenstehen (Regeln des CH-Rechts substantiieren, zwecks Comity-Analyse);

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

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

* * *

[redacted]

10

ORACLE

ORACLE CLOUD SERVICES-VERTRAG

Der Text dieses Vertrags unterscheidet sich von dem des standard Oracle Cloud Services-Vertrag

Dieser Oracle Cloud Services-Vertrag (dieser „Vertrag") wird zwischen Oracle Software (Schweiz) GmbH („Oracle", „wir", „uns" oder „unser(e)) und der natürlichen oder juristischen Person abgeschlossen, in deren Namen dieser Vertrag unten unterzeichnet worden ist („Sie", „Ihnen" oder „Ihr(e)). Dieser Vertrag legt die Bedingungen und Konditionen fest, denen die im Rahmen dieses Vertrags erteilten Aufträge unterliegen.

1. NUTZUNG DER SERVICES

1.1 Wir stellen Ihnen die in Ihrem Auftrag aufgeführten Oracle Services (die „Services") gemäss diesem Vertrag und Ihres Auftrags zur Verfügung. Sofern in diesem Vertrag oder in Ihrem Auftrag nichts anderes vereinbart wurde, haben Sie das nicht ausschliessliche, weltweite, beschränkte Recht, die Services während des in Ihrem Auftrag festgelegten Zeitraums ausschliesslich für Ihren internen Geschäftsbetrieb zu nutzen ***(einschließlich einer angemessenen Anzahl von Kopien der in der jeweiligen Leistungsbeschreibung angegebenen Dokumentation (Programmdokumentation)***, sofern es nicht gemäss diesem Vertrag oder Ihrem Auftrag früher beendet wird (der „Servicezeitraum"). Sie dürfen Ihren Benutzern (wie unten definiert) die Nutzung der Services zu diesem Zweck gestatten, und Sie sind dafür verantwortlich, dass sie dabei die Bestimmungen dieses Vertrags und Ihres Auftrags einhalten.

1.2 Die Servicebeschreibungen beschreiben und regeln die Services. Wir sind während des Servicezeitraums berechtigt, die Services und Servicebeschreibungen zu aktualisieren (mit Ausnahme des Datenverarbeitungsvertrags wie unten beschrieben), um unter anderem Änderungen in Bezug auf Gesetze, Vorschriften, Regeln, Technologie, Industriepraktiken, Systemnutzungsverhalten und die Verfügbarkeit von Inhalten Dritter (wie unten definiert) Rechnung zu tragen. Durch die Aktualisierungen der Services oder Servicebeschreibungen durch Oracle wird der Umfang der Leistung, Funktionalität, Sicherheit oder Verfügbarkeit der Services während des Servicezeitraums Ihres Auftrags nicht wesentlich verringert.

1.3 Es ist Ihnen nicht gestattet, und Sie dürfen andere nicht veranlassen oder ihnen gestatten: (a) die Services zu verwenden, um Personen zu belästigen, Schäden oder Verletzungen von Personen oder Eigentum zu verursachen, Materialien zu veröffentlichen, die falsch, verleumderisch, belästigend oder obszön sind, Datenschutzrechte zu verletzen, Fanatismus, Rassismus, Hass oder Leid zu fördern, unerbetene Massen-E-Mails, „Junk-E-Mails", „Spam" oder Kettenbriefen zu versenden, Eigentumsrechte zu verletzen, oder auf sonstige Weise gegen geltendes Recht, Verordnungen oder Vorschriften zu verstossen, (b) Benchmark- oder Verfügbarkeitstests der Services durchzuführen oder offenzulegen oder (c) Leistungs- oder Schwachstellentests der Services ohne die vorherige schriftliche Zustimmung von Oracle durchzuführen oder offenzulegen oder Netzerkennung, Port- und Service-Identifizierung, Schwachstellen-Scans, Knacken von Passwörtern oder Remote-Zugriff-Tests der Services durchzuführen oder offenzulegen; oder (d) die Services zum Schürfen von Cyber-Währung oder Crypto-Währung zu nutzen ((a) durch (d) zusammen gefasst die „Richtlinie zur akzeptablen Nutzung"). Neben anderen Rechten, die wir durch diesen Vertrag und Ihren Auftrag haben, haben wir das Recht, Abhilfemassnahmen zu ergreifen, wenn gegen die Richtlinie zur akzeptablen Nutzung verstossen wird, und zu diesen Abhilfemassnahmen können das Entfernen oder Deaktivieren des Zugriffs auf Materialien gehören, die gegen diese Richtlinie verstossen.

2. GEBÜHREN UND BEZAHLUNG

2.1 Alle zahlbaren Gebühren sind innerhalb von 30 Tagen ab Rechnungsdatum zur Zahlung fällig. Erteilte Aufträge können weder storniert werden, noch können die Beträge erstattet werden, sofern es in diesem Vertrag oder in Ihrem jeweiligen Auftrag nicht anders vereinbart ist. Sie stimmen zu, alle nach geltendem Recht erhobenen Verkaufs-, Mehrwert- oder ähnlichen Steuern zu zahlen, die wir für die von Ihnen bestellten Services entrichten müssen, wobei hiervon die auf der Grundlage unseres Einkommens erhobenen Steuern ausgenommen sind. Solche Spesen sowie Steuern sind in den in einem Auftrag für Services genannten Gebühren nicht inbegriffen.

2.2 Wenn Sie die Menge der bestellten Services überschreiten, müssen Sie die überschreitende Menge unverzüglich erwerben und die entsprechenden Gebühren dafür zahlen.

2.3 Sie erkennen an, dass Sie möglicherweise mehrere Rechnungen für die bestellten Services erhalten.

Rechnungen werden Ihnen gemäss der Oracle Richtlinie für Fakturierungsstandards (Oracle Invoicing Standards Policy) zugestellt, die http://www.oracle.com/us/corporate/contracts/invoicing-standards-policy-1863799.pdf eingesehen werden kann.

3. SCHUTZRECHTE UND EINSCHRÄNKUNGEN

3.1 Sie oder Ihre Lizenzgeber behalten alle Eigentumsrechte und gewerblichen Schutzrechte an Ihren Inhalten (wie unten definiert). Wir oder unsere Lizenzgeber behalten alle Eigentumsrechte und gewerblichen Schutzrechte an den Services, davon abgeleiteten Werken und allen von uns oder in unserem Auftrag im Rahmen dieses Vertrags entwickelten oder bereitgestellten Arbeitsergebnissen.

3.2 Möglicherweise haben Sie durch Nutzung der Services Zugriff auf Inhalte Dritter. Sofern in Ihrem Auftrag nichts anderes dargelegt ist, unterliegen sämtliche Eigentumsrechte und gewerblichen Schutzrechte an Inhalten Dritter sowie die Nutzung dieser Inhalte gesonderten Bestimmungen Dritter, die zwischen Ihnen und dem Dritten vereinbart wurden.

3.3 Sie räumen uns das Recht ein, Ihre Inhalte zu hosten, zu verwenden, zu verarbeiten, anzuzeigen oder zu übertragen, um die Services gemäss diesem Vertrag und Ihrem Auftrag bereitzustellen. Sie tragen die alleinige Verantwortung für die Richtigkeit, Qualität, Integrität, Rechtmässigkeit, Zuverlässigkeit und Angemessenheit Ihrer Inhalte sowie für die Beschaffung sämtlicher Rechte im Zusammenhang mit Ihren Inhalten, die Oracle zur Erbringung der Services benötigt.

3.4 Es ist Ihnen nicht gestattet, und Sie dürfen andere nicht veranlassen oder Ihnen gestatten: (a) irgendeinen Teil der Services zu verändern, abgeleitete Werke davon zu erstellen, zu disassemblieren, zu dekompilieren, zurückzuentwickeln (Reverse Engineering), zu reproduzieren, wieder zu veröffentlichen, herunterzuladen oder zu kopieren (darunter Datenstrukturen oder ähnliche Materialien, die von Programmen produziert werden), (b) auf die Services zuzugreifen und sie zu verwenden, um mit Oracle konkurrierende Produkte oder Services direkt oder indirekt zu erstellen oder zu unterstützen, oder (c) die Services zu lizenzieren, zu verkaufen, zu übertragen, abzutreten, zu vertreiben, auszulagern, Timesharing oder Servicebüronutzung der Services zu gestatten, sie kommerziell zu verwerten oder Dritten zur Verfügung zu stellen, ausser wie durch diesen Vertrag oder Ihren Auftrag zugelassen.

4. GEHEIMHALTUNG

4.1 Aufgrund dieses Vertrags dürfen die Parteien sich gegenseitig Informationen, die vertraulich sind („vertrauliche Informationen"), offenlegen. Vertrauliche Informationen sind auf die im Vertrag oder Ihrem Auftrag vereinbarten Bestimmungen und Preise, Ihre Inhalte in den Services sowie auf alle zum Zeitpunkt der Offenlegung ausdrücklich als vertraulich gekennzeichneten Informationen beschränkt.

4.2 Vertrauliche Informationen der jeweiligen Partei umfassen nicht Informationen, die: (a) ohne Zutun oder Unterlassen der anderen Partei öffentlich bekannt sind oder werden, (b) vor der Offenlegung im rechtmässigen Besitz der anderen Partei waren und deren Besitz die andere Partei weder direkt noch indirekt über die offenlegende Partei erhalten hat, (c) der anderen Partei rechtmässig von einem Dritten ohne Einschränkung zur Geheimhaltung offengelegt werden, oder (d) von der jeweils anderen Partei unabhängig entwickelt werden.

4.3 Jede Partei erklärt sich bereit, für die Dauer von fünf Jahren ab der Offenlegung von vertraulichen Informationen durch die offenlegende Partei keine vertraulichen Informationen der jeweils anderen Partei gegenüber Dritten, die nicht im folgenden Satz angeführt sind, offenzulegen. Wir schützen jedoch die Vertraulichkeit Ihrer Inhalte in den Services, sofern sich diese Informationen in den Services befinden. Die Parteien dürfen vertrauliche Informationen nur den Mitarbeitern, Vertretern oder Unterauftragnehmern offenlegen, die sie ebenso wirksam gegen eine nicht autorisierte Offenlegung schützen, wie es gemäss diesem Vertrag vorgesehen ist, und jede Partei ist berechtigt, die vertraulichen Informationen der anderen Partei in einem rechtlichen Verfahren oder gegenüber einer staatlichen Stelle offenzulegen, wenn dies gesetzlich vorgeschrieben ist. Oracle gewährleistet eine vertrauliche Behandlung Ihrer in den Services befindlichen Inhalte in Übereinstimmung mit den Sicherheitspraktiken von Oracle, die in den für Ihren jeweiligen Auftrag geltenden Servicebeschreibungen definiert sind.

5. SCHUTZ IHRER INHALTE

5.1 Um Ihre Inhalte, die Oracle im Rahmen der Bereitstellung der Services zur Verfügung gestellt werden, zu schützen, hält Oracle die für die betreffenden Services geltenden administrativen, physischen, technischen und

sonstigen Schutzmassnahmen und sonstige entsprechende Aspekte der System- und Inhalteverwaltung ein; diese sind einsehbar unter http://www.oracle.com/us/corporate/contracts/cloud-services/index.html.

5.2 Soweit Ihre Inhalte personenbezogene Daten enthalten (im Sinne der Begriffsdefinitionen in den entsprechenden Datenschutzrichtlinien und dem Datenverarbeitungsvertrag (Definition siehe unten)), wird Oracle darüber hinaus Folgendes einhalten:

a. die für die Services geltenden Datenschutzrichtlinien von Oracle, die unter http://www.oracle.com/us/legal/privacy/overview/index.html zur Verfügung stehen; und

b. die jeweils anwendbare Fassung des Datenverarbeitungsvertrags für Oracle Services (der „Datenverarbeitungsvertrag"), sofern in Ihrem Auftrag nichts anderes bestimmt ist. Die für Ihren Auftrag gültige Fassung des Datenverarbeitungsvertrags *(a)* kann unter https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing eingesehen werden und ist durch Verweis integraler Bestandteil dieses Vertrags und (b) bleibt während des Servicezeitraums Ihres Auftrags in Kraft. Im Falle eines Konflikts zwischen den Bestimmungen des Datenverarbeitungsvertrags und den Bestimmungen der Servicebeschreibungen (einschliesslich aller geltenden Oracle-Datenschutzrichtlinien) haben die Bestimmungen des Datenverarbeitungsvertrags Vorrang.

5.3 Unbeschadet der vorstehenden Abschnitte 5.1 und 5.2 sind Sie verantwortlich für (a) alle erforderlichen Mitteilungen, Zustimmungen und/oder Genehmigungen im Zusammenhang mit Ihrer Bereitstellung und unserer Verarbeitung Ihrer Inhalte (einschliesslich personenbezogener Daten) als Teil der Services, (b) Sicherheitslücken und die Konsequenzen dieser Lücken, die durch Ihre Inhalte, einschliesslich Viren, Trojaner, Würmer oder sonstige schädliche Programmierroutinen, die in Ihren Inhalten enthalten sind, und (c) Ihre Nutzung und die Nutzung der Services durch Ihre Nutzer, die nicht den Bestimmungen dieses Vertrags entspricht. Soweit Sie Ihre Inhalte Dritten gegenüber offenlegen oder an Dritte übermitteln, tragen wir keine Verantwortung für die Sicherheit, Vollständigkeit oder Vertraulichkeit solcher Inhalte, ausserhalb der Kontrolle von Oracle.

5.4 Sofern in Ihrem Auftrag (einschliesslich in den Servicebeschreibungen) nichts anderes bestimmt ist, dürfen Ihre Inhalte keine sensible oder spezielle persönliche Daten beinhalten, die Oracle bestimmte Datensicherheits- oder Datenschutzverpflichtungen auferlegen, neben den in den Servicebeschreibungen niedergelegten Verpflichtungen oder die sich von diesen dort niedergelegten Verpflichtungen unterscheiden. Sofern für die Services verfügbar, können Sie von uns zusätzliche Services erwerben (z. B. Oracle Payment Card Industry Compliance Services), die auf die spezifischen geltenden Datensicherheits- oder Datenschutzanforderungen für solch sensible oder spezielle Daten, die Sie in Ihren Inhalten einbeziehen möchten, abgestimmt sind.

6. GEWÄHRLEISTUNGEN, HAFTUNGSAUSSCHLÜSSE UND AUSSCHIESSLICHE RECHTSBEHELFE

6.1 Jede Partei erklärt, dass sie diesen Vertrag rechtsgültig abgeschlossen hat und hierfür die entsprechende Befugnis und Ermächtigung besitzt. Wir gewährleisten, dass wir die Services innerhalb des Servicezeitraums in allen wesentlichen Aspekten mit wirtschaftlich angemessener Sorgfalt und Kompetenz wie in den Servicebeschreibungen dargelegt erbringen. Falls die Services nicht wie zugesichert erbracht wurden, müssen Sie uns unverzüglich schriftlich informieren und die Mängel der Services beschreiben (und gegebenenfalls die Nummer des Service Requests angeben, mit dem wir über die Service-Mängel in Kenntnis gesetzt wurden).

6.2 WIR GEWÄHRLEISTEN NICHT DIE FEHLER- ODER UNTERBRECHUNGSFREIE ERBRINGUNG DER SERVICES, DIE BEHEBUNG ALLER SERVICE-FEHLER DURCH UNS ODER DIE ERFÜLLUNG IHRER ANFORDERUNGEN ODER ERWARTUNGEN DURCH DIE SERVICES. WIR SIND NICHT FÜR PROBLEME IM ZUSAMMENHANG MIT DER LEISTUNG, DEM BETRIEB ODER DER SICHERHEIT DER SERVICES VERANTWORTLICH, DIE SICH AUS IHREN INHALTEN ODER DEN INHALTEN DRITTER ODER VON DRITTEN ERBRACHTEN SERVICES ERGEBEN.

6.3 BEI EINEM VERSTOSS GEGEN DIE GEWÄHRLEISTUNG FÜR SERVICES BESTEHT IHR AUSSCHLIESSLICHER ABHILFEANSPRUCH UND UNSERE GESAMTE HAFTUNG IN DER KORREKTUR DER MANGELHAFTEN SERVICES, DIE DEN VERSTOSS GEGEN DIE GEWÄHRLEISTUNG VERURSACHT HABEN, ODER, SOFERN WIR DEN MANGEL NICHT IN WIRTSCHAFTLICH ANGEMESSENER WEISE IM WESENTLICHEN BEHEBEN KÖNNEN, SIND SIE BERECHTIGT, DAS BEZIEHEN DER MANGELHAFTEN SERVICES ZU BEENDEN, WORAUFHIN WIR IHNEN DIE GEBÜHREN FÜR DIE BEENDETEN SERVICES FÜR DEN ZEITRAUM NACH DEM DATUM DES INKRAFTTRETENS DER BEENDIGUNG DES BEZUGS ERSTATTEN, DIE SIE IM VORAUS AN UNS BEZAHLT HABEN.

[redacted]

6.4 SOWEIT GESETZLICH ZULÄSSIG, HANDELT ES SICH BEI DEN VORSTEHEND GENANNTEN GEWÄHRLEISTUNGSRECHTEN UM AUSSCHLIESSLICHE UND ES BESTEHEN KEINE SONSTIGEN AUSDRÜCKLICHEN ODER IMPLIZIERTEN GARANTIEN ODER BEDINGUNGEN FÜR SOFTWARE, HARDWARE, SYSTEME, NETZWERKE ODER UMGEBUNGEN ODER FÜR DIE MARKTTAUGLICHKEIT, BEFRIEDIGENDE QUALITÄT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

7. HAFTUNGSBEGRENZUNG

7.1 UNTER KEINEN UMSTÄNDEN HAFTET EINE PARTEI ODER IHRE KONZERNGESELLSCHAFTEN FÜR INDIREKTE ODER FOLGESCHÄDEN ODER FÜR ENTGANGENE EINNAHMEN ODER GEWINNE (MIT AUSNAHME VON GEBÜHREN IM RAHMEN DIESES VERTRAGS) ODER FÜR DEN VERLUST VON UMSÄTZEN, DATEN, DER DATENNUTZUNG, VON GOODWILL ODER DER REPUTATION.

7.2 SOWEIT GESETZLICH ZULÄSSIG, IST DIE GESAMTHAFTUNG VON ORACLE UND UNSEREN KONZERNGESELLSCHAFTEN, DIE SICH AUS ODER IM ZUSAMMENHANG MIT DIESEM VERTRAG ODER IHREM AUFTRAG ERGIBT, OB VERTRAGS-, DELIKTSRECHTLICH ODER ANDERWEITIG, AUF DEN GESAMTBETRAG BESCHRÄNKT, DER FÜR DIE SERVICES, DURCH DEN DIE HAFTUNG VERURSACHT WURDE, IN DEN ZWÖLF (12) MONATEN VOR DEM AUFTRETEN DES HAFTUNGSANSPRUCHS TATSÄCHLICH IM RAHMEN IHRES AUFTRAGS GEZAHLT WURDE.

8. FREISTELLUNG

8.1 Für den Fall, dass ein Dritter Ansprüche gegen Sie oder uns („Empfänger", entweder Sie oder wir, je nachdem, welche Partei das Material empfangen hat) mit der Begründung geltend macht, dass von Ihnen oder uns („Anbieter", entweder Sie oder wir, je nachdem, welche Partei das Material bereitgestellt hat) gelieferte und vom Empfänger verwendete Informationen, technische Konzepte, Spezifikationen, Anleitungen, Software, Service, Daten, Hardware oder sonstiges Material (gemeinsam „Material") gegen die gewerblichen Schutzrechte dieses Dritten verstossen, leistet der Anbieter dem Empfänger gegenüber auf eigene Kosten Rechtsverteidigung und stellt ihn von allen Schadenersatzforderungen, Haftungsansprüchen und Kosten frei, die das Gericht dem Dritten, der eine derartige Rechtsverletzung geltend macht, gewährt oder im Rahmen eines Vergleichs festsetzt, dem der Anbieter zugestimmt hat. Voraussetzung dafür ist, dass der Empfänger die folgenden Bestimmungen einhält:

a. den Anbieter unverzüglich in Kenntnis setzen, und zwar schriftlich und spätestens 30 Tage nach Kenntnisnahme von dem Anspruch (oder früher, falls gesetzlich vorgeschrieben),
b. dem Anbieter die alleinige Kontrolle über die Verteidigungs- und Vergleichsverhandlungen gewähren und
c. dem Anbieter die für die Rechtsverteidigung und vergleichsweise Beilegung erforderlichen Informationen überlassen, dem Anbieter geeignete Unterstützung gewähren und ihm alle entsprechenden Vollmachten erteilen.

8.2 Wenn der Anbieter meint oder festgestellt wird, dass irgendeine Komponente der Materialien die gewerblichen Schutzrechte eines Dritten verletzt haben könnte, hat der Anbieter die Wahl, entweder das Material so zu ändern, dass es keine Schutzrechte mehr verletzt (dabei aber seinen Zweck oder seine Funktionalität im Wesentlichen beibehält), oder eine Berechtigung zur weiteren Nutzung zu verschaffen. Falls keine dieser Möglichkeiten wirtschaftlich vertretbar ist, ist der Anbieter berechtigt, das betreffende Material zurückzuziehen und dem Empfänger eventuell im Voraus bezahlte Gebühren für das Material zurückzuerstatten. Falls eine solche Rückerstattung unsere Fähigkeit, Verpflichtungen aus dem jeweiligen Auftrag nachzukommen, wesentlich beeinträchtigt, können wir nach eigenem Ermessen den Auftrag mit einer Frist von 30 Tagen schriftlich kündigen. Wenn es sich bei solchem Material um Technologie von Drittanbietern handelt und die Kündigung der Lizenz unsererseits durch die Bedingungen der Drittanbieterlizenz untersagt wird, sind wir berechtigt, unter Einhaltung einer Frist von 30 Tagen die in Verbindung mit solchem Material stehenden Services durch schriftliche Mitteilung zu kündigen und Ihnen nicht verwendete Gebühren zurückzuerstatten, die Sie für solche Services im Voraus gezahlt haben.

8.3 Der Anbieter entschädigt den Empfänger nicht, wenn dieser (a) das Material verändert oder zu anderen als den durch die Benutzer- und Programmdokumentation oder die Servicebeschreibungen des Anbieters festgelegten Verwendungszwecken verwendet oder (b) eine überholte Version des Materials verwendet und der Anspruch wegen Rechtsverletzung durch die Nutzung der aktuellen Version des Materials, die dem Empfänger zur Verfügung gestellt worden war, hätte vermieden werden können. Der Anbieter stellt den Empfänger nicht frei, sofern ein Anspruch wegen Rechtsverletzung auf Materialien beruht, die nicht vom Anbieter bereitgestellt wurden. Wir stellen Sie nicht frei, sofern ein Anspruch wegen Rechtsverletzung auf Inhalten von Drittanbietern oder aus einem Drittportal oder einer anderen externen Quelle stammenden Materialien beruht, auf die Sie im Rahmen der Services (z. B. ein Posting eines Blogs oder Forums Dritter in sozialen Netzwerken, eine über einen Hyperlink

[redacted]

erreichte Webseite Dritter, Marketingdaten von externen Datenanbietern) Zugriff haben.

8.4 Dieser Abschnitt 8 regelt den gesamten Umfang der Freistellung bei Rechtsverletzung und alle Ansprüche der Parteien in diesem Zusammenhang abschliessend.

9. LAUFZEIT UND BEENDIGUNG

9.1 Sofern dieser Vertrag nicht früher beendet wird, können Sie während eines Zeitraums ***bis zum 31. August 2026*** ab Annahme dieses Vertrags durch Sie unter diesem Vertrag Aufträge erteilen. Solche Aufträge unterfallen dann für die Dauer des Servicezeitraums des jeweiligen Auftrags weiter den Bestimmungen dieses Vertrags.

9.2 Services werden für den in Ihrem Auftrag festgelegten Servicezeitraum erbracht.

9.3 Wir sind berechtigt, den Zugriff oder die Nutzung der Services für Sie oder Ihre Benutzer auszusetzen, wenn wir annehmen, dass (a) eine erhebliche Bedrohung für die Funktionalität, Sicherheit, Integrität oder Verfügbarkeit der Services oder von Inhalten, Daten oder Anwendungen in den Services besteht, (b) Sie oder Ihre Benutzer zum Begehen unerlaubter Handlungen auf die Services zugreifen oder diese nutzen oder (c) die Richtlinie zur akzeptablen Nutzung verletzt wird. Sofern angemessen durchführbar und gesetzlich zulässig, kündigen wir Ihnen eine solche Aussetzung im Voraus an. Wir ergreifen angemessene Massnahmen, um die Services unverzüglich wiederherzustellen, sobald wir festgestellt haben, dass das für die Aussetzung ursächliche Problem behoben wurde. Während des Aussetzungszeitraums stellen wir Ihnen Ihre Inhalte (wie zum Datum der Aussetzung vorhanden) zur Verfügung. Eine Aussetzung im Rahmen dieses Abschnitts entbindet Sie nicht von Ihrer Verpflichtung, Zahlungen im Rahmen dieses Vertrags zu leisten.

9.4 Sollte einer von uns gegen eine wesentliche Bestimmung dieses Vertrags oder eines Auftrags verstossen und diese Vertragsverletzung nicht innerhalb von 30 Tagen ab Eingang der schriftlichen Abmahnung beheben, ist die jeweils andere Partei zur berechtigt, (a) im Falle eines Verstosses gegen einen Auftrag, den Auftrag zu kündigen, in dessen Rahmen die Vertragsverletzung aufgetreten ist oder (b) im Falle eines Verstosses gegen einen Vertrag, den Vertrag und jedweden Vertrag, der im Rahmen dieses Vertrages zustande gekommen ist, zu kündigen. Falls wir Aufträge wie in dem vorstehenden Satz vorgesehen kündigen, sind Sie verpflichtet, innerhalb von 30 Tagen alle Beträge zu bezahlen, die bis zu einer solchen Kündigung aufgelaufen sind, sowie alle noch nicht bezahlten Beträge für die Services gemäss solcher Aufträge zuzüglich Steuern und Spesen. Ausser bei der Nichtzahlung von Gebühren kann die nicht vertragsbrüchige Partei im eigenen Ermessen zustimmen, den Zeitraum von 30 Tagen so lange zu verlängern, wie die vertragsbrüchige Partei weiterhin angemessene Anstrengungen zur Abhilfe des Verstosses unternimmt. Sie stimmen zu, dass Sie keine bestellten Services nutzen, wenn Sie im Rahmen dieses Vertrags in Verzug geraten.

9.5 Am Ende des Servicezeitraums stellen wir Ihnen Ihre Inhalte (wie am Ende des Servicezeitraums vorhanden) zur Verfügung, sodass Sie diese während eines in den Servicebeschreibungen festgelegten Abrufzeitraums abrufen können. Nach Ablauf dieses Abrufzeitraums und vorbehaltlich eventueller gesetzlicher Anforderungen löschen wir alle Ihre noch in den Services vorhandenen Inhalte oder machen sie auf andere Weise nicht wiederherstellbar. Unsere Praktiken der Datenvernichtung sind ausführlicher in den Servicebeschreibungen beschrieben.

9.6 Bestimmungen, die aufgrund ihrer Rechtsnatur fortbestehen sollen, darunter insbesondere auch solche in Bezug auf Haftung, Freistellung, Zahlung und andere, die aufgrund ihrer Rechtsnatur auf Fortbestand ausgerichtet sind, gelten trotz Kündigung oder Ablauf dieses Vertrags weiter.

10. INHALTE, SERVICES UND WEBSITES DRITTER

10.1 Die Services ermöglichen Ihnen unter Umständen die Verknüpfung mit, die Übermittlung Ihrer Inhalte oder von Inhalten Dritter an, oder den Zugriff auf Websites, Plattformen, Inhalte, Produkte, Services und Informationen Dritter (zusammen „Services Dritter"). Oracle hat keinen Einfluss auf, und ist nicht verantwortlich für, solche Services Dritter. Sie tragen die alleinige Verantwortung für die Einhaltung der Zugangs- und Nutzungsbedingungen von Services Dritter. Sofern Oracle zur Erbringung der Services Ihretwegen auf Services Dritter zugreift oder diese nutzt, sind Sie allein dafür verantwortlich sicherzustellen, dass dieser Zugriff und diese Nutzung, einschliesslich durch an Sie ausgegebene oder Ihnen anderweitig zur Verfügung gestellte Passwörter, Zugangsdaten oder Token, nach den Zugangs- und Nutzungsbedingungen dieser Services gestattet sind. Wenn Sie Ihre Inhalte oder Inhalte Dritter von den Services in einen Service Dritter oder an einen anderen Standort übertragen oder übertragen lassen, stellt diese Übertragung eine Verbreitung durch Sie und nicht durch Oracle dar.

[redacted]

10.2 Inhalte von Dritten, die wir zugänglich machen, werden „wie besehen" („as is") und in der vorhandenen Form ohne jegliche Garantie verfügbar gemacht. Sie erkennen an und erklären sich damit einverstanden, dass wir nicht für Inhalte Dritter verantwortlich und nicht verpflichtet sind, diese zu kontrollieren, zu überwachen oder zu korrigieren. Wir schliessen jegliche Haftung für Inhalte Dritter oder in Verbindung mit Dritten aus.

10.3 Sie erkennen an, dass: (i) die Beschaffenheit, der Typ, die Qualität und die Verfügbarkeit von Inhalten Dritter sich jederzeit während des Servicezeitraums ändern kann und (ii) Funktionen der Services, die mit Services Dritter interagieren, wie beispielsweise Facebook™, YouTube™ oder Twitter™, abhängig sind von der fortwährenden Verfügbarkeit der jeweiligen Anwendungsprogrammierschnittstellen (API). Möglicherweise müssen wir die Services im Rahmen dieses Vertrags in Folge von Veränderungen oder der Nichtverfügbarkeit von Inhalten oder Services Dritter oder von APIs aktualisieren, verändern oder abwandeln. Sollte ein Dritter seine Inhalte Dritter oder APIs nach unserem alleinigen Ermessen nicht mehr zu angemessenen Bedingungen für die Services verfügbar machen, können wir den Zugriff auf die betreffenden Inhalte oder Services Dritter ohne jegliche Haftung Ihnen gegenüber einstellen. Etwaige Änderungen der Inhalte oder Services Dritter oder von APIs sowie auch ihre Verfügbarkeit oder Nichtverfügbarkeit während des jeweiligen Servicezeitraums haben keine Auswirkungen auf Ihre Verpflichtungen im Rahmen dieses Vertrags oder des betreffenden Auftrags, und Sie erlangen keinen Anspruch auf eine Erstattung, Gutschrift oder sonstige Entschädigung für derartige Veränderungen.

11. SERVICEÜBERWACHUNG, ANALYSEN UND ORACLE SOFTWARE

11.1 Die Services werden von uns kontinuierlich überwacht, um Oracle beim Betrieb der Services zu unterstützen, Ihre Service Requests zu bearbeiten, Bedrohungen der Funktionalität, Sicherheit, Integrität und Verfügbarkeit der Services sowie von Inhalten, Daten oder Anwendungen in den Services zu erkennen und zu beheben sowie unerlaubte Handlungen oder Verletzungen der Richtlinie zur akzeptablen Nutzung zu erkennen und zu beheben. Mit den Überwachungstools von Oracle werden Ihre Inhalte in den Services weder gesammelt noch gespeichert, ausser wie für diese Zwecke erforderlich. Nicht von Oracle stammende Software, die von Ihnen oder einem Ihrer Benutzer zur Verfügung gestellt wurde und in den Services gespeichert ist oder in den oder über die Services ausgeführt wird, wird von Oracle nicht überwacht, und es werden keine damit zusammenhängenden Probleme von Oracle bearbeitet. Die durch die Überwachungstools von Oracle erfassten Daten (Ihre Inhalte ausgenommen) können auch zur Unterstützung bei der Verwaltung des Produkt- und Serviceportfolios von Oracle, zur Verbesserung der von Oracle angebotenen Produkte und Services und zur Lizenzverwaltung eingesetzt werden.

11.2 Wir sind berechtigt, (i) statistische und andere Informationen über Leistung, Funktion und Nutzung der Services zusammenzustellen und (ii) Daten aus den Services für das Sicherheits- und Betriebsmanagement und zur Erstellung statistischer Analysen sowie zu Forschungs- und Entwicklungszwecken in zusammengefasster Form zu nutzen (die Bestimmungen i und ii werden als „Leistungsanalysen" bezeichnet). Wir sind berechtigt, die Leistungsanalysen öffentlich verfügbar zu machen. Leistungsanalysen werden jedoch nicht Ihre Inhalte, personenbezogene Daten oder vertrauliche Informationen von Ihnen in einer Form enthalten, die Sie oder andere Personen identifizierbar machen. Oracle behält alle gewerblichen Schutzrechte an den Leistungsanalysen.

11.3 Wir sind berechtigt, Ihnen die Möglichkeit zur Beschaffung bestimmter Oracle Software (wie unten definiert) für die Verwendung mit den Services zur Verfügung zu stellen. Wenn wir Ihnen Oracle Software zu Verfügung stellen und keine gesonderten Bestimmungen für diese Software angeben, dann wird diese Oracle Software als Bestandteil der Services bereitgestellt, und Sie verfügen über das nicht ausschliessliche, weltweite, beschränkte Recht, diese Oracle Software gemäss den Bestimmungen aus diesem Vertrag und Ihrem Auftrag (mit Ausnahme von gesondert lizenzierten Elementen der Oracle Software, für die gesondert lizenzierten Elemente gelten die jeweils geltenden gesonderten Bestimmungen), ausschliesslich für Ihre Nutzung der Services zu verwenden. Sie sind berechtigt, Ihren Benutzern die Verwendung der Oracle Software für diesen Zweck zu erlauben, und Sie sind dafür verantwortlich, dass diese die Lizenzbestimmungen einhalten. Ihr Recht auf Nutzung jedweder Oracle Software endet bei Mitteilung durch uns (durch entsprechende Mitteilung im Internet oder auf andere Weise) oder mit Ende der mit der Oracle Software zusammenhängenden Services, je nachdem, welches Ereignis früher eintritt. Dessen ungeachtet, wenn Oracle Software auf der Grundlage gesonderter Bestimmungen an Sie lizenziert wird, unterliegt Ihre Nutzung dieser Software ausschliesslich diesen gesonderten Bestimmungen. Ihr Recht zur Nutzung eines Teils der Oracle-Software, das unter den gesonderten Bestimmungen lizenziert ist, wird durch diesen Vertrag in keiner Weise eingeschränkt.

12. EXPORT

12.1 Für die Services gelten die Ausfuhrgesetze und -bestimmungen der USA und weitere Ausfuhrgesetze und -bestimmungen relevanter Regionen. Die Nutzung der Services (einschliesslich technischer Daten) sowie etwaiger Arbeitsergebnisse aus Services, die im Rahmen dieses Vertrags bereitgestellt werden, unterliegt diesen Ausfuhrgesetzen, und Sie und wir stimmen zu, alle diese Ausfuhrgesetze und -bestimmungen (einschliesslich der

[redacted]

Bestimmungen für Transportgeschäfte, die als Exporte bzw. Reexporte gelten) einzuhalten. Sie stimmen zu, dass keine Daten, Informationen, Produkte und/oder Ergebnisse von Services (oder unmittelbaren Produkten von diesen) direkt oder indirekt unter Verstoss gegen diese Gesetze ausgeführt oder für andere, von diesen Gesetzen verbotene Zwecke wie die Proliferation nuklearer, chemischer oder biologischer Waffen oder die Entwicklung von Raketentechnik, verwendet werden.

12.2 Sie erkennen an, dass die Services so konzipiert sind, dass Sie und Ihre Benutzer unabhängig vom Standort auf die Services zugreifen und Ihre Inhalte zwischen den Services und an andere Standorte wie die Arbeitsplätze der Benutzer verlegen oder übertragen können. Sie allein sind für die Autorisierung und Verwaltung der Benutzerkonten sowie die Exportkontrolle und die geographische Verlegung Ihrer Inhalte verantwortlich.

13. HÖHERE GEWALT

Weder Sie noch wir haften für eine unterlassene oder verzögerte Erbringung von Services, wenn diese durch eine der folgenden Ursachen hervorgerufen wird: kriegerische oder feindliche Handlungen oder Sabotage, Naturkatastrophen, Pandemien, Ausfälle der Stromversorgung, des Internets oder des Telekommunikationsverkehrs, die nicht durch die verpflichtete Partei verursacht wurden, staatliche Beschränkungen (einschliesslich der Verweigerung oder Aufhebung einer Export- oder Importlizenz oder sonstiger Genehmigungen) oder sonstige Ereignisse, die ausserhalb der zumutbaren Kontrolle der verpflichteten Partei liegen. Sowohl Sie als auch wir werden zumutbare Anstrengungen unternehmen, um die Auswirkungen von Ereignissen höherer Gewalt zu mindern. Sollte ein solches Ereignis für mehr als 30 Tage andauern, können sowohl Sie als auch wir die nicht geleisteten Services und betroffenen Aufträge schriftlich kündigen. Dieser Abschnitt entbindet die Parteien nicht von ihrer Verpflichtung, zumutbare Schritte im Rahmen ihrer normalen Disaster Recovery-Verfahren durchzuführen, noch hebt er Ihre Verpflichtung auf, für die Services zu bezahlen.

14. RECHT UND GERICHTSSTAND

Der Vertrag unterliegt dem Recht der Schweiz, und beide Parteien vereinbaren, sich bei etwaigen Rechtsstreitigkeiten im Rahmen dieses Vertrags der ausschliesslichen Gerichtsbarkeit der Gerichte in ***Bern***, Schweiz zu unterwerfen. Das UN-Kaufrecht (C.I.S.G.) ist ausgeschlossen.

15. MITTEILUNGEN

15.1 Alle Mitteilungen an die jeweils andere Partei, die im Rahmen dieses Vertrags erforderlich sind, bedürfen der Schriftform. Bei Rechtsstreitigkeiten mit uns, oder falls Sie auf der Grundlage des in diesem Vertrag enthaltenen Abschnitts zur Freistellung eine Mitteilung machen möchten oder wenn Sie Gegenstand eines Insolvenz- oder anderen ähnlichen Rechtsverfahrens werden, machen Sie unverzüglich schriftlich Mitteilung an: ORACLE Software (Schweiz) GmbH, The Circle 32, 8058 Zürich, Schweiz, z.H.: Rechtsabteilung.

15.2 Wir können an unsere Services-Kunden Hinweise in Form von allgemeinen Hinweisen im Oracle Portal für die Services erstellen und an Sie persönlich gerichtete Hinweise per E-Mail an Ihre bei uns gespeicherte E-Mail-Adresse oder in einem Schreiben per „First Class Mail" oder frankierter Post an Ihre bei uns gespeicherte Postadresse senden.

16. ABTRETUNG

Sie dürfen diesen Vertrag weder abtreten noch die zu erbringenden Services bzw. Ansprüche daran an dritte natürliche oder juristische Personen weitergeben oder übertragen.

17. SONSTIGES

17.1 Wir sind ein unabhängiger Vertragspartner, und die Parteien stimmen überein, dass zwischen ihnen keinerlei Partnerschaft, Joint Venture oder Vertretungsverhältnis besteht.

17.2 Unser Geschäftspartner sowie andere Dritte, darin eingeschlossen alle Drittparteien, die sich in einem Integrationsprozess mit den Services befinden, oder alle von Ihnen für die Bereitstellung von Beratungs- oder Implementierungsservices oder von mit den Services interagierenden Anwendungen beauftragten Drittparteien, sind von Oracle unabhängig und keine Vertreter von Oracle. Wir sind nicht für aufgrund von Handlungen solcher Geschäftspartner oder Drittparteien entstehende Probleme mit den Services oder Ihren Inhalten haftbar oder verantwortlich, es sei denn, der Geschäftspartner oder die Drittpartei erbringt Services als unser Unterauftragnehmer im Rahmen einer Beauftragung gemäss diesem Vertrag. In diesem Fall haften wir nur im gleichen Masse, wie es auch für unsere Ressourcen im Rahmen dieses Vertrags vorgesehen ist.

[redacted]

17.3 Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt, und eine derartige Bestimmung ist durch eine andere Bestimmung zu ersetzen, die dem Zweck und der Absicht dieses Vertrags entspricht.

17.4 Abgesehen von Klagen wegen Nichtzahlung oder Verletzung gewerblicher Schutzrechte von Oracle dürfen Klagen, gleich welcher Art, die sich aus oder im Zusammenhang mit dem vorliegenden Vertrag ergeben, von keiner Partei mehr als zwei Jahre nach Entstehung des Klagegrundes erhoben werden.

17.5 Vor Erteilung eines Auftrags, der diesem Vertrag unterliegt, liegt es allein in Ihrer Verantwortung, festzustellen, ob die Services Ihren technischen, geschäftlichen oder aufsichtsrechtlichen Anforderungen entsprechen. Oracle wird Sie in Ihren Bemühungen unterstützen, um festzustellen, ob die Verwendung der standardmässigen Services diesen Anforderungen entspricht. Für von Oracle geleistete zusätzliche Arbeiten oder Änderungen der Services können zusätzliche Gebühren anfallen. Sie tragen die alleinige Verantwortung für die Erfüllung der gesetzlichen Vorschriften in Verbindung mit Ihrer Nutzung der Services.

17.6 Bei schriftlicher Vorankündigung mit einer Frist von fünfundvierzig (45) Tagen und maximal einmal innerhalb von zwölf (12) Monaten ist Oracle berechtigt Ihre Nutzung der Cloud Services zu prüfen, um sicherzustellen, dass Sie die Cloud Services gemäss den Bestimmungen aus dem zugehörigen Auftrag und diesem Vertrag nutzen. Eine solche Prüfung darf Ihren normalen Geschäftsbetrieb nicht übermässig stören.

Sie verpflichten sich, bei derartigen Audits durch Oracle zu kooperieren, angemessene Unterstützung zu leisten und Zugriff auf Informationen zu gewähren, die Oracle in angemessenem Umfang anfordert.

Die Durchführung des Audit und die dabei gewonnenen nicht öffentlichen Daten (einschliesslich der aus dem Audit resultierenden Feststellungen oder Berichte) unterliegen den Bestimmungen aus Abschnitt 4 (Geheimhaltung) dieses Vertrags.

Wenn beim Audit eine Nichteinhaltung festgestellt wird, erklären Sie sich damit einverstanden, diese innerhalb von 30 Tagen nach schriftlicher Mitteilung über diese Nichteinhaltung zu beheben (was ohne Einschränkung auch die Zahlung von Gebühren für zusätzliche Cloud Services beinhalten kann). Sie stimmen zu, dass Oracle nicht für Ihre Kosten haftet, die durch die Zusammenarbeit bei dem Audit entstehen.

18. GESAMTER VERTRAG

18.1 Sie sind damit einverstanden, dass dieser Vertrag und die durch schriftlichen Verweis ausdrücklich als Vertragsbestandteil aufgenommenen Informationen (darunter auch Hinweise auf Angaben, die einer URL oder einschlägigen Richtlinien von Oracle zu entnehmen sind) zusammen mit dem dazugehörigen Auftrag den gesamten Vertrag für die von Ihnen bestellten Services darstellen und dass dieser Vertrag alle zuvor oder gleichzeitig, mündlich oder schriftlich getroffenen Verträge oder Abmachungen in Bezug auf derartige Services ersetzt.

18.2 Es wird ausdrücklich vereinbart, dass die Bestimmungen des vorliegenden Vertrags und jeglicher Aufträge mit Oracle vorrangig im Verhältnis zu den Bestimmungen, die gegebenenfalls in nicht von Oracle verwendeten Bestelldokumenten, Portalen oder sonstigen Dokumenten enthalten sind, gelten; solche Bestimmungen haben keinerlei Geltung für die bestellten Services. Bei Unstimmigkeiten zwischen den Bestimmungen eines Auftrags und dem Vertrag hat der Auftrag Vorrang. Sofern es jedoch nicht ausdrücklich anders in einem Auftrag festgelegt wird, gelten die Bestimmungen des Datenverarbeitungsvertrags vorrangig vor jeglichen abweichenden Bestimmungen in einem Auftrag. Änderungen dieses Vertrags und darunter erteilter Aufträge sind nicht zulässig, und Änderungen der Rechte und Einschränkungen bzw. der Verzicht darauf müssen schriftlich von autorisierten Vertretern von Ihnen und Oracle genehmigt oder online angenommen werden; Oracle ist jedoch berechtigt, die Servicebeschreibungen zu aktualisieren, darunter durch Veröffentlichen aktualisierter Dokumente auf den Websites von Oracle. Durch diesen Vertrag entstehen keine Beziehungen zu Drittbegünstigten.

19. VERTRAGSDEFINITIONEN

19.1 „**Oracle Software**" bezeichnet jede Art von Software-Agent, Anwendung oder Tool, den/die/das Oracle Ihnen zum Download bereitstellt, um Ihnen den Zugriff auf die sowie den Betrieb der und/oder die Nutzung mit den Services zu erleichtern.

19.2 „**Programmdokumentation**" bezeichnet die Benutzerhandbücher, Hilfe-Fenster und Readme-Dateien für

[redacted]

die Services sowie jegliche Oracle Software. Die Dokumentation können Sie unter http://oracle.com/contracts oder einer anderen, von Oracle eventuell genannten Internetadresse einsehen.

19.3 „**Servicebeschreibungen**" bezeichnet die folgenden Dokumente, die jeweils auf die bestellten Services anwendbar sind: (a) die Oracle Cloud Hosting and Delivery Policies, die Programmdokumentation, die Oracle Service Descriptions und der Datenverarbeitungsvertrag wie in diesem Vertrag definiert, (b) in den Datenschutzrichtlinien von Oracle und (c) alle anderen Oracle Dokumente, auf die in Ihrem Auftrag verwiesen wird bzw. die Bestandteil Ihres Auftrags sind. Folgendes gilt nicht für Services, die keine Cloud-Serviceangebote von Oracle sind und mit Ihrem Auftrag erworben werden, wie beispielsweise Beratungsservices: die Oracle Cloud Hosting and Delivery Policies und die Programmdokumentation. Folgendes gilt nicht für Oracle Software: die Oracle Cloud Hosting and Delivery Policies, Oracle Service Descriptions und der Datenverarbeitungsvertrag.

19.4 „**Inhalte Dritter**" bezeichnet alle Software, Daten, Texte, Bilder, Audio- und Videomaterialien, Fotografien und sonstigen Inhalte und Materialien in jedem Format, die von nicht zu Oracle gehörenden Dritten übernommen oder abgeleitet und Ihnen im Rahmen oder in Verbindung mit Ihrer Nutzung der Services bereitgestellt werden. Beispiele für Inhalte Dritter sind Data-Feeds von Social Network-Services, RSS-Feeds von Blog-Posts, Oracle Datenmärkte und -bibliotheken, Wörterbücher sowie Marketingdaten. Inhalte Dritter umfassen auch von Dritten stammendes Material, auf das durch Ihre Nutzung der Services oder von durch Oracle bereitgestellten Tools zugegriffen oder das auf diese Weise beschafft wird.

19.5 „**Benutzer**" bezeichnet, für die Services, diejenigen Mitarbeiter, Auftragnehmer und Endnutzer, die durch Sie oder in Ihrem Namen ermächtigt sind, die Services in Übereinstimmung mit diesem Vertrag und Ihrem jeweiligen Auftrag zu nutzen. Für Services, die speziell dafür entworfen sind, Ihren Klienten, Vertretern, Kunden, Lieferanten oder anderen Dritten den Zugriff auf die Services zur Interaktion mit Ihnen zu gewähren, werden solche Dritte als „Benutzer" betrachtet, für die die Bestimmungen dieses Vertrags und Ihres Auftrags gelten.

19.6 „**Ihre Inhalte**" bezeichnet alle Software, Daten (einschliesslich persönlicher Daten), Texte, Bilder, Audio- und Videomaterialien, Fotografien, nicht von Oracle stammenden Anwendungen oder Anwendungen Dritter sowie sonstigen Inhalte und Materialien in jedem Format, die von Ihnen oder im Auftrag Ihrer Benutzer bereitgestellt werden und in den Services gespeichert sind, in den oder über die Services ausgeführt werden. Diesem Vertrag unterliegende Services, Oracle Software, andere Oracle Produkte und Services sowie das geistige Eigentum von Oracle und alle Bearbeitungen hiervon unterfallen nicht dem Begriff „Ihre Inhalte". Ihre Inhalte umfassen auch jegliche Inhalte Dritter, die Sie durch Ihre Nutzung der Services oder von durch Oracle bereitgestellten Tools in die Services einbringen.

20. DATUM DES INKRAFTTRETENS DER CLOUD SERVICES VERTRAGS

Dieser Vertrag über Cloud Services tritt am 18.08.2022 in Kraft. (DAS DATUM WIRD VON ORACLE EINGESETZT)

DER REST DIESER SEITE WURDE ABSICHTLICH LEER GELASSEN. DER UNTERSCHRIFTENBLOCK FÜR DIESEN VERTRAG FOLGT AUF DER NÄCHSTEN SEITE.

[redacted]

21. 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, 16.8.2022.

[redacted]

[redacted]

Für die Bedarfsstelle
Bundeskanzlei - BK
Ort und Datum: ....Bern 15.8.2022

[redacted]

[redacted]

Für die Firma
Oracle Software (Schweiz) GmbH
Ort und Datum: ....Zürich, 18.08.2022

[redacted]

[redacted]

11

ORACLE

Data Processing Agreement for Oracle Services

("Data Processing Agreement")

The text of this Data Processing Agreement for Oracle Services differs from the standard

Version June 26, 2019

1. Scope and Applicability

1.1 This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

1.2 In addition, any Processing of Personal Information subject to Applicable European Data Protection Law is subject to the additional terms of the European DPA Addendum set out in Exhibit 1 and the Oracle Processor Code referenced therein.

2. Responsibility for Processing of Personal Information and Your instructions

2.1 The Bezugsberechtigte is a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Oracle will Process Personal Information solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In addition to the Bezugsberechtigte's instructions incorporated into the Services Agreement, the Bezugsberechtigte may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist the Bezugsberechtigte to comply with its Controller obligations under Applicable Data Protection Law relevant to its use of the Services.

2.4 Oracle will follow the Bezugsberechtigte's instructions at no additional cost to it and within the timeframes reasonably necessary for the Bezugsberechtigte to comply with its obligations under Applicable Data Protection Law. To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform the Bezugsberechtigte thereof upon receiving itsinstructions. Without prejudice to Oracle's obligation to comply with the Bezugsberechtigte's instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

2.5 The Bezugsberechtigte may provide Oracle access to sensitive or special categories of Personal Information, provided that (i) Oracle will indistinctly process such sensitive or special Personal Information pursuant to the terms of the Data Processing Agreement; and (ii) the Bezugsberechtigte will remain responsible for compliance with specific regulatory, legal or industry data security obligations which may apply to such sensitive or special Personal Information."

3. Privacy Inquiries and Requests from Individuals

[redacted]

3.1 If the Bezugsberechtigte receives a request or inquiry from an Individual related to Personal Information processed by Oracle for the provision of Services, the Bezugsberechtigte can either (i) securely access the Services environment that holds Personal Information to address the request, or (ii) to the extent such access is not available to the Bezugsberechtigte, submit a "service request" via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Oracle's project manager) with detailed written instructions to Oracle on how to assist the Bezugsberechtigte with such request.

3.2 If Oracle directly receives any requests or inquiries from Individuals that have identified the Bezugsberechtigte as the Controller, it will promptly pass on such requests to the Bezugsberechtigte without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

4. Oracle Affiliates and Third Party Subprocessors

4.1 To the extent Oracle engages Third Party Subprocessors and/or Oracle Affiliates to Process Personal Information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement. Oracle is responsible for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

5. Cross-border data transfers

5.1 Without prejudice to any applicable regional data center restrictions for hosted Services specified in the Services Agreement, Oracle may Process Personal Information globally as necessary to perform the Services.

5.2 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable Data Protection Law, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law, **including Clause 10 below.**

6. Security and Confidentiality

6.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services the Bezugsberechtigte have ordered are set out in the relevant security practices for these Services:

- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at:

[redacted]

http://www.netsuite.com/portal/resource/terms-of-service.shtml;

- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: https://www.oracle.com/support/policies.html;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: http://www.oracle.com/us/corporate/contracts/consulting-services/index.html.

6.2 All Oracle and Oracle Affiliates employees, as well as any Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

7. Audit Rights
Intentionally Left Blank

8. Incident Management and Breach Notification

8.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence.

8.2 Oracle will notify the Bezugsberechtigte for each respective Order of a confirmed Personal Information Breach regarding the respective Services covered by each Order without undue delay but at the latest within 24 hours. As information regarding the Personal Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide the Bezugsberechtigte with (i) a description of the nature and reasonably anticipated consequences of the Personal Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of Personal Information that were the subject of the Personal Information Breach. The Bezugsberechtigte and Oracle agree to coordinate on the content of intended public statements of the Bezugsberechtigte or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Personal Information Breach.

9. Return and Deletion of Personal Information
Intentionally Left Blank

10. Disclosure Requests in Domestic or Foreign Proceedings

Section 4 of "Anhang Zugriff auf Daten durch Unberechtigte" does apply.

11. Definitions

"**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, which may include Applicable European Data Protection Law.

"**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as **amended (e.g. 25**

[redacted]

September 2020) plus ordinance(s); and/or (iii) the UK Data Protection Act 2018.

"**Europe**" means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway; (ii) Switzerland and (iii) the UK after it withdraws from the EU.

"**Individual**" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

"**Process/Processing**", "**Controller**", "**Processor**" and "**Binding Corporate Rules**" (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

"**Oracle Affiliate(s)**" means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in Section 4.

"**Oracle Intra-Company Data Transfer and Mandate Agreement**" means the Oracle Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

"**Oracle Processor Code**" means Oracle's Privacy Code for Processing Personal Information of Customer Individuals referenced in the European DPA Addendum.

"**Oracle**" means the Oracle Affiliate that has executed the Services Agreement.

"**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.

"**Personal Information Breach**" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Information.

"**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.

"**Services**" or the equivalent terms "Service Offerings" or "services" means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

"**Services Agreement**" means (i) the applicable order for the Services the Bezugsberechtigte has purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications.

"**Third Party Subprocessor**" means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in Section 4.

"You" means the respective Bezugsberechtigte that places the order under the Services Agreement. Other capitalized terms have the definitions provided for them in the Services Agreement.

[redacted]

Exhibit 1: European Data Processing Addendum for Oracle Services

("European DPA Addendum")

This European DPA Addendum supplements the Data Processing Agreement to include additional Processor terms applicable to the Processing of Personal Information subject to Applicable European Data Protection Law.

Except as expressly stated otherwise in the Data Processing Agreement, the Services Agreement, this European DPA Addendum or the Oracle Processor Code, in the event of any conflict between these documents, the following order of precedence applies (in descending order): (i) the Oracle Processor Code; (ii) this European DPA Addendum; (iii) the body of the Data Processing Agreement; and (iv) the Services Agreement.

1. Cross-Border Data Transfers – Oracle Processor Code

1.1 The Oracle Processor Code (Binding Corporate Rules for Processors) applies to the Processing of Personal Information by Oracle on behalf of the Bezugsberechtigte in its role as a Processor as part of the provision of Services under the Services Agreement and this European DPA Addendum, where such Personal Information is: (i) subject to any data transfer restrictions under Applicable European Data Protection Law; and (ii) processed by Oracle or an Oracle Affiliate in a country outside Europe.

1.2 The most current version of the Oracle Processor Code is available on https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing, and is incorporated by reference into the Services Agreement and this European DPA Addendum. Oracle has obtained EEA authorization for its Processor Code and will maintain such authorization for the duration of the Services Agreement.

1.3 Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with the Oracle Processor Code, the Data Processing Agreement and the Services Agreement.

2. Description of Processing

2.1 *Duration of processing activities.* Oracle may Process Personal Information during the term of the Services Agreement and to perform its obligations under Section 9 of the Data Processing Agreement, unless otherwise required by applicable law.

2.2 *Processing activities.* Oracle may Process Personal Information as necessary to perform the Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.3 *Categories of Personal Information.* In order to perform the Services and depending on the Services the Bezugsberechtigte has ordered, Oracle may Process some or all of the following categories of Personal Information: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or

children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; IP addresses and online behavior and interest data.

2.4 *Categories of Data Subjects.* Categories of Data Subjects whose Personal Information may be Processed in order to perform the Services may include, among others, Your representatives and end users, such as Your employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Additional or more specific descriptions of Processing activities, categories of Personal Information and Data Subjects may be described in the Services Agreement.

3. Your Instructions

3.1 The Bezugsberechtigte's right to provide instructions to Oracle under the respective Order as specified in Section 2 of the Data Processing Agreement encompasses instructions regarding (i) data transfers as set forth in Section 1 of this European DPA Addendum; and (ii) assistance with Data Subject requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information or sets of Personal Information as described in Section 3 of the Data Processing Agreement.

3.2 To the extent required by the Applicable **European** Data Protection Law, Oracle will immediately inform the Bezugsberechtigte if, in its opinion, its instruction infringes Applicable European Data Protection Law. The Bezugsberechtigte acknowledges and agree sthat Oracle is not responsible for performing legal research and/or for providing legal advice to the Bezugsberechtigte.

4. Notice and Objection Right to New Oracle Affiliates and Third Party Subprocessors

4.1 Subject to the terms and restrictions specified in this Section 4 of the European DPA Addendum and Section 4 of the Data Processing Agreement, the Bezugsberechtigte provides Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors to assist in the performance of the Services.

4.2 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the NetSuite Support Portal or Your Oracle project manager). If You would like to receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, the Bezugsberechtigte can (i) sign up per the instructions on My Oracle Support, Document ID 2288528.1; or (ii) Oracle will provide you notice of intended changes where a sign up mechanism is not available. For ACS and Consulting Services, any additional Third Party Subprocessors that Oracle intends to use will be listed in the order for ACS or Consulting Services, or in a subsequent "Oracle Subprocessor Notice", which Oracle will send to the Bezugsberechtigte by e-mail as necessary.

4.3 Within fourteen (14) calendar days of Oracle providing such notice to the Bezugsberechtigte under Section 4.2 above, the Bezugsberechtigte may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Information in accordance with the Data Processing Agreement or Applicable European Data Protection Law in writing by submitting a "service request" via (i) My Oracle Support (or other applicable primary

[redacted]

support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. The Bezugsberechtigte and Oracle will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable European Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 4.3 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

5. Information and Assistance

5.1 For hosted Services, the Bezugsberechtigte's audit rights under Section 7 of the Data Processing Agreement include the right to conduct inspections of the applicable Services data center facility that hosts Personal Information.

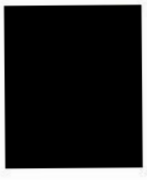
5.2 In addition, the Bezugsberechtigte may request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations. The Bezugsberechtigte will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Information.

5.3 Oracle provides the Bezugsberechtigte with information and assistance reasonable necessary for it to conduct Your data protection impact assessments or consult with its Regulator(s), by granting it electronic access to a record of Processing activities and any available privacy & security functionality guides for the Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Services, such as the NetSuite Support Portal, or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to the Bezugsberechtigte.

6. Data Protection Officer

6.1 Oracle has appointed a Global Data Protection Officer and, in some European countries, a local Data Protection Officer. Further details on how to contact Oracle's Global Data Protection Officer and, where applicable, the local Data Protection Officer, are available here.

6.2 If the Bezugsberechtigte has appointed a Data Protection Officer, it may request Oracle to include the contact details of its Data Protection Officer in the relevant Services order.



12

ORACLE

EU Standard Contractual Clauses for Controller to Processor Transfers ("Clauses")

Preamble

1. The Clauses apply to the Processing of Personal Information by Oracle in its role as a Processor as part of the provision of Services under the applicable order with its effective date, and the applicable master agreement referenced in the order (the "Agreement") between You and Oracle, where such Personal Information is processed by Oracle or an Oracle Affiliate in a third country outside the EU/EEA or Switzerland that has not received an adequacy finding under Applicable European Data Protection Law.

2. The Clauses will be read in conjunction with the Agreement and the Supplementary Measures to the Clauses attached as Annex 4 to the Clauses. To the extent permissible under Clauses 4 and 5 of the Clauses, the Parties agree that:

   (a) the modalities of the audit rights under Clauses 8.9. (c) and (d) of the Clauses are further detailed in the audit provisions specified in the Agreement, including with regard to the audit interval under clause 8.9 (c);

   (b) the liability between the Parties under clause 12 of the Clauses is subject to the applicable liability terms of the Agreement.

3. Only to the extent applicable with regards to the processing of Swiss personal information , the Parties wish to clarify that (1) references to EU member states in these Clauses shall not be interpreted in such a way that data subjects in Switzerland are excluded from exercising their rights at their habitual residence in Switzerland, (2) references in these Clauses to Applicable European Data Protection Law, most prominently the Regulation (EU) 2016/679 , shall be interpreted as a reference to the corresponding clauses in the Swiss Federal Act of 19 June 1992 on Data Protection including the Ordinance to the FADP, as amended by the revised Swiss Federal Data Protection Act incl. Ordinance to the FADP which will come into force in 2023 and any amendment thereof (3) these Clauses also protect data pertaining to legal entities as long as the Swiss Federal Act of 19 June 1992 on Data Protection, as amended, including the Ordinance to the FADP, remain in force; and that (4) the Swiss Regulator is the competent authority for the purposes of the Agreement.

4. The Parties wish to establish additional safeguards for their data transfers outside of the EU/EEA or Switzerland in consideration of the Court of Justice of the European Union Schrems II ruling of 16 July 2020 (Case C-311/18), and therefore an addendum describing supplementary measures is attached as Annex 4 to the Clauses.

5. The Clauses apply as of the effective date of the Agreement and will automatically terminate upon the end of the Services Period.

[redacted]

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

[redacted]

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

[redacted]

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

[redacted]

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken

or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

[redacted]

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall

notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

[redacted]

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

[redacted]

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

[redacted]

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

[redacted]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of Switzerland, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of Switzerland.

(b) The Parties agree that those shall be the courts of Switzerland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

[redacted]

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: *Customer name specified in the Agreement*

Address: *Customer address as specified in the Agreement*

Contact person's name, position and contact details: *Customer contact person as specified in the Agreement*

Activities relevant to the data transferred under these Clauses:

The provision of the services under the Agreement, as further specified in the Service Specifications

Signature and date: Effective date of the agreement

Role (controller/processor): CONTROLLER

2. ...

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:

A list of Oracle Affiliates relevant for the service offerings as defined in the Agreement, is available at www.oracle.com/corporate/oracle-affiliates.html.

Address: The registered address of the Oracle Affiliates is available through https://www.oracle.com/corporate/contact/global.html

Contact person's name, position and contact details: Refer to Section 3 of the Oracle Services Privacy Policy, available at: https://www.oracle.com/legal/privacy/services-privacy-policy.html#1-6

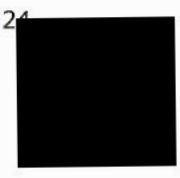
Activities relevant to the data transferred under these Clauses:

Oracle may process personal data as necessary to perform the Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing. For a more specific description of the activities, refer to the Service Specifications.

[redacted]

Signature and date: Effective date of the agreement

Role (controller/processor): PROCESSOR



B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects whose personal data may be transferred in order to perform the Services may include, among others, the Data Exporter's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

Categories of personal data transferred

Categories of personal data, as determined by the Data Exporter, may include, among other information: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; IP addresses and online behavior and interest data.

Additional or more specific descriptions of processing activities, categories of personal data and data subjects may be described in the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Throughout the Services Period of the Agreement, personal data may be transferred on a continuous basis.

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

Purpose(s) of the data transfer and further processing

The Data Importers may process personal data as necessary to perform the Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

[redacted]

Personal Data will be retained for the duration of the Service Period of the Agreement and any applicable data retrieval period at the end of the Services Period.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Oracle maintains lists of Third Party Subprocessors that may Process Personal Information. These lists contain the subject matter and nature of the processing and are available via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the NetSuite Support Portal or Your Oracle project manager).

The duration of the processing with regard to Third Party Subprocessors is consistent with the Services Period.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Swiss Federal Data Protection and Information Commissioner

The competent supervisory authority of the EU/EEA/CH country in which the data exporter has its main establishment.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Oracle has implemented and will maintain appropriate technical and organizational security measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services are set out in the relevant security practices for these Services:

- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at: http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: http://www.netsuite.com/portal/resource/terms-of-service.shtml;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: https://www.oracle.com/support/policies.html;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: http://www.oracle.com/us/corporate/contracts/consulting-services/index.html.

The Oracle security policies & practices, and documents referenced therein, are subject to change. However, policy changes will not result in a material reduction in the level of protection for personal data that is provided during the services period of the Agreement to which these Clauses relate.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

To the extent Oracle engages Third Party Subprocessors that transfer personal data, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement, specified in the Oracle Supplier Information and Physical Security Standards, available at https://www.oracle.com/us/assets/oracle-supplier-contractor-security-070672.pdf.

[redacted]

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

NOT APPLICABLE FOR OPTION 2 (General written authorisation)

The controller has authorised the use of the following sub-processors:

1. *Name: ...*

   Address: ...

   Contact person's name, position and contact details: ...

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[redacted]

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

[redacted]

ANNEX IV

Supplementary Measures to the Clauses

("Supplementary Measures")

1. Scope and Applicability

1.1 These Supplementary Measures provide additional safeguards in consideration of the Court of Justice of the European Union Schrems II ruling of 16 July 2020 (Case C-311/18) in addition to those safeguards established in the Clauses.

1.2 In the event of any conflict between these Supplementary Measures and the Clauses, the terms of the Clauses will take precedence.

2. Hosting Locations

To the extent the provision of the Services You have ordered involves the Processing of Personal Information, the hosting location(s) will be specified as follows:

2.1 For **Oracle Cloud Applications and Oracle Industry Cloud Applications**, the data center region is specified in Your order;

2.2 For **Oracle Cloud Infrastructure and Platform Services**, Oracle will host Personal Information in the Cloud region selected by You. The current list of Cloud regions for Oracle Cloud Infrastructure and Platform Services is available at https://www.oracle.com/cloud/data-regions/;

2.3 For **Global Technical Support Services**, to the extent You have submitted Personal Information in service request attachments on the My Oracle Support customer portal in accordance with Section VII of the Oracle Global Customer Support Security Practices available at https://www.oracle.com/assets/customer-support-security-practices-069170.pdf, such service request attachments will be hosted on servers located in the United States;

2.4 For **Consulting and Advanced Customer Support Services**, details on the delivery and hosting locations are specified in Your order or will otherwise be available with Your project manager

3. Encryption, encryption key management and other technical safeguards

3.1 Oracle employs data security controls, including encryption for data at rest and in transit, where applicable, as set forth in the Agreement and the security and delivery policies referenced therein, such as the Hosting and Delivery Policies for Oracle Cloud Services and Section 6 of the Data Processing Agreement.

[redacted]

3.2 Additional documentation about encryption and encryption key management controls, and relevant anonymization, pseudonymization, data masking or truncation controls which can be employed or configured by You to restrict access to Personal Information by Oracle and/or within Your organization, is available in the applicable Privacy & Security Feature guidance on My Oracle Support, Document ID 2121811.1.

4. Additional obligations of the data importer in case of access by public authorities

3.1 Oracle has implemented and shall maintain internal policies and procedures designed to enable compliance with Clause 15, including legal oversight by EU-based Legal teams, procedural steps and training on applicable principles of European Data Protection law.

3.2 Oracle periodically publishes a transparency report to provide aggregated information regarding the number and type of legally binding requests it received in the preceding 12-month period, and Oracle's response to the request (e.g., 'full or partial response provided', 'declined to respond', or 'evaluating response'). The most current version of the report is available at https://www.oracle.com/a/ocom/docs/cloud/oracle-law-enforcement-requests-report.pdf.

5. Oracle Software Security Assurance Program and Safeguards Against Backdoors

5.1 Oracle has implemented and maintains the Oracle Software Security Assurance (OSSA) program, which prohibits the introduction of features intended to allow a malicious attacker to bypass security functionality in the Services, such as authentication, auditing, or access control ("Backdoor").

5.2 Without prejudice to Oracle's ability to use remote access functionality as necessary for the provision of the Services, Oracle confirms that it has not purposely introduced a Backdoor in the Services that could be used to access Personal Information in a manner not consistent with the Clauses, including Clause 15 of the Clauses.

6. Additional Safeguards and Remedies

6.1 You and Oracle will review any supplemental measures, which may be required based on applicable European Data Protection Law for the transfer of Personal Information under the Clauses. In order to submit an inquiry regarding available supplemental measures with Oracle, You can submit a "service request" via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. You and Oracle will work together in good faith to find a mutually acceptable resolution to address such request, including but not limited to reviewing technical documentation for the Services, and discussing additional available technical safeguards and security services.

6.2 To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 6.2 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.