1

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang Abrufverfahren

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

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

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

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

1. Vorgehen im Überblick

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

2. Bestimmung des Bedarfs und der Abrufkriterien

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

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

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

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

3. Evaluation, Entscheid und Leistungsbezug

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

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

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

4. Allfällige weitere Interaktionen mit Zuschlagsempfängerinnen

4.1 Die Bezugsberechtigte prüft nach Massgabe der von ihr im Einzelfall festgelegten Abrufkriterien (Ziff. 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).

6. Kein Anspruch auf Berücksichtigung

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

7. Mitteilung der Entscheide gem. Ziff. 3.2

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

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

7.3 Die Bezugsberechtigte teilt Folgendes mit:

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

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

8. Allgemeine Bestimmungen

Die Regeln des Rahmenvertrags kommen kraft Verweises zur Anwendung.

* * *

2

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Audit

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Audits, welche Cloud-Services im Sinne von Ziffer 1 CSA der Firma oder die zur Erbringung der Cloud-Services verwendete IBM Rechenumgebung etc. zum Gegenstand haben, richten sich ausschliesslich und abschliessend nach Anhang Datenschutz (Ziffer 13 EB-AV). Die nachfolgenden Regelungen gelten für Themen «Out of the Cloud» wie zum Beispiel Rechnungsprüfung.

1. Begriffsdefinitionen

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

a) **Auditberechtigte Stellen** sind: die Vergabestelle(n) und die jeweils Bezugsberechtigten sowie jeweils deren interne und externe Revisionsstellen (eine externe Revision darf nicht Mitbewerber von IBM sein) und deren Aufsichtsbehörden und -stellen. Die Firma anerkennt ausdrücklich, dass auch die folgenden Stellen als Auditberechtigte Stellen gelten:

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

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

1.2 Ansonsten gelten die Begriffe gemäss Rahmenvertrag.

2. Kontrollrechte (Audit)

2.1 Die Firma räumt jeder Auditberechtigten Stelle hiermit das Recht ein, die Grundlagen der Rechnungsstellung und die dazu gehörenden Unterlagen einzusehen und zu prüfen.

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

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

3. Mitwirkungspflichten der Firma

Die Firma verschafft der Auditberechtigten Stelle auf Anfrage Zugriffe entsprechend dem Verfahren in Ziff. 13 im Anhang Datenschutz.

4. Zweck des Audits

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

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

b) Anfragen von Aufsichtsbehörden zu erfüllen;

c) die Richtigkeit der Vergütung festzustellen.

5. Prüfer der Auditberechtigten Stelle

Ein Audit kann (i) von internen Mitarbeitenden einer Auditberechtigten Stelle, (ii) von unabhängigen, von der Auditberechtigten Stelle beauftragten Dritten, der nicht Mitbewerber von IBM ist (Ziffern (i) und (ii) nachfolgend zusammengefasst als "**Prüfer der**

Auditberechtigten Stelle" bezeichnet) sowie (iii) von Aufsichtsbehörden und den von diesen bezeichneten Vertreter/innen durchgeführt werden.

6. Kosten des Audits

Beide Parteien tragen ihre Kosten in Bezug auf die Absätze a. und b. von Ziffer 13.1 EB-AV Audit jeweils selbst, im Übrigen findet Ziffer 16.4 im EB-AV Datenschutz Anwendung.

* * *

[redacted]

3

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Datenschutz

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Inhaltsübersicht:

[redacted]

I. ALLGEMEINE BESTIMMUNGEN

1. Anwendbares Recht

1.1 vgl. hierzu Ziffer 2.1

2. Zu diesem Vertragsanhang

2.1 Dieser Datenschutzanhang und die zugehörigen servicespezifischen Anlagen zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) (Anlagen) regeln die Rollen, Zuständigkeiten und Verantwortlichkeiten sowie die Rechte und Pflichten in Bezug auf die Bearbeitung personenbezogener im Rahmen der Leistungserbringung der Firma im Auftrag der Bezugsberechtigten. Sie finden Anwendung, wenn und soweit die Firma personenbezogene Daten im Auftrag der Bezugsberechtigten (personenbezogenen Daten des Bezugsberechtigten) im Rahmen der Erbringung der in der Vereinbarung aufgeführten Services (Services) bearbeitet und (i) die europäische Datenschutz-Grundverordnung 2016/679 (DSG-VO); (ii) das Schweizer Bundesgesetz über den Datenschutz (DSG) oder (iii) eines der unter http://www.ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze (zusammen 'Datenschutzgesetze') hierauf Anwendung finden. Die jeweilige Anlage ist im Auftragsdokument des entsprechenden Service aufgeführt. Bei Widersprüchen haben die jeweiligen Anlagen zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) Vorrang vor diesem Anhang Datenschutz.

2.2 Verweise auf die 'Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV)' in den Vertragsdokumenten der Firma sind grundsätzlich immer zu verstehen als Verweis auf diesen Anhang – Datenschutz.

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, sofern in Kraft, in der Folge "nDSG") beziehungsweise (wenn Firma eine in der EU niedergelassene Anbieterin ist) von Artikel 28 EU-DSGVO, sichergestellt werden.

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

3.3 Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit Datenübermittlungen von der Schweiz ins Ausland gemäss Art. 6 DSG (resp. Art. 16 nDSG) bzw. von EU/EWR-Mitgliesstaaten in Drittstaaten gemäss Art. 44 ff. EU-DSGVO erfüllt werden. Diesbezüglich gelten zusätzlich die Bestimmungen in Abschnitt III (Ziff. 21 ff.).

4. Auslegung

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

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

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

5. Vorrang

Es gilt die Rangfolge gemäss Ziff. 4.2 des Rahmenvertrag, in Verbindung mit Ziff. 2.1 oben.

6. Beschreibung der Auftragsbearbeitung

6.1 Die Bezugsberechtigte (a) ist Verantwortliche im Hinblick auf die personenbezogenen Daten der Bezugsberechtigten oder (b) handelt als Auftragsbearbeiterin im Auftrag sonstiger Verantwortlicher und wurde von diesen angewiesen und hat von diesen die Genehmigung eingeholt, die Firma als Unterauftragsbearbeiter mit der Bearbeitung der personenbezogenen Daten der Bezugsberechtigten gemäss dieses Datenschutzanhangs zu beauftragen. Die Bezugsberechtigte ernennt die Firma zur Auftragsbearbeiterin für die Bearbeitung der personenbezogenen Daten der Bezugsberechtigten. Sofern es noch weitere Verantwortliche gibt, wird die Bezugsberechtigte diese vor Übermittlung derer personenbezogener Daten, wie in der Anlage aufgeführt, identifizieren und der Firma mitteilen. Eine Liste der Kategorien betroffener Personen, der Arten personenbezogener Daten der Bezugsberechtigten, der besonderen Kategorien personenbezogener Daten und der Bearbeitungstätigkeiten sind in der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) enthalten. Die Dauer der Bearbeitung entspricht der Laufzeit des Service, sofern in der jeweiligen Anlage nicht abweichend vereinbart. Zweck und Gegenstand der Bearbeitung ist die Erbringung des Service gemäss der Beschreibung in der Vereinbarung.

6.3 Die jeweilige Bezugsberechtigte ist Ansprechpartner für die Firma für die bezogenen Services.Gleichermassen ist die Firma einziger Ansprechpartner für Vergabestelle und Bezugsberechtigte in Bezug auf ihre Pflichten als Auftragsbearbeiterin im Rahmen dieses Anhangs Datenschutz.

6.4 Die Firma verpflichtet sich zur Einhaltung aller für die Firma als Auftragsbearbeiterin in Bezug auf die Services geltenden Datenschutzgesetze. die Firma ist weder für die Ermittlung der für die Vergabestelle und Bezugsberechtigte anwendbaren gesetzlichen oder regulatorischen Anforderungen verantwortlich noch dafür, dass ein Service diesen Anforderungen entspricht. Im Verhältnis zwischen den Parteien ist die Bezugsberechtigte für die Rechtmässigkeit der Bearbeitung der personenbezogenen Daten der Bezugsberechtigten verantwortlich.

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

B. Pflichten der Parteien

7. Weisungen

7.1 Die Firma bearbeitet personenbezogene Daten der Bezugsberechtigten gemäss den dokumentierten Weisungen der Bezugsberechtigten. Der Umfang der Weisungen der Bezugsberechtigten für die Bearbeitung personenbezogener Daten der Bezugsberechtigten wird durch die Vereinbarung und, sofern zutreffend, die Nutzung und Konfiguration der Funktionen des Service durch die Bezugsberechtigte und dessen berechtigte Benutzer festgelegt. Die Bezugsberechtigte kann in Übereinstimmung mit

Ziff. 16 weitere gesetzlich erforderliche Weisungen für die Bearbeitung personenbezogener Daten der Bezugsberechtigten (zusätzliche Weisungen) erteilen. Sollte die Firma die Bezugsberechtigte informieren, dass einer zusätzlichen Weisung nicht entsprochen werden kann, werden die Parteien zusammenarbeiten, um eine Alternative zu finden. Falls die Firma die Bezugsberechtigte informiert, dass weder der zusätzlichen Weisung noch einer Alternative entsprochen werden kann, kann die Bezugsberechtigte den betroffenen Service gemäss den einschlägigen Bedingungen der Vereinbarung kündigen. Ist die Firma der Auffassung, dass eine Weisung gegen die Datenschutzgesetze verstösst, wird die Firma die Bezugsberechtigte unverzüglich darüber informieren. die Firma kann die Erfüllung einer solchen Weisung aussetzen, bis die Bezugsberechtigte entweder deren Rechtmässigkeit schriftlich bestätigt oder diese ändert.

8. Zweckbindung

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

8.2 Die Firma, die mit der Firma verbundenen Unternehmen und ihre jeweiligen Auftragnehmer werden ausschliesslich zur Erbringung und dem Betrieb der Firma Cloud-Services auf die Inhalte zugreifen und diese nutzen.

9. Dauer der Bearbeitung von Personendaten

Die Daten werden von der Auftragsbearbeiterin gemäss Ziff. 7 nur für die vereinbarte Dauer bearbeitet.

10. Sicherheit der Bearbeitung

10.1 Die Vergabestelle und die Firma vereinbaren, dass die Firma die in der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) aufgeführten technischen und organisatorischen Massnahmen, die ein dem Risiko angemessenes Schutzniveau gewährleisten, in ihrem Verantwortungsbereich implementieren und aufrechterhalten wird. Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dementsprechend behält sich die Firma das Recht vor, die technischen und organisatorischen Massnahmen zu ändern, sofern die Funktionalität und Sicherheit der Services nicht negativ beeinträchtigt werden.

11. Dokumentation und Einhaltung der Klauseln

11.1 Die Auftragsbearbeiterin muss die Einhaltung dieser Klauseln nach Massgabe Ziff. 13 (Audit) nachweisen können.

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

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

[redacted]

12. Anforderungen Dritter und Vertraulichkeit

12.1 Die Firma verpflichtet sich, personenbezogene Daten der Vergabestelle und der Bezugsberechtigten nicht gegenüber Dritten offenzulegen, es sei denn, die Bezugsberechtigte hat dies gestattet oder es ist gesetzlich erforderlich. Sollte eine Behörde oder Aufsichtsbehörde Zugriff auf personenbezogene Daten der Bezugsberechtigten anfordern, informiert die Firma den Vergabestelle und Bezugsberechtigte vor der Offenlegung entsprechend, sofern eine solche Information nicht gesetzlich verboten ist.

12.2 Die Firma verpflichtet alle Mitarbeiter, die Zugang zu personenbezogenen Daten der Bezugsberechtigten haben, diese Daten vertraulich zu behandeln und sie ausschliesslich nach den Weisungen der Vergabestelle oder der Bezugsberechtigten zu bearbeiten, es sei denn, dass die Firma nach geltendem Recht zur Bearbeitung verpflichtet ist.

13. Audit

13.1 Die Firma wird Überprüfungen, einschliesslich Inspektionen, die von der Bezugsberechtigten oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, entsprechend dem nachfolgend dargestellten Verfahren ermöglichen und dazu beitragen.

a) Auf schriftliche Anfrage der Vergabestelle stellt die Firma der Vergabestelle oder dem von ihr beauftragten Prüfer die aktuellen Zertifizierungen und/oder zusammenfassenden Prüfberichte bereit, die von IBM beauftragt wurden, um die Effektivität der technischen und organisatorischen Massnahmen regelmässig zu testen, zu beurteilen und auszuwerten, sofern solche in der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) aufgeführt sind.

b) Die Firma wird in angemessenem Umfang mit der Vergabestelle zusammenarbeiten, indem die Firma zusätzliche verfügbare Informationen in Bezug auf die technischen und organisatorischen Massnahmen bereitstellt, um die Vergabestelle zu unterstützen, diese Massnahmen besser nachvollziehen zu können.

c) Sollte die Vergabestelle weitere Informationen benötigen, um ihrer eigenen Auditverpflichtungen oder denen sonstiger Verantwortlicher nachzukommen oder der Anforderung einer zuständigen Aufsichtsbehörde gerecht zu werden, wird sie die Firma schriftlich informieren, damit die Firma diese Informationen bereitstellen oder Zugriff darauf erteilen kann.

d) Sollte es nicht möglich sein, einem entweder sich aus dem öffentlichen Recht zwingend ergebenden oder von den Parteien ausdrücklich wie hier in Ziffer 12 b) vereinbarten Auditrecht bzw. Auditbedürfnis anderweitig nachzukommen, können nur gesetzlich verpflichtete Parteien (z. B. eine Regulierungsbehörde, die die Aufsicht über das operative Geschäft der Bezugsberechtigten hat), die Vergabestelle oder der von ihr beauftragte Prüfer die für die Serviceerbringung genutzten Betriebsstätten besuchen. Ein solcher Besuch ist zeitlich mit der Firma während der üblichen Geschäftszeiten zu koordinieren, darf die Betriebsabläufe möglichst nicht stören und hat in Übereinstimmung mit den gegebenenfalls in der Anlage beschriebenen Auditverfahren zu erfolgen, um Risiken für andere Kunden der Firma zu reduzieren.

13.2 Jeder andere von der Vergabestelle beauftragte Prüfer darf kein direkter Wettbewerber von der Firma in Bezug auf die Services sein und muss entsprechend zur Vertraulichkeit verpflichtet werden.

13.3 Beide Parteien tragen ihre Kosten in Bezug auf die Absätze a. und b. von Ziffer 13.1 jeweils selbst, im Übrigen findet Ziffer 16.2 Anwendung.

14. Einsatz von Unterauftragsbearbeitern

14.1 Die Vergabestelle genehmigt die Beauftragung anderer Auftragsbearbeiter mit der Bearbeitung personenbezogener Daten der Bezugsberechtigten (Unterauftragsbearbeiter). Eine Liste der aktuellen Unterauftragsbearbeiter ist in der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) enthalten. Die Firma informiert die Bezugsberechtigten vorab über jede beabsichtigte Hinzufügung oder jeden beabsichtigten Austausch von Unterauftragsbearbeitern gemäss der Beschreibung in der jeweiligen Anlage. Innerhalb eines Zeitraums von 30 Tagen nach der Benachrichtigung durch die Firma über eine beabsichtigte Änderung kann die Vergabestelle gegen die Hinzufügung oder den Austausch eines Unterauftragsbearbeiters aus wichtigen datenschutzrechtlichen Gründen (z.B. entsprechende nachweisliche Beanstandung der Aufsichtsbehörde) Einspruch erheben. Der Einspruch der Vergabestelle muss schriftlich erfolgen und die konkreten Gründe für den Einspruch sowie ggf. Kompromissvorschläge beinhalten. Falls die Vergabestelle den Unterauftragsbearbeiter innerhalb dieses Zeitraums nicht ablehnt, kann dieser mit der Bearbeitung personenbezogener Daten der Bezugsberechtigten beauftragt werden. Bevor der Unterauftragsbearbeiter mit der Bearbeitung personenbezogener Daten der Bezugsberechtigten beginnt, wird die Firma diesem Datenschutzverpflichtungen auferlegen, die jenen dieser EB-AV im Wesentlichen vergleichbar sind und nicht zu einem Absinken des Schutzniveaus führen.

14.2 Falls die Vergabestelle gegen einen Unterauftragsbearbeiter berechtigt Einspruch erhebt und die Firma diesem Einspruch nicht Rechnung tragen kann, wird die Firma die Vergabestelle entsprechend informieren. Die Bezugsberechtigte kann die betroffenen Services gemäss den einschlägigen Bedingungen der Vereinbarung (siehe bspw. Ziffer 7.c CSA) kündigen. Anderenfalls werden die Parteien zusammenarbeiten, um in Übereinstimmung mit dem Streitbeilegungsprozess eine realisierbare Lösung zu finden.

14.3 Für die Verpflichtungen im Rahmen des Anhang Datenschutz ist die Firma verantwortlich, selbst wenn die Firma einen Unterauftragsbearbeiter beauftragt, und Die Firma wird geeignete Vereinbarungen abschliessen, die der Firma die Einhaltung ihrer Verpflichtungen für die IBM Cloud-Services ermöglichen.

14.4 Die Firma erklärt sich bereit, bei der Vereinbarung einzelner Abrufe in Abstimmung mit der Bezugsberechtigten zu prüfen, ob für Unterauftragsbearbeiter, welche dann zu bestimmende, wichtige Funktionen im Rahmen der Unterauftragsbearbeitung erfüllen, eine Ankündigung eines Wechsel dieser Unterauftragsbearbeiter mit einem Vorlauf von 90 Tagen umsetzbar ist. Sofern möglich, wird dies schriftlich vereinbart. Die Regelung in 14.1 wird in einem solchen Fall nicht ausser Kraft gesetzt.

15. Internationale Datenübermittlungen

15.1 Im Falle einer Übermittlung personenbezogener Daten der Bezugsberechtigten in ein Land, in dem gemäss den Datenschutzgesetzen kein angemessenes Datenschutzniveau gewährleistet ist (Land ohne angemessenes Datenschutzniveau), werden die Parteien zusammenarbeiten, um die Einhaltung der geltenden Datenschutzgesetze gemäss den Angaben in den folgenden Abschnitten, im DSG/nDSG oder in den Datenschutzgesetzen unter http://www.ibm.com/dpa/dpl sicherzustellen. Falls die Bezugsberechtigte der Ansicht ist, dass die Massnahmen nicht ausreichen, um die gesetzlichen Bestimmungen einzuhalten, wird sie die Firma benachrichtigen und die Parteien werden zusammenarbeiten, um eine Alternative zu finden.

15.2 Mit Abschluss der Vereinbarung schliessen die Vergabestelle und die Firma gleichzeitig die EU-Standardvertragsklauseln ab, wie in der jeweiligen Anlage zu den EB-AV (EU-Standardvertragsklauseln) dargelegt, wenn die Bezugsberechtigte, die Firma oder beide in einem Land ohne angemessenes Datenschutzniveau ansässig sind. Wenn die EU-

Standardvertragsklauseln nicht erforderlich sind, weil beide Parteien in einem Land ansässig sind, das nach den Datenschutzgesetzen als Land mit angemessenem Datenschutzniveau angesehen wird, das Land, in dem die Firma oder die Bezugsberechtigte ansässig ist, jedoch während der Serviceerbringung als Land ohne angemessenes Datenschutzniveau eingestuft wird, kommen die EU-Standardvertragsklauseln zur Anwendung.

15.3 Die Vergabestelle erklärt sich damit einverstanden, dass die EU-Standardvertragsklauseln, einschliesslich der daraus resultierenden Ansprüche, den in der Vereinbarung enthaltenen Bedingungen, einschliesslich der Haftungsbegrenzungen, unterliegen. Bei Widersprüchen haben die EU-Standardvertragsklauseln Vorrang.

15.4 Die Firma wird die EU-Standardvertragsklauseln mit jedem Unterauftragsbearbeiter abschliessen, der gemäss der jeweils geltenden Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) in einem Land ohne angemessenes Datenschutzniveau ansässig ist.

C. Koordination und Compliance

16. Unterstützung der Verantwortlichen

16.1 Die Firma informiert die Bezugsberechtigte über Anträge von betroffenen Personen, die ihre Betroffenenrechte (z. B. einschliesslich aber nicht begrenzt auf Berichtigung, Löschung und Sperrung von Daten) direkt gegenüber der Firma in Bezug auf personenbezogene Daten der Bezugsberechtigten geltend machen. Die Bezugsberechtigte ist für die Beantwortung solcher Anträge von betroffenen Personen zuständig. Die Firma unterstützt die Bezugsberechtigte in angemessenem Umfang bei der Beantwortung von Anträgen von betroffenen Personen in Übereinstimmung mit Ziffer 16.4.

16.2 Falls eine betroffene Person einen Anspruch aufgrund der Verletzung ihrer Betroffenenrechte direkt gegenüber der Firma geltend macht, erstattet die Bezugsberechtigte die Firma sämtliche Kosten, Gebühren, Schäden, Aufwendungen oder Verluste, die sich aus einem solchen Anspruch ergeben, sofern die Firma die Bezugsberechtigte über den Anspruch in Kenntnis gesetzt und ihr die Möglichkeit gegeben hat, bezüglich der Abwehr und Beilegung des Anspruchs mit der Firma zusammenzuarbeiten. Vorbehaltlich der in der Vereinbarung enthaltenen Bedingungen kann die Vergabestelle oder die Bezugsberechtigte gegenüber der Firma Schadensersatz für Ansprüche betroffener Personen geltend machen, deren Betroffenenrechte durch einen Verstoss von der Firma gegen ihre Verpflichtungen aus dieser Anlage Datenschutz und der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) verletzt wurden.

16.3 Die Firma unterstützt die Bezugsberechtigte mit technischen und organisatorischen Massnahmen bei der Erfüllung ihrer Verpflichtungen zur Einhaltung der Betroffenenrechte und bei der Einhaltung ihrer Verpflichtungen in Bezug auf die Sicherheit der Bearbeitung, die Mitteilung und Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten und die Durchführung einer Datenschutz-Folgenabschätzung, einschliesslich, sofern erforderlich, der vorherigen Konsultation mit der zuständigen Aufsichtsbehörde, unter Berücksichtigung der Art der Bearbeitung und der Firma zur Verfügung stehenden Informationen.

16.4 Die Bezugsberechtigte wird von der Firma im Rahmen dieser EB-AV benötigte Unterstützung schriftlich anfordern. Die Firma darf der Bezugsberechtigten für diese Unterstützung oder eine zusätzliche Weisung höchstens eine angemessene Gebühr berechnen. Diese Gebühren müssen in einem Angebot enthalten sein und von den Parteien schriftlich vereinbart werden oder entsprechend einem in der Vereinbarung

[redacted]

geregelten Änderungsmanagementverfahrens festgelegt werden. Sollte die Bezugsberechtigte dem Angebot nicht zustimmen, vereinbaren die Parteien, in angemessenem Umfang zusammenzuarbeiten, um entsprechend dem Streitbeilegungsprozess eine realisierbare Lösung zu finden.

17. Meldung von Verletzungen der Datensicherheit, allgemeine Bestimmungen

Die Firma wird die Bezugsberechtigte unverzüglich informieren, wenn ihr eine Verletzung des Schutzes personenbezogener Daten in Bezug auf die Services bekannt wird. Die Firma wird die Verletzung des Schutzes personenbezogener Daten unverzüglich untersuchen, sofern sich diese in der Infrastruktur der Firma oder in einem anderen Bereich, für den die Firma verantwortlich ist, ereignet hat, und wird die Bezugsberechtigte entsprechend Ziffer 16 unterstützen.

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

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

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

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

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

18.2 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 entsprechend Ziffer 16 zu unterstützen.

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

Im Falle einer Verletzung der Datensicherheit im Zusammenhang mit den von der Verantwortlichen bearbeiteten Personendaten unterstützt die Auftragsbearbeiterin die Verantwortliche wie folgt entsprechend Ziffer 16:

d) 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);

e) 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 so weit 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;

f) 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).

20. Verstösse gegen die Klauseln und Beendigung

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

20.2 Die Verantwortliche ist berechtigt, den betroffenen Leistungsabruf zu kündigen (gemäss Ziffer 7.c CSA), soweit er die Bearbeitung von Personendaten gemäss diesen Klauseln betrifft, wenn

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

b) die Auftragsbearbeiterin in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstösst oder ihre Verpflichtungen gemäss DSG oder (bei Auftragsbearbeiterinnen mit Niederlassung in EU/EWR) EU-DSGVO nicht erfüllt;

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

20.3 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 gemäss Ziffer 2.1 verstossen.

20.4 Nach Kündigung oder Ablauf eines Abrufs wird die Firma die sich in ihrem Besitz befindenden personenbezogenen Daten der Bezugsberechtigten gemäss den Angaben in der jeweiligen Anlage zu den Ergänzenden Bestimmungen Auftragsbearbeitung (EB-AV) löschen, sofern nicht durch zwingende Rechtsvorschriften etwas anderes vorgesehen ist

III. KLAUSELN BETREFFEND DIE ÜBERMITTLUNG VON PERSONENDATEN INS AUSLAND

21. Übermittlung von Personendaten ins Ausland durch die Bezugsberechtigte

21.1 Werden im Falle von lit. c) die Standarddatenschutzklauseln der EU-Kommission vom 4. Juni 2021 verwendet[1], verpflichtet sich die Firma zur Umsetzung der für die Schweiz spezifisch notwendigen Anpassungen gemäss Empfehlung des EDÖB vom 27. August 2021[2].

22. Übermittlung von Personendaten ins Ausland im Rahmen der Leistungserbringung

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

Regionale Bindung:

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

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

22.2 Die Firma sorgt dafür, dass die Datenhaltung gemäss Festlegung durch die Bezugsberechtigte oder die Vergabestelle gemäss Absatz (1) in Ziff. 22.1 umgesetzt wird. Sollte die Firma davon abweichen wollen oder müssen, wird sie die Vergabestelle vorgängig informieren. Die Firma sorgt dafür, dass diese Information mindestens 20 Arbeitstage vor Umsetzung der Anpassung bei der Vergabestelle eingeht; Ausnahmen sind 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.

22.3 Die Firma bestätigt, dass Bezugsberechtigte für die Mehrzahl der im Pflichtenheft aufgeführten Services die Möglichkeit haben, Datenstandorte in mindestens einem Land zu wählen, das die Anforderungen gem. Ziff. 22.1 Absatz (2) erfüllt.

22.4 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) [3]. Liegt kein Entscheid des Bundesrates vor, so dürfen personenbezogene Daten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

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

---

1 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

2 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 SCC def. D 24082021.pdf.download.pdf/Paper SCC def. D 24082021.pdf

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

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.

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

22.6 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).

* * *

---

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

5 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB – Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge, 27. August 2021; https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Paper SCC def. D 24082021.pdf.download.pdf/Paper SCC def. D 24082021.pdff

[redacted]

4

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – IT- und Datensicherheit

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

1. 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.

Begriffsbestimmungen

In diesem Dokument verwendete Begriffe haben die nachstehende Bedeutung. Alle hier nicht definierten Begriffe haben die Bedeutung, mit der sie im massgeblichen schriftlichen Vertrag zwischen der Firma und der Vergabestelle für die Services der Firma festgelegt sind.

Komponenten – die Anwendung, Plattform oder Infrastrukturelemente eines Service, der von der Firma betrieben und verwaltet wird.

Inhalte – sämtliche Daten, Software und Informationen, die von der Bezugsberechtigten oder ihrer berechtigten Benutzern in Services bereitgestellt, für den Zugriff freigegeben oder eingegeben werden.

Datensicherheits- und Datenschutzrichtlinien – die in diesem Dokument beschriebenen Datensicherheits- und Datenschutzrichtlinien.

IBM Cloud-Services – „as-a-Service"-Angebote von der Firma, die von der Firma über ein Netzwerk zur Verfügung gestellt werden, wie z. B. als Software-as-a-Service, Platform-as-a-Service oder Infrastructure-as-a-Service.

IBM Servicedokument – ein Auftragsdokument oder ein beliebiges anderes Dokument, das durch Bezugnahme in einen schriftlichen Vertrag zwischen der Firma und der Vergabestelle einbezogen wird und in dem Details eines bestimmten IBM Service beschrieben werden.

IBM Services – (a) IBM Cloud-Services, (b) andere IBM Serviceangebote, einschliesslich Infrastruktur- oder Anwendungsserviceangebote, die von der Firma bereitstellt und einer Bezugsberechtigten dediziert zuordnet oder für eine Bezugsberechtigte anpasst, und (c) alle anderen Serviceleistungen, einschliesslich Beratung, Wartung oder Support, die IBM für eine Bezugsberechtigte erbringt.

Sicherheitsvorfall – der unbefugte Zugriff auf Inhalte oder deren unbefugte Nutzung.

Auftragsdokument – ein Dokument, in dem die Details der spezifischen Transaktion, wie z. B. Gebühren und eine Beschreibung eines IBM Cloud-Service sowie entsprechende Informationen, enthalten sind. Beispiele für Auftragsdokumente sind unter anderem Leistungsbeschreibungen, Servicebeschreibungen, Bestellungen und Rechnungen für einen IBM Cloud-Service. Für eine Transaktion können mehrere Auftragsdokumente zur Anwendung kommen.

[redacted]

Auf dieser Grundlage vereinbaren die Parteien somit Folgendes:

2. Sicherheit auf IT-Infrastrukturen der Firma

2.1 Übersicht

Die technischen und organisatorischen Massnahmen, die in diesem Anhang IT- und Datensicherheit beschrieben werden, gelten nur dann für IBM Services (einschliesslich der Komponenten), wenn die Firma die Einhaltung der darin enthaltenen Datensicherheits- und Datenschutzrichtlinien in einem schriftlichen Vertrag mit der Vergabestelle ausdrücklich vereinbart hat. Es wird ausdrücklich darauf hingewiesen, dass diese Massnahmen nicht zur Anwendung kommen, wenn die Bezugsberechtigte im Verhältnis zwischen IBM und der Bezugsberechtigten für Sicherheit und Datenschutz verantwortlich ist oder wie nachstehend angegeben oder wenn in einem IBM Servicedokument abweichende Regelungen enthalten sind.

a) Die Bezugsberechtigte ist dafür verantwortlich, zu entscheiden, ob ein IBM Service für seine beabsichtigte Nutzung geeignet ist, und die Sicherheits- und Datenschutzmassnahmen für Komponenten umzusetzen und zu verwalten, die nicht von IBM innerhalb der IBM Services bereitgestellt oder verwaltet werden. Beispiele für Verantwortlichkeiten der Bezugsberechtigten für IBM Services sind: (1) die Sicherheit von Systemen und Anwendungen, die von Bezugsberechtigten auf einem Infrastructure-as-a-Service- oder Platform-as-a-Service-Angebot oder auf Infrastruktur, Komponenten oder Software, die die Firma für die Bezugsberechtigte verwaltet, erstellt oder eingesetzt werden, (2) die Vergabe von Zugriffsrechten an Endbenutzer der Bezugsberechtigten und die Sicherheitskonfiguration auf Anwendungsebene für ein Software-as-a-Service-Angebot, das IBM für die Bezugsberechtigte verwaltet, oder ein Anwendungsserviceangebot, das IBM für die Bezugsberechtigte bereitstellt.

b) Die Vergabestelle bestätigt, dass die Firma die IBM Datensicherheits- und Datenschutzrichtlinien von Zeit zu Zeit nach eigenem Ermessen ändern kann, und dass frühere Versionen durch diese Änderungen ab dem Datum ihrer Veröffentlichung ausser Kraft gesetzt werden. Sollte sich durch eine Änderung ein Widerspruch zu den Bestimmungen in diesem Anhang IT- und Datensicherheit ergeben, so gilt die Regelung in den IBM Datensicherheits- und Datenschutzrichtlinien vorrangig. Ungeachtet gegenteiliger Bestimmungen in einem schriftlichen Vertrag zwischen der Firma und der Vergabestelle werden alle Änderungen mit der Absicht durchgeführt, (1) bestehende Verpflichtungen von der Firma zu verbessern oder transparenter zu gestalten, (2) der Firma zu ermöglichen, den Sicherheitsfokus auf aufkommende Bedrohungen und Probleme bei der Daten- und Cybersicherheit zu richten, (3) die Umsetzung neu eingeführter Standards und anwendbarer Gesetze sicherzustellen oder (4) zusätzliche Features und Funktionen bereitzustellen. Durch die Änderungen werden die Sicherheits- oder Datenschutzfeatures oder -funktionen von IBM Services nicht beeinträchtigt.

c) Bei Widersprüchen zwischen diesem Anhang IT- und Datensicherheit und einem IBM Servicedokument hat das IBM Servicedokument Vorrang. Wenn die entgegenstehenden Bedingungen in einem Auftragsdokument enthalten sind, werden diese als übergeordnete Bedingungen angegeben, die Vorrang vor diesem Anhang IT- und Datensicherheit haben, und gelten nur für die bestimmte Transaktion.

2.2 Compliance

a) Die von der Firma in jedem IBM Standard-Cloud-Service (mit Ausnahme von angepassten Cloud-Services) implementierten und durchgeführten Massnahmen unterliegen einer jährlichen Zertifizierung, bei der die Einhaltung von ISO 27001 oder SSAE SOC 2 oder von beiden Normen geprüft wird, sofern in einem IBM Servicedokument nichts anderes festgelegt ist.

b) Darüber hinaus wird die Firma die Compliance und Akkreditierung für die IBM Services gemäss der Definition in einem IBM Servicedokument aufrechterhalten.

[redacted]

c) Auf Anfrage wird die Firma einen Nachweis über die gemäss den Abschnitten 2.2a) und 2.2b) geforderte Compliance und Akkreditierung erbringen, wie z. B. Zertifikate, Bescheinigungen oder Berichte über die von akkreditierten unabhängigen Dritten durchgeführten Audits (von akkreditierten unabhängigen Dritten durchgeführte Audits finden mit der vom jeweiligen Standard geforderten Häufigkeit statt).

d) Die Firma ist auch dann für diese Sicherheits- und Datenschutzmassnahmen verantwortlich, wenn ein Auftragnehmer oder Lieferant (einschliesslich Unterauftragsverarbeitern) für die Bereitstellung oder den Support eines IBM Service eingesetzt wird.

3. Schutzziele

Die Sicherheit auf IT-Infrastrukturen der Firma muss 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 (im Folgenden „Verletzung des Schutzes von Daten").

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.

Diese Informationen finden sich für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet), die in Ziff. 2 der Service Description des Dienstes verlinkt ist.

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

Diese Informationen finden sich für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet), die in Ziff. 2 der Service Description des Dienstes verlinkt ist.

5.1 Die Firma wird die zum Zeitpunkt des Vertragsabschlusses gehaltenen Zertifizierungen aufrechterhalten, die für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet) aufgelistet sind, wie in Ziff. 2.2 b) dieses Anhangs dargelegt.

5.2 Sollte die Firma eine dieser Zertifizierungen ungewollt verlieren, informiert sie umehend die Vergabestelle darüber, indem die betreffende 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet) aktualisiert wird.

5.3 Die Firma stellt der Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Zertifikate zu.

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

Diese Informationen finden sich für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet), die in Ziffer 2 der Service Description des Dienstes verlinkt ist.

6.1 Sollte der Firma eine Attestierung einer Audit-Unternehmung aberkannt worden sein, informiert sie umgehend die Vergabestelle darüber, indem die betreffende 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet) aktualisiert wird.

6.2 Die Firma stellt Vergabestelle auf Wunsch jederzeit (auch mehrfach möglich) die eingeholten Audit-Berichte zu.

6.3 Die Firma wird die Vergabestelle auf Anfrage über allfällige Beanstandungen, Umsetzung der Mitigierungsmassnahmen sowie die Re-Evaluierung der Zertifizierungssituation bzw. der Beanstandung durch die auditierende Stelle informieren, soweit sie in einem SOC2 Report festgehalten wurden.

7. Verschlüsselte Datenhaltung

Diese Informationen finden sich für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet), die in Ziff. 2 der Service Description des Dienstes verlinkt ist.

Ruhende Inhalte werden von der Firma verschlüsselt, wenn und soweit dies in einem IBM Servicedokument angegeben ist. Ist die Verwaltung von Verschlüsselungsschlüsseln bei einem IBM Service eingeschlossen, wird die Firma dokumentierte Verfahren für die sichere Erstellung, Ausgabe, Weitergabe, Speicherung, Rotation, den Widerruf sowie die Wiederherstellung, Sicherung, Löschung, den Zugriff und die Verwendung von Schlüsseln einrichten.

8. Verschlüsselte Datenübermittlungen

Diese Informationen finden sich für jeden IBM Cloud Service in der dienstspezifischen 'Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung' (Data Sheet), die in Zif. 2 der Service Description des Dienstes verlinkt ist.

Die Firma wird Inhalte, die nicht für die Veröffentlichung oder Einsichtnahme ohne Authentifizierung bestimmt sind, bei der Übertragung über öffentliche Netze verschlüsseln und die Verwendung eines Verschlüsselungsprotokolls, wie z. B. HTTPS, SFTP oder FTPS, ermöglichen, damit die Inhalte von der Bezugsberechtigten sicher in die und aus den IBM Services über öffentliche Netze übertragen werden können.

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

9.1 Sicherheitsrichtlinien

a) Die Firma wird die schriftlichen IT-Sicherheitsrichtlinien und -verfahren, die ein integraler Bestandteil der Geschäftstätigkeit von der Firma und für alle Mitarbeiter der Firmaverbindlich sind, aufrechterhalten und befolgen. Der Chief Information Security Officer der Firma hat die Verantwortung für die Überwachung und Umsetzung dieser Richtlinien, insbesondere für das formale Governance- und Revisionsmanagement, die Mitarbeiterausbildung und die Durchsetzung der Compliance.

b) Die IT-Sicherheitsrichtlinien werden von der Firma mindestens einmal jährlich überprüft und ergänzt oder geändert, wenn die Firma dies zum Schutz der IBM Services und Inhalte für angemessen erachtet.

c) Die Firma wird ihre verbindlichen Standardanforderungen in Bezug auf die Überprüfung aller neu eingestellten Beschäftigten aufrechterhalten und befolgen und diese Anforderungen auf ihre 100-prozentigen Tochtergesellschaften ausweiten. Diese Anforderungen werden gemäss den internen Prozessen und Verfahren von der Firma regelmässig überprüft und können unter anderem die Überprüfung möglicher Vorstrafen und der Identität sowie zusätzliche Prüfungen umfassen, die von der Firma als notwendig erachtet werden. Jede Gesellschaft der Firma ist für die Umsetzung dieser Anforderungen im Rahmen ihres Einstellungsverfahrens verantwortlich, sofern diese anwendbar und unter der jeweils geltenden Rechtsordnung zulässig sind.

d) Mitarbeiter der Firma werden jährlich Firmen Schulungen für Sicherheit und Datenschutz absolvieren und jedes Jahr nachweisen, dass sie die Anforderungen von der

Firma in Bezug auf Unternehmensethik, Vertraulichkeit und Sicherheitsrichtlinien gemäss den Geschäftsgrundsätzen der Firma (Business Conduct Guidelines) einhalten. Personen mit privilegiertem Zugriff auf Komponenten erhalten zusätzliche Schulungen, die speziell auf ihre Rolle beim Betrieb und Support der IBM Services abgestimmt und zur Aufrechterhaltung der im massgeblichen IBM Servicedokument beschriebenen Compliance und Akkreditierungen erforderlich sind.

9.2 Zugriffskontrolle

a) Wenn die Firma zur Erbringung der IBM Services Zugriff auf Inhalte benötigt und dieser Zugriff von der Firma verwaltet wird, wird er von der Firma auf das notwendige Mindestmass beschränkt. Dieser Zugriff sowie der Verwaltungszugriff auf die zugrunde liegenden Komponenten (privilegierter Zugriff) sind individuell, rollenbasiert und unterliegen regelmässigen Prüfungen durch autorisierte Mitarbeiter gemäss den Richtlinien für die Aufgabentrennung. Die Firma wird Massnahmen zur Aufdeckung und Löschung redundanter und inaktiver Konten mit privilegiertem Zugriff ergreifen und bei Ausscheiden oder Wechsel des Kontoeigners oder auf Anforderung von autorisierten Firma Mitarbeitern, wie beispielsweise durch den Vorgesetzten des Kontoeigners, den Zugriff unverzüglich entziehen.

b) Im Einklang mit branchenüblichen Verfahren und insoweit dies von jeder Komponente nativ unterstützt wird, setzt die Firma technische Massnahmen ein, die das Timeout inaktiver Sitzungen, die Sperrung von Konten nach mehreren aufeinanderfolgenden, fehlgeschlagenen Anmeldeversuchen, die Authentifizierung über sichere Kennwörter oder Kennphrasen, Kennwortänderungsintervalle und eine sichere Übertragung und Speicherung dieser Kennwörter und Kennphrasen erzwingen.

c) Die Firma wird die Verwendung des privilegierten Zugriffs überwachen sowie Sicherheitsinformations- und Ereignismanagementmassnahmen ergreifen, um (1) unbefugte Zugriffe und Aktivitäten aufzudecken, (2) rechtzeitiges und angemessenes Reagieren zu erleichtern und (3) sowohl interne als auch von unabhängigen Dritten durchgeführte Audits auf Einhaltung der dokumentierten Firma Richtlinie zu ermöglichen.

d) Die Protokolle, in denen privilegierte Zugriffe und Aktivitäten aufgezeichnet werden, werden gemäss dem IBM Worldwide Records Management Plan aufbewahrt. Die Firma wird Massnahmen ergreifen, mit denen diese Protokolle vor unbefugtem Zugriff, unbefugter Änderung und zufälliger oder absichtlicher Zerstörung geschützt werden.

10. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

a) Die Firma kann Personal und Betriebsmittel an Standorten weltweit sowie Auftragnehmer zur Unterstützung bei der Bereitstellung von IBM Cloud-Services einsetzen.

b) Die Nutzung der Cloud-Services durch die Bezugsberechtigten kann die grenzüberschreitende Übermittlung von Inhalten, einschliesslich personenbezogener Daten, zur Folge haben.

c) Eine Liste der Länder, in die Inhalte übertragen und für einen IBM Cloud-Service verarbeitet werden können, ist im massgeblichen Auftragsdokument angegeben.

d) Für die Verpflichtungen im Rahmen der Vereinbarung ist die Firma verantwortlich, selbst wenn die Firma einen Auftragnehmer beauftragt, und die Firma wird geeignete Vereinbarungen abschliessen, die der Firma die Einhaltung ihrer Verpflichtungen für die IBM Cloud-Services ermöglichen.

11. Datenschutz

a) IBM wird sämtliche Inhalte vertraulich behandeln, indem Inhalte nur Mitarbeitern, Auftragnehmern und Lieferanten (einschliesslich Unterauftragsverarbeitern) von der Firma und ausschliesslich in dem Umfang offengelegt werden, der zur Erbringung der IBM Services erforderlich ist.

b) Die Sicherheits- und Datenschutzmassnahmen für jeden IBM Service werden gemäss dem Firmen-Grundsatz der eingebauten Sicherheit und Privatsphäre umgesetzt, um die von einem IBM Service bearbeiteten Inhalte zu schützen und die Verfügbarkeit dieser Inhalte nach Massgabe des anwendbaren schriftlichen Vertrags zwischen der Firma und der Vergabestelle sowie der anwendbaren IBM Servicedokumente aufrechtzuerhalten.

c) Im IBM Servicedokument oder in anderen Standarddokumenten können zusätzliche Sicherheits- und Datenschutzinformationen für einen bestimmten IBM Service enthalten sein, um die Bezugsberechtigte bei der anfänglichen und fortlaufenden Beurteilung der Eignung eines IBM Service für seine beabsichtigte Nutzung zu unterstützen. Diese Informationen können Nachweise über angegebene Zertifizierungen und Akkreditierungen, weiterführende Informationen zu diesen Zertifizierungen und Akkreditierungen, Datenblätter, häufig gestellte Fragen (FAQs) und andere allgemein verfügbare Dokumente umfassen. Falls die Bezugsberechtigte die Firma auffordert, von ihm bevorzugte Fragebögen zu Sicherheit oder Datenschutz auszufüllen, wird die Firma die Bezugsberechtigte auf die verfügbaren Standarddokumente verweisen.

12. Sicherheitsvorfälle

a) Die Firma wird dokumentierte Richtlinien zur Behebung von Sicherheitsvorfällen nach den Richtlinien des National Institute of Standards and Technology (NIST-Richtlinien), einer Bundesbehörde im Geschäftsbereich des Handelsministeriums der USA, oder nach vergleichbaren Branchenstandards für den Umgang mit IT-Sicherheitsvorfällen etablieren und befolgen und die Bedingungen zur Meldung von Datenschutzverletzungen im massgeblichen schriftlichen Vertrag zwischen IBM und der Vergabestelle einhalten.

b) Die Firma wird Sicherheitsvorfälle, von denen die Firma Kenntnis erlangt hat, untersuchen und innerhalb des Geltungsbereichs der IBM Services einen entsprechenden Interventionsplan definieren und umsetzen. Die Bezugsberechtigte kann die Firma über den für einen IBM Service vorgesehenen Prozess zur Meldung von Sicherheitsvorfällen (wie in einem IBM Servicedokument angegeben) oder, wenn ein solcher Prozess nicht besteht, in Form einer Anfrage an den technischen Support über mutmassliche Sicherheitslücken oder Vorfälle benachrichtigen.

c) Die Firma wird die Bezugsberechtigte unverzüglich über einen bestätigten Sicherheitsvorfall informieren, von dem bekannt ist oder bei dem ein begründeter Verdacht besteht, dass er Auswirkungen auf die Bezugsberechtigte hat. Die Firma wird der Bezugsberechtigten in angemessenem Umfang Informationen über einen solchen Sicherheitsvorfall und den Status der Abhilfe- und Wiederherstellungsmassnahmen der Firma bereitstellen.

13. Physische Sicherheit und Zutrittskontrolle

a) Die Firma wird geeignete physische Zutrittskontrollen, wie Schranken, durch Kartenleser kontrollierte Zutrittspunkte, Überwachungskameras und mit Personen besetzte Empfangsbereiche, einrichten, um von der Firma verwaltete Einrichtungen (Rechenzentren), in denen IBM Services gehostet werden, vor unbefugtem Zutritt

zu schützen. Weitere Zutrittspunkte zu diesen Rechenzentren, wie Anlieferungsbereiche und Ladedocks, werden kontrolliert und von den IT-Ressourcen strikt getrennt.

b) Der Zutritt zu von der Firma verwalteten Rechenzentren und kontrollierten Bereichen innerhalb dieser Rechenzentren wird entsprechend der ausgeübten Funktion eines Mitarbeiters beschränkt und ist genehmigungspflichtig. Der Zutritt wird protokolliert und die Protokolle werden mindestens ein Jahr lang aufbewahrt. Bei Ausscheiden oder Wechsel eines autorisierten Mitarbeiters wird die Firma den Zutritt zu den von der Firma verwalteten Rechenzentren sperren. Dabei befolgt die Firma die formalen dokumentierten Verfahren, die beim Ausscheiden oder Wechsel von Mitarbeitern einzuhalten sind, die das unverzügliche Entfernen aus Zutrittskontrolllisten und die Rückgabe von Ausweisen einschliessen.

c) Jede Person, der eine temporäre Zutrittsgenehmigung für ein von der Firma verwaltetes Rechenzentrum oder einen kontrollierten Bereich innerhalb eines solchen Rechenzentrums erteilt wurde, wird beim Betreten der Räumlichkeiten registriert, muss bei der Registrierung einen Identitätsnachweis vorlegen und wird von autorisierten Mitarbeitern begleitet. Jede temporäre Zutrittsgenehmigung, auch für Anlieferungen, wird vorab geplant und bedarf der Genehmigung durch autorisierte Mitarbeiter.

d) Die Firma wird Vorkehrungen zum Schutz der physischen Infrastruktur der von der Firma verwalteten Rechenzentrumseinrichtungen vor natürlichen als auch vor von Menschen verursachten Umweltgefahren treffen, wie z. B. extrem hohe Umgebungstemperatur, Feuer, Hochwasser, Feuchtigkeit, Diebstahl und Vandalismus.

14. Zugangs-, Weitergabe- und Trennungskontrolle

a. Die Firma wird eine dokumentierte Sicherheitsarchitektur der Komponenten aufrechterhalten. Dazu wird die Sicherheitsarchitektur, einschliesslich der Massnahmen zur Verhinderung von nicht autorisierten Netzverbindungen zu Systemen, Anwendungen und Netzeinheiten, vor der Implementierung gesondert auf Einhaltung der Standards für sichere Segmentierung, Isolation und tiefengestaffelte Sicherheit überprüft.

b. Die Firma kann drahtlose Netztechnologie für die Wartung und den Support der IBM Services und der zugehörigen Komponenten einsetzen. Falls drahtlose Netze zum Einsatz kommen, werden diese verschlüsselt und verlangen eine sichere Authentifizierung. Sie ermöglichen keinen direkten Zugriff auf IBM Cloud-Service-Netze. Bei IBM Cloud-Service-Netzen wird keine drahtlose Netztechnologie verwendet.

c. Die Firma wird Massnahmen für einen IBM Service durchführen, die dazu ausgelegt sind, Inhalte logisch zu trennen und zu verhindern, dass sie für Unbefugte verfügbar oder zugänglich sind. Die Produktions- und Nicht-Produktionsumgebungen der Firma werden in angemessener Weise isoliert, und wenn Inhalte in eine Nicht-Produktionsumgebung übertragen werden, um zum Beispiel auf Anforderung der Bezugsberechtigten einen Fehler zu reproduzieren, entsprechen die Sicherheits- und Datenschutzvorkehrungen denjenigen, die in der Produktion angewendet werden.

d. Soweit Unterstützung durch geräte- und betriebssystemeigene Funktionen gegeben ist, wird die Firma Schutzmassnahmen für Endbenutzersysteme bereitstellen. Dazu gehören unter anderem Endpunktfirewalls, vollständige Plattenverschlüsselung, signaturbasierte Malware-Erkennung und -Entfernung, zeitbasierte Bildschirm-sperren und Endpunktmanagementlösungen, die Sicherheitskonfigurations- und Patching-Anforderungen durchsetzen.

e. Im Einklang mit den NIST-Richtlinien wird die Firma sämtliche Daten auf physischen Datenträgern, die zur Wiederverwendung vorgesehen sind, vor einer erneuten Verwendung der Datenträger sicher löschen und physische Datenträger, die nicht zur Wiederverwendung vorgesehen sind, vernichten.

[redacted]

15. Serviceintegrität und Verfügbarkeitskontrolle

a) Die Firma wird (1) mindestens einmal jährlich Sicherheits- und Datenschutzrisikoabschätzungen für die IBM Services durchführen, (2) vor der Freigabe für die Produktion und danach mindestens jährlich Sicherheitstests und Schwachstellenanalysen der IBM Services durchführen, (3) einen qualifizierten unabhängigen Dritten, IBM X-Force™ oder, sofern in einem IBM Servicedokument angegeben, einen anderen qualifizierten Testservice damit beauftragen, mindestens jährlich Penetrationstests der IBM Cloud-Services durchzuführen, (4) eine automatisierte Schwachstellensuche der zugrunde liegenden Komponenten der IBM Services anhand der bewährten Branchenverfahren für Sicherheitskonfigurationen durchführen, (5) die bei den Sicherheitstests und Suchvorgängen aufgedeckten Schwachstellen abhängig von dem damit verbundenen Risiko, der Exploit-Anfälligkeit und der Auswirkung beheben und (6) angemessene Massnahmen ergreifen, um eine Unterbrechung der IBM Services bei der Ausführung der Tests, Prüfungen, Schwachstellensuche und Abhilfemassnahmen zu vermeiden.

b) Die Firma wird Massnahmen durchführen, die dazu ausgelegt sind, Security Advisory Patches für die IBM Services und die zugehörigen Systeme, Netze, Anwendungen und zugrunde liegenden Komponenten im Rahmen der IBM Services zu beurteilen, zu testen und einzuspielen. Wenn sich herausstellt, dass ein Security Advisory Patch anwendbar und geeignet ist, wird IBM den Patch gemäss den dokumentierten Richtlinien zur Bewertung der Dringlichkeit und Risiken auf der Grundlage der Patch-Einstufungen nach dem Common Vulnerability Scoring System, sofern verfügbar, einspielen. Das Einspielen von Security Advisory Patches unterliegt der IBM Change-Management-Richtlinie.

c) Die Firma wird Richtlinien und Verfahren anwenden, die für das Management von Risiken im Zusammenhang mit der Durchführung von Änderungen an IBM Services ausgelegt sind. Änderungen an einem IBM Service, den zugehörigen Systemen, Netzen und zugrunde liegenden Komponenten werden vor der Implementierung in einer registrierten Änderungsanforderung dokumentiert, die eine Beschreibung sowie den Grund für die Änderungen, Einzelheiten der Implementierung und den Terminplan, eine Risikoerklärung hinsichtlich der Auswirkung auf den IBM Service und seine Kunden, das erwartete Ergebnis, einen Rollback-Plan und die dokumentierte Genehmigung durch autorisierte Mitarbeiter enthält.

d) Die Firma wird ein Inventar aller IT-Assets pflegen, die beim Betrieb von IBM Services verwendet werden. Der Zustand, einschliesslich der Kapazität, und die Verfügbarkeit von IBM Services und der zugrunde liegenden Komponenten werden von IBM fortlaufend überwacht und gesteuert.

e) Jeder IBM Service wird separat durch eine Business-Impact-Analyse und Risikobeurteilungen in Bezug auf Business-Continuity- und Disaster-Recovery-Anforderungen hin überprüft, um kritische Geschäftsfunktionen zu ermitteln und zu priorisieren. Sofern aufgrund dieser Risikobeurteilungen gerechtfertigt, werden für jeden IBM Service Business-Continuity- und Disaster-Recovery-Pläne in Übereinstimmung mit branchenüblichen Verfahren separat definiert, dokumentiert, gepflegt und jährlich überprüft. Zielvorgaben hinsichtlich Wiederherstellungspunkt und -zeit (RPO und RTO) für einen IBM Service, sofern im massgeblichen IBM Servicedokument vorgesehen, werden unter Berücksichtigung der Architektur und der vorgesehenen Nutzung des IBM Service festgelegt. Physische Datenträger, die zur Auslagerung an einen anderen Standort vorgesehen sind, wie z. B. Datenträger, auf denen sich Sicherungsdateien befinden, werden vor dem Transport verschlüsselt.

* * *

5

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Migration und Löschung der Daten

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

Auf dieser Grundlage vereinbaren die Parteien Folgendes:

Im Einzelnen:

I. Datenmigration

1. Datenmigration in die IT-Infrastrukturen der Firma

1.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch und nach Massgabe einer vorgängig zwischen den Parteien abzuschliessenden Vereinbarung und Kostenregelung bei der Migration von Daten in die IT-Infrastrukturen der Firma.

1.2 Die Firma gibt Auskunft über:

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

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

c) weitere notwendige oder nützliche Massnahmen.

2. Anspruch auf Herausgabe

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

2.2 Der Anspruch gemäss Ziff. 2.1 bezieht sich auf:

[redacted]

a) Inhalte, welche die Bezugsberechtigte im Rahmen der Leistungen unter dem Rahmenvertrag auf IT-Infrastrukturen der Firma speichert, bekannt gibt oder bearbeitet.

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

2.3 Die Firma ermöglicht, die Herausgabe gemäss Wunsch der Bezugsberechtigten entweder an die Bezugsberechtigte oder an eine von der Bezugsberechtigten bezeichnete Dritte auszuführen. Die Firma ermöglicht der Bezugsberechtigten die Identität derjenigen Personen sicher zu stellen, die für die Bezugsberechtigte das Recht gemäss Ziff. 2.1 ausüben, ebenso deren Berechtigung, die herauszugebenden Daten zu erhalten. Ziff. 2.4 gilt ergänzend. Die zweifelsfreie Identität der bezugsberechtigten Person wird über die Authentifizierung am Cloud Portal sichergestellt. Die Verwaltung der bezugsberechtigten Personen obliegt der Bezugsberechtigten.

2.4 Die Firma erfüllt Ziff. 2.3, wenn sie die herausverlangten Inhalte zum Download in einer gesicherten Umgebung bereitstellt, die erst nach zweifelsfreier Identifikation der für die Bezugsberechtigte handelnden Personen zugänglich ist, solange die restlichen Voraussetzungen dieser Ziff. 2 ebenfalls eingehalten sind.

2.5 Der Anspruch auf Herausgabe der Inhalte besteht bis zur Vertragsbeendigung und kann nur davor geltend gemacht werden.

2.6 Herausgabe im Sinne von Ziff. 2.1 bedeutet Folgendes:

a) Transformation des herauszugebenden Datenbestands in ein Datenformat gemäss Absprache mit der Bezugsberechtigten oder, wenn eine solche nicht stattfindet, in einem Format, das den Anforderungen gemäss Ziff. 2.1 genügt.

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

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

3.1 Die Firma unterstützt die Bezugsberechtigte auf Wunsch und nach Massgabe einer vorgängig zwischen den Parteien abzuschliessenden Vereinbarung und Kostenregelung bei der Migration von Daten aus den IT-Infrastrukturen der Firma heraus.

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

II. Haltung der Inhalte während der Nutzung

4. Sicherung von Inhalten

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

4.2 Die Sicherung der Inhalte erfolgt gemäss dem Datensicherungskonzept der Bezugsberechtigten. Die Implementation des Datensicherungskonzepts obliegt der Bezugsberechtigten.

4.3 Es gelten die Service Levels der Bezugsberechtigten.

5. Wiederherstellung

5.1 Die Firma ermöglicht, dass die Bezugsberechtigte auf Methoden zur Wiederherstellung ihrer Inhalte zurückgreifen kann, die mindestens dem Stand der Technik entsprechen, sofern eine Implementation einer Datensicherung wie unter Ziff. 4 beschrieben, existiert.

5.1.1 Die Sicherung und Wiederherstellungs-Funktionalität der Inhalte ist kostenpflichtig.

5.1.2 Unter Vorbehalt von Ziff. 5.1.3 gelten die Service Levels der Bezugsberechtigten.

5.1.3 Ein Recovery Time Objective kann im Rahmen einer zusätzlichen Vereinbarungn als Minimum definiert werden.

6. Allgemeine Regeln betreffend Haltung von Inhalten

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

6.2 Die Firma stellt sicher, dass der Standort der Inhalte für bezogene Leistungen in jedem Fall klar dokumentiert ist.

6.3 Die Firma informiert die Vergabestelle und auf Wunsch der Stelle gemäss Ziff. 6.5 auch diese schriftlich über die Methoden, den Standort der Inhalte zweifelsfrei feststellen zu können.

6.4 Die Firma beantwortet Rückfragen über den Standort der Inhalte in angemessener Frist. Solche Rückfragen können sowohl die Bezugsberechtigte, die Vergabestelle als auch die Stelle gemäss Ziff. 6.5 stellen.

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

III. Haltung der Inhalte nach Beendigung des Leistungsbezugs

7. Definition «Vertragsbeendigung»

7.1 Als Vertragsbeendigung im Sinne dieses Abschnitts III. gilt der Zeitpunkt, auf welchen eine Partei den Nutzungsvertrag rechtmässig gekündigt hat oder auf welchen die Bezugsberechtigte den Leistungsbezug eingestellt hat. Ergänzend gilt Folgendes:

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

b) Die Firma informiert die Vergabestelle und auf Wunsch der Stelle gemäss Ziff. 7.2 auch diese schriftlich über die Methoden, diesen Zeitpunkt zweifelsfrei feststellen zu können.

c) Die Firma beantwortet Rückfragen über den Zeitpunkt der Vertragsbeendigung in angemessener Frist. Solche Rückfragen können sowohl die Vergabestelle als auch die Stelle gemäss Ziff. 7.2 stellen.

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

8. Maximale Haltedauer der Inhalte

8.1 Mit der Beendigung der Services werden die Daten umgehend gem. Ziff. 11 gelöscht.

8.2 Die Firma sorgt dafür, dass die Inhalte der Bezugsberechtigten anschliessend gelöscht wird. Die Anforderungen der Datenlöschung ergeben sich aus Abschnitt IV.

8.3 Ziff. 8.1 gilt nicht in den folgenden Fällen:

a) falls die Bezugsberechtigte den Leistungsbezug nach Vertragskündigung reaktiviert (sofern die Firma dies überhaupt zulässt): Die maximale Haltedauer der Inhalte beginnt ab dem Zeitpunkt der definitiven Vertragsbeendigung)

b) in Bezug auf Nutzungsdaten (gemäss Ziff. 2.2a), nur soweit sie für Zwecke der Abrechnung massgeblich sind: 10 Jahre ab deren Erstellung, mit Ausnahme von Rechnungen, die eine 15 jährige Haltedauer verlangen

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

9. Koordinationsregeln im Umfeld der Vertragsbeendigung

9.1 Ab dem Zeitpunkt der Vertragsbeendigung gemäss Ziff. 7.1 hat die Bezugsberechtigte keinen Zugriff auf ihre Inhalte und Daten mehr.

9.2 Sollte nach Vertragsbeendigung ein Zugriff auf Inhalte notwendig sein, ermöglicht die Firma der Bezugsberechtigten den Download der Inhalte vor Vertragsbeendigung.

9.3 Nach Vertragsbeendigung wird die Firma die Inhalte gemäss Ziff. 8.2 löschen. Die Bezugsberechtigte kann eine frühere Löschung instruieren. Eine frühere Löschung kann sich auch aus Anordnungen von Dritten oder von zuständigen Gerichten ergeben, aufgrund welcher die Bezugsberechtigte zur früheren Löschung der gespeicherten Daten verpflichtet wurde.

IV. Datenlöschung

10. Vorbemerkungen

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

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

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

a) Instruktionen im Einzelfall (z.B. gem. Ziff. 8.3, Ziff. 9, gem. Vertragsanhang Datenschutz)

b) Vertragsanhang Vertraulichkeit der Daten

c) Vertragsanhang Zugriff auf Daten durch Unberechtigte

11. Unwiderrufliche Löschung

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

11.2 Anforderungen an das Löschverfahren:

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

---

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

[redacted]

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[2]. Daran anknüpfende Verfahren (z.B. mehrfaches Überschreiben) beseitigen Daten dauerhaft[3]. Anschliessend knüpfen gemäss den Verfahren der Firma physikalische Verfahren zur Vernichtung der Speichermedien an (dazu Ziff. 11.2d) und Ziff. 11.2e)).

d) In Bezug auf Speichermedien (Festplatten, etc.) verwendet die Firma einen Vernichtungsprozess, der für unwiederbringliche Zerstörung des Datenträgers und der darauf gespeicherten Daten sorgt. Dies bedingt, dass die Wiederherstellung (Lesbarmachen) von Daten unmöglich ist. Die Löschung von Daten bzw. physische Zerstörung von Speichermedien kann z.B. gemäss den Standards DIN 66399 oder BSI IT-Grundschutz-Baustein CON.6 erfolgen.

e) Die Firma spezifiziert, inwiefern Verfahren nach NIST 800-88 der Stufe DESTROY (z.B. Zerkleinern/Shreddern, Zersetzen, Pulverisieren oder Schmelzen) standardmässig oder nur auf Anfrage (z.B. für klassifizierte Informationen) eingesetzt werden.

f) Die Löschverfahren verhindern eine Wiederherstellung mit forensischen Mitteln.

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

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

11.3 Die Löschung umfasst:

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

b) Daten sowohl in den aktiven Umgebungen als auch Daten in Hilfsumgebungen der Firma (z.B. Datensicherungsumgebungen, Legal Hold-Umgebungen, etc.); Gemäss den Aufbewahrungsverfahren für Sicherungen (Back-ups) können jedoch Teile der Daten in Back-ups gespeichert bleiben, bis deren Ablaufdatum erreicht ist und in einem angemessenen Zeitraum wieder überschrieben wird.

c) Verschlüsselungsmittel, welche den Zugriff auf a) und b) geben.

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

12. Dokumentation der Löschung

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

12.2 Anforderungen an die Löschprotokolle:

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

b) Ein Prüfer muss die Löschprotokolle anschliessend mittels automatisierter Auswertung überprüfen können. Zudem muss der Prüfer den Systemstatus des Verfahrens zur Löschung der Daten überprüfen können.

---

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

[3] «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).

[redacted]

12.3 Die Firma bewahrt Löschprotokolle gemäss des IBM Worldwide Records Management Plans ab deren Erstellung auf.

13. Vernichtungspflichten von Unterlagen oder Datenträgern

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

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

13.2 Die Firma bestätigt die Vernichtung von Unterlagen / Datenträgern bzw. die Löschung von Daten unaufgefordert und schriftlich.

* * *

[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 – Technische Anforderungen

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

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

[redacted]

5. Technische Spezifikationen

Des Weiteren gelten die in der WTO-20007 beschriebenen «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 – Vertraulichkeit der Daten

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

Der vorliegende Vertragsanhang beschreibt die Vertraulichkeitspflichten der Firma.

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

Im Verhältnis der Parteien gelten auch andere Bundesstellen als Dritte.

Eigene Mitarbeitende sowie Verbundener Unternehmen der Firma und ihre jeweiligen Subunternehmen gelten nicht als Dritte. «Verbundene Unternehmen» sind Unternehmen, die durch die Firma kontrolliert werden, von denen die Firma kontrolliert wird oder mit denen sie unter gemeinsamer Kontrolle steht. «Kontrollieren» bzw. «unter Kontrolle stehen» bedeutet, mehr als 50 Prozent der entsprechenden Stimmrechtsanteile direkt oder indirekt zu halten oder zu kontrollieren.

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

Soweit die Firma gegenüber der Bundesverwaltung die Erwartung zum Schutz von Vertraulichem hat, regeln die eigenen Vertragsunterlagen der Firma diese Pflichten; ergänzend gilt Ziff. 18 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 vereinbaren die Parteien somit Folgendes:

1. Vertraulichkeit im Allgemeinen

1.1 Die Firma ist verpflichtet, Vertraulichkeit zu gewährleisten. Die Firma darf somit Vertrauliches (wie in Ziff. 1.4 definiert) nicht offenbaren, die Firma muss Vertrauliches gegen unbefugte Klartextzugriffe schützen und darf Vertrauliches nicht zu Zwecken von Firma, ihrer Subunternehmen oder zu Zwecken Dritter verwenden.

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

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

1.4 Information der Bezugsberechtigten, egal ob fixiert oder nicht, egal in welcher Speicherform (d.h. Kenntnisse, Daten, etc.) und egal auf welchem Datenträger (Dokumente wie Unterlagen, Speichermedien, etc.), gilt als **Vertrauliches**. Ergänzend gilt Folgendes:

a) Wenn die Bundesverwaltung Quelle der Information ist oder wenn Information für die Bundesverwaltung bestimmt ist oder wenn die Firma sie im Rahmen der Vertragsbeziehung im Interesse der Bundesverwaltung erstellt hat, liegt Information der Bundesverwaltung und somit Vertrauliches vor.

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

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

a) Information, die von Ziff. 1.4 a) oder b) abgeleitet ist (z.B. Nutzungsprofile; Metadaten; Randdaten; Parametrisierungsdaten; Nutzungsdaten, etc.).

b) Information, die unter Beobachtung der Angaben gemäss Ziff. 1.4 bei der Firma entstanden ist, gilt als Vertrauliches.

2. Verweis auf Ziff. 2 des CSA der Firma

2.1 Die Regelungen in Ziff. 2 des CSA der Firma schützen Vertrauliches im Sinne von Ziff. 1.4 abschliessend; Ziff. 2.2 gilt ergänzend.

2.2 Über das CSA der Firma hinausgehend gilt:
a) Ziff. 7 betreffend Amtsgeheimnis gilt zusätzlich für Inhalte im Sinne von Ziff. 2 des CSA;
b) Regeln des Datenschutzanhangs und des Anhangs Zugriff auf Daten durch Unberechtigte gelten auch für Inhalte im Sinne von Ziff. 2 des CSA.

3. Verweis auf Ziff. 9d des CSA der Firma

3.1 Vertrauliches im Sinne von Ziff. 1.5 wird abschliessend nach den Bestimmungen im CSA der Firma geschützt.

4. Verschwiegenheitspflicht und Schutzpflichten

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

4.2 Die Firma verpflichtet sich, in Bezug auf Vertrauliches Klartextzugriffe von Unbefugten aktiv zu verhindern.

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

5. Datenherausgabeverbot (Einwilligungsvorbehalt)

5.1 Sofern eine Weitergabe von Vertraulichem nicht gesetzlich oder durch gerichtliche Verfügung erforderlich ist, verpflichtet sich die Firma, Vertrauliches nur mit vorgängiger schriftlicher Zustimmung der Bezugsberechtigten an Dritte herauszugeben (Datenherausgabe). Als Datenherausgabe gilt auch das Gewähren von Klartextzugriff auf Vertrauliches in anderer Form als durch Herausgabe von Daten, Unterlagen oder dergleichen.

5.2 Die Firma verlangt von ihren Subunternehmen, dass sie Vertrauliches, sofern nicht verboten, nicht ohne vorgängige schriftliche Zustimmung der Firma an Dritte weitergeben.

6. Verwendungsverbot

6.1 Die Firma verpflichtet sich, Vertrauliches ausschliesslich zum Zwecke einer ordnungsgemässen Abwicklung und Erfüllung dieses Vertrags zu verwenden.

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

7. Amtsgeheimnisse, Berufsgeheimnisse, Datengeheimnisse

7.1 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.

7.2 Die für die Bezugsberechtigten bearbeiteten Daten und Informationen unterstehen mindestens einer der in Ziff. 7.1 genannten Geheimnispflichten (dies gilt generell für generell, ausser die Bezugsberechtigte bezeichnet Ausnahmen). Die Firma ist sich dessen bewusst.

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

8. Pflicht zur Überbindung innerhalb der gesamten Organisation und Subunternehmen

8.1 Für die Verpflichtungen unter diesem Vertragsanhang ist die Firma verantwortlich, selbst wenn die Firma ein Subunternehmen beauftragt, und die Firma wird geeignete Vereinbarungen abschliessen, die der Firma dieEinhaltung ihrer entsprechenden Verpflichtungen ermöglichen.

9. Allgemeine Regeln

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

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

* * *

9

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Anhang – Zugriff auf Daten durch Unberechtigte

zum Rahmenvertrag für die Erbringung von Leistungen im Informatikbereich

basierend auf der Vergabe der öffentlichen Ausschreibung

(20007) 608 Public Clouds Bund

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

[redacted]

Präambel

Dieser Vertragsanhang präzisiert die Pflichten der Firma zur Wahrung der Vertraulichkeit von Vertraulichem gemäss Definition im Anhang Vertraulichkeit der Daten. Er dient der Umsetzung der Anforderungen aus der Ausschreibung (Mindestbedingungen gem. Ziff. 8.1 des Pflichtenhefts: «Der Anbieter ist verpflichtet, die Vertraulichkeit der Daten des Auftraggebers zu gewährleisten.» Mit Vertraulichkeit ist nicht die Vertraulichkeit gemäss IschV gemeint. Eigene Mitarbeitende sowie Verbundene Unternehmen der Firma und ihre jeweiligen Subunternehmen gelten nicht als unbefugte Personen oder Dritte.

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, wie in den einschlägigen vertraglichen Regelungen zur Aufbewahrung festgehalten; (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).

In jedem der vorgenannten Fälle unter Vorbehalt und nach Massgabe der einschlägigen vertraglichen Regelungen sowie der geltenden gesetzlichen und regulatorischen Anforderungen.

2. Informations- und Dokumentationspflichten allgemeiner Art

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

2.2 Die Firma unterstützt die Bezugsberechtigte auf Wunsch und nach Massgabe einer vorgängig zwischen den Parteien abzuschliessenden Vereinbarung und Kostenregelung darin Vorsorgeplanungen für allfällige schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben der Bezugsberechtigten gefährden können zu erstellen.

2.3 Die Firma informiert die Bezugsberechtigte regelmässig, mindestens alle sechs Monate, mittels «IBM's Law Enforcement Request Transparency Report» welcher hier gefunden werden kann: https://www.ibm.com/trust/privacy über Auskunftsersuchen, die IBM von Strafverfolgungsbehörden erhält, und über die Schritte, die IBM zum Schutz der Integrität von Kundendaten unternimmt.

2.4 Die Firma informiert die Bezugsberechtigte über bei Vertragsschluss bestehende Datenherausgabepflichten gegenüber ausländischen Behörden, namentlich für die folgenden Rechtsordnungen gemäss den von IBM zur Verfügung gestellten TIA (Transfer Impact Assessment):

a) USA

b) Spanien

c) Deutschland

3. Cybervorfälle

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

3.2 Die Firma sorgt in ihrem Zuständigkeitsbereich dafür, dass allfällige Risiken für die Informationssicherheit laufend beurteilt werden und informiert die Bezugsberechtigte regelmässig, mindestens jedoch alle sechs Monate.

3.3 Die Bezugsberechtigte definiert in Zusammenarbeit mit der Firma der Bedarfsstelle und der zuständigen Stelle für Cybersicherheit einen Prozess für die Bewältigung von Cybervorfällen. Darin werden namentlich die Entscheidkompetenzen für Sofortmassnahmen geregelt.

3.4 Die Firma meldet der Bezugsberechtigten und den gesetzlich vorgeschriebenen Stellen unverzüglich entdeckte Schwachstellen und Sicherheitsvorfälle, die deren Informatikschutzobjekte betreffen und die eine direkte Auswirkung auf die Bezugsberechtigte haben.

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

4.1 Sofern es ihr nicht gesetzlich untersagt ist, verpflichtet sich die Firma, die Bezugsberechtigte umgehend über das Auftreten eines oder mehrerer der folgenden Ereignisse zu informieren (Meldepflichten):

a) die Firma oder eines ihrer Subunternehmen, wie von ihrem Subunternehmen benachrichtigt, werden in ein Verfahren verwickelt, in dem eine Regierung oder Regulierungsbehörde die Firma oder das Subunternehmen zur Herausgabe von Vertraulichem auffordert (der Erhalt einer *subpoena* oder eines *warrants* ist der Verfahrenseröffnung gleichgestellt).

b) Sofern nicht gesetzlich untersagt, informiert die Firma auch über das Auskunftsersuchen auf Zugang zu Vertraulichem, um der Bezugsberechtigten die Möglichkeit zu geben, alle erforderlichen Massnahmen zu treffen, die für eine direkte Kommunikation mit der betreffenden Behörde und auf ein solches Ersuchen zu reagieren, erforderlich sind.

4.2 Sofern die Firma vom ausländischen Staat zum Stillschweigen über solche Vorgänge verpflichtet wurde, wird sie angemessene Anstrengungen unternehmen, diese Verpflichtung anzufechten und informiert die Bezugsberechtigte und die Bedarfsstelle so rasch wie möglich darüber, nachdem die Verpflichtung zum Stillschweigen dahingefallen ist. Die Firma verpflichtet sich, bei der Beantwortung solcher Herausgabeersuchen nur die Informationen weiterzugeben, die nach angemessener Auslegung des Auskunftsverlangens unbedingt erforderlich sind.

4.3 Die Firma wird die Bezugsberechtigte über solche Ersuchen einer Regierung oder Regulierungsbehörden informieren und angemessenen Anstrengungen unternehmen, um die Regierung oder Regulierungsbehörde zu veranlassen, ihr Ersuchen direkt an die Bezugsberechtigte zu richten.

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

4.5 Wenn eine ausländische Behörde oder Amtsstelle von der Firma die Herausgabe von Vertraulichem fordert, verlangt die Firma, dass die Behörde oder die Amtsstelle die Voraussetzungen für die von ihr/ihnen beantragte erzwungene Datenherausgabe in dokumentierter Weise substantiiert.

4.6 Sofern nicht untersagt, leitet die Firma die Informationen gemäss Ziff. 4.5 an die Bezugsberechtigte und die Bedarfsstelle weiter.

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

5.1 Sofern es ihr nicht gesetzlich untersagt ist, verpflichtet sich die Firma, die Bedarfsstelle umgehend über das Auftreten eines oder mehrere der folgenden Ereignisse zu informieren (Meldepflichten):

a) die Firma beantragt konkursrechtliche Schutzmassnahmen.

b) die Firma nimmt eine generelle Abtretung zu Gunsten der Gläubiger vor.

c) ein Gläubiger oder die Firma stellen beim Gericht Antrag auf einen Konkurs (Artikel 190 und 191 SchKG) oder Nachlassverfahren welcher innert Frist von sechzig (60) Tagen nach dem Eingang des jeweiligen Antrags nicht abgewiesen ist.

d) es wird ein Konkursverwalter oder Treuhänder über das Vermögen der Firma bestellt.

In jedem der vorgenannten Fälle unter Vorbehalt und nach Massgabe der einschlägigen vertraglichen Regelungen sowie der geltenden gesetzlichen und regulatorischen Anforderungen.

5.2 Die Firma wird dafür Sorge tragen, dass Vertrauliches unter der Bestimmungsgewalt der Bezugsberechtigten verbleibt und trifft Massnahmen, damit Dritte nicht auf Vertrauliches zugreifen können, all dies jeweils vorbehältlich und nach Massgabe der einschlägigen Regelungen im CSA der Firma, im vorliegenden Anhang sowie in den Anhängen IT- und Datensicherheit und Datenschutz. Die Konkurs- und Nachlassbehörden im In- und Ausland gelten nicht als Dritte sofern sie wirksamen Geheimhaltungspflichten unterstehen.

5.3 Die Firma verlangt von ihren Subunternehmen, dass sie Vertrauliches, sofern nicht verboten, nicht ohne vorgängige schriftliche Zustimmung der Firma an Dritte weitergeben und behält sich das Recht vor, Verträge mit Subunternehmen im Falle ihres Konkurses zu kündigen. Für die Verpflichtungen unter diesem Vertrag ist die Firma verantwortlich, selbst wenn die Firma ein Subunternehmen beauftragt, und die Firma wird geeignete Vereinbarungen abschliessen, die der Firma die Einhaltung ihrer entsprechenden Verpflichtungen ermöglichen.

---

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

6. Milderungsmassnahmen betreffend Datenherausgaben und Gefahren betreffend Beeinträchtigung der Verfügbarkeit

6.1 Die Firma ergreift angemessene *Milderungsmassnahmen* für den Fall, dass die Abwehrmassnahmen gemäss Ziff. 4 keine vollständige Wirkung entfalten. Milderungsmassnahmen haben das Ziel, dass Verpflichtungen zur Datenherausgabe im Umfang oder sonst wie in ihrer Wirkung reduziert werden.

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

a) Die Firma wird keinen Zugriff auf Vertrauliches gewähren, das ausserhalb des rechtmässigen Zuständigkeitsbereichs einer Regierung oder Regulierungsbehörde gespeichert ist, die solche Daten anfordert, es sei denn, das Ersuchen erfolgt über international anerkannte rechtliche Kanäle wie Rechtshilfeabkommen (MLATs).;

b) die Firma wird Ersuchen von Dritten auf Vertrauliches und auf andere Zwangsmassnahmen (z.B. Gag Orders), welche keine Jurisdiktion über dieselben haben, widersprechen.

c) die Firma wird bei Ersuchen auf Vertrauliches, welche über die Zuständigkeit hinausgehen, eine oder mehrere der folgenden Massnahmen treffen: der Aufforderung widersprechen, den Dritten an die Bezugsberechtigte verweisen; den Dritten auf den Rechtshilfeweg verweisen, Antrag auf Aufhebung des Ersuchens stellen, Antrag auf Feststellung, dass das Ersuchen über die Zuständigkeit hinausgeht, und/oder alle der oben genannten Massnahmen.

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

* * *

[redacted]

10

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vertragswerke der Firma:

11

Vereinbarung für Cloud-Services

Vollständige Vereinbarung: Diese Vereinbarung für Cloud-Services sowie die anwendbaren Anlagen und Auftragsdokumente bilden die vollständige Vereinbarung in Bezug auf jede Transaktion unter dieser Vereinbarung (gemeinsam „Vereinbarung" genannt), auf deren Basis der Kunde Cloud-Services bestellen kann.

Auftragsdokumente: In Auftragsdokumenten sind die Details der spezifischen Transaktion, wie z. B. Gebühren und eine Beschreibung der Cloud-Services sowie entsprechende Informationen, enthalten. Beispiele für Auftragsdokumente sind unter anderem Leistungsbeschreibungen, Servicebeschreibungen, Bestellungen und Rechnungen. Für eine Transaktion können mehrere Auftragsdokumente zur Anwendung kommen.

Anlagen: Anlagen sind Dokumente, die ergänzende Bedingungen enthalten, die für bestimmte Arten von Transaktionen gelten, wie z. B. eine Anlage für eine Servicebeschreibung.

Abweichende Bedingungen in einer Anlage oder einem Auftragsdokument, die Vorrang vor den Bedingungen dieser Vereinbarung für Cloud-Services haben, werden in dem Auftragsdokument oder der Anlage, die vom Kunden akzeptiert wird, explizit aufgeführt und gelten nur für die jeweilige Transaktion.

1. Cloud-Services

a. IBM Cloud-Services

- IBM Cloud-Services sind „as-a-Service"-Angebote von IBM, die von IBM über ein Netzwerk zur Verfügung gestellt werden, wie z. B. als Software-as-a-Service, Platform-as-a-Service oder Infrastructure-as-a-Service.
- Die einzelnen IBM Cloud-Services werden in einem Auftragsdokument beschrieben.
- IBM Cloud-Services sind für durchgängige Verfügbarkeit (24x7) ausgelegt, vorbehaltlich der Wartung. Der Kunde wird von IBM vorab über planmässige Wartungen informiert.
- Technische Unterstützung und etwaige Service-Level-Zusagen sind in einer Anlage oder einem Auftragsdokument angegeben.

b. Services anderer Anbieter (Non-IBM Cloud-Services)

- IBM kann Non-IBM Cloud-Services anderer Anbieter (Dritter) anbieten oder IBM Cloud-Services können den Zugriff auf Non-IBM Cloud-Services anderer Anbieter ermöglichen.
- Die Bedingungen anderer Anbieter, die für die Nutzung ihrer Non-IBM Cloud-Services durch den Kunden zur Anwendung kommen, sind in einem Auftragsdokument angegeben. Durch die Nutzung der Non-IBM Cloud-Services anderer Anbieter erteilt der Kunde seine Zustimmung zu deren Bedingungen.
- IBM ist an den Vereinbarungen anderer Anbieter nicht beteiligt und für die Non-IBM Cloud-Services anderer Anbieter nicht verantwortlich.

c. Annahme der Bestellung

- Der Kunde erklärt sein Einverständnis mit den für Cloud-Services geltenden Anlagen oder Auftragsdokumenten, indem er einen Cloud-Service bestellt, registriert, nutzt oder bezahlt.
- Die Bestellung des Kunden gilt als angenommen, wenn sie von IBM bestätigt oder der Zugriff freigeschaltet wird.

d. Was stellt IBM bereit

- IBM stellt die für die Erbringung von IBM Cloud-Services erforderlichen Einrichtungen und Mitarbeiter, die Ausrüstung, Software und weitere Ressourcen bereit.
- IBM stellt allgemein verfügbare Benutzerhandbücher und Dokumentationen bereit, um die Nutzung von IBM Cloud-Services durch den Kunden zu unterstützen.

e. Aktivierungs-software

- Aktivierungssoftware ist Software, die der Kunde auf seine Systeme herunterladen muss, um die Nutzung eines Cloud-Service zu ermöglichen, und wird in einem Auftragsdokument angegeben.
- Die Aktivierungssoftware ist nicht Bestandteil des Cloud-Service und darf vom Kunden nur in Verbindung mit dem Cloud-Service und gemäss den Lizenzbedingungen verwendet werden, die in einem Auftragsdokument angegeben sind.
- In den Lizenzbedingungen wird auf gegebenenfalls zur Anwendung kommende Gewährleistungen hingewiesen. **Ist ein solcher Hinweis nicht enthalten, wird die Aktivierungssoftware im gegenwärtigen Zustand (auf „as-is"-Basis) ohne jegliche Gewährleistungen bereitgestellt.**

f.	**Was stellt der Kunde bereit**	• Der Kunde stellt die Hardware, Software und Verbindungen für den Zugriff auf die Cloud-Services und deren Nutzung, einschliesslich der erforderlichen kundenspezifischen URL-Adressen und zugehörigen Zertifikate, bereit.
g.	**Nutzungsrecht und Verantwort-lichkeiten des Kunden**	• Die berechtigten Benutzer des Kunden dürfen nur im Rahmen der vom Kunden erworbenen Berechtigungen auf Cloud-Services zugreifen. • Der Kunde trägt die Verantwortung für die Nutzung der Cloud-Services durch sämtliche Benutzer, die mit seinen Kontoanmeldedaten auf den Cloud-Service zugreifen.
h.	**Nutzungs-bedingungen**	• Cloud-Services dürfen nicht für rechtswidrige, verletzende, obszöne, beleidigende oder betrügerische Inhalte oder Aktivitäten genutzt werden. Beispiele für verbotene Aktivitäten sind Handlungen, die Schaden verursachen oder dazu beitragen, die Beeinträchtigung oder Verletzung der Integrität oder Sicherheit eines Netzwerks oder Systems, die Umgehung von Filtern, das Senden nicht angeforderter, beleidigender oder irreführender Nachrichten, die Einführung von Viren oder potenziell gefährlichem Code oder die Verletzung der Rechte Dritter. • Der Kunde darf die Cloud-Services nicht nutzen, wenn ein Versagen oder eine Unterbrechung der Cloud-Services zu Todesfällen, schwerwiegenden Personenschäden, Sach- oder Umweltschäden führen kann. • Es ist dem Kunden nicht gestattet, (1) Teile eines Cloud-Service rückzuentwickeln (durch Reverse Engineering); (2) den direkten Zugriff auf einen Cloud-Service an Dritte ausserhalb der Unternehmensgesellschaften des Kunden abzutreten oder weiterzuverkaufen; oder (3) einen Cloud-Service mit dem Value-Add des Kunden zu kombinieren, um eine Lösung mit dem Logo des Kunden zu erstellen, die der Kunde an seine Endkunden vertreibt, sofern nicht zwischen den Parteien etwas Abweichendes vereinbart wurde.
i.	**Preview-Cloud-Services**	• Cloud-Services oder Features von Cloud-Services werden als „Preview" (Vorschau) angesehen, wenn IBM solche Services oder Features kostenlos, mit eingeschränkter oder Vorabrelease-Funktionalität oder für einen begrenzten Zeitraum zur Verfügung stellt, damit die verfügbare Funktionalität getestet werden kann. Beispiele für Preview-Cloud-Services sind Cloud-Services, die als Beta-, Test-, Preview- oder kostenlose Version gekennzeichnet sind. • Preview-Cloud-Services fallen nicht unter verfügbare Service-Level-Agreements und werden möglicherweise ohne Unterstützung bereitgestellt. • IBM kann einen Preview-Cloud-Service jederzeit und ohne Mitteilung ändern. • IBM ist nicht verpflichtet, Preview-Cloud-Services freizugeben oder einen vergleichbaren Service allgemein verfügbar zu machen.

Inhalte und Datenschutz

a.	**Vom Kunden bereitgestellte Inhalte**	• Inhalte sind sämtliche Daten, Software und Informationen, die vom Kunden oder seinen berechtigten Benutzern in IBM Cloud-Services bereitgestellt, für den Zugriff freigegeben oder eingegeben werden. • Der Kunde erteilt IBM, den mit IBM verbundenen Unternehmen und ihren jeweiligen Auftragnehmern die Berechtigungen und Genehmigungen, Inhalte ausschliesslich zum Zweck der Erbringung der IBM Cloud-Services zu nutzen, bereitzustellen, zu speichern und anderweitig zu verarbeiten. • Die Nutzung der IBM Cloud-Services berührt nicht die Eigentums- oder Lizenzrechte des Kunden an den Inhalten.
b.	**Nutzung von Inhalten**	• IBM, die mit IBM verbundenen Unternehmen und ihre jeweiligen Auftragnehmer werden ausschliesslich zur Erbringung und dem Betrieb der IBM Cloud-Services auf die Inhalte zugreifen und diese nutzen. • Die Inhalte werden von IBM vertraulich behandelt und nur Mitarbeitern und Auftragnehmern von IBM und ausschliesslich in dem Umfang offengelegt, der zur Erbringung der IBM Cloud-Services erforderlich ist.

c.	**Verantwortlich-keiten des Kunden**	• Der Kunde ist dafür verantwortlich, alle Berechtigungen und Genehmigungen einzuholen, die erforderlich sind, um die Verarbeitung von Inhalten in den IBM Cloud-Services zu gestatten. • Der Kunde wird alle Auskünfte erteilen und alle gesetzlich vorgeschriebenen Einwilligungen einholen, bevor Informationen über Personen, insbesondere personenbezogene oder andere regulierte Daten, für die Verarbeitung in den IBM Cloud-Services bereitgestellt, zum Zugriff freigegeben oder eingegeben werden. • Falls Inhalte staatlichen Vorschriften unterliegen könnten oder Sicherheitsmassnahmen erforderlich machen, die den Umfang der von IBM für die IBM Cloud-Services angegebenen Massnahmen überschreiten, wird der Kunde die Inhalte nicht für die Verarbeitung in den IBM Cloud-Services bereitstellen, zum Zugriff freigeben oder eingeben, ausser wenn dies im massgeblichen Auftragsdokument ausdrücklich erlaubt ist oder IBM vorab schriftlich zugestimmt hat, zusätzliche Sicherheitsmassnahmen oder sonstige Massnahmen zu implementieren.
d.	**Datenschutz**	• Die unter http://www.ibm.com/cloud/data-security verfügbaren Datensicherheits- und Datenschutzrichtlinien gelten für IBM Standard-Cloud-Services, die allgemein verfügbar sind. • Besondere Sicherheitsfeatures und -funktionen eines IBM Cloud-Service werden in der zugehörigen Anlage oder im Auftragsdokument beschrieben. • Der Kunde ist verantwortlich für die Auswahl, Bestellung, Aktivierung und Anwendung verfügbarer Datenschutzfeatures, um die vom Kunden genutzten Cloud-Services zu unterstützen. • Es obliegt dem Kunden, zu beurteilen, ob die Cloud-Services für die Inhalte und die von ihm beabsichtigte Nutzung geeignet sind. Der Kunde bestätigt, dass die eingesetzten Cloud-Services seinen Anforderungen und Verarbeitungsanweisungen entsprechen, um die Einhaltung geltender Gesetze sicherzustellen.
e.	**Ergänzende Bedingungen zur Auftrags-verarbeitung von IBM**	• Die Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV) von IBM sind unter http://ibm.com/dpa verfügbar. • Für jeden IBM Cloud-Service gibt es eine Anlage zu den Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV), in der beschrieben ist, wie die Daten des Kunden von IBM verarbeitet werden. • Die Ergänzenden Bedingungen zur Auftragsverarbeitung von (EB-AV) sowie die jeweilige Anlage zu den EB-AV finden Anwendung und ergänzen die Vereinbarung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO); ii) das Schweizer Bundesgesetz über den Datenschutz (DSG); oder iii) eines der unter http://www.ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet. • Auf Anforderung einer der beiden Parteien werden IBM, der Kunde oder ihre jeweiligen verbundenen Unternehmen zusätzliche Vereinbarungen in der vorgeschriebenen Form schliessen, die nach dem Gesetz zum Schutz der in Inhalten enthaltenen regulierten personenbezogenen Daten erforderlich sind. Die Parteien kommen überein (und werden sicherstellen, dass ihre jeweiligen verbundenen Unternehmen zustimmen), dass diese zusätzlichen Vereinbarungen den Bedingungen der Vereinbarung unterliegen.
f.	**Entfernen von Inhalten**	• Bei IBM Cloud-Services mit Features für Selbstverwaltung kann der Kunde Inhalte jederzeit selbst entfernen. Anderenfalls werden die Inhalte auf IBM IT-Ressourcen bei Ablauf oder Beendigung der IBM Cloud-Services, oder auf Antrag des Kunden zu einem früheren Zeitpunkt, an den Kunden zurückgegeben oder entfernt. • IBM kann bestimmte auf Anforderung des Kunden durchgeführte Massnahmen in Rechnung stellen (z. B. die Bereitstellung der Inhalte in einem speziellen Format). • IBM archiviert keine Inhalte; gemäss den IBM Aufbewahrungsverfahren für Sicherungen (Back-ups) können jedoch Teile der Inhalte in IBM Cloud-Services Back-ups gespeichert bleiben, bis deren Ablaufdatum erreicht ist.

[redacted]

3. Änderung oder Zurückziehung von Cloud-Services

a. Recht von IBM zur Änderung von Cloud-Services

- IBM kann jederzeit und nach eigenem Ermessen
  (1) die IBM Cloud-Services, einschliesslich der zugehörigen veröffentlichten Beschreibungen, und
  (2) die Datensicherheits- und Datenschutzrichtlinien sowie andere veröffentlichte Datensicherheits- und Datenschutzdokumentationen für die IBM Cloud-Services ändern.
- Alle zuvor aufgeführten Änderungen werden mit der Absicht durchgeführt,
  (1) zusätzliche Features und Funktionen bereitzustellen;
  (2) bestehende Verpflichtungen von IBM zu verbessern oder transparenter zu gestalten; oder
  (3) die Umsetzung neu eingeführter Betriebs- und Sicherheitsstandards und anwendbarer Gesetze sicherzustellen.
- Es ist nicht beabsichtigt, die Sicherheits- oder Datenschutzfeatures oder Funktionalitäten der IBM Cloud-Services zu beeinträchtigen.
- Änderungen an veröffentlichten Beschreibungen, den Datensicherheits- und Datenschutzrichtlinien oder an anderen veröffentlichten Dokumenten, wie oben angegeben, gelten ab der Veröffentlichung oder dem genannten Wirksamkeitsdatum.
- Alle anderen Änderungen, die nicht die oben genannten Bedingungen erfüllen, werden erst wirksam und gelten als vom Kunden akzeptiert,
  (1) wenn der Kunde eine Neubestellung aufgibt;
  (2) ab dem Verlängerungsdatum für Cloud-Services mit automatischer Verlängerung; oder
  (3) wenn IBM dem Kunden das Wirksamkeitsdatum der Änderung für fortlaufende Services ohne feste Laufzeit mitteilt.

b. Zurückziehung eines Cloud-Service

- IBM kann IBM Cloud-Services mit einer Frist von 12 Monaten zurückziehen.
- IBM wird einen zurückgezogenen IBM Cloud-Service bis zum Ende der verbleibenden Vertragslaufzeit bereitstellen oder mit dem Kunden eine Lösung zur Migration auf ein anderes allgemein verfügbares IBM Angebot erarbeiten.
- Non-IBM Cloud-Services anderer Anbieter können jederzeit zurückgezogen werden, wenn der andere Anbieter seine Services einstellt oder IBM diese Non-IBM Cloud-Services nicht mehr anbietet.

4. Gewährleistungen

a. IBM Gewährleistungen

- IBM gewährleistet, dass die IBM Cloud-Services oder andere IBM Services mit wirtschaftlich angemessener Sorgfalt und Fachkenntnis gemäss der Beschreibung im massgeblichen Auftragsdokument bereitgestellt werden.
- Die Gewährleistung erlischt mit der Beendigung der IBM Cloud-Services oder der anderen IBM Services.
- **Diese Gewährleistungen sind abschliessend und ersetzen sämtliche sonstigen eventuell bestehenden Ansprüche des Kunden.**

b. Eingeschränkte Gewährleistung

- **IBM gewährleistet nicht den unterbrechungs- oder fehlerfreien Betrieb der IBM Cloud-Services.**
- **IBM gewährleistet nicht, dass alle Mängel behoben werden.**
- **Obwohl IBM bestrebt ist, Sicherheitsmassnahmen zum Schutz aller Daten bereitzustellen, übernimmt IBM keine Gewähr dafür, dass alle von Dritten verursachte Unterbrechungen oder unbefugte Zugriffe durch Dritte verhindert werden können.**
- **Die IBM Gewährleistungen gelten nicht im Falle von unsachgemässem Gebrauch, Änderungen, Schäden, die nicht von IBM verursacht wurden, oder Nichteinhaltung der von IBM bereitgestellten schriftlichen Anweisungen.**
- **Preview-Cloud-Services oder Non-IBM Cloud-Services anderer Anbieter werden unter dieser Vereinbarung im gegenwärtigen Zustand (auf „as-is"-Basis) und ohne jegliche Gewährleistungen von IBM zur Verfügung gestellt. Garantien anderer Anbieter für deren Services werden ohne eigene Verpflichtung von IBM an den Kunden weitergegeben.**

5. Gebühren, Steuern und Zahlung

a. Gebühren

- Der Kunde verpflichtet sich zur Zahlung aller festgelegten anwendbaren Gebühren sowie aller Gebühren, die durch Nutzungsüberschreitungen entstehen.
- Die Gebühren verstehen sich zuzüglich aller anwendbaren Zölle, Steuern und sonstigen Abgaben, die von einer Behörde im Zusammenhang mit dem Erwerb von Produkten oder Services unter der Vereinbarung auferlegt werden.
- Rechnungsbeträge sind bei Erhalt der Rechnung fällig und die Zahlung muss innerhalb von 30 Tagen auf ein von IBM angegebenes Konto erfolgen. Es können Verzugszinsen berechnet werden.
- Vorausbezahlte Services müssen innerhalb des vereinbarten Zeitraums in Anspruch genommen werden.
- IBM gewährt keine Gutschriften oder Rückerstattungen für vorausbezahlte Einmalgebühren oder sonstige bereits fällige oder bezahlte Vergütungen, ausser wie in der Vereinbarung vorgesehen.
- Die in einem Auftragsdokument mit IBM vereinbarten Preise werden während der angegebenen Laufzeit von IBM nicht geändert. Wenn keine Preisvereinbarung getroffen wurde, kann IBM die Preise mit einer Frist von dreissig Tagen ändern.

Quellensteuern

- Der Kunde erklärt sich damit einverstanden,
  (1) Quellensteuern, soweit gesetzlich erforderlich, direkt an die zuständige Behörde zu entrichten;
  (2) IBM eine Steuerbescheinigung als Nachweis der geleisteten Zahlung vorzulegen;
  (3) IBM nur den Nettobetrag nach Steuern zu bezahlen; und
  (4) in dem Bestreben, eine Steuerbefreiung oder Ermässigung dieser Steuern zu erreichen, umfassend mit IBM zusammenzuarbeiten und unverzüglich alle relevanten Dokumente auszufüllen und einzureichen.

c. Rechnungs-stellung

- IBM wird
  (1) wiederkehrende Gebühren zu Beginn des gewählten Abrechnungszeitraums in Rechnung stellen;
  (2) Gebühren für Nutzungsüberschreitungen und Nutzungsgebühren rückwirkend berechnen; und
  (3) Einmalgebühren bei Annahme eines Auftrags durch IBM in Rechnung stellen.

6. Haftung und Entschädigung

a. Haftung im Schadenfall

- Unabhängig von der Rechtsgrundlage ist die Gesamthaftung von IBM für alle Ansprüche des Kunden im Zusammenhang mit der Vereinbarung bei tatsächlichen unmittelbaren Schäden begrenzt auf den Betrag (bei wiederkehrenden Gebühren auf maximal 12 Monatsgebühren), den der Kunde für den streitgegenständlichen Service bezahlt hat.
- **IBM übernimmt keine Haftung für mittelbare/indirekte Schäden oder wirtschaftliche Folgeschäden, entgangenen Gewinn, entgangene Geschäftsabschlüsse, Wertverlust oder Umsatzverlust, Schädigung des guten Rufs oder ausgebliebene Einsparungen.**
- Diese Haftungsbegrenzungen gelten gemeinschaftlich für IBM, ihre verbundenen Unternehmen, Auftragnehmer und Lieferanten.

b. Bei welchen Schäden ist eine Haftungs-begrenzung nicht zulässig

- Die folgenden Beträge fallen nicht unter die vorstehenden Begrenzungen:
  (1) Zahlungen an Dritte, auf die im nachstehenden Unterabschnitt „Verletzung von Schutzrechten" verwiesen wird; und
  (2) Schäden, für die nach geltendem Recht keine Haftungsbegrenzung zulässig ist.

c. Verletzung von Schutzrechten

- Wenn ein Dritter Ansprüche gegen den Kunden geltend macht, die aus einer Verletzung eines gewerblichen Schutzrechts oder Urheberrechts durch den IBM Cloud-Service hergeleitet werden, wird IBM den Kunden gegen alle Ansprüche Dritter verteidigen und dem Kunden alle Schadenersatzbeträge erstatten, die von einem Gericht auferlegt wurden oder in einem Vergleich enthalten sind, der zuvor von IBM gebilligt wurde.

- Damit IBM Abwehrmassnahmen übernimmt und für Verletzungen von Schutzrechten aufkommt, muss der Kunde unverzüglich
  (1) IBM von der Geltendmachung eines solchen Anspruchs schriftlich benachrichtigen;
  (2) die von IBM angeforderten Informationen bereitstellen; und
  (3) IBM alle Abwehrmassnahmen und Vergleichsverhandlungen überlassen und sich zu einer angemessenen Mitwirkung, einschliesslich Bemühungen um Schadenbegrenzung, bereiterklären.
- Die Verpflichtung von IBM zur Abwehr von Ansprüchen und die Zahlungsverpflichtungen von IBM bei Verletzungen von Schutzrechten bestehen auch bei Ansprüchen in Bezug auf Open-Source-Code, den IBM auswählt und in die IBM Cloud-Services einbettet. Open-Source-Code ist Software, die von einer Drittpartei lizenziert wird und der unter https://opensource.org/osd angegebenen „Open Source Definition" entspricht.

d. Haftungs-ausschlüsse

- IBM übernimmt keine Haftung für Ansprüche im Zusammenhang mit
  (1) Produkten und Non-IBM Cloud-Services anderer Anbieter;
  (2) Liefergegenständen, die nicht von IBM bereitgestellt wurden; oder
  (3) Ansprüchen, die auf Rechtsverletzungen oder Verletzungen der Rechte Dritter beruhen, die durch Inhalte, Materialien, Entwürfe oder Spezifikationen verursacht wurden.

Laufzeit und Kündigung

a. Laufzeit eines Cloud-Service

- Die Laufzeit beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf die Cloud-Services freigeschaltet ist.
- Im Auftragsdokument ist angegeben, ob sich die Cloud-Services automatisch verlängern, auf fortlaufender Basis genutzt werden können oder am Ende der Laufzeit ablaufen.
- Bei automatischer Verlängerung werden die Cloud-Services automatisch um die angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM oder dem IBM Business Partner, über den er den Cloud-Service bezogen hat, mindestens 30 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht.
- Bei fortlaufender Nutzung stehen die Cloud-Services auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 30 Tagen IBM oder dem IBM Business Partner eine schriftliche Kündigung zukommen lässt. Die Cloud-Services bleiben nach Ablauf der 30-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

b. Aussetzung eines IBM Cloud-Service

- IBM kann die Nutzung eines IBM Cloud-Service durch den Kunden in folgenden Fällen aussetzen oder im erforderlichen Umfang einschränken, wenn IBM dies für notwendig hält:
  (1) bei einem Verstoss des Kunden gegen wesentliche vertragliche Verpflichtungen;
  (2) bei einer Sicherheitsverletzung;
  (3) bei einer Rechtsverletzung; oder
  (4) bei einem Verstoss gegen die Nutzungsbedingungen.
- IBM wird den Kunden, falls wirtschaftlich vertretbar, vorab von einer Aussetzung in Kenntnis setzen.
- Wenn die Ursache einer Aussetzung mit angemessenen Mitteln beseitigt werden kann, teilt IBM dem Kunden mit, welche Massnahmen er zur Wiedereinsetzung der IBM Cloud-Services ergreifen muss. Falls der Kunde es versäumt, diese Massnahmen innerhalb einer angemessenen Frist zu ergreifen, kann IBM die Cloud-Services kündigen.

c. Kündigung von Cloud-Services

- Der Kunde kann die IBM Cloud-Services in folgenden Fällen unter Einhaltung einer Frist von 30 Tagen kündigen:
  (1) bei schriftlicher Empfehlung einer Regierungs- oder Regulierungsbehörde infolge einer Änderung der gesetzlichen Rahmenbedingungen oder der IBM Cloud-Services;
  (2) wenn eine Änderung der IBM Cloud-Services dazu führt, dass der Kunde geltende Gesetze nicht mehr einhält;

[redacted]

(3) wenn IBM den Kunden über eine Änderung an den IBM Cloud-Services informiert, die erhebliche nachteilige Auswirkungen auf die Nutzung der IBM Cloud-Services durch den Kunden hat, unter der Voraussetzung, dass IBM ein Zeitraum von 90 Tagen zugestanden wird, um diese Auswirkungen in Zusammenarbeit mit dem Kunden zu minimieren.

- Im Fall einer solchen Kündigung oder einer Kündigung eines Non-IBM Cloud-Service eines anderen Anbieters aus den gleichen Gründen wird IBM einen Teil der für den betroffenen Cloud-Service für den Zeitraum nach dem Datum der Kündigung vorausbezahlten Beträge zurückerstatten.
- Der Kunde kann die IBM Cloud-Services bei einem Verstoss von IBM gegen wesentliche vertragliche Verpflichtungen kündigen, sofern der Kunde IBM schriftlich mahnt und ihr eine angemessene Nachfrist zur Erfüllung ihrer Verpflichtungen einräumt.
- Werden die Cloud-Services aus einem anderen Grund gekündigt, wird der Kunde IBM am Datum der Kündigung die gemäss der Vereinbarung fälligen Gesamtbeträge bezahlen.
- IBM kann den Kunden im Kündigungsfall gegen Zahlung einer zusätzlichen Gebühr und auf der Basis separat vereinbarter Bedingungen bei der Übertragung von Inhalten auf eine alternative Technologie unterstützen.

---

d. Kündigung der Vereinbarung für Cloud-Services

- Beide Vertragsparteien können diese Vereinbarung für Cloud-Services wie folgt kündigen:
  (1) durch ordentliche Kündigung nach Ablauf oder Beendigung ihrer Verpflichtungen unter der Vereinbarung mit einer Frist von mindestens 30 Tagen; oder
  (2) unmittelbar durch ausserordentliche Kündigung, wenn die jeweils andere gegen eine wesentliche vertragliche Verpflichtung verstösst, sofern die kündigende Vertragspartei die andere schriftlich mahnt und ihr eine angemessene Nachfrist zur Erfüllung ihrer Verpflichtungen einräumt.
- Bedingungen, die ihrer Natur nach nicht zeitlich befristet sind, bleiben bis zu ihrer Erfüllung in Kraft und gelten auch für eventuelle Rechtsnachfolger oder Zessionare.
- Die Kündigung dieser Vereinbarung für Cloud-Services hat keine Auswirkung auf die Auftragsdokumente, und Bestimmungen dieser Vereinbarung, die sich auf die Auftragsdokumente beziehen, bleiben bis zu ihrer Erfüllung oder bis sie anderweitig gemäss ihren Bedingungen gekündigt werden, in Kraft.

---

8. Geltendes Recht und Geltungsbereich

a. Einhaltung von Gesetzen

- Die Vertragsparteien sind verantwortlich für die Einhaltung
  (1) der Gesetze und Bestimmungen, die sich auf ihre Geschäftstätigkeit und ihre Inhalte beziehen; sowie
  (2) der Import-, Export- und Sanktionsgesetze und -bestimmungen, einschliesslich der Kontrollvorschriften eines Landes in Bezug auf den Handel mit Waffen, Rüstungs- und Verteidigungsgütern, insbesondere der International Traffic in Arms Regulations (ITAR; Regelungen des internationalen Waffenhandels) und der Kontrollvorschriften der USA, die den Export, Reexport oder Transfer von Produkten, Technologien, Services oder Daten, direkt oder indirekt, in bestimmte Länder, für bestimmte Nutzungsarten oder an bestimmte Endnutzer verbieten oder beschränken.

---

b. Geltendes Recht

- Beide Vertragsparteien sind damit einverstanden, dass für die Vereinbarung die Gesetze des Landes zur Anwendung kommen, in dem sich die Geschäftsadresse des Kunden befindet, unter Ausschluss der Prinzipien des Kollisionsrechts.
- Die Rechte und Pflichten der Vertragsparteien gelten nur in dem Land, in dem sich die Geschäftsadresse des Kunden befindet.
- Wenn der Kunde oder ein Benutzer Inhalte exportiert oder importiert oder Teile der Cloud-Services ausserhalb des Landes verwendet, in dem sich die Geschäftsadresse des Kunden befindet, fungiert IBM weder als Exporteur noch als Importeur, ausser wenn IBM nach den Datenschutzgesetzen dazu verpflichtet ist.
- Falls eine der Bedingungen der Vereinbarung im Rahmen des geltenden Rechts ungültig oder undurchführbar ist, sind die übrigen Bedingungen davon nicht betroffen und gelten weiterhin in vollem Umfang.
- Gesetzlich unabdingbare Verbraucherschutzrechte haben Vorrang vor den Bedingungen der Vereinbarung.

[redacted]

		• Die Vertragskonvention der Vereinten Nationen für den internationalen Warenverkauf kommt unter der Vereinbarung nicht zur Anwendung.
c.	**Gerichtsstand**	• Sämtliche Rechtsstreitigkeiten fallen ausschliesslich in die Zuständigkeit des Handelsgerichts im Kanton Zürich.

9. Allgemeines

a.	**Rolle von IBM**	• IBM ist ein unabhängiger Vertragsnehmer und weder im Auftrag oder im Rahmen eines Joint Venture noch als Partner- oder Treuhandunternehmen für den Kunden tätig. • IBM übernimmt keine rechtlichen Verpflichtungen des Kunden oder die Verantwortung für die Geschäftstätigkeit oder den Geschäftsbetrieb des Kunden. Der Kunde ist für seine Nutzung von Cloud-Services selbst verantwortlich. • IBM fungiert ausschliesslich als Anbieter von Informationstechnologie. • Alle Anweisungen, empfohlenen Vorgehensweisen, Anleitungen oder die Nutzung der Cloud-Services durch IBM stellen keine medizinische, klinische, rechtliche, betriebswirtschaftliche oder anderweitige lizenzierte fachliche Beratung dar. Der Kunde und seine berechtigten Benutzer sind für die Nutzung der Cloud-Services in einem Arbeitsumfeld verantwortlich und sollten sich auf eigene Initiative von fachlich kompetenter Stelle beraten lassen. • Jede Vertragspartei entscheidet selbst über den Einsatz sowie die Steuerung, Kontrolle und Entlohnung ihrer Mitarbeiter und der Mitarbeiter ihrer verbundenen Unternehmen und der jeweiligen Auftragnehmer.
b.	**Änderung der Vereinbarung für Cloud-Services**	• IBM kann diese Vereinbarung für Cloud-Services unter Einhaltung einer Frist von mindestens drei Monaten ändern. • Rückwirkende Änderungen der Vereinbarung für Cloud-Services sind ausgeschlossen. Alle Änderungen gelten ab dem Wirksamkeitsdatum nur (1) für Neubestellungen; (2) fortlaufende Cloud-Services, die nicht ablaufen; und (3) Verlängerungen. • Bei Transaktionen mit einer vorbestimmten, verlängerbaren Vertragslaufzeit gemäss den Angaben in einem Auftragsdokument kann der Kunde verlangen, dass die Änderungen erst zum Beginn der Verlängerungsperiode wirksam werden. • Der Kunde erklärt sich mit den Änderungen einverstanden, wenn er nach dem Wirksamkeitsdatum der Änderungen Neubestellungen aufgibt, die Nutzung fortsetzt oder nach Erhalt der Änderungsmitteilung keine Einwände gegen die Verlängerung von Transaktionen erhebt. • Soweit in diesem Abschnitt und dem vorstehenden Abschnitt „Änderung oder Zurückziehung von Cloud-Services" nicht abweichend angegeben, müssen alle anderen Änderungen an der Vereinbarung schriftlich erfolgen und von beiden Vertragsparteien akzeptiert werden.
c.	**Geschäfts-verhalten**	• IBM hat umfassende geschäftliche Verhaltensregeln und zugehörige Richtlinien eingeführt, die sich auf den Umgang mit Interessenkonflikten, Marktmissbrauch, Bestechung, Korruption und Betrug beziehen. • IBM und ihre Mitarbeiter halten sich an diese Richtlinien und IBM verlangt von ihren Auftragnehmern die Festlegung vergleichbarer Richtlinien.
d.	**Geschäfts-bezogene Kontakt-informationen und Informationen zur Kontonutzung**	• IBM, die mit IBM verbundenen Unternehmen und ihre jeweiligen Auftragnehmer benötigen Zugang zu geschäftsbezogenen Kontaktinformationen und Informationen zur Kontonutzung. Diese Informationen sind keine Inhalte. • Geschäftsbezogene Kontaktinformationen werden zu Kommunikationszwecken und im Geschäftsverkehr mit dem Kunden verwendet. Beispiele für geschäftsbezogene Kontaktinformationen sind Name, Geschäftsadresse und -telefon, E-Mail und Benutzer-ID.

[redacted]

- Informationen zur Kontonutzung sind für die Aktivierung, Bereitstellung, den Betrieb, die Unterstützung, Verwaltung und Verbesserung von Cloud-Services erforderlich. Beispiele für Informationen zur Kontonutzung sind digitale Informationen, die mit Tracking-Technologien bei der Nutzung der IBM Cloud-Services erfasst werden, wie z. B. Cookies und Web-Beacons.
- Weitere Informationen über die Erfassung, die Nutzung und den Umgang mit geschäftsbezogenen Informationen und Informationen zur Kontonutzung sind in der IBM Datenschutzerklärung unter https://www.ibm.com/privacy/ zu finden.
- Wenn der Kunde IBM Informationen bereitstellt und für die Verarbeitung dieser Informationen die Benachrichtigung der betroffenen Personen und deren Zustimmung erforderlich ist, wird der Kunde dies entsprechend veranlassen.

e. IBM Business Partner

- IBM Business Partner, die Cloud-Services verwenden oder verfügbar machen, sind von IBM unabhängig und entscheiden allein über ihre Preise und Bedingungen. IBM ist weder für deren Handlungen noch für deren Unterlassungen, Äusserungen oder Angebote verantwortlich.
- Wenn IBM den Kunden davon in Kenntnis setzt, dass sein derzeitiger IBM Business Partner zukünftig keine Cloud-Services mehr vertreiben wird, kann der Kunde Cloud-Services mit automatischer Verlängerung oder fortlaufender Nutzung direkt von IBM oder einem anderen autorisierten IBM Business Partner erwerben.

f. Abtretung

- Die Abtretung von Rechten aus der Vereinbarung bedarf der vorherigen schriftlichen Zustimmung der anderen Vertragspartei.
- IBM ist zur Abtretung von Zahlungsansprüchen berechtigt, bleibt aber für die Erfüllung ihrer Verpflichtungen verantwortlich.
- Die Abtretung von Rechten durch IBM in Verbindung mit dem Verkauf des IBM Geschäftsteils, zu dem die Cloud-Services gehören, bedarf keiner Zustimmung.
- IBM kann diese Vereinbarung und zugehörige Dokumente in Verbindung mit einer Abtretung weitergeben.

g. Unternehmens-gesellschaften

- Diese Vereinbarung für Cloud-Services gilt für IBM und den Kunden (der diese Vereinbarung für Cloud-Services akzeptiert) sowie ihre jeweiligen Unternehmensgesellschaften, die unter dieser Vereinbarung Cloud-Services erbringen oder erwerben.
- Die Vertragsparteien verpflichten sich zur Koordination der Aktivitäten ihrer Unternehmensgesellschaften im Rahmen der Vereinbarung für Cloud-Services.
- Unternehmensgesellschaften umfassen:
  (1) Unternehmen im selben Land, die der Kunde oder IBM kontrolliert (als Eigentümer von mehr als 50 % der stimmberechtigten Anteile); und
  (2) andere Unternehmen, die den Kunden oder IBM kontrollieren, die der Kunde oder IBM kontrolliert oder die unter gemeinsamer Kontrolle mit dem Kunden oder IBM stehen und die eine Teilnahmevereinbarung unterzeichnet haben.

h. Mitteilungen und Verwaltung

- Alle Mitteilungen unter der Vereinbarung müssen in Schriftform erfolgen und an die für die Vereinbarung angegebene Geschäftsadresse gerichtet sein, sofern nicht von einer Vertragspartei eine andere Adresse schriftlich mitgeteilt wird.
- Die Vertragsparteien erklären sich mit der Verwendung von elektronischen Mitteln und Faxübertragungen für die Kommunikation einverstanden. Diese Kommunikation wird einem unterzeichneten Dokument gleichgestellt.
- Jede originalgetreue Vervielfältigung der Vereinbarung wird als Original angesehen.
- Die Vereinbarung setzt etwaige Handelsbräuche, Absprachen oder Erklärungen zwischen den Vertragsparteien ausser Kraft.
- Soweit unter der Vereinbarung Freigaben, Abnahmen, Einwilligungen, Zugriffsberechtigungen, Mitwirkungshandlungen oder ähnliche Massnahmen seitens einer Vertragspartei erforderlich sind, dürfen diese nicht ohne triftigen Grund verzögert oder verweigert werden.

i. Geltendmachung von Ansprüchen

- Aus der Vereinbarung oder einer Transaktion unter der Vereinbarung ergeben sich weder Rechte noch Ansprüche zugunsten Dritter.

[redacted]

- Beide Vertragsparteien kommen überein, keine rechtlichen Schritte im Zusammenhang mit der Vereinbarung später als zwei Jahre nach Entstehen eines Anspruches einzuleiten.
- Mit Ausnahme von Zahlungsverpflichtungen ist keine der Vertragsparteien für die Nichterfüllung von Verpflichtungen aus Gründen verantwortlich, die ausserhalb ihres Einflussbereichs liegen.
- Die Vertragsparteien sind sich einig, dass eventuelle Meinungsverschiedenheiten oder Beanstandungen zunächst im partnerschaftlichen Sinne einer Lösung zugeführt werden sollen.

---

j. Globale Ressourcen

- IBM kann Personal und Betriebsmittel an Standorten weltweit sowie Auftragnehmer zur Unterstützung bei der Bereitstellung von IBM Cloud-Services einsetzen.
- Die Nutzung der Cloud-Services durch den Kunden kann die grenzüberschreitende Übermittlung von Inhalten, einschliesslich personenbezogener Daten, zur Folge haben.
- Eine Liste der Länder, in die Inhalte übertragen und für einen IBM Cloud-Service verarbeitet werden können, ist im massgeblichen Auftragsdokument angegeben.
- Für die Verpflichtungen im Rahmen der Vereinbarung ist IBM verantwortlich, selbst wenn IBM einen Auftragnehmer beauftragt, und IBM wird geeignete Vereinbarungen abschliessen, die IBM die Einhaltung ihrer Verpflichtungen für die IBM Cloud-Services ermöglichen.

---

k. Sonstige Services

- IBM kann zusätzliche Anpassungs- und Konfigurationsservices oder sonstige Services zur Unterstützung der Cloud-Services anbieten, die in einem Auftragsdokument ausführlich beschrieben werden.

[redacted]

12

Ergänzende Bedingungen zur Auftragsverarbeitung

Diese Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV) und die zugehörigen servicespezifischen Anlagen zu den EB-AV (Anlagen) finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden (personenbezogenen Daten des Kunden) im Rahmen der Erbringung der in der Vereinbarung aufgeführten Services (Services) verarbeitet und die europäische Datenschutz-Grundverordnung 2016/679 (DSGVO) oder eines der unter http://www.ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze (zusammen 'Datenschutzgesetze') hierauf Anwendung finden. Die jeweilige Anlage ist im Auftragsdokument des entsprechenden Service aufgeführt. Diese EB-AV sind Bestandteil der Vereinbarung. Begriffe, die in diesem Dokument verwendet, jedoch nicht definiert werden, haben die in den einschlägigen Datenschutzgesetzen festgelegte Bedeutung. Bei Widersprüchen haben die jeweiligen Anlagen Vorrang vor den EB-AV, die wiederum Vorrang vor dem Rest der Vereinbarung haben.

1. Verarbeitung

1.1 Der Kunde (a) ist Verantwortlicher im Hinblick auf die personenbezogenen Daten des Kunden oder (b) handelt als Auftragsverarbeiter im Auftrag sonstiger Verantwortlicher und wurde von diesen angewiesen und hat von diesen die Genehmigung eingeholt, IBM als Unterauftragsverarbeiter mit der Verarbeitung der personenbezogenen Daten des Kunden gemäß dieser EB-AV zu beauftragen. Der Kunde ernennt IBM zum Auftragsverarbeiter für die Verarbeitung der personenbezogenen Daten des Kunden. Sofern es noch weitere Verantwortliche gibt, wird der Kunde diese vor Übermittlung derer personenbezogener Daten, wie in der Anlage aufgeführt, identifizieren und IBM mitteilen.

1.2 Eine Liste der Kategorien betroffener Personen, der Arten personenbezogener Daten des Kunden, der besonderen Kategorien personenbezogener Daten und der Verarbeitungstätigkeiten sind in der jeweiligen Anlage enthalten. Die Dauer der Verarbeitung entspricht der Laufzeit des Service, sofern in der jeweiligen Anlage nicht abweichend vereinbart. Zweck und Gegenstand der Verarbeitung ist die Erbringung des Service gemäß der Beschreibung in der Vereinbarung.

1.3 IBM verarbeitet personenbezogene Daten des Kunden gemäß den dokumentierten Weisungen des Kunden. Der Umfang der Weisungen des Kunden für die Verarbeitung personenbezogener Daten des Kunden wird durch die Vereinbarung und, sofern zutreffend, die Nutzung und Konfiguration der Funktionen des Service durch den Kunden und dessen berechtigte Benutzer festgelegt. Der Kunde kann in Übereinstimmung mit Ziffer 10.2 weitere gesetzlich erforderliche Weisungen für die Verarbeitung personenbezogener Daten des Kunden (zusätzliche Weisungen) erteilen. Sollte IBM den Kunden informieren, dass einer zusätzlichen Weisung nicht entsprochen werden kann, werden die Parteien zusammenarbeiten, um eine Alternative zu finden. Falls IBM den Kunden informiert, dass weder der zusätzlichen Weisung noch einer Alternative entsprochen werden kann, kann der Kunde den betroffenen Service gemäß den einschlägigen Bedingungen der Vereinbarung kündigen. Ist IBM der Auffassung, dass eine Weisung gegen die Datenschutzgesetze verstößt, wird IBM den Kunden unverzüglich darüber informieren. IBM kann die Erfüllung einer solchen Weisung aussetzen, bis der Kunde entweder deren Rechtmäßigkeit schriftlich bestätigt oder diese ändert.

1.4 Der Kunde ist einziger Ansprechpartner für IBM. Da sonstige Verantwortliche gegebenenfalls über direkte Rechte gegenüber IBM verfügen, verpflichtet sich der Kunde, diese Rechte in deren Namen auszuüben und alle hierzu erforderlichen Genehmigungen von den sonstigen Verantwortlichen einzuholen. IBM wird von ihrer Verpflichtung befreit, einen sonstigen Verantwortlichen zu informieren oder zu benachrichtigen, wenn die entsprechende Information oder Benachrichtigung gegenüber dem Kunden erfolgt ist. Gleichermaßen ist IBM einziger Ansprechpartner für den Kunden in Bezug auf ihre Pflichten als Auftragsverarbeiter im Rahmen dieser EB-AV.

1.5 IBM verpflichtet sich zur Einhaltung aller für IBM als Auftragsverarbeiter in Bezug auf die Services geltenden Datenschutzgesetze. IBM ist weder für die Ermittlung der für den Kunden anwendbaren gesetzlichen oder regulatorischen Anforderungen verantwortlich noch dafür, dass ein Service diesen Anforderungen entspricht. Im Verhältnis zwischen den Parteien ist der Kunde für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten des Kunden verantwortlich. Die Services dürfen vom Kunden nicht auf eine Art und Weise genutzt werden, die gegen geltende Datenschutzgesetze verstoßen.

2. Technische und organisatorische Maßnahmen

2.1 Der Kunde und IBM vereinbaren, dass IBM die in der jeweiligen Anlage aufgeführten technischen und organisatorischen Maßnahmen, die ein dem Risiko angemessenes Schutzniveau gewährleisten, in ihrem Verantwortungsbereich implementieren und aufrechterhalten wird. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dementsprechend behält sich IBM das Recht vor, die technischen und organisatorischen Maßnahmen zu ändern, sofern die Funktionalität und Sicherheit der Services nicht negativ beeinträchtigt werden.

3. Rechte und Anträge betroffener Personen

3.1 IBM informiert den Kunden über Anträge von betroffenen Personen, die ihre Betroffenenrechte (z. B. einschließlich aber nicht begrenzt auf Berichtigung, Löschung und Sperrung von Daten) direkt gegenüber IBM in Bezug auf personenbezogene Daten des Kunden geltend machen. Der Kunde ist für die Beantwortung solcher Anträge von

betroffenen Personen zuständig. IBM unterstützt den Kunden in angemessenem Umfang bei der Beantwortung von Anträgen von betroffenen Personen in Übereinstimmung mit Ziffer 10.2.

3.2 Falls eine betroffene Person einen Anspruch aufgrund der Verletzung ihrer Betroffenenrechte direkt gegenüber IBM geltend macht, erstattet der Kunde IBM sämtliche Kosten, Gebühren, Schäden, Aufwendungen oder Verluste, die sich aus einem solchen Anspruch ergeben, sofern IBM den Kunden über den Anspruch in Kenntnis gesetzt und ihm die Möglichkeit gegeben hat, bezüglich der Abwehr und Beilegung des Anspruchs mit IBM zusammenzuarbeiten. Vorbehaltlich der in der Vereinbarung enthaltenen Bedingungen kann der Kunde gegenüber IBM Schadensersatz für Ansprüche betroffener Personen geltend machen, deren Betroffenenrechte durch einen Verstoß von IBM gegen ihre Verpflichtungen aus diesen EB-AV und der jeweiligen Anlage verletzt wurden.

4. Anforderungen Dritter und Vertraulichkeit

4.1 IBM verpflichtet sich, personenbezogene Daten des Kunden nicht gegenüber Dritten offenzulegen, es sei denn, der Kunde hat dies gestattet oder es ist gesetzlich erforderlich. Sollte eine Behörde oder Aufsichtsbehörde Zugriff auf personenbezogene Daten des Kunden anfordern, informiert IBM den Kunden vor der Offenlegung entsprechend, sofern eine solche Information nicht gesetzlich verboten ist.

4.2 IBM verpflichtet alle Mitarbeiter, die Zugang zu personenbezogenen Daten des Kunden haben, diese Daten vertraulich zu behandeln und sie ausschließlich nach den Weisungen des Kunden zu verarbeiten, es sei denn, dass IBM nach geltendem Recht zur Verarbeitung verpflichtet ist.

5. Audit

5.1 IBM wird Überprüfungen, einschließlich Inspektionen, die vom Kunden oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, entsprechend dem nachfolgend dargestellten Verfahren ermöglichen und dazu beitragen:

a. Auf schriftliche Anfrage des Kunden stellt IBM dem Kunden oder dem von ihm beauftragten Prüfer die aktuellen Zertifizierungen und/oder zusammenfassenden Prüfberichte bereit, die von IBM beauftragt wurden, um die Effektivität der technischen und organisatorischen Maßnahmen regelmäßig zu testen, zu beurteilen und auszuwerten, sofern solche in der jeweiligen Anlage aufgeführt sind.

b. IBM wird in angemessenem Umfang mit dem Kunden zusammenarbeiten, indem IBM zusätzliche verfügbare Informationen in Bezug auf die technischen und organisatorischen Maßnahmen bereitstellt, um den Kunden zu unterstützen, diese Maßnahmen besser nachvollziehen zu können.

c. Sollte der Kunde weitere Informationen benötigen, um seinen eigenen Auditverpflichtungen oder denen sonstiger Verantwortlicher nachzukommen oder der Anforderung einer zuständigen Aufsichtsbehörde gerecht zu werden, wird er IBM schriftlich informieren, damit IBM diese Informationen bereitstellen oder Zugriff darauf erteilen kann.

d. Sollte es nicht möglich sein, einem gesetzlich zwingend einzuräumenden oder von den Parteien ausdrücklich vereinbarten Auditrecht anderweitig nachzukommen, können nur gesetzlich verpflichtete Parteien (z. B. eine Regulierungsbehörde, die die Aufsicht über das operative Geschäft des Kunden hat), der Kunde oder der von ihm beauftragte Prüfer die für die Serviceerbringung genutzten IBM Betriebsstätten besuchen. Ein solcher Besuch ist zeitlich mit IBM während der üblichen Geschäftszeiten zu koordinieren, darf die Betriebsabläufe möglichst nicht stören und hat in Übereinstimmung mit den gegebenenfalls in der Anlage beschriebenen Auditverfahren zu erfolgen, um Risiken für andere IBM Kunden zu reduzieren.

Jeder andere vom Kunden beauftragte Prüfer darf kein direkter Wettbewerber von IBM in Bezug auf die Services sein und muss entsprechend zur Vertraulichkeit verpflichtet werden.

5.2 Beide Parteien tragen ihre Kosten in Bezug auf die Absätze a. und b. von Ziffer 5.1 jeweils selbst, im Übrigen findet Ziffer 10.2 Anwendung.

6. Rückgabe oder Löschung personenbezogener Daten des Kunden

6.1 Nach Kündigung oder Ablauf der Vereinbarung wird IBM die sich in ihrem Besitz befindenden personenbezogenen Daten des Kunden gemäß den Angaben in der jeweiligen Anlage entweder löschen oder zurückgeben, sofern nicht durch zwingende Rechtsvorschriften etwas anderes vorgesehen ist.

7. Unterauftragsverarbeiter

7.1 Der Kunde genehmigt die Beauftragung anderer Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten des Kunden (Unterauftragsverarbeiter). Eine Liste der aktuellen Unterauftragsverarbeiter ist in der jeweiligen Anlage enthalten. IBM informiert den Kunden vorab über jede beabsichtigte Hinzufügung oder jeden beabsichtigten Austausch von Unterauftragsverarbeitern gemäß der Beschreibung in der jeweiligen Anlage. Innerhalb eines Zeitraums von 30 Tagen nach der Benachrichtigung durch IBM über eine beabsichtigte Änderung kann der Kunde gegen die Hinzufügung oder den Austausch eines Unterauftragsverarbeiters Einspruch erheben, wenn hierdurch geltende Rechtsvorschriften verletzt würden. Der Einspruch des Kunden muss schriftlich erfolgen und die konkreten Gründe des Kunden für den Einspruch sowie ggf. Kompromissvorschläge beinhalten. Falls der Kunde den Unterauftragsverarbeiter innerhalb dieses Zeitraums nicht ablehnt, kann dieser mit der Verarbeitung personenbezogener Daten des Kunden beauftragt werden. Bevor der Unterauftragsverarbeiter mit der Verarbeitung

[redacted]

personenbezogener Daten des Kunden beginnt, wird IBM diesem Datenschutzverpflichtungen auferlegen, die jenen dieser EB-AV im Wesentlichen vergleichbar sind und nicht zu einem Absinken des Schutzniveaus führen.

7.2 Falls der Kunde gegen einen Unterauftragsverarbeiter berechtigt Einspruch erhebt und IBM diesem Einspruch nicht Rechnung tragen kann, wird IBM den Kunden entsprechend informieren. Der Kunde kann die betroffenen Services gemäß den einschlägigen Bedingungen der Vereinbarung kündigen. Anderenfalls werden die Parteien zusammenarbeiten, um in Übereinstimmung mit dem Streitbeilegungsprozess eine realisierbare Lösung zu finden.

8. Grenzüberschreitende Datenverarbeitung

8.1 Im Falle einer Übermittlung personenbezogener Daten des Kunden in ein Land, in dem gemäß den Datenschutzgesetzen kein angemessenes Datenschutzniveau gewährleistet ist (Land ohne angemessenes Datenschutzniveau), werden die Parteien zusammenarbeiten, um die Einhaltung der geltenden Datenschutzgesetze gemäß den Angaben in den folgenden Abschnitten oder in den Datenschutzgesetzen unter http://www.ibm.com/dpa/dpl sicherzustellen. Falls der Kunde der Ansicht ist, dass die Maßnahmen nicht ausreichen, um die gesetzlichen Bestimmungen einzuhalten, wird er IBM benachrichtigen und die Parteien werden zusammenarbeiten, um eine Alternative zu finden.

8.2 Mit Abschluss der Vereinbarung schließen der Kunde und IBM gleichzeitig die EU-Standardvertragsklauseln ab, wie in der jeweiligen Anlage zu den EB-AV (EU-Standardvertragsklauseln) dargelegt, wenn der Kunde, IBM oder beide in einem Land ohne angemessenes Datenschutzniveau ansässig sind. Wenn die EU-Standardvertragsklauseln nicht erforderlich sind, weil beide Parteien in einem Land ansässig sind, das nach den Datenschutzgesetzen als Land mit angemessenem Datenschutzniveau angesehen wird, das Land, in dem IBM oder der Kunde ansässig ist, jedoch während der Serviceerbringung als Land ohne angemessenes Datenschutzniveau eingestuft wird, kommen die EU-Standardvertragsklauseln zur Anwendung.

Die Parteien erkennen an, dass das anwendbare Modul der EU-Standardvertragsklauseln durch ihre Rolle als Verantwortlicher und/oder Auftragsverarbeiter nach den Umständen des Einzelfalls bestimmt wird und dass sie dafür verantwortlich sind, die korrekte Rolle festzulegen, um die jeweiligen Verpflichtungen im Rahmen des anwendbaren Moduls zu erfüllen.

8.3 Der Kunde erklärt sich damit einverstanden, dass die EU-Standardvertragsklauseln, einschließlich der daraus resultierenden Ansprüche, den in der Vereinbarung enthaltenen Bedingungen, einschließlich der Haftungsbegrenzungen, unterliegen. Bei Widersprüchen haben die EU-Standardvertragsklauseln Vorrang.

8.4 IBM wird die EU-Standardvertragsklauseln mit jedem Unterauftragsverarbeiter abschließen, der gemäß der jeweils geltenden Anlage in einem Land ohne angemessenes Datenschutzniveau ansässig ist.

9. Verletzung des Schutzes personenbezogener Daten

9.1 IBM wird den Kunden unverzüglich informieren, wenn ihr eine Verletzung des Schutzes personenbezogener Daten in Bezug auf die Services bekannt wird. IBM wird die Verletzung des Schutzes personenbezogener Daten unverzüglich untersuchen, sofern sich diese in der IBM Infrastruktur oder in einem anderen Bereich, für den IBM verantwortlich ist, ereignet hat, und wird den Kunden entsprechend Ziffer 10 unterstützen.

10. Unterstützung

10.1 IBM unterstützt den Kunden mit technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Verpflichtungen zur Einhaltung der Betroffenenrechte und bei der Einhaltung seiner Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Mitteilung und Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten und die Durchführung einer Datenschutz-Folgenabschätzung, einschließlich, sofern erforderlich, der vorherigen Konsultation mit der zuständigen Aufsichtsbehörde, unter Berücksichtigung der Art der Verarbeitung und der IBM zur Verfügung stehenden Informationen.

10.2 Der Kunde wird von IBM im Rahmen dieser EB-AV benötigte Unterstützung schriftlich anfordern. IBM darf dem Kunden für diese Unterstützung oder eine zusätzliche Weisung höchstens eine angemessene Gebühr berechnen. Diese Gebühren müssen in einem Angebot enthalten sein und von den Parteien schriftlich vereinbart werden oder entsprechend einem in der Vereinbarung geregelten Änderungsmanagementverfahrens festgelegt werden. Sollte der Kunde dem Angebot nicht zustimmen, vereinbaren die Parteien, in angemessenem Umfang zusammenzuarbeiten, um entsprechend dem Streitbeilegungsprozess eine realisierbare Lösung zu finden.

[redacted]

13

IBM Datensicherheits- und Datenschutzrichtlinien

1. Begriffsbestimmungen

In diesem Dokument verwendete Begriffe haben die nachstehende Bedeutung. Alle hier nicht definierten Begriffe haben die Bedeutung, mit der sie im maßgeblichen schriftlichen Vertrag zwischen IBM und dem Kunden für die IBM Services festgelegt sind.

Kunde – das Unternehmen, für das IBM die IBM Services im Rahmen eines IBM Servicedokuments erbringt.

Komponenten – die Anwendung, Plattform oder Infrastrukturelemente eines IBM Service, der von IBM betrieben und verwaltet wird.

Inhalte – sämtliche Daten, Software und Informationen, die vom Kunden oder seinen berechtigten Benutzern in IBM Services bereitgestellt, für den Zugriff freigegeben oder eingegeben werden.

Datensicherheits- und Datenschutzrichtlinien – die in diesem Dokument beschriebenen Datensicherheits- und Datenschutzrichtlinien.

IBM Cloud-Services – „as-a-Service"-Angebote von IBM, die von IBM über ein Netzwerk zur Verfügung gestellt werden, wie z. B. als Software-as-a-Service, Platform-as-a-Service oder Infrastructure-as-a-Service.

IBM Servicedokument – ein Auftragsdokument oder ein beliebiges anderes Dokument, das durch Bezugnahme in einen schriftlichen Vertrag zwischen IBM und einem Kunden einbezogen wird und in dem Details eines bestimmten IBM Service beschrieben werden.

IBM Services – (a) IBM Cloud-Services, (b) andere IBM Serviceangebote, einschließlich Infrastruktur- oder Anwendungsserviceangebote, die IBM bereitstellt und einem Kunden dediziert zuordnet oder für einen Kunden anpasst, und (c) alle anderen Serviceleistungen, einschließlich Beratung, Wartung oder Support, die IBM für einen Kunden erbringt.

Sicherheitsvorfall – der unbefugte Zugriff auf Inhalte oder deren unbefugte Nutzung.

Auftragsdokument – ein Dokument, in dem die Details der spezifischen Transaktion, wie z. B. Gebühren und eine Beschreibung eines IBM Cloud-Service sowie entsprechende Informationen, enthalten sind. Beispiele für Auftragsdokumente sind unter anderem Leistungsbeschreibungen, Servicebeschreibungen, Bestellungen und Rechnungen für einen IBM Cloud-Service. Für eine Transaktion können mehrere Auftragsdokumente zur Anwendung kommen.

2. Übersicht

Die technischen und organisatorischen Maßnahmen, die in diesen Datensicherheits- und Datenschutzrichtlinien beschrieben werden, gelten nur dann für IBM Services (einschließlich der Komponenten), wenn IBM die Einhaltung der Datensicherheits- und Datenschutzrichtlinien in einem schriftlichen Vertrag mit dem Kunden ausdrücklich vereinbart hat. Es wird ausdrücklich darauf hingewiesen, dass diese Maßnahmen nicht zur Anwendung kommen, wenn der Kunde für Sicherheit und Datenschutz verantwortlich ist oder wie nachstehend angegeben oder wenn in einem IBM Servicedokument abweichende Regelungen enthalten sind.

a. Der Kunde ist dafür verantwortlich, zu entscheiden, ob ein IBM Service für seine beabsichtigte Nutzung geeignet ist, und die Sicherheits- und Datenschutzmaßnahmen für Komponenten umzusetzen und zu verwalten, die nicht von IBM innerhalb der IBM Services bereitgestellt oder verwaltet werden. Beispiele für Verantwortlichkeiten des Kunden für IBM Services sind: (1) die Sicherheit von Systemen und Anwendungen, die vom Kunden auf einem Infrastructure-as-a-Service- oder Platform-as-a-Service-Angebot oder auf Infrastruktur, Komponenten oder Software, die IBM für den Kunden verwaltet, erstellt oder eingesetzt werden, (2) die Vergabe von Zugriffsrechten an Endbenutzer des Kunden und die Sicherheitskonfiguration auf Anwendungsebene für ein Software-as-a-Service-Angebot, das IBM für den Kunden verwaltet, oder ein Anwendungsserviceangebot, das IBM für den Kunden bereitstellt.

b. Der Kunde bestätigt, dass IBM diese Datensicherheits- und Datenschutzrichtlinien von Zeit zu Zeit nach eigenem Ermessen ändern kann und dass frühere Versionen durch diese Änderungen ab dem Datum ihrer Veröffentlichung außer Kraft gesetzt werden. Ungeachtet gegenteiliger Bestimmungen in einem schriftlichen Vertrag zwischen IBM und dem Kunden werden alle Änderungen mit der Absicht durchgeführt, (1) bestehende Verpflichtungen von IBM zu verbessern oder transparenter zu

gestalten, (2) IBM zu ermöglichen, den Sicherheitsfokus auf aufkommende Bedrohungen und Probleme bei der Daten- und Cybersicherheit zu richten, (3) die Umsetzung neu eingeführter Standards und anwendbarer Gesetze sicherzustellen oder (4) zusätzliche Features und Funktionen bereitzustellen. Durch die Änderungen werden die Sicherheits- oder Datenschutzfeatures oder -funktionen von IBM Services nicht beeinträchtigt.

c. Bei Widersprüchen zwischen diesen Datensicherheits- und Datenschutzrichtlinien und einem IBM Servicedokument hat das IBM Servicedokument Vorrang. Wenn die entgegenstehenden Bedingungen in einem Auftragsdokument enthalten sind, werden diese als übergeordnete Bedingungen angegeben, die Vorrang vor diesen Datensicherheits- und Datenschutzrichtlinien haben, und gelten nur für die bestimmte Transaktion.

3. Datenschutz

a. IBM wird sämtliche Inhalte vertraulich behandeln, indem Inhalte nur Mitarbeitern, Auftragnehmern und Lieferanten (einschließlich Unterauftragsverarbeitern) von IBM und ausschließlich in dem Umfang offengelegt werden, der zur Erbringung der IBM Services erforderlich ist.

b. Die Sicherheits- und Datenschutzmaßnahmen für jeden IBM Service werden gemäß dem IBM Grundsatz der eingebauten Sicherheit und Privatsphäre umgesetzt, um die von einem IBM Service verarbeiteten Inhalte zu schützen und die Verfügbarkeit dieser Inhalte nach Maßgabe des anwendbaren schriftlichen Vertrags zwischen IBM und dem Kunden sowie der anwendbaren IBM Servicedokumente aufrechtzuerhalten.

c. Im IBM Servicedokument oder in anderen Standarddokumenten können zusätzliche Sicherheits- und Datenschutzinformationen für einen bestimmten IBM Service enthalten sein, um den Kunden bei der anfänglichen und fortlaufenden Beurteilung der Eignung eines IBM Service für seine beabsichtigte Nutzung zu unterstützen. Diese Informationen können Nachweise über angegebene Zertifizierungen und Akkreditierungen, weiterführende Informationen zu diesen Zertifizierungen und Akkreditierungen, Datenblätter, häufig gestellte Fragen (FAQs) und andere allgemein verfügbare Dokumente umfassen. Falls der Kunde IBM auffordert, von ihm bevorzugte Fragebögen zu Sicherheit oder Datenschutz auszufüllen, wird IBM den Kunden auf die verfügbaren Standarddokumente verweisen.

4. Sicherheitsrichtlinien

a. IBM wird die schriftlichen IT-Sicherheitsrichtlinien und -verfahren, die ein integraler Bestandteil der Geschäftstätigkeit von IBM und für alle IBM Mitarbeiter verbindlich sind, aufrechterhalten und befolgen. Der IBM Chief Information Security Officer hat die Verantwortung für die Überwachung und Umsetzung dieser Richtlinien, insbesondere für das formale Governance- und Revisionsmanagement, die Mitarbeiterausbildung und die Durchsetzung der Compliance.

b. Die IT-Sicherheitsrichtlinien werden von IBM mindestens einmal jährlich überprüft und ergänzt oder geändert, wenn IBM dies zum Schutz der IBM Services und Inhalte für angemessen erachtet.

c. IBM wird ihre verbindlichen Standardanforderungen in Bezug auf die Überprüfung aller neu eingestellten Beschäftigten aufrechterhalten und befolgen und diese Anforderungen auf ihre 100-prozentigen Tochtergesellschaften ausweiten. Diese Anforderungen werden gemäß den internen Prozessen und Verfahren von IBM regelmäßig überprüft und können unter anderem die Überprüfung möglicher Vorstrafen und der Identität sowie zusätzliche Prüfungen umfassen, die von IBM als notwendig erachtet werden. Jede IBM Gesellschaft ist für die Umsetzung dieser Anforderungen im Rahmen ihres Einstellungsverfahrens verantwortlich, sofern diese anwendbar und unter der jeweils geltenden Rechtsordnung zulässig sind.

d. IBM Mitarbeiter werden jährlich IBM Schulungen für Sicherheit und Datenschutz absolvieren und jedes Jahr nachweisen, dass sie die Anforderungen von IBM in Bezug auf Unternehmensethik, Vertraulichkeit und Sicherheitsrichtlinien gemäß den IBM Geschäftsgrundsätzen (Business Conduct Guidelines) einhalten. Personen mit privilegiertem Zugriff auf Komponenten erhalten zusätzliche Schulungen, die speziell auf ihre Rolle beim Betrieb und Support der IBM Services abgestimmt und zur Aufrechterhaltung der im maßgeblichen IBM Servicedokument beschriebenen Compliance und Akkreditierungen erforderlich sind.

5. Compliance

a. Die von IBM in jedem IBM Standard-Cloud-Service (mit Ausnahme von angepassten Cloud-Services) implementierten und durchgeführten Maßnahmen unterliegen einer jährlichen Zertifizierung, bei der die Einhaltung von ISO 27001 oder SSAE SOC 2 oder von beiden Normen geprüft wird, sofern in einem IBM Servicedokument nichts anderes festgelegt ist.

b. Darüber hinaus wird IBM die Compliance und Akkreditierung für die IBM Services gemäß der Definition in einem IBM Servicedokument aufrechterhalten.

c. Auf Anfrage wird IBM einen Nachweis über die gemäß den Abschnitten 5a. und 5b. geforderte Compliance und Akkreditierung erbringen, wie z. B. Zertifikate, Bescheinigungen oder Berichte über die von akkreditierten unabhängigen Dritten durchgeführten Audits (von akkreditierten unabhängigen Dritten durchgeführte Audits finden mit der vom jeweiligen Standard geforderten Häufigkeit statt).

d. IBM ist auch dann für diese Sicherheits- und Datenschutzmaßnahmen verantwortlich, wenn ein Auftragnehmer oder Lieferant (einschließlich Unterauftragsverarbeitern) für die Bereitstellung oder den Support eines IBM Service eingesetzt wird.

6. Sicherheitsvorfälle

a. IBM wird dokumentierte Richtlinien zur Behebung von Sicherheitsvorfällen nach den Richtlinien des National Institute of Standards and Technology (NIST-Richtlinien), einer Bundesbehörde im Geschäftsbereich des Handelsministeriums der USA, oder nach vergleichbaren Branchenstandards für den Umgang mit IT-Sicherheitsvorfällen etablieren und befolgen und die Bedingungen zur Meldung von Datenschutzverletzungen im maßgeblichen schriftlichen Vertrag zwischen IBM und dem Kunden einhalten.

b. IBM wird Sicherheitsvorfälle, von denen IBM Kenntnis erlangt hat, untersuchen und innerhalb des Geltungsbereichs der IBM Services einen entsprechenden Interventionsplan definieren und umsetzen. Der Kunde kann IBM über den für einen IBM Service vorgesehenen Prozess zur Meldung von Sicherheitsvorfällen (wie in einem IBM Servicedokument angegeben) oder, wenn ein solcher Prozess nicht besteht, in Form einer Anfrage an den technischen Support über mutmaßliche Sicherheitslücken oder Vorfälle benachrichtigen.

c. IBM wird den Kunden unverzüglich über einen bestätigten Sicherheitsvorfall informieren, von dem bekannt ist oder bei dem ein begründeter Verdacht besteht, dass er Auswirkungen auf den Kunden hat. IBM wird dem Kunden in angemessenem Umfang Informationen über einen solchen Sicherheitsvorfall und den Status der IBM Abhilfe- und Wiederherstellungsmaßnahmen bereitstellen.

7. Physische Sicherheit und Zutrittskontrolle

a. IBM wird geeignete physische Zutrittskontrollen, wie Schranken, durch Kartenleser kontrollierte Zutrittspunkte, Überwachungskameras und mit Personen besetzte Empfangsbereiche, einrichten, um von IBM verwaltete Einrichtungen (Rechenzentren), in denen IBM Services gehostet werden, vor unbefugtem Zutritt zu schützen. Weitere Zutrittspunkte zu diesen Rechenzentren, wie Anlieferungsbereiche und Ladedocks, werden kontrolliert und von den IT-Ressourcen strikt getrennt.

b. Der Zutritt zu von IBM verwalteten Rechenzentren und kontrollierten Bereichen innerhalb dieser Rechenzentren wird entsprechend der ausgeübten Funktion eines Mitarbeiters beschränkt und ist genehmigungspflichtig. Der Zutritt wird protokolliert und die Protokolle werden mindestens ein Jahr lang aufbewahrt. Bei Ausscheiden oder Wechsel eines autorisierten Mitarbeiters wird IBM den Zutritt zu den von IBM verwalteten Rechenzentren sperren. Dabei befolgt IBM die formalen dokumentierten Verfahren, die beim Ausscheiden oder Wechsel von Mitarbeitern einzuhalten sind, die das unverzügliche Entfernen aus Zutrittskontrolllisten und die Rückgabe von Ausweisen einschließen.

c. Jede Person, der eine temporäre Zutrittsgenehmigung für ein von IBM verwaltetes Rechenzentrum oder einen kontrollierten Bereich innerhalb eines solchen Rechenzentrums erteilt wurde, wird beim Betreten der Räumlichkeiten registriert, muss bei der Registrierung einen Identitätsnachweis vorlegen und wird von autorisierten Mitarbeitern begleitet. Jede temporäre Zutrittsgenehmigung, auch für Anlieferungen, wird vorab geplant und bedarf der Genehmigung durch autorisierte Mitarbeiter.

[redacted]

d. IBM wird Vorkehrungen zum Schutz der physischen Infrastruktur der von IBM verwalteten Rechenzentrumseinrichtungen vor natürlichen als auch vor von Menschen verursachten Umweltgefahren treffen, wie z. B. extrem hohe Umgebungstemperatur, Feuer, Hochwasser, Feuchtigkeit, Diebstahl und Vandalismus.

8. Zugangs-, Zugriffs-, Weitergabe- und Trennungskontrolle

a. IBM wird eine dokumentierte Sicherheitsarchitektur der Komponenten aufrechterhalten. Dazu wird die Sicherheitsarchitektur, einschließlich der Maßnahmen zur Verhinderung von nicht autorisierten Netzverbindungen zu Systemen, Anwendungen und Netzeinheiten, vor der Implementierung gesondert auf Einhaltung der Standards für sichere Segmentierung, Isolation und tiefengestaffelte Sicherheit überprüft.

b. IBM kann drahtlose Netztechnologie für die Wartung und den Support der IBM Services und der zugehörigen Komponenten einsetzen. Falls drahtlose Netze zum Einsatz kommen, werden diese verschlüsselt und verlangen eine sichere Authentifizierung. Sie ermöglichen keinen direkten Zugriff auf IBM Cloud-Service-Netze. Bei IBM Cloud-Service-Netzen wird keine drahtlose Netztechnologie verwendet.

c. IBM wird Maßnahmen für einen IBM Service durchführen, die dazu ausgelegt sind, Inhalte logisch zu trennen und zu verhindern, dass sie für Unbefugte verfügbar oder zugänglich sind. Die IBM Produktions- und Nicht-Produktionsumgebungen werden in angemessener Weise isoliert, und wenn Inhalte in eine Nicht-Produktionsumgebung übertragen werden, um zum Beispiel auf Anforderung des Kunden einen Fehler zu reproduzieren, entsprechen die Sicherheits- und Datenschutzvorkehrungen denjenigen, die in der Produktion angewendet werden.

d. IBM wird Inhalte, die nicht für die Veröffentlichung oder Einsichtnahme ohne Authentifizierung bestimmt sind, bei der Übertragung über öffentliche Netze verschlüsseln und die Verwendung eines Verschlüsselungsprotokolls, wie z. B. HTTPS, SFTP oder FTPS, ermöglichen, damit die Inhalte vom Kunden sicher in die und aus den IBM Services über öffentliche Netze übertragen werden können.

e. Ruhende Inhalte werden von IBM verschlüsselt, wenn und soweit dies in einem IBM Servicedokument angegeben ist. Ist die Verwaltung von Verschlüsselungsschlüsseln bei einem IBM Service eingeschlossen, wird IBM dokumentierte Verfahren für die sichere Erstellung, Ausgabe, Weitergabe, Speicherung, Rotation, den Widerruf sowie die Wiederherstellung, Sicherung, Löschung, den Zugriff und die Verwendung von Schlüsseln einrichten.

f. Wenn IBM zur Erbringung der IBM Services Zugriff auf Inhalte benötigt und dieser Zugriff von IBM verwaltet wird, wird er von IBM auf das notwendige Mindestmaß beschränkt. Dieser Zugriff sowie der Verwaltungszugriff auf die zugrunde liegenden Komponenten (privilegierter Zugriff) sind individuell, rollenbasiert und unterliegen regelmäßigen Prüfungen durch autorisierte Mitarbeiter gemäß den Richtlinien für die Aufgabentrennung. IBM wird Maßnahmen zur Aufdeckung und Löschung redundanter und inaktiver Konten mit privilegiertem Zugriff ergreifen und bei Ausscheiden oder Wechsel des Kontoeigners oder auf Anforderung von autorisierten IBM Mitarbeitern, wie beispielsweise durch den Vorgesetzten des Kontoeigners, den Zugriff unverzüglich entziehen.

g. Im Einklang mit branchenüblichen Verfahren und insoweit dies von jeder Komponente nativ unterstützt wird, setzt IBM technische Maßnahmen ein, die das Timeout inaktiver Sitzungen, die Sperrung von Konten nach mehreren aufeinanderfolgenden, fehlgeschlagenen Anmeldeversuchen, die Authentifizierung über sichere Kennwörter oder Kennphrasen, Kennwortänderungsintervalle und eine sichere Übertragung und Speicherung dieser Kennwörter und Kennphrasen erzwingen.

h. IBM wird die Verwendung des privilegierten Zugriffs überwachen sowie Sicherheitsinformations- und Ereignismanagementmaßnahmen ergreifen, um (1) unbefugte Zugriffe und Aktivitäten aufzudecken, (2) rechtzeitiges und angemessenes Reagieren zu erleichtern und (3) sowohl interne als auch von unabhängigen Dritten durchgeführte Audits auf Einhaltung der dokumentierten IBM Richtlinie zu ermöglichen.

i. Die Protokolle, in denen privilegierte Zugriffe und Aktivitäten aufgezeichnet werden, werden gemäß dem IBM Worldwide Records Management Plan aufbewahrt. IBM wird Maßnahmen ergreifen, mit denen diese Protokolle vor unbefugtem Zugriff, unbefugter Änderung und zufälliger oder absichtlicher Zerstörung geschützt werden.

j. Soweit Unterstützung durch geräte- und betriebssystemeigene Funktionen gegeben ist, wird IBM Schutzmaßnahmen für IBM Endbenutzersysteme bereitstellen. Dazu gehören unter anderem

[redacted]

Endpunktfirewalls, vollständige Plattenverschlüsselung, signaturbasierte Malware-Erkennung und -Entfernung, zeitbasierte Bildschirmsperren und Endpunktmanagementlösungen, die Sicherheitskonfigurations- und Patching-Anforderungen durchsetzen.

k. Im Einklang mit den NIST-Richtlinien wird IBM sämtliche Daten auf physischen Datenträgern, die zur Wiederverwendung vorgesehen sind, vor einer erneuten Verwendung der Datenträger sicher löschen und physische Datenträger, die nicht zur Wiederverwendung vorgesehen sind, vernichten.

9. Serviceintegrität und Verfügbarkeitskontrolle

a. IBM wird (1) mindestens einmal jährlich Sicherheits- und Datenschutzrisikoabschätzungen für die IBM Services durchführen, (2) vor der Freigabe für die Produktion und danach mindestens jährlich Sicherheitstests und Schwachstellenanalysen der IBM Services durchführen, (3) einen qualifizierten unabhängigen Dritten, IBM X-Force™ oder, sofern in einem IBM Servicedokument angegeben, einen anderen qualifizierten Testservice damit beauftragen, mindestens jährlich Penetrationstests der IBM Cloud-Services durchzuführen, (4) eine automatisierte Schwachstellensuche der zugrunde liegenden Komponenten der IBM Services anhand der bewährten Branchenverfahren für Sicherheitskonfigurationen durchführen, (5) die bei den Sicherheitstests und Suchvorgängen aufgedeckten Schwachstellen abhängig von dem damit verbundenen Risiko, der Exploit-Anfälligkeit und der Auswirkung beheben und (6) angemessene Maßnahmen ergreifen, um eine Unterbrechung der IBM Services bei der Ausführung der Tests, Prüfungen, Schwachstellensuche und Abhilfemaßnahmen zu vermeiden.

b. IBM wird Maßnahmen durchführen, die dazu ausgelegt sind, Security Advisory Patches für die IBM Services und die zugehörigen Systeme, Netze, Anwendungen und zugrunde liegenden Komponenten im Rahmen der IBM Services zu beurteilen, zu testen und einzuspielen. Wenn sich herausstellt, dass ein Security Advisory Patch anwendbar und geeignet ist, wird IBM den Patch gemäß den dokumentierten Richtlinien zur Bewertung der Dringlichkeit und Risiken auf der Grundlage der Patch-Einstufungen nach dem Common Vulnerability Scoring System, sofern verfügbar, einspielen. Das Einspielen von Security Advisory Patches unterliegt der IBM Change-Management-Richtlinie.

c. IBM wird Richtlinien und Verfahren anwenden, die für das Management von Risiken im Zusammenhang mit der Durchführung von Änderungen an IBM Services ausgelegt sind. Änderungen an einem IBM Service, den zugehörigen Systemen, Netzen und zugrunde liegenden Komponenten werden vor der Implementierung in einer registrierten Änderungsanforderung dokumentiert, die eine Beschreibung sowie den Grund für die Änderungen, Einzelheiten der Implementierung und den Terminplan, eine Risikoerklärung hinsichtlich der Auswirkung auf den IBM Service und seine Kunden, das erwartete Ergebnis, einen Rollback-Plan und die dokumentierte Genehmigung durch autorisierte Mitarbeiter enthält.

d. IBM wird ein Inventar aller IT-Assets pflegen, die beim Betrieb von IBM Services verwendet werden. Der Zustand, einschließlich der Kapazität, und die Verfügbarkeit von IBM Services und der zugrunde liegenden Komponenten werden von IBM fortlaufend überwacht und gesteuert.

e. Jeder IBM Service wird separat durch eine Business-Impact-Analyse und Risikobeurteilungen in Bezug auf Business-Continuity- und Disaster-Recovery-Anforderungen hin überprüft, um kritische Geschäftsfunktionen zu ermitteln und zu priorisieren. Sofern aufgrund dieser Risikobeurteilungen gerechtfertigt, werden für jeden IBM Service Business-Continuity- und Disaster-Recovery-Pläne in Übereinstimmung mit branchenüblichen Verfahren separat definiert, dokumentiert, gepflegt und jährlich überprüft. Zielvorgaben hinsichtlich Wiederherstellungspunkt und -zeit (RPO und RTO) für einen IBM Service, sofern im maßgeblichen IBM Servicedokument vorgesehen, werden unter Berücksichtigung der Architektur und der vorgesehenen Nutzung des IBM Service festgelegt. Physische Datenträger, die zur Auslagerung an einen anderen Standort vorgesehen sind, wie z. B. Datenträger, auf denen sich Sicherungsdateien befinden, werden vor dem Transport verschlüsselt.