IBM Cognos Controller on Cloud

Servicebeschreibung für die Bestellung des Kunden:

1. Cloud-Service

Im Folgenden wird das Cloud-Service-Angebot beschrieben, das im Auftragsdokument des Kunden näher spezifiziert wird. Das Auftragsdokument besteht aus dem vorgelegten Angebot und dem Berechtigungsnachweis (Proof of Entitlement = PoE), mit dem IBM das Startdatum und die Laufzeit der Cloud-Services bestätigt. Die Rechnungsstellung beginnt nach der Bereitstellung des Cloud-Service.

1.1 IBM Cognos Controller User on Cloud

IBM Cognos Controller ist eine Finanzkonsolidierungssoftware, die den kompletten Abschluss-, Konsolidierungs- und Berichtsprozess unterstützt. Das Angebot ermöglicht die Bereitstellung von Finanzergebnissen, die Erstellung von Finanz- und Managementberichten und eine unternehmensweite Sicht auf wichtige finanzwirtschaftliche Kennzahlen und Messgrößen.

IBM Cognos Controller User on Cloud kann für Konsolidierungen, Berichterstellung und die Systemverwaltung eingesetzt werden.

1.2 IBM Cognos Controller Jump Start on Cloud

Der Remote Service IBM Cognos Controller Jump Start on Cloud schließt bis zu 80 Stunden an Coaching und Unterstützung ein, insbesondere einfachere Identifizierung eines ersten CCoC-Anwendungsfalls (CCoC = IBM Cognos Controller on Cloud), Coaching bei der Projektplanung und der Initiierung der IBM CCoC-Implementierung, Coaching bei bewährten Verfahren zur Erstellung von IBM CCoC-Berichten sowie Coaching bei der Wartung und Verwaltung von IBM CCoC. Die Services werden pro Kundenprojekt erworben und enden 90 Tage nach dem Erwerb, unabhängig davon, ob das Stundenkontingent ausgeschöpft wurde.

1.3 IBM Cognos Controller Additional Non-Production Instance

Mit diesem Angebot können weitere Nicht-Produktionsinstanzen für IBM Cognos Controller hinzugefügt werden. Das Angebot kann nur im Rahmen nicht produktionsbezogener Aktivitäten eingesetzt werden, einschließlich, aber nicht abschließend zum Testen, zur Leistungsoptimierung, zur Fehlerdiagnose, zum Benchmarking, zur Bereitstellung, zur Qualitätssicherung und/oder zur Entwicklung intern verwendeter Zusätze oder Erweiterungen des Angebots unter Verwendung veröffentlichter Anwendungsprogrammierschnittstellen.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM verfügt über ein Team für Informationssicherheit und hat außerdem Datenschutz- und Sicherheitsrichtlinien festgelegt, die an die IBM Mitarbeiter kommuniziert werden. Mitarbeiter, die in IBM Rechenzentren Support leisten, sind verpflichtet, an Schulungen zu Datenschutz und Sicherheit teilzunehmen. Die IBM Sicherheitsrichtlinien und -standards werden jährlich überprüft und neu bewertet. Bei IBM internen Sicherheitsverstößen wird ein umfassendes Verfahren zur Behebung von Sicherheitsvorfällen in Gang gesetzt.

2.2 Zugriffskontrolle

Der Zugriff auf Kundendaten, sofern erforderlich, ist nur autorisierten IBM Supportmitarbeitern nach dem Grundsatz der Aufgabentrennung gestattet. Die IBM Mitarbeiter verwenden Zwei-Faktor-Authentifizierung für einen zwischengeschalteten „Gateway“-Management-Host. Beim Zugriff auf Kundendaten laufen alle Verbindungen über verschlüsselte Kanäle. Sämtliche Zugriffe auf Kundendaten und alle Datenübertragungen in die oder aus der Hosting-Umgebung werden protokolliert. In den IBM Rechenzentren, die diesen Cloud-Service unterstützen, ist der Einsatz von Wifi untersagt.

2.3 Service-Integrität und Verfügbarkeit

Änderungen an Betriebssystemen und Anwendungssoftware werden gemäß dem Change-Management-Prozess von IBM durchgeführt. Änderungen an Firewallregeln unterliegen ebenfalls dem Change-Management-Prozess und werden vor der Implementierung vom IBM Sicherheitsteam geprüft. Das Rechenzentrum wird von IBM rund um die Uhr (24x7) überwacht. Autorisierte Administratoren und

externe Anbieter führen regelmäßig Scans zur Ermittlung interner und externer Schwachstellen durch, um potenzielle Systemsicherheitsrisiken aufzudecken und zu beheben. In allen IBM Rechenzentren sind Malware-Erkennungssysteme (Virenschutz, Erkennung unbefugter Zugriffe, Schwachstellensuche und Abwehr unbefugter Zugriffe) installiert. Die Services der IBM Rechenzentren unterstützen eine Vielzahl von Protokollen für die Übertragung von Daten über öffentliche Netze. Beispiele dafür sind HTTPS/SFTP/FTPS/S/MIME und Site-to-Site-VPN. Sicherungsdaten, die zur Auslagerung an einen anderen Standort vorgesehen sind, werden vor dem Transport verschlüsselt.

2.4 Aktivitätsprotokollierung

IBM protokolliert alle Aktivitäten für Systeme, Anwendungen, Datenrepositorys, Middleware und Netzinfrastrukturgeräte, die sich zur Protokollierung eignen und entsprechend konfiguriert sind. Um Manipulationsmöglichkeiten zu minimieren sowie zentrale Analyse, Alerting und Berichterstellung zu ermöglichen, wird die Aktivitätsprotokollierung in Echtzeit durchgeführt und die Protokolle werden in zentralen Protokollrepositorys abgelegt. Zur Vermeidung von Manipulationen werden die Daten signiert. Die Protokolle werden in Echtzeit und mithilfe periodischer Analyseberichte analysiert, um Unregelmäßigkeiten aufzudecken. Die Systembediener werden bei Unregelmäßigkeiten benachrichtigt und wenden sich bei Bedarf an einen rund um die Uhr im Einsatz befindlichen Sicherheitsspezialisten.

2.5 Physische Sicherheit

Die IBM Standards für physische Sicherheit sind dazu ausgelegt, den unbefugten Zutritt zu IBM Rechenzentren zu verhindern. Die Rechenzentren verfügen nur über eine begrenzte Anzahl von Eingängen, die durch Zwei-Faktor-Authentifizierung kontrolliert und mit Kameras überwacht werden. Der Zutritt ist nur autorisierten Mitarbeitern gestattet, die über eine Zutrittsgenehmigung verfügen. Das Sicherheitspersonal überprüft die Zutrittsgenehmigungen und stellt Ausweise aus, die den Zutritt ermöglichen. Mitarbeiter, für die Ausweise ausgestellt werden, müssen alle anderen Zutrittsausweise abgeben und dürfen für die Dauer ihrer Tätigkeit nur im Besitz des Ausweises für den Zutritt zum Rechenzentrum sein. Die Nutzung der Ausweise wird protokolliert. Externe Besucher werden beim Betreten der Rechenzentren registriert und während ihres Aufenthalts dort begleitet. Anlieferungsbereiche und Ladedocks sowie andere Eingänge, über die unbefugte Personen in die Rechenzentren gelangen können, werden kontrolliert und isoliert.

2.6 Compliance

IBM zertifiziert jährlich ihre Datenschutzverfahren auf Übereinstimmung mit den Safe-Harbor-Grundsätzen des United States Department of Commerce in Bezug auf Benachrichtigung, Wahlmöglichkeit, Weitergabe (Übermittlung an Dritte), Zugriff und Richtigkeit, Sicherheit, Durchsetzung und Überwachung. In den IBM Produktionsrechenzentren werden jährlich Prüfungen nach dem Branchenstandard SSAE 16 oder einem vergleichbaren Standard durchgeführt. IBM überprüft die IBM Geschäftstätigkeit auf Einhaltung aller sicherheits- und datenschutzrelevanten Anforderungen. Von IBM werden regelmäßig Prüfungen und Audits durchgeführt, um die Einhaltung der IBM Richtlinien zur Informationssicherheit zu gewährleisten. Sowohl die IBM Mitarbeiter als auch die externen Mitarbeiter nehmen einmal pro Jahr an Sicherheitsschulungen und Sensibilisierungstrainings teil. Die Mitarbeiter werden jährlich an ihre Zielvorgaben erinnert und auf ihre Verantwortung zur Einhaltung der Unternehmensethik, der Vertraulichkeit und der IBM Sicherheitsverpflichtungen hingewiesen.

3. Vereinbarte Service-Levels

IBM stellt das folgende Service-Level-Agreement („SLA“) für den Cloud-Service zur Verfügung. Der Kunde nimmt zur Kenntnis, dass das SLA keine Gewährleistung darstellt.

3.1 Begriffsbestimmungen

a. „Berechtigte Kontaktperson“ ist diejenige Person, die der Kunde IBM als Kontaktperson genannt hat und die zur Einreichung von Ansprüchen im Rahmen dieses SLA autorisiert ist.

b. „Gutschrift für Ausfallzeiten“ ist der Schadensersatz, den IBM für einen bestätigten Anspruch leistet. Die Gutschrift für Ausfallzeiten wird in Form einer Gutschrift oder eines Nachlasses gewährt und mit einer zukünftigen Rechnung über Subscription-Gebühren für den Cloud-Service verrechnet.

c. „Anspruch“ ist ein vom Kunden gemäß dem SLA bei IBM eingereichter Anspruch, der besagt, dass ein Service-Level während eines Vertragsmonats nicht erfüllt wurde.

d. „Kunde“ ist eine juristische Person, die den Service direkt von IBM bezieht und keine wesentlichen Verpflichtungen, einschließlich Zahlungsverpflichtungen, aus ihrem Vertrag mit IBM für den Service verletzt hat.

e. „Vertragsmonat“ ist jeder volle Monat während der Laufzeit, der um 00:00 Uhr MEZ am ersten Kalendertag des Monats beginnt und um 23:59 MEZ am letzten Kalendertag des Monats endet.

f. „Ausfallzeit“ ist ein Zeitraum, in dem die Verarbeitung auf dem Produktionssystem für den Cloud-Service gestoppt ist und die Benutzer des Kunden nicht in der Lage sind, alle Aspekte des Cloud-Service zu nutzen, für die sie berechtigt sind. Ausfallzeiten umfassen nicht den Zeitraum, in dem der Cloud-Service aus einem der folgenden Gründe nicht verfügbar ist:

   (1) Vorab geplante oder angekündigte Unterbrechungen zur Durchführung von Wartungsarbeiten

   (2) Ereignisse oder Gründe, die IBM nicht zu vertreten hat (z. B. Naturkatastrophen, Internetausfälle, Notfallwartung usw.)

   (3) Probleme mit Anwendungen, Geräten oder Daten des Kunden oder Dritter

   (4) Nichtbeachtung erforderlicher Systemkonfigurationen und unterstützter Plattformen für den Zugriff auf den Cloud-Service

   (5) Unterbrechungen, die dadurch verursacht werden, dass IBM Entwürfe, Spezifikationen oder Anweisungen des Kunden oder eines in seinem Auftrag handelnden Dritten zu beachten hat

g. „Vorfall“ ist ein Umstand oder eine Reihe von Umständen, die zur Nichteinhaltung eines Service-Levels geführt haben.

h. „Service-Level“ ist der nachstehend erläuterte Standard, nach dem IBM den Level des Service misst, den sie in diesem SLA bereitstellt.

3.2 Gutschriften für Ausfallzeiten

a. Damit der Kunde einen Anspruch geltend machen kann, muss er für jeden Vorfall innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass der Vorfall die Nutzung des Cloud-Service beeinträchtigt, ein Support-Ticket der Fehlerklasse 1 (wie nachstehend im Abschnitt „Technische Unterstützung“ definiert) beim IBM Help-Desk für technische Unterstützung öffnen. Der Kunde muss alle erforderlichen Informationen zu dem Vorfall zur Verfügung stellen und IBM bei der Diagnose des Vorfalls und der Problemlösung angemessen unterstützen.

b. Der Anspruch auf eine Gutschrift für Ausfallzeiten muss spätestens drei (3) Arbeitstage nach Ablauf des Vertragsmonats geltend gemacht werden, in dem der Anspruch entstanden ist.

c. Die Gutschriften für Ausfallzeiten richten sich nach der Dauer der Ausfallzeit, die ab dem Zeitpunkt gemessen wird, zu dem der Kunde zum ersten Mal eine Beeinträchtigung bedingt durch die Ausfallzeit gemeldet hat. Für jeden berechtigten Anspruch wird IBM die höchstmögliche Gutschrift für Ausfallzeiten basierend auf dem während jedes einzelnen Vertragsmonats erreichten Service-Levels anwenden (siehe die nachstehende Tabelle). IBM gewährt keine Mehrfachgutschriften für Ausfallzeiten für den gleichen Vorfall in ein und demselben Vertragsmonat.

d. Die Gesamtsumme der Gutschriften für Ausfallzeiten, die für einen beliebigen Vertragsmonat gewährt wird, wird unter keinen Umständen 10 Prozent (10 %) von einem Zwölftel (1/12) der Jahresgebühr überschreiten, die der Kunde IBM für den Cloud-Service bezahlt hat.

3.3 Service-Levels

Verfügbarkeit des Cloud-Service in einem Vertragsmonat

Verfügbarkeit in einem Vertragsmonat	**Gutschrift für Ausfallzeiten (in Prozent (%) der monatlichen Subscription-Gebühr für den Vertragsmonat, der Gegenstand des Anspruchs ist)**
99 % – 99,75 %	2 %
95 % – 98,99 %	5 %
Unter 95,0 %	10 %

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: (a) Gesamtzahl der Minuten in einem Vertragsmonat, minus (b) der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch (c) die Gesamtzahl der Minuten in einem Vertragsmonat.

Beispiel: 476 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 476 Minuten Ausfallzeit = 42.724 Minuten _____ 43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen	= Gutschrift für Ausfallzeiten in Höhe von 5 % bei einer Verfügbarkeit von 98,9 % in einem Vertragsmonat

3.4 Weitere Informationen zu diesem SLA

Dieses SLA wird nur IBM Kunden zur Verfügung gestellt und gilt nicht für Ansprüche, die von Benutzern, Gästen, Teilnehmern und eingeladenen Personen des Kunden, die den Cloud-Service nutzen, oder in Bezug auf von IBM bereitgestellte Beta- oder Testservices eingereicht werden. Das SLA bezieht sich nur auf die Cloud-Services im Produktionseinsatz und nicht auf Nicht-Produktionsumgebungen, einschließlich, aber nicht beschränkt auf Tests, Disaster-Recovery, Qualitätssicherung oder Entwicklung.

4. Informationen zu Berechtigungen und Abrechnung

4.1 Gebührenmetriken

Der Cloud-Service wird unter einer der folgenden Gebührenmetriken entsprechend der Angabe im Auftragsdokument zur Verfügung gestellt:

a. „Instanz“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Instanz ermöglicht den Zugriff auf eine bestimmte Konfiguration des Cloud-Service. Der Kunde muss ausreichende Berechtigungen für alle Instanzen des Cloud-Service erwerben, die während des Abrechnungszeitraums, der im Auftragsdokument angegeben ist, zum Zugriff und zur Nutzung bereitgestellt werden.

b. „Berechtigter Benutzer“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein berechtigter Benutzer ist eine bestimmte Person, der Zugriff auf den Cloud-Service erteilt wird. Der Kunde muss für jeden berechtigten Benutzer, der auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) während des im Auftragsdokument angegebenen Abrechnungszeitraums auf das Cloud-Service-Angebot zugreift, eine separate, dedizierte Berechtigung erwerben. Eine Berechtigung für einen berechtigten Benutzer ist diesem eindeutig zugeordnet und darf weder gemeinsam genutzt noch neu zugeordnet werden, außer zur permanenten Übertragung der Berechtigung für einen berechtigten Benutzer auf eine andere Person. Der Kunde kann Benutzern außerhalb seines Unternehmens Zugriff auf den Cloud-Service erteilen. Diese Benutzer gelten als berechtigte Benutzer und müssen über entsprechende Berechtigungen verfügen.

c. „Kundenprojekt“ (Engagement) ist eine Maßeinheit für den Erwerb der Services. Ein Kundenprojekt besteht aus Professional Services und/oder Schulungsservices im Zusammenhang mit dem Cloud-Service. Der Kunde muss ausreichende Berechtigungen zur Abdeckung aller Kundenprojekte erwerben.

4.2 Gebühren und Abrechnung

Der für den Cloud-Service zu zahlende Betrag ist im Auftragsdokument angegeben.

4.3 Einrichtungsgebühren

Anfallende Einrichtungsgebühren (Setup-Gebühren) sind im Auftragsdokument angegeben.

4.4 Anteilige Monatsgebühren

Die anteilige Monatsgebühr ist eine auf Basis des Tagessatzes ermittelte anteilige Gebühr. Die anteiligen Monatsgebühren werden, basierend auf der Anzahl der restlichen Tage in dem betreffenden Monat, ab dem Datum berechnet, an dem der Kunde von IBM darüber benachrichtigt wird, dass sein Zugriff auf das Cloud-Service-Angebot freigeschaltet ist.

4.5 On-Demand-Gebühren

Im Auftragsdokument aufgeführte On-Demand-Optionen werden erst in Rechnung gestellt, wenn der Kunde die Aktivierung der On-Demand-Optionen anfordert. Nach der Aktivierung wird der im Auftragsdokument festgelegte Gebührensatz berechnet.

5. Laufzeit und Verlängerungsoptionen

5.1 Laufzeit

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf den Cloud-Service gemäß der Beschreibung im Auftragsdokument freigeschaltet ist. Das genaue Start- und Enddatum der Laufzeit ist im PoE-Teil des Auftragsdokuments angegeben. Der Nutzungsumfang des Cloud-Service kann während der Laufzeit durch eine entsprechende Mitteilung an IBM oder den zuständigen IBM Business Partner erhöht werden. Die Erhöhung des Nutzungsumfangs wird von IBM in einem Auftragsdokument bestätigt.

5.2 Verlängerungsoptionen für die Laufzeit der Cloud-Services

Im Auftragsdokument des Kunden ist durch folgende Optionen geregelt, ob sich der Cloud-Service am Ende der Laufzeit verlängert:

5.2.1 Automatische Verlängerung

Ist im Auftragsdokument des Kunden angegeben, dass sich die Laufzeit automatisch verlängert, kann der ablaufende Cloud-Service durch schriftliche Mitteilung mit einer Frist von mindestens neunzig (90) Tagen vor dem im Auftragsdokument genannten Ablaufdatum gekündigt werden. Wenn IBM oder der zuständige IBM Business Partner kein solches Kündigungsschreiben vor dem Ablaufdatum erhält, wird die ablaufende Laufzeit automatisch entweder um ein (1) Jahr oder um die im Berechtigungsnachweis genannte ursprüngliche Laufzeit verlängert.

5.2.2 Fortlaufende Abrechnung

Wird gemäß dem Auftragsdokument des Kunden eine fortlaufende Abrechnung erstellt, bedeutet dies, dass der Kunde auch nach Ablauf der Laufzeit kontinuierlichen Zugriff auf den Cloud-Service hat und der Cloud-Service fortlaufend in Rechnung gestellt wird. Um die Nutzung des Cloud-Service und den fortlaufenden Abrechnungsprozess zu beenden, muss der Kunde in einer schriftlichen Mitteilung an IBM oder den zuständigen IBM Business Partner unter Einhaltung einer Frist von neunzig (90) Tagen die Einstellung des Cloud-Service beantragen. Bei Einstellung des Zugriffs werden dem Kunden evtl. ausstehende Zugriffsgebühren für den Monat berechnet, in dem die Beendigung wirksam wurde.

5.2.3 Verlängerung erforderlich

Ist im Auftragsdokument eine befristete Laufzeit angegeben, wird der Cloud-Service zum Laufzeitende abgeschaltet und der Zugriff des Kunden auf den Cloud-Service entfernt. Um den Cloud-Service über das Enddatum hinaus nutzen zu können, muss der Kunde eine neue Subscription-Laufzeit erwerben, indem er beim zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner eine entsprechende Bestellung aufgibt.

6. Technische Unterstützung

Während der Subscription-Laufzeit wird technische Unterstützung für den Cloud-Service erbracht.

Reguläre Unterstützungszeiten per Telefon und E-Mail sind:

Support-Ticket oder E-Mail: Jederzeit, die Tickets werden entsprechend den zugeordneten Fehlerklassen verarbeitet. Die Fehlerklassen 2 bis 4 werden während der regulären Geschäftszeiten bearbeitet.

Telefon: Montag bis Freitag von 9:00 Uhr bis 17:00 Uhr Ortszeit (von IBM eingehaltene gesetzliche Feiertage ausgenommen)

Unterstützung außerhalb der regulären Geschäftszeiten:

Unterstützung an Arbeitstagen, Wochenenden und Feiertagen außerhalb der regulären Geschäftszeiten (siehe oben) ist nur für Probleme der Fehlerklasse 1 verfügbar.

Support-Hotline: 1-877-465-5444

E-Mail: vsupport@ca.ibm.com

Zum Einstellen eines Tickets per E-Mail muss die vorläufige Varicent/IBM Adresse verwendet werden.

Support-Webportal: http://support.varicent.com

Der Technical Support Guide ist unter dem folgenden Link verfügbar: http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html.

Fehlerklasse	Definition der Fehlerklasse	Angestrebte Reaktionszeiten	Deckungszeiten
1	**Kritische Auswirkung auf den Geschäftsbetrieb/Serviceausfall:** Geschäftskritische Funktionen sind nicht funktionsfähig oder eine kritische Schnittstelle ist ausgefallen. Dies betrifft normalerweise eine Produktionsumgebung und weist darauf hin, dass der Zugriff auf die Services nicht möglich ist, mit kritischen Auswirkungen auf betriebliche Abläufe. In diesem Fall ist eine sofortige Lösung erforderlich.	Innerhalb von 1 Stunde	24x7
2	**Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines geschäftsrelevanten Service-Features oder einer Servicefunktion ist stark eingeschränkt, oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann.	Innerhalb von 2 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
3	**Geringe Auswirkung auf den Geschäftsbetrieb:** Der Service oder die Funktionalität kann genutzt werden und das Problem hat keine kritische Auswirkung auf betriebliche Abläufe.	Innerhalb von 4 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
4	**Minimale Auswirkung auf den Geschäftsbetrieb:** Eine Anfrage oder eine Frage nicht technischer Art.	Innerhalb 1 Arbeitstages	Mo-Fr zu den Geschäftszeiten

7. Einhaltung des Safe-Harbor-Abkommens

IBM hat nicht geprüft, ob durch diesen Cloud-Service die Einhaltung des Safe-Harbor-Abkommens zwischen den USA und der EU bzw. den USA und der Schweiz gewährleistet ist.

8. Zusätzliche Informationen

8.1 Bevorzugte Standorte

Soweit möglich, orientieren sich die Steuern an dem Standort/den Standorten, für den/die die Cloud-Services erbracht werden. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung des Cloud-Service als primärer Standort angegeben wird, es sei denn, der Kunde stellt IBM zusätzliche Informationen bereit. Der Kunde ist dafür verantwortlich, diese Informationen auf dem aktuellen Stand zu halten und IBM über Änderungen zu informieren.

8.2 Keine persönlichen Gesundheitsdaten

Der Cloud-Service ist nicht für die Einhaltung des von den USA erlassenen Health Insurance Portability and Accountability Act („HIPAA“) ausgelegt und darf nicht für die Übermittlung oder Speicherung persönlicher Gesundheitsdaten verwendet werden.

8.3 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für den Cloud-Service über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der Nutzung des Cloud-Service im Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität des Cloud-Service erfassen, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder die Interaktionen mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholen wird oder eingeholt hat, damit IBM die erhobenen personenbezogenen Daten für die vorstehenden Zwecke innerhalb von IBM, durch andere IBM Unternehmen und deren Unterauftragnehmer in allen Ländern, in denen wir und unsere Unterauftragnehmer geschäftlich tätig sind, in Übereinstimmung mit der geltenden Gesetzgebung verarbeiten darf. IBM wird den Anforderungen der Mitarbeiter und Auftragnehmer des Kunden nachkommen, die sich auf den Zugriff, die Aktualisierung, die Korrektur oder die Löschung ihrer personenbezogenen Daten beziehen.

8.4 Disaster-Recovery und Sicherung der Inhalte

Dieser Cloud-Service enthält ferner Disaster-Recovery- und Sicherungsservices für Inhalte:

Im Fall von Katastrophen, die als „Höhere Gewalt“ definiert sind und zu denen unabwendbare Ereignisse, Terrorismus, Streiks, Brände, Überflutungen, Erdbeben, Unruhen, Kriege, staatliche Maßnahmen, Anordnungen und Beschränkungen, Viren, Denial-of-Service-Attacken sowie arglistiges Verhalten, Strom- und Netzausfälle oder sonstige Ursachen für die Nichtverfügbarkeit des Cloud-Service gehören, die außerhalb des angemessenen Einflussbereichs von IBM liegen, wird IBM daran arbeiten, den Zugriff des Kunden auf den Cloud-Service wie folgt wiederherzustellen:

a. Standard Option – IBM stellt die Hardware, die Software und die Netzinfrastruktur im Netz des IBM Rechenzentrums bereit, die dem Kunden die Wiederaufnahme des Cloud-Service innerhalb von 14 Tagen ermöglichen.

b. Premium Option – IBM stellt die Hardware, die Software und die Netzinfrastruktur im Netz des IBM Rechenzentrums bereit, die dem Kunden die Wiederaufnahme des Cloud Service innerhalb von 5 Tagen ermöglichen.

Die Umgebung wird unter Verwendung der zuletzt erstellten Sicherung des Inhalts, wie nachfolgend beschrieben, wiederhergestellt, wobei der Datenverlust bei der Wiederherstellung maximal 24 Stunden beträgt.

Es werden täglich Sicherungen durchgeführt und an einen anderen Standort kopiert, für den Fall, dass am primären Standort ein Ereignis höherer Gewalt eintritt. IBM bewahrt Sicherungen auf rollierender Basis auf: Alle sieben (7) Tage wird eine Datenbankgesamtsicherung und an jedem Folgetag innerhalb der Woche wird eine Differenzsicherung durchgeführt. Die täglichen Differenzsicherungen der letzten sieben (7) Tage und die vier (4) vorherigen Gesamtsicherungen (die einen Zeitraum von 28 Tagen abdecken) werden von IBM aufbewahrt. Nachdem eine neue Gesamtsicherung erstellt wurde, wird die älteste Version gelöscht. Die Sicherungen werden zur Speicherung auf einem plattenbasierten Sicherungssystem und während der Übertragung an den externen Standort verschlüsselt.