

Beschreibung des IBM Cloud-Service

IBM OpenPages GRC 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 speziellen Angebot und dem Berechtigungsnachweis (Proof of Entitlement = PoE), mit dem IBM das Startdatum sowie die Laufzeit der Cloud-Services und den Beginn der Abrechnung bestätigt.

1.1 IBM OpenPages GRC on Cloud

IBM OpenPages GRC on Cloud (eine erforderliche Komponente) bietet eine Standardkonfiguration für Operational Risk Management und ermöglicht die unternehmensweite Identifizierung, Verwaltung und Überwachung von Risikomanagement- und Compliance-Initiativen sowie die Erstellung entsprechender Berichte. Mit dieser Lösung können alle Risikodaten, einschließlich Risk and Control Self Assessments (RCSA), Schadensereignissen, Szenarioanalysen, externer Verluste und Key Risk Indicators (KRIs), in einem einzigen integrierten Modul zusammengefasst werden.

Leistungsspektrum von Operational Risk Management:

- Hauptmerkmale:
 - (1) Ermöglicht die Identifizierung, Messung und Minderung von Risiken
 - (2) Ermöglicht das Testen und Dokumentieren interner Kontrollmechanismen
- Schadensereignisse, die folgende Maßnahmen ermöglichen:
 - (1) Verfolgung, Beurteilung und Management sowohl interner als auch externer Vorfälle, die operative Verluste zur Folge haben können
 - (2) Management mehrerer Auswirkungseignisse und Abhilfemaßnahmen im Falle von operativen Verlusten
- Bei externen Schadensereignissen können Verlustdaten aus den Verlustdatenbanken von IBM Algo FIRST, Operational Risk data eXchange Association (ORX) und Operational Risk Consortium (ORIC) (separate Subscription erforderlich) für Szenarioanalysen, zu Benchmarking-Zwecken und zur Berichterstellung in IBM OpenPages Operational Risk Management importiert werden. Es können auch Verlustdaten in Analysetools oder Kapitalallokationsanwendungen exportiert werden.
- KRIs, die zur Überwachung von Leistungsmetriken verwendet werden können, um das potenzielle Vorhandensein oder den Status einer Risikobedingung oder eines Trends aufzuzeigen.
- Szenarioanalysen, bei denen es sich um ein Beurteilungsverfahren handelt, das zum Erkennen und Messen bestimmter Risikoarten eingesetzt werden kann, insbesondere für Ereignisse mit geringer Eintrittshäufigkeit, aber hoher Dringlichkeit.
- Berichterstellung, Überwachung und Analyse.
- IBM SoftLayer-Cloudimplementierung.

1.2 IBM OpenPages GRC Non-Production Instance on Cloud

IBM OpenPages GRC Non-Production Instance on Cloud stellt eine Instanz des Cloud-Service für die nicht produktive Nutzung für interne Entwicklungs- und Testaktivitäten zur Verfügung.

1.3 IBM OpenPages GRC Data Storage on Cloud

IBM OpenPages GRC Data Storage on Cloud (eine erforderliche Komponente) stellt den Speicher für die GRC-Daten der Kundeninstanz des Cloud-Service zur Verfügung. Der Speicher wird in Zuteilungen von 150 Gigabyte verkauft.

1.4 IBM OpenPages GRC Administrator User on Cloud

IBM OpenPages GRC Administrator User on Cloud-Benutzer (mindestens einer ist erforderlich) haben Zugriff auf alle Verwaltungsfunktionen sowie auf die Operational-Risk-Management-Funktionen des Cloud-Service.

1.5 IBM OpenPages Operational Risk Management User on Cloud

IBM OpenPages Operational Risk Management User on Cloud-Benutzer dürfen nur mit den vorstehend beschriebenen Operational-Risk-Management-Funktionen interagieren.

1.6 IBM OpenPages GRC Operational Risk Management Jump Start on Cloud

IBM OpenPages GRC Operational Risk Management Jump Start on Cloud (eine erforderliche Komponente) stellt die Services für die Erstimplementierung des Cloud-Service bereit und schließt ein erstes Coaching sowie Unterstützung bei der Projektplanung, Wartung, Verwaltung und Prüfung praxistauglicher Prozesse ein.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM verfügt über Datenschutz- und Sicherheitsrichtlinien, die an die IBM Mitarbeiter weitergegeben werden. IBM verlangt, dass Mitarbeiter, die in IBM Rechenzentren Support leisten, an Schulungen zu Datenschutz- und Sicherheitsmaßnahmen teilnehmen. IBM verfügt über ein Team, das sich mit Fragen der Informationssicherheit beschäftigt. 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 Support-Mitarbeitern 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

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 regelmäßige 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. „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.
- b. „Anspruch“ ist ein vom Kunden gemäß dem SLA bei IBM eingereicherter Anspruch, der besagt, dass ein Service-Level während eines Vertragsmonats nicht erfüllt wurde.
- c. „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.
- d. „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
- e. „Vorfall“ ist ein Umstand oder eine Reihe von Umständen, die zur Nichteinhaltung eines Service-Levels geführt haben.
- f. „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 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)
< 98 %	2 %
< 97 %	5 %
< 93 %	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: 900 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 900 Minuten Ausfallzeit = 42.300 Minuten <hr style="width: 50%; margin: 10px auto;"/> 43.200 Minuten insgesamt	= Gutschrift für Ausfallzeiten in Höhe von 2 % bei einem erreichten Service-Level von 97,9 %
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

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 geltend gemacht 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

Die Cloud-Services werden unter der folgenden Gebührenmetrik entsprechend der Angabe im Auftragsdokument zur Verfügung gestellt:

- a. „Berechtigter Benutzer“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Der Kunde muss für jeden einzelnen berechtigten Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) Zugriff auf den Cloud-Service erteilt wird, eine separate, dedizierte Berechtigung erwerben. Es müssen ausreichende Berechtigungen erworben werden, um die Anzahl der berechtigten Benutzer abzudecken, denen während des im Auftragsdokument angegebenen Abrechnungszeitraums Zugriff auf den Cloud-Service erteilt wird.
- b. „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.

- c. „Gigabyte“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Gigabyte entspricht $2 \text{ hoch } 30$ Byte (1.073.741.824 Byte). Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Gigabytes abzudecken, die vom Cloud-Service während des im Auftragsdokument angegebenen Abrechnungszeitraums verwaltet oder verarbeitet werden.
- d. „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 im Auftragsdokument angegebenen Abrechnungszeitraums zum Zugriff und zur Nutzung bereitgestellt werden.

4.2 Gebühren und Abrechnung

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

4.3 Einrichtungsgebühren

Standardeinrichtungsservices (einschließlich der anfallenden Gebühren) werden über das Angebot IBM OpenPages Operational Risk Management Jump Start on Cloud bereitgestellt.

Falls zusätzliche Konfigurationen oder Services erforderlich sind, muss der Kunde diese IBM OpenPages GRC on Cloud-Services über eine ergänzende Leistungsbeschreibung beauftragen.

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 Zusatzgebühren

Wenn die tatsächliche Nutzung des Cloud-Service während des Abrechnungszeitraums die im PoE-Teil des Auftragsdokuments angegebene Berechtigung überschreitet, wird dem Kunden die Nutzungsüberschreitung gemäß dem Auftragsdokument in Rechnung gestellt.

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 Kunde hat die Möglichkeit, den Nutzungsumfang des Cloud-Service während der Laufzeit durch eine entsprechende Mitteilung an IBM oder den zuständigen IBM Business Partner zu erhöhen. Die Erhöhung des Nutzungsumfangs wird von IBM in das Auftragsdokument aufgenommen.

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 gekündigt werden, indem der Kunde IBM durch schriftliche Mitteilung mindestens neunzig (90) Tage vor dem im Auftragsdokument genannten Ablaufdatum davon in Kenntnis setzt. 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 Laufzeit des Cloud-Service wird technische Unterstützung für den Cloud-Service gemäß den Angaben unter http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf oder einer von IBM zu einem späteren Zeitpunkt bekannt gegebenen URL erbracht. Die technische Unterstützung ist Bestandteil des Cloud-Service und nicht als separates Angebot erhältlich.

7. Einhaltung des Safe-Harbor-Abkommens

IBM hat nicht geprüft, ob durch den 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 Datenerfassung

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 statistische Daten und Informationen über die Effektivität des Cloud-Service erfassen, um die Attraktivität für den Benutzer zu verbessern bzw. die Interaktionen mit dem Kunden optimal an die jeweiligen Bedürfnisse anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholt 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 sie 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.

8.2 Bevorzugte Standorte

Soweit möglich, basieren die Steuern auf dem Standort, den der Kunde als bevorzugten Standort für die Cloud-Services angibt. 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.

8.3 Beschränkung auf nicht produktive Nutzung (Non-Production)

Wenn der Cloud-Service als "Non-Production" gekennzeichnet ist, darf er nur für interne nicht produktionsbezogene Aktivitäten eingesetzt werden, einschließlich aber nicht abschließend zum Testen, zur Leistungsoptimierung, zur Fehlerdiagnose, für internes Benchmarking, für Staging-Zwecke, zur Qualitätssicherung und/oder zur Entwicklung intern verwendbarer Zusätze oder Erweiterungen für den Cloud-Service über veröffentlichte Anwendungsprogrammierschnittstellen. Der Kunde ist nicht berechtigt, Bestandteile des Cloud-Service für andere Zwecke zu nutzen, ohne entsprechende Produktionsberechtigungen zu erwerben.

8.4 Keine Compliance-Garantie

Der Cloud-Service kann verwendet werden, um den Kunden bei der Einhaltung seiner Compliance-Verpflichtungen zu unterstützen, die auf Gesetzen, Verordnungen, Normen oder Verfahren beruhen können. Sämtliche Anweisungen, empfohlenen Vorgehensweisen oder Anleitungen, die vom Cloud-Service bereitgestellt werden, stellen keine rechtliche, betriebswirtschaftliche oder anderweitige fachliche Beratung dar und dem Kunden wird dringend geraten, sich von juristisch oder fachlich kompetenter Stelle beraten zu lassen. Der Kunde ist allein dafür verantwortlich, sicherzustellen, dass von ihm selbst und durch die von ihm ausgeübten Aktivitäten alle anwendbaren Gesetze, Verordnungen, Normen und Verfahren eingehalten werden. Durch die Verwendung des Cloud-Service ist die Einhaltung von Gesetzen, Verordnungen, Normen oder Verfahren nicht garantiert.

Der Kunde bestätigt weiterhin, dass es sich bei dem Cloud-Service um ein Tool zur Unterstützung des Kunden handelt und dass der Cloud-Service keinen Ersatz für das Know-how, das Urteilsvermögen und die Erfahrung des Managements und der Mitarbeiter des Kunden bei der Beratung Dritter oder bei Investitionsentscheidungen oder anderen Unternehmens- und Risikomanagemententscheidungen darstellt. Für die Ergebnisse aus der Nutzung des Cloud-Service ist der Kunde selbst verantwortlich.

8.5 Links zu Websites oder anderen Services Dritter

Überträgt der Kunde oder ein Cloud-Service-Benutzer Inhalt an die Website eines Dritten oder an einen anderen Service, der mit dem Cloud-Service verlinkt oder über den Cloud-Service zugänglich ist, oder erfolgt eine Übertragung von einer solchen Website oder aus einem solchen Service, erteilen der Kunde und der Benutzer des Cloud-Service IBM die Zustimmung zur Übertragung des Inhalts, wobei eine derartige Interaktion ausschließlich zwischen dem Kunden und der Website oder dem Service des jeweiligen Dritten stattfindet. IBM übernimmt keinerlei Gewährleistung oder Haftung für die Websites, die Services oder die Qualität der Daten Dritter.

8.6 Beschränkungen bei der Nutzung zum Vorteil Dritter

Der Kunde darf den Cloud-Service oder zugehörige Komponenten, einschließlich der vom Cloud-Service erzeugten Ausgabedaten und Berichte, nur mit schriftlicher Genehmigung von IBM verwenden, um Leistungen eines Servicebüros, Hosting-Services oder andere kommerzielle IT-Services für Dritte bereitzustellen.

8.7 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.