IBM Emptoris Managed Cloud Delivery

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 Emptoris Managed Cloud Delivery

Die folgenden Cloud-Services sind als Managed Cloud Delivery-Angebot erhältlich:

- IBM Emptoris Contract Management for Commercial Banking Agreements Managed Cloud Delivery
- IBM Emptoris Contract Management Sell Side Managed Cloud Delivery
- IBM Emptoris Contract Management Buy Side Managed Cloud Delivery
- IBM Emptoris Contract Management for Commercial Banking Agreements Managed Cloud Delivery
- IBM Emptoris Services Procurement Managed Cloud Delivery
- IBM Emptoris Sourcing Managed Cloud Delivery
- IBM Emptoris Spend Analysis Managed Cloud Delivery
- IBM Emptoris Supplier Lifecycle Management Managed Cloud Delivery
- IBM Emptoris Program Management Managed Cloud Delivery
- IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery

In Verbindung mit dem Betrieb, der Nutzung und dem Zugriff auf die lizenzierte Software, einschließlich Produktionsservern, Produktionsspeicher und einer Verbindung zwischen dem/den Produktionsserver(n) und dem Internet, werden für den Kunden Managed Cloud Delivery Services erbracht. Gegebenenfalls stellt IBM außerdem eine optionale Anwendungsplattform für nicht produktive Zwecke (wie nachstehend beschrieben) zur Verfügung, sofern eine zusätzliche Instanz im Auftragsdokument angegeben ist. IBM übernimmt die Integration, Einrichtung und Konfiguration der Ausrüstung, die für die Bereitstellung der Managed Cloud Delivery Services für die im Auftragsdokument beschriebene lizenzierte Software erforderlich ist. Die Managed Cloud Delivery Services beinhalten keine Datenmigration, die bei entsprechender Beauftragung jedoch auf Zeit- und Materialbasis durchgeführt wird. Des Weiteren wird IBM die gesamte Hardware und Software, Telekommunikationshardware und -software, Sicherheitssoftware und sonstige Software bereitstellen und warten, die zum Betrieb der Managed Cloud Delivery Services üblicherweise erforderlich ist. Sobald die Internet-URL veröffentlicht wird, können berechtigte Benutzer über einen Computer mit Internetanschluss und einem modernen Web-Browser auf die Software zugreifen. Die Spezifikationen werden zum Zeitpunkt der Initialisierung der verwalteten Anwendung bekannt gegeben.

Eine Anwendung für nicht produktive Zwecke ist eine Anwendung, die getrennt von der Produktionsanwendungsplattform bereitgestellt wird. Die Anwendungsplattform für nicht produktive Zwecke kann sich nach Ermessen von IBM in einer anderen Einrichtung als die Produktionsanwendungsplattform befinden. Diese Plattform ist in erster Linie für Test- und Staging-Zwecke, Schulungen oder Qualitätssicherung vorgesehen und kann nach Wahl des Kunden entsprechend verwendet werden.

1.2 Optionale Features

1.2.1 IBM Emptoris Sourcing on Cloud Burst Mode

Mit diesem Cloud-Service besteht die Möglichkeit, die Kapazität durch Hinzufügen zusätzlicher Server zur Konfiguration zu erhöhen, wenn der Kapazitätsbedarf die Standardserverkonfiguration überschreitet.

1.2.2 IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Extended Data Retention

Mit diesem Cloud-Service besteht die Möglichkeit, die von IBM geladenen Daten (einschließlich EDI-Rechnungen und Papierimages) während der SaaS-Erstlaufzeit von 36 Monaten (nachfolgend „Erstlaufzeit“ genannt) aufbewahren zu lassen. Wenn dieser Service nicht erworben wird, werden die Daten von IBM unter Umständen nur für die Dauer eines Jahres aufbewahrt, und IBM behält sich das Recht vor, die Daten aus dem System zu löschen. Mit diesem Cloud-Service erhält der Kunde ferner die Möglichkeit, seine von IBM geladenen Daten (einschließlich EDI-Rechnungen und Papierimages) auch dann aufbewahren zu lassen, wenn er den Cloud-Service IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery nicht verlängert. Bei Kündigung von IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery zum Ende der Erstlaufzeit kann der Kunde entweder eine Vereinbarung mit IBM schließen, 1) dass seine Rechnungsdaten nach Ablauf der Erstlaufzeit an ihn zurückübertragen werden oder 2) dass seine bei Ablauf der Erstlaufzeit in IBM Rivermine TEMEDR SaaS vorhandenen Daten weiterhin aufbewahrt werden, indem er IBM Emptoris Rivermine Telecom Expense Management Managed Cloud Delivery Extended Data Retention für bis zu sieben (7) weitere Jahre erwirbt.

1.2.3 IBM Emptoris Managed Cloud Edge Delivery Web Application Accelerator

IBM Emptoris Edge Delivery Web Application Accelerator bietet die folgende Funktionalität:

- Ein dynamisches Zuordnungssystem leitet Benutzeranforderungen für sichere Anwendungsinhalte an den optimalen Server
- Routenoptimierungstechnologie ermittelt den optimalen Pfad zurück zur Ursprungsinfrastruktur für das Abrufen dynamischer Anwendungsinhalte
- Ein Transportprotokoll optimiert die Kommunikation zwischen Server und Ausgangspunkt auf transparente Art und Weise
- Der Server ruft die angeforderten Anwendungsinhalte ab und überträgt sie über sichere optimierte Verbindungen zurück an den Benutzer

1.2.4 IBM Emptoris Managed Cloud Delivery Virtual Private Network Connection

IBM Emptoris Virtual Private Network Connection on Cloud stellt eine verschlüsselte Site-to-Site-Verbindung zwischen dem Endpunkt im Netz des Kunden und dem Hosting-Endpunkt des Emptoris-SaaS zur Verfügung. Der gesamte Datenverkehr zwischen diesen beiden Endpunkten wird sicher verschlüsselt. Die Daten werden mit branchenüblichen Verschlüsselungsschlüsseln und -methoden auf der Sendeseite verschlüsselt und auf der Empfangsseite entschlüsselt.

1.2.5 IBM Emptoris Strategic Supply Management Managed Cloud Delivery Encrypted Database

Mit IBM Emptoris Strategic Supply Management Managed Cloud Delivery Encrypted Database on Cloud werden die in einer dedizierten Datenbankinstanz gespeicherten Kundendaten unter Verwendung eines Verschlüsselungsschlüssels für die folgenden Cloud-Services verschlüsselt, sofern diese im Auftragsdokument angegeben sind:

- IBM Emptoris Contract Management Sell Side Managed Cloud Delivery
- IBM Emptoris Contract Management Buy Side Managed Cloud Delivery
- IBM Emptoris Services Procurement Managed Cloud Delivery
- IBM Emptoris Sourcing Managed Cloud Delivery

Verschlüsselungsschlüssel sind in einem Schlüsselsafe gespeichert. Für jede Datenbankinstanz sind dedizierte eindeutige Schlüssel erforderlich. Es werden keine Schlüssel gemeinsam verwendet, selbst dann nicht, wenn sich die Datenbankinstanzen auf gemeinsam genutzter Hardware befinden. IBM Emptoris Contract Management Buy Side on Cloud, IBM Emptoris Contract Management Sell Side on Cloud und IBM Emptoris Contract Management for Commercial Banking Agreements on Cloud speichern keine Anhänge in der Datenbank, sodass die in den Anhängen enthaltenen Daten nicht verschlüsselt werden.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM hat 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. Des Weiteren verfügt IBM über ein Team für Informationssicherheit. 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 Betriebspersonal 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. IBM beauftragt einen anderen Anbieter damit, jährlich Prüfungen nach dem Branchenstandard SSAE 16 (oder einem vergleichbaren Standard) in den Produktionsrechenzentren

durchzuführen. 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 im Auftragsdokument des Kunden angegeben ist. 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 eingereichter 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 seitens des Kunden

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

   (6) Fehler bei einer vom Kunden bereitgestellten Internet-URL oder Zertifikatsfehler

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.

e. Gutschriften für Ausfallzeiten basieren ausschließlich auf den Kosten eines bestimmten Cloud-Service und beinhalten weder die Kosten anderer Cloud-Services noch die Gebühren für Softwarelizenzen, Unterstützungsleistungen und Serviceimplementierungen durch das Labor oder jährliche Unterstützungskosten und Upgrade-Gebühren, da diese nicht als Kosten im Zusammenhang mit dem Cloud-Service betrachtet werden.

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)**
< 99,0 %	2 %
< 97,0 %	5 %
< 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: 500 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 500 Minuten Ausfallzeit - 200 Minuten geplante Systemausfallzeit = 42.500 Minuten _____ 43.200 Minuten insgesamt - 200 Minuten geplante Systemausfallzeit = 43.000 Minuten	= Gutschrift für Ausfallzeiten in Höhe von 2 % bei einem erreichten Service-Level von 98,8 %

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. Bei Überschreitung der Anzahl der gleichzeitig angemeldeten Benutzer, für die das System gemäß Ziffer 7.9 konfiguriert wurde, kommt das SLA nicht zur Anwendung. Wenn der Kunde wesentliche Verpflichtungen aus seinem Vertrag für den Cloud-Service, einschließlich, aber nicht beschränkt auf die Verletzung von Zahlungsverpflichtungen, nicht erfüllt hat, darf er keinen Anspruch unter diesem SLA geltend machen.

4. Informationen zu Berechtigungen und Abrechnung

4.1 Gebührenmetriken

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

a. „Verbindung“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Verbindung ist die Anbindung oder Zuordnung einer Datenbank, einer Anwendung, eines Servers oder einer anderen Art von Einheit zum Cloud-Service. Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Verbindungen abzudecken, die während des Abrechnungszeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, zum Cloud-Service hergestellt wurden oder hergestellt werden.

b. „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 Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, 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

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.

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

Nachdem IBM dem Kunden mitgeteilt hat, dass sein Zugriff auf den Cloud-Service freigeschaltet ist, wird technische Unterstützung für den Cloud-Service per Telefon, per E-Mail, in Online-Foren und über ein Onlinesystem für die Problemmeldung erbracht. Alle funktionalen Erweiterungen, Updates und sonstigen Materialien, die von IBM im Rahmen der technischen Unterstützung bereitgestellt werden, sind als

Bestandteil des Cloud-Service zu betrachten und unterliegen daher dieser Servicebeschreibung. Die technische Unterstützung ist beim Cloud-Service eingeschlossen und nicht als separates Angebot erhältlich.

Weitere Informationen über die Zeiten der Erreichbarkeit, E-Mail-Adressen, Telefonnummern, Onlinesysteme für die Problemmeldung und andere Übertragungswege und Prozesse der technischen Unterstützung werden im IBM Software as a Service Support Handbook beschrieben.

Support-Tickets für den Cloud-Service werden anhand der folgenden Fehlerklassen überwacht:

Fehlerklasse	Definition der Fehlerklasse
1	**Probleme mit kritischer Auswirkung auf den Geschäftsbetrieb/Serviceausfall:** ● Das Produkt kann in der Produktionsumgebung nicht verwendet werden oder die Arbeit in der Produktionsumgebung wird durch das Produkt auf unzumutbare Weise beeinträchtigt ● Die Produktsicherheit wurde verletzt ● Daten werden beschädigt ● Lieferanten und Einkäufer können keine Angebote (über die Benutzerschnittstelle (UI) oder per Import) abgeben ● Es können weder Verträge erstellt, genehmigt oder ausgeführt noch Vertragstexte geöffnet werden ● Es wird keine Datei der AP-/GL-Buchungen erstellt oder das Ergebnis entspricht nicht den Erwartungen, sodass keine Rechnungen ohne Fehlerumgehung bezahlt werden können
2	**Probleme mit erheblicher Auswirkung auf den Geschäftsbetrieb:** ● Kritische Produktkomponenten funktionieren nicht ordnungsgemäß ● Das Verhalten hat beträchtliche nachteilige Auswirkungen auf die Produktivität ● Benutzer erhalten keine Einladungen zu Ereignissen ● Vertragsgenehmigungsworkflows und -regeln funktionieren nicht ordnungsgemäß ● Aufträge werden nicht erfolgreich an die Lieferanten übertragen ● Rechnungsleser ist nicht betriebsbereit ● Rechnungsgenehmigungsworkflow funktioniert nicht wie vorgesehen ● Rechnungen werden nicht wie vorgesehen zugeordnet
3	**Probleme mit geringer Auswirkung auf den Geschäftsbetrieb:** ● Produktkomponenten funktionieren nicht ordnungsgemäß, obwohl eine Alternativlösung verfügbar ist ● Ein unwesentliches Feature ist nicht verfügbar und es gibt keine Alternativlösung ● Den Positionen eines Ereignisses kann kein Dokument zugeordnet werden ● Benachrichtigungsvorlage wird nicht korrekt formatiert ● Unkritische Software-Features liefern unerwartete Ergebnisse
4	**Probleme mit minimaler Auswirkung auf den Geschäftsbetrieb:** ● Anforderung von Produktinformationen ● Erläuterung zur Produktdokumentation ● Vorgehensweise zum Exportieren eines Ereignisses ● Vorgehensweise zur Planung eines Reporting-Jobs

7. Zusätzliche Informationen

7.1 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.

7.2 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.

7.3 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 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 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.

7.4 Gastbenutzer

Der Kunde kann seine Handelspartner oder andere Drittparteien zum Zugriff auf den Cloud-Service berechtigen, damit diese Daten mit ihm austauschen oder den Cloud-Service in seinem Namen nutzen können (nachfolgend „Gastbenutzer“ genannt). Der Kunde ist für die Gastbenutzer verantwortlich, insbesondere für a) jegliche Forderungen der Gastbenutzer in Bezug auf den Cloud-Service, b) die für die Gastbenutzer anfallenden Gebühren oder c) missbräuchliche Verwendung des Cloud-Service durch die Gastbenutzer.

7.5 Zugehörige IBM Programme

Die IBM Emptoris Managed Cloud Delivery Services enthalten keine Subscription und Support für das zugehörige IBM Programm. Der Kunde versichert, dass er die (1) erforderlichen Lizenzberechtigungen und (2) Subscription und Support für das IBM Programm erworben hat. Um Subscription und Support für die IBM Programme während der Subscription-Laufzeit des Cloud-Service zu erhalten, muss der Kunde seinen laufenden Subscription- und Support-Vertrag für die IBM Programme aufrechterhalten. Während der Laufzeit dieser Vereinbarung dürfen für jede im Auftragsdokument angegebene Instanz des Cloud-Service nur unterstützte Versionen von IBM Programmen verwendet werden, für die im IBM Support Lifecycle-Dokument angegeben ist, dass derzeit Standardunterstützung für diese Programme erbracht wird.

7.6 Rückgabe der Inhalte

Vor Beendigung oder Kündigung des Cloud-Service können über die Berichterstellungs- oder Exportfunktionen des Cloud-Service Daten extrahiert werden. Wenn IBM innerhalb von 30 Tagen nach Beendigung oder Kündigung des Cloud-Service eine entsprechende Anforderung des Kunden erhält, wird IBM eine elektronische Kopie der Kundeninhalte im nativen Anwendungsformat bereitstellen.

7.7 Ausfallzeit

Das Zeitfenster für geplante Wartungsmaßnahmen findet samstags zwischen 16:00 Uhr GMT und 4:00 Uhr GMT statt. Während dieser Zeit steht der Cloud-Service abhängig von den geplanten Wartungsmaßnahmen ggf. nicht zur Verfügung. Durch das Wartungsfenster bedingte Ausfallzeiten werden bei der Berechnung von SLA-Gutschriften nicht berücksichtigt. IBM behält sich das Recht vor, außerplanmäßige Ausfallzeiten anzuberaumen. IBM wird alle Anstrengungen unternehmen, um geplante Ausfallzeiten rechtzeitig über den Kundendienst anzukündigen.

7.8 Vom Kunden bereitgestellte Zertifikate

Der Cloud-Service wird für einen von IBM bereitgestellten Uniform Resource Locator (URL) für das Internet konfiguriert, außer wenn auf ausdrücklichen Wunsch des Kunden eine kundeneigene URL verwendet werden soll. Bei Verwendung einer kundeneigenen Internet-URL für den Cloud-Service trägt der Kunde die gesamte Verantwortung und Wartung sowie sämtliche Kosten für die Verlängerung der URL und der erforderlichen Zertifikate. Der Kunde muss IBM die erforderlichen Zertifikate und Setup-Informationen zur Verfügung stellen, bevor der Cloud-Service vollständig eingerichtet werden kann.

7.9 Disaster-Recovery

Während der gesamten Laufzeit des Cloud-Service bestehen für alle betriebskritischen Funktionen Disaster-Recovery-Pläne. Diese formalen Pläne sind dokumentiert und werden (mindestens) jährlich revalidiert.

Im Rahmen der IBM Disaster-Recovery sind Wiederherstellungsmaßnahmen für die Produktionsinstanz des Kunden zur Fortsetzung des Betriebs in einer Disaster-Recovery-Einrichtung vorgesehen. IBM wird mit wirtschaftlich vertretbarem Aufwand Disaster-Recovery-Maßnahmen zur Wiederherstellung des Service mit einer Zielsetzung für die Wiederherstellungsdauer (Recovery Time Objective, RTO) von 72

Stunden und einer Zielsetzung für den Wiederherstellungspunkt (Recovery Point Objective, RPO) von 24 Stunden für Produktionsinstanzen durchführen.

7.10 Aufbewahrungsdauer für Sicherungskopien

Sicherungskopien der Kundendaten werden für einen Zeitraum von maximal 90 Tagen aufbewahrt. Die Sicherungen werden von IBM ausschließlich für Disaster-Recovery-Maßnahmen und weitere Bemühungen zur Wiederherstellung des Service aufbewahrt und sind nicht für die Wiederherstellung von Daten vorgesehen, die vom Kunden im Cloud-Service gelöscht wurden. Der Kunde ist dafür verantwortlich, die Sicherheit des Cloud-Service so zu konfigurieren, dass einzelne Benutzer keine Daten löschen können. Werden trotzdem Daten gelöscht, ist sich der Kunde dessen bewusst, dass IBM die gelöschten Daten nicht wiederherstellen kann.

7.11 Beschränkungen bei IBM Sourcing Managed Cloud Delivery

Die Infrastruktur des Angebots IBM Emptoris Sourcing Managed Cloud Delivery wurde zur Unterstützung der folgenden Benutzerzahlen konfiguriert:

- 300 gleichzeitig angemeldete Benutzer, die RFPs, RFIs, RFQs oder Käuferumfragen ausführen, oder
- 270 gleichzeitig angemeldete Benutzer, die englische umgekehrte und englische klassische Auktionen ausführen, oder
- 60 gleichzeitig angemeldete Benutzer, die japanische oder niederländische umgekehrte oder klassische Auktionen ausführen.

Gleichzeitig angemeldete Benutzer sind als Benutzer definiert, die zeitgleich beim System angemeldet und aktiv sind. Abhängig von verschiedenen Faktoren kann das System so konfiguriert werden, dass die von den gleichzeitig angemeldeten Benutzern generierten Volumen verarbeitet werden können. Für die Unterstützung größerer Nutzungsvolumen können zusätzliche Infrastrukturressourcen erforderlich sein.

Wenn der Kunde das OJEU-Feature (Official Journal of the European Union = Amtsblatt der Europäischen Union) nutzt, mit dem das Einkaufssystem Daten an die Site „Tenders Electronic Daily“ (TED) überträgt, ist der Kunde für die Beachtung des OJUE und die Absolvierung des GAMMA-Tests verantwortlich. (Tenders Electronic Daily ist die Online-Version des Supplements zum Amtsblatt.) Die Datenübertragung findet ausschließlich zwischen dem Kunden und dieser Site der Drittpartei statt. IBM übernimmt keinerlei Gewährleistung oder Haftung für die Websites oder die Services Dritter.