IBM Payments Gateway

Diese Servicebeschreibung bezieht sich auf den Cloud-Service, den IBM für den Kunden bereitstellt. Als Kunde werden das Unternehmen, seine berechtigten Benutzer und die Empfänger des Cloud-Service bezeichnet.

1. Cloud-Service

Das von IBM bereitgestellte Cloud-Service-Angebot wird im Folgenden beschrieben. Das maßgebliche Angebot und der Berechtigungsnachweis (Proof of Entitlement = PoE) werden als separate Auftragsdokumente zur Verfügung gestellt.

IBM Payments Gateway

IBM Payments Gateway bietet die Möglichkeit zur Anbindung an Entwicklungs-, Vorproduktions- und Produktionsumgebungen. Zu den verfügbaren Funktionen gehören:

- Ein Payment Card Industry (PCI) Vault, eine Speichereinrichtung, die für die Sicherheit sensibler Zahlungsinformationen entwickelt wurde
- Ein Payment Gateway für die Abwicklung von Zahlungstransaktionen (Weiterleitung, Switching und Verarbeitung) mit externen Dienstleistern
- Ein virtuelles Terminal, bei dem es sich um ein Web-Tool handelt, das für das Inkasso in Call-Centern sowie Kreditmanagement und Back-Office-Zahlungsoperationen ausgelegt ist
- Authentifizierung mit Sicherheitsfunktionen
- Tools für Betrugsprävention
- Berichterstellungsfunktionen
- Dokumentation

1.1 Zusätzliche Services

Der Kunde muss das IBM Payments Gateway in Verbindung mit mindestens einem (1) der folgenden Cloud Service-Payment-Angebote erwerben:

a. IBM Payments Gateway API Payment

Zu den Funktionen gehören:

- Die Transaktionen werden über eine API übertragen, die aus einer Reihe von Web-Services besteht, die eine vereinfachte Integration mit Kundensystemen ermöglichen. Die API bietet eine einzelne Schnittstelle für weltweite Zahlungen zwischen Banken und Dienstleistern in einer Vielzahl von Ländern und Währungen.

b. IBM Payments Gateway Hosted-Page Payment

Zu den Funktionen gehören:

- Die Transaktionen werden über die Hosted Payment Page (HPP), eine Inkasso- und Wallet-Management-GUI übertragen, die in Websites, mobile Commerce-Sites, Smartphone-Apps, Call-Center-Anwendungen und Back-Office-Erfassungssysteme integrierbar ist. Die Hosted Payment Page wird in einem HTML-Inline-Frame (I-Frame) zur Verfügung gestellt.

c. IBM Payments Gateway Advanced API Payment

Zu den Funktionen gehören:

- Die Transaktionen werden über die JSON-Schnittstelle (JSON = JavaScript Object Notation) übertragen, die die Entwicklung von Zahlungsfunktionen in nativen Smartphone-Anwendungen ermöglicht.
- Die JSON-Schnittstelle bietet eine Reihe von Zahlungs-APIs, die über HTTP-Methoden auf der zugehörigen URL ausgeführt werden, wobei die Datenbereitstellung im JSON-Format erfolgt.

Das folgende IBM Payments Gateway-Angebot kann optional erworben werden:

d. IBM Payments Gateway Settlement

Zu den Funktionen gehören:

- Transaktionen, die Zahlungsinformationen für die Zahlungsabwicklung enthalten, werden vom Verkäufer an das Geldinstitut des Käufers übertragen.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM verfügt über ein Team für Informationssicherheit und hat Datenschutz- und Sicherheitsrichtlinien festgelegt, die an die IBM Mitarbeiter kommuniziert werden. IBM verlangt, dass die Mitarbeiter, jährlich an Schulungen zu Datenschutz- und Sicherheitsmaßnahmen teilnehmen. Die IBM Sicherheitsrichtlinien werden jedes Jahr basierend auf branchenüblichen Standards und gemäß den IBM Geschäftsanforderungen erneut validiert. Bei Sicherheitsverstößen wird ein umfassendes Verfahren zur Behebung von Sicherheitsvorfällen in Gang gesetzt. Aufgrund der IBM Standards für physische Sicherheit ist der Zugang zu IBM Rechenzentren auf autorisierte Mitarbeiter beschränkt. Zu diesem Sicherheitskonzept gehört auch eine begrenzte Anzahl von Eingängen, die überwacht werden. Besucher werden beim Betreten des Rechenzentrums registriert und während ihres Aufenthalts dort begleitet.

2.2 Zugriffskontrolle

Die autorisierten IBM Mitarbeiter verwenden Zwei-Faktor-Authentifizierung für einen zwischengeschalteten „Gateway"-Management-Host. IP-Adressen können blockiert werden, um den Zugriff durch bekannte kompromittierende Internet-Sites und durch Benutzer in Ländern, die einem US-Embargo unterliegen, zu verhindern. Zugriffe auf Kundendaten und Datenübertragungen in die oder aus der Hosting-Umgebung werden protokolliert. In IBM Rechenzentren, die diesen Cloud-Service unterstützen, ist der Einsatz von Wifi untersagt.

Im Rahmen des Cloud-Service müssen die Inhalte bei der Datenübertragung zwischen dem IBM Netz und dem Netzeingangspunkt des Kunden verschlüsselt werden. Die spezifischen Verschlüsselungsverfahren werden vertraglich mit dem Kunden vereinbart und für die Verschlüsselung müssen sowohl auf der IBM Seite als auch der Kundenseite SSL-Zertifikate installiert werden. Es werden nur persönliche Daten erfasst, die für die Zahlungsabwicklung erforderlich sind. Im Cloud-Service vorhandene Inhalte, die auf ihre Übertragung warten, werden nicht verschlüsselt.

2.3 Service-Integrität und Verfügbarkeit

Änderungen der Betriebssysteme, Anwendungssoftware und Firewallregeln werden gemäß dem Change-Management-Prozess von IBM durchgeführt. Änderungen an Firewallregeln 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) im Einsatz. 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 Compliance

In den IBM Payments Gateway-Produktionsrechenzentren werden jährlich Prüfungen nach dem Branchenstandard ISAE3402 (oder einem vergleichbaren Standard) durchgeführt, um die Einhaltung der IBM Richtlinien zur Informationssicherheit zu gewährleisten. Die jährliche PCI-DSS-Zertifizierung von IBM beinhaltet Audits vor Ort durch externe Qualified Security Assessors (Trustwave) in allen IBM Payments Gateway-Rechenzentren. Die Bescheinigung (Attestation of Compliance = AoC) oder das Bestätigungsschreiben über die Einhaltung der Bestimmungen (Compliance Letter) wird dem Kunden und seinen Prüfern auf Anforderung zur Verfügung gestellt.

2.6 Erklärung zu Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugte Zugriffe innerhalb des Unternehmens und von außen. Unbefugte Zugriffe können das Ändern, Löschen oder die missbräuchliche oder unsachgemäße Nutzung von Informationen sowie die Beschädigung oder den Missbrauch der Kundensysteme für Attacken auf andere zur Folge haben. Ohne einen umfassenden Sicherheitsansatz sollte kein IT-System oder -Produkt als vollständig sicher angesehen werden und kein einzelnes Produkt und keine einzelne Sicherheitsmaßnahme kann unbefugte Zugriffe vollständig verhindern. IBM Systeme und Produkte werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keinerlei Gewähr dafür, dass Systeme und Produkte vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind.

2.7 Datenschutz

IBM und der Kunde sind für die Einhaltung ihrer jeweiligen Verpflichtungen unter den geltenden Datenschutzgesetzen in Bezug auf personenbezogene Daten (gemäß der Definition des Begriffs in den geltenden Datenschutzgesetzen), die von IBM unter diesem Vertrag für den Kunden gespeichert oder verarbeitet werden (nachfolgend „Kundendaten“ genannt) selbst verantwortlich. Durch Abschluss dieses Vertrags ernennt der Kunde IBM zum Auftragsverarbeiter für die Kundendaten. Der Kunde bleibt allein dafür verantwortlich, über die Zwecke und Mittel der Verarbeitung der Kundendaten durch IBM unter diesem Vertrag zu entscheiden, insbesondere dafür, dass IBM durch die Verarbeitung gemäß seinen Anweisungen nicht gegen geltende Datenschutzgesetze verstößt. IBM und der Kunde bestätigen jeweils, dass sie die Maßnahmen der anderen Partei zur Einhaltung der geltenden Datenschutzgesetze nicht überprüfen werden. Durch die Bestimmungen dieses Vertrags ist weder IBM noch der Kunde daran gehindert, alle Maßnahmen durchzuführen, die zur Einhaltung der geltenden Datenschutzgesetze für notwendig erachtet werden. Wenn der Kunde zusätzliche oder andere Services zur Einhaltung der geltenden Datenschutzgesetze benötigt, kann er für die Erbringung der erforderlichen Services separate Servicevereinbarungen abschließen. Der Kunde bestätigt, dass er allein die Verantwortung dafür trägt, zu entscheiden, ob die in diesem Vertrag angegebenen Sicherheitsmaßnahmen geeignete technische und organisatorische Maßnahmen zum Schutz der Kundendaten im Sinne der geltenden Datenschutzgesetze darstellen. IBM ist nicht verpflichtet, andere außer den in diesem Vertrag angegebenen oder den für Auftragsverarbeiter geltenden Sicherheitsmaßnahmen für die Kundendaten durchzuführen oder zu beachten. IBM wird die Kundendaten gemäß diesem Vertrag und in dem Umfang verarbeiten, den IBM zur Bereitstellung der Services für notwendig oder angebracht hält. Der Kunde entscheidet alleine darüber, ob grenzüberschreitende Datenübermittlungen von Kundendaten durch IBM oder den Kunden unter diesem Vertrag den geltenden Datenschutzgesetzen entsprechen.

3. Service-Level-Agreement

Das folgende Service-Level-Agreement („SLA“) von IBM, das im Auftragsdokument angegeben ist, beinhaltet Angaben zur Verfügbarkeit des Cloud-Service. Das SLA stellt keine Gewährleistung dar.

3.1 Begriffsbestimmungen

a. **Servicegutschrift** ist der Schadensersatz, den IBM für einen bestätigten Anspruch leistet. Die Servicegutschrift wird in Form einer Gutschrift gewährt und mit einer zukünftigen Rechnung für den Cloud-Service verrechnet, sofern der Cloud-Service direkt von IBM erworben wurde. Wurde der Cloud-Service von einem IBM Business Partner erworben, zahlt IBM eine Rückvergütung, die direkt an den Kunden geleistet wird.

b. **Anspruch** ist ein vom Kunden bei IBM eingereichter Anspruch, der besagt, dass ein Service-Level während eines Vertragsmonats nicht erfüllt wurde.

c. **Vertragsmonat** ist jeder volle Kalendermonat während der Laufzeit des Cloud-Service, 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 das Produktionssystem für die Verarbeitung des Cloud-Service, für den der Kunde berechtigt ist, nicht zur Verfügung steht. 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 den Inhalten, Geräten oder Anwendungen, die vom Kunden in Verbindung mit dem Cloud-Service genutzt werden, oder Probleme mit der Software, Hardware oder sonstigen Technologien Dritter

   (4) Nichtbeachtung erforderlicher Systemkonfigurationen und unterstützter Plattformen durch den Kunden oder Probleme bedingt durch die Systemverwaltung, Befehle oder Programmierfehler des Kunden

   (5) vom Kunden verursachte Sicherheitsverletzungen oder vom Kunden durchgeführte Sicherheitstests

   (6) 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. **Antwortzeit** ist die Zeitspanne ab dem Zeitpunkt, zu dem die Web-Services CheckoutStartSession und/oder CardAuthorize eine Anforderung am Eingangspunkt der IBM Systeme empfangen, bis zu dem Zeitpunkt, zu dem die IBM Web-Services eine Rückantwort an den Kunden senden.

3.2 Servicegutschriften

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 und Problemlösung angemessen unterstützen.

Der Anspruch auf eine Servicegutschrift muss innerhalb von drei (3) Arbeitstagen nach Ablauf des Vertragsmonats geltend gemacht werden, in dem der Anspruch entstanden ist.

IBM misst intern die insgesamt während jedes einzelnen Vertragsmonats aufgelaufene Ausfallzeit gemäß den anwendbaren Service-Levels in den nachstehenden Tabellen. Die Gutschriften 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.

a. Wenn der Kunde Ausfallzeiten bei den Web-Services, der Hosted Payment Page und dem virtuellen Terminal meldet und die Vorfälle gleichzeitig aufgetreten sind, behandelt IBM sich überschneidende Ausfallzeiten als eine einzige Ausfallzeit, und nicht als separate Ausfallzeiten.

b. Wenn der Kunde Beeinträchtigungen bei der Antwortzeit der Web-Services CheckoutStartSession und CardAuthorize meldet und die Vorfälle gleichzeitig aufgetreten sind, behandelt IBM sich überschneidende Beeinträchtigungen bei der Antwortzeit als eine einzige Ausfallzeit, und nicht als zwei separate Ausfallzeiten.

Für jeden gültigen Anspruch wird IBM die höchstmögliche Servicegutschrift basierend auf dem während jedes einzelnen Vertragsmonats erreichten Service-Level anwenden (siehe die nachstehenden Tabellen). IBM gewährt keine Mehrfachgutschriften für den gleichen Vorfall/die gleichen Vorfälle in ein und demselben Vertragsmonat.

Wurde der Cloud-Service von einem IBM Business Partner erworben, so wird die Servicegutschrift anhand der monatlichen Subscription-Gebühr auf der Basis des zum jeweiligen Zeitpunkt gültigen Listenpreises für den Cloud-Service berechnet, der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%).

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

3.3 Service-Levels

Die IBM Schnittstellen für die Web-Services, die Hosted Payment Page und das virtuelle Terminal stehen den Kunden während eines Vertragsmonats mit einer Verfügbarkeit von mindestens 99,95 % zur Verfügung.

Verfügbarkeit in Prozent (in einem Vertragsmonat)	Servicegutschrift (in Prozent (%) der monatlichen Subscription-Gebühr für den Vertragsmonat, der Gegenstand des Anspruchs ist)
< 99,95 %	2 %
< 99,80 %	4 %
< 99,60 %	6 %
< 99,30 %	8 %
< 99,00 %	10 %

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat, in denen die Web-Services, die Hosted Payment Page und das virtuelle Terminal von IBM verfügbar sind und auf Kundenanforderungen reagieren, dividiert durch die Gesamtzahl der Minuten in einem Vertragsmonat, multipliziert mit 100.

3.4 Antwortzeit der IBM Web-Services in einem Vertragsmonat

IBM bietet zwei SLAs für die Antwortzeit an:

3.4.1 Gemittelte Antwortzeit der IBM Web-Services

Die gemittelte IBM Antwortzeit bei den Web-Services CheckoutStartSession und CardAuthorize liegt unter 100 Millisekunden.

Die IBM Antwortzeit für einen bestimmten Web-Service wird ermittelt, indem die Zeitspanne ab dem Zeitpunkt des Eintreffens der Web-Service-Anforderung am Eingangspunkt des IBM Systems bis zum Zeitpunkt der Rückantwort des IBM Web-Service an den Kunden gemessen wird, abzüglich der Zeit, die das IBM System auf Antworten von nachgeordneten externen Dienstleistern gewartet hat.

Das Service-Level-Ziel wird bei den Web-Services CheckoutStartSession und CardAuthorize als gemittelte IBM Antwortzeit über alle Web-Service-Anforderungen in einem bestimmten Vertragsmonat berechnet.

Gemittelte Antwortzeit (in einem Vertragsmonat)	Servicegutschrift (in Prozent (%) der monatlichen Subscription-Gebühr für den Vertragsmonat, der Gegenstand des Anspruchs ist)
> 100 ms	2 %
> 500 ms	6 %
> 1 Sekunde	10 %

3.4.2 Antwortzeit bei 99 % der IBM Web-Services

Bei 99 % der Web-Services CheckoutStartSession und CardAuthorize liegt die IBM Antwortzeit unter 1 Sekunde.

Die Antwortzeit wird auf die gleiche Weise berechnet wie die oben beschriebene gemittelte Antwortzeit bei IBM Web-Services.

Das Service-Level-Ziel wird bei den Web-Services CheckoutStartSession und CardAuthorize als 99 %-Perzentil der IBM Antwortzeit über alle Web-Service-Anforderungen in einem bestimmten Vertragsmonat berechnet.

Antwortzeit bei 99 % der IBM Web-Services (in einem Vertragsmonat)	Servicegutschrift (in Prozent (%) der monatlichen Subscription-Gebühr für den Vertragsmonat, der Gegenstand des Anspruchs ist)
> 1 Sekunde	2 %
> 5 Sekunden	6 %
> 10 Sekunden	10 %

3.5 Weitere Informationen zu diesem SLA

Dieses SLA wird dem Kundenunternehmen zur Verfügung gestellt und gilt nicht für Ansprüche, die von Benutzern des Cloud-Service oder in Bezug auf Beta- oder Testservices geltend gemacht werden. Das SLA bezieht sich nur auf produktiv genutzte Cloud-Services und nicht auf Nicht-Produktionsumgebungen, einschließlich, aber nicht beschränkt auf Tests, Disaster-Recovery, Qualitätssicherung oder Entwicklung. IBM wird keine Ansprüche auf Servicegutschriften in Bezug auf nicht erreichte Antwortzeiten verarbeiten, wenn die Service-Levels im selben Zeitraum nicht erfüllt wurden.

4. Service-Level-Ziele

Die folgenden Service-Level-Ziele sind Zielvorgaben und können gegenüber dem Kunden nicht garantiert werden. Falls IBM die Service-Level-Ziele nicht einhält, werden keine Rückerstattungen, Gutschriften oder Ersatzleistungen gewährt.

Service	Ziel
Durchlaufzeit bei der Batchverarbeitung	90 % aller Transaktionsbatches werden innerhalb von 60 Minuten nach dem Empfang vollständig abgearbeitet.
Reaktionsfähigkeit auf E-Mails	95 % der an die gemeinsam genutzte Support-Mailbox gesendeten E-Mails werden innerhalb von 24 Stunden während der Geschäftszeiten beantwortet.
Antwortzeit des 24x7-Help-Desks	Der Help-Desk von IBM, der rundum die Uhr im Einsatz ist (24x7), beantwortet Telefonanrufe in weniger als 60 Sekunden.
Sicherheitsmanagement	● Die Zertifizierung von IBM nach PCI-DSS Level 1 (PCI-DSS = Payment Card Industry Data Security System) wird mindestens einmal pro Jahr erneuert. ● IBM wird Sicherheitslücken, die ein hohes Risiko darstellen, innerhalb von 10 Tagen beheben. ● IBM wird Sicherheitslücken, die ein geringes Risiko darstellen, innerhalb von 30 Tagen beheben.
Verfügbarkeit des Vorproduktionssystems	● Verfügbarkeit für Kundentests rund um die Uhr (24x7). ● Das Vorproduktionssystem arbeitet außerhalb der regulären Arbeitszeiten (MEZ) unbeaufsichtigt. ● Vorfälle, die das Vorproduktionssystem betreffen, werden standardmäßig nach Fehlerklasse 3 behandelt.

5. Technische Unterstützung

Die technische Unterstützung für den Cloud-Service wird per E-Mail und telefonisch 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, Onlinesysteme für die Problemmeldung und andere Übertragungswege und Prozesse der technischen Unterstützung werden im IBM Software as a Service Support Handbook beschrieben.

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.	Benachrichtigung des Kunden innerhalb von 15 Minuten	24x7
2	**Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines Service-Features oder einer Servicefunktion ist stark eingeschränkt oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann.	Benachrichtigung des Kunden innerhalb von 15 Minuten	Mo-Fr zu den lokalen 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.	Keine Benachrichtigung erforderlich	Mo-Fr zu den lokalen Geschäftszeiten
4	**Minimale Auswirkung auf den Geschäftsbetrieb:** Eine Anfrage oder eine Frage nicht technischer Art.	Keine Benachrichtigung erforderlich	Mo-Fr zu den lokalen Geschäftszeiten

6. Informationen zu Berechtigungen und Abrechnung

6.1 Gebührenmetriken

Der Cloud-Service ist mit der im Auftragsdokument angegebenen Gebührenmetrik verfügbar:

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 Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, zum Zugriff und zur Nutzung bereitgestellt werden.

b. **Tausend Ereignisse** ist eine Maßeinheit für den Erwerb des Cloud-Service. Die Berechtigungen für tausend Ereignisse basieren auf der Häufigkeit eines bestimmten Ereignisses im Zusammenhang mit der Nutzung des Cloud-Service und werden in Paketen von jeweils eintausend Ereignissen gemessen. Diese Berechtigungen sind spezifisch für den Cloud-Service und der Ereignistyp darf nicht gegen die Berechtigungen für tausend Ereignisse für einen anderen Cloud-Service oder einen anderen Ereignistyp ausgetauscht, umgetauscht oder mit diesen zusammengefasst werden. Der Kunde muss ausreichende Berechtigungen erwerben, um jedes Ereignis abzudecken, das während des Abrechnungszeitraums auftritt, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist.

c. **Ereignis** ist bei diesem Cloud-Service als Mastertransaktion definiert, die als Pakete mit jeweils eintausend Mastertransaktionen gezählt werden. Eine Mastertransaktion besteht aus einer Folge von Anweisungen, die von einer programmexternen Anwendung (z. B. einem Web-Channel für Business-Banking oder einem Channel für manuelle Nachrichteneingabe) oder von einem Ereignis in dem Programm (z. B. einer wiederkehrenden Zahlung oder der Uhrzeit zum Starten der Massenverarbeitung) ausgelöst wird. Die Mastertransaktion steuert die zugehörige Geschäftsaktivität und logische Arbeitseinheit, einschließlich aller Updates und Ereignisse, die den diversen Verarbeitungsschritten zugeordnet sind, und endet, wenn die letzte Anweisung an eine externe Anwendung gesendet wird oder der Verarbeitungslebenszyklus abgeschlossen ist. Eine Mastertransaktion löst während ihres Verarbeitungslebenszyklus zugrunde liegende Transaktionen aus.

6.2 Anteilige Monatsgebühren

Die im Auftragsdokument angegebene anteilige Monatsgebühr wird anteilig basierend auf der Nutzung ermittelt.

6.3 Zusatzgebühren

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

7. Laufzeit und Verlängerungsoptionen

7.1 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 Angabe im Berechtigungsnachweis freigeschaltet ist. 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 wird in einem Auftragsdokument bestätigt.

7.2 Verlängerungsoptionen

Im Auftragsdokument ist ersichtlich, welche der folgenden Optionen für die Laufzeitverlängerung des Cloud-Service gelten.

7.2.1 Automatische Verlängerung

Bei einer automatischen Verlängerung verlängert sich der Cloud-Service automatisch um die im Auftragsdokument angegebene Laufzeit (entweder um ein (1) Jahr oder um denselben Zeitraum wie die ablaufende Laufzeit), sofern der Kunde nicht mindestens 90 Tage vor dem Ablaufdatum der Laufzeit den Cloud-Service schriftlich gekündigt hat.

7.2.2 Fortlaufende Abrechnung

Bei fortlaufender Abrechnung hat der Kunde auch nach Ablauf der Laufzeit kontinuierlichen Zugriff auf den Cloud-Service und die Nutzung wird fortlaufend berechnet. Um die Nutzung des Cloud-Service einzustellen und den fortlaufenden Abrechnungsprozess zu beenden, muss der Kunde unter Einhaltung einer Frist von 90 Tagen in einer schriftlichen Mitteilung die Einstellung des Cloud-Service beantragen. Eventuell ausstehende Zugriffsgebühren, die bis zum Ende des Monats anfallen, in dem die Einstellung des Cloud-Service wirksam wird, werden dem Kunden in Rechnung gestellt.

7.2.3 Verlängerung erforderlich

Bei einer befristeten Laufzeit wird der Cloud-Service zum Laufzeitende abgeschaltet und der Zugriff des Kunden beendet. Um den Cloud-Service über das Enddatum der Laufzeit hinaus nutzen zu können, muss der Kunde eine neue Subscription-Laufzeit erwerben.

8. Allgemeines

Soweit möglich, orientieren sich die Steuern an dem Standort/den Standorten, für den/die der Cloud-Service erbracht wird. IBM weist die Steuern gemäß der Geschäftsadresse in der Kundenbestellung aus, 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.