Beschreibung des IBM Cloud-Service

IBM Digital Data Exchange

Servicebeschreibung für die Bestellung des Kunden:

1. Cloud-Service

Im Folgenden wird das Cloud-Service-Angebot einschließlich des Basisangebots und der verfügbaren optionalen Features beschrieben, die Bestandteil des Auftragsdokuments sein können. 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 Digital Data Exchange

IBM Digital Data Exchange ist eine Lösung, mit der Tags für Websites und mobile Seiten über eine einzige Schnittstelle konfiguriert und implementiert werden können.

Mit IBM Digital Data Exchange können IBM Tags und Tags von IBM Business Partnern auf der Website oder der mobilen Site eines Kunden platziert werden. Die IBM Digital Data Exchange-Benutzerschnittstelle ermöglicht die direkte Kontrolle des Tagging-Prozesses sowie die Definition von Seitentags und Seitengruppen basierend auf einer Reihe von Regeln, mit denen die Ausführung der Tags festgelegt wird. Mit IBM Digital Data Exchange kann die aktuelle und bestehende Implementierung von IBM Tags, IBM Business Partner-Tags sowie angepasstem JavaScript-Code oder proprietärem Code in einer Vielzahl von Umgebungen gesteuert werden.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM verfügt über Datenschutz- und Sicherheitsrichtlinien, die veröffentlicht und an die IBM Mitarbeiter weitergegeben werden. IBM verlangt, dass Mitarbeiter, die in IBM Rechenzentren weltweit Support leisten, an Schulungen zu Datenschutz- und Sicherheitsmaßnahmen teilnehmen. Des Weiteren verfügt IBM über ein Sicherheitsteam, das sich speziell 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 Zugriffssteuerung

IBM sorgt für die logische Trennung der Kundendaten. Die Kundendaten befinden sich in einem eigenen kundenspezifischen Schema und der Zugriff darauf erfolgt über den Cloud-Service oder durch einen vom Kunden angegebenen Datenexport. Der Zugriff auf den Cloud-Service und die Kundendaten wird von einem vom Kunden benannten Administrator kontrolliert und verwaltet. IBM verwendet beim Zugriff auf die Kundensysteme Mehrfaktorauthentifizierung und verschlüsselte VPN-Tunneltechnologie. Der Zugriff ist auf Personen beschränkt, die für die Wartung und Verwaltung des Cloud-Service und der zugehörigen Hardware- und Softwareinfrastruktur in externen Rechenzentren zuständig sind. IBM verwendet WiFi (auch 802.11) für den Datenverkehr im Netz mit WPA2-Verschlüsselung und AES (Advanced Encryption Standard) und bietet beim Zugriff auf Systeme, auf denen sich Kundendaten befinden, die Möglichkeit zur Unterdrückung der SSID sowie zur gegenseitigen Authentifizierung zwischen dem Server und den Endgeräten.

2.3 Service-Integrität und Verfügbarkeit

Änderungen an Betriebssystemressourcen und Anwendungssoftware werden gemäß dem Change-Management-Prozess von IBM durchgeführt. Innerhalb der Netzinfrastruktur und auf den Workstations der Mitarbeiter, die in IBM Rechenzentren oder mit Kundendaten in IBM Rechenzentren arbeiten, werden Kontrollmechanismen in Hardware und Software, Zugriffsprotokolle, Lesezugriff und Verschlüsselung eingesetzt, um die Wahrscheinlichkeit der Weitergabe und Ausführung von Computerviren und anderen Formen bekannter potenziell gefährlicher Codes zu verringern. IBM verwendet SSL-Verschlüsselung für die Datenübertragung im Netz (https) und in der IBM Infrastruktur kommen technologische Lösungen für End-to-End-Sicherheit zum Einsatz, wie z. B. Firewalls, Abwehr unbefugter Zugriffe und Malware-Schutztechnologien. Berechtigte Administratoren führen regelmäßig TCP/IP-Scans (Transmission Control Protocols/Internet Protocols) zur Ermittlung von Schwachstellen durch, um potenzielle

Systemsicherheitsrisiken aufzudecken und zu beheben. IBM Warehouse-Daten werden auf sekundäre Speicher im IBM Rechenzentrum kopiert und die tertiäre Archivierung (Band) wird zur Speicherung an einem externen Standort eines Drittanbieters für Disaster-Recovery verschlüsselt und dupliziert.

2.4 Aktivitätsprotokollierung

IBM protokolliert alle Aktivitäten für Systeme, Anwendungen, Datenrepositorys, Middleware und Netzinfrastrukturgeräte, die sich zur Protokollierung eignen und entsprechend konfiguriert sind. IBM führt Protokolle mit Aufzeichnungen über i) erfolgreiche und nicht erfolgreiche Anmeldeversuche, ii) erfolgreiche und nicht erfolgreiche Versuche, von einem fernen Standort aus Zugriff auf die Infrastruktur zu erlangen, iii) Zugriffsversuche zum Aktualisieren der Betriebssystemressourcen und iv) Aktivitäten, die unter Verwendung der Berechtigung eines System- oder Sicherheitsadministrators durchgeführt werden.

2.5 Physische Sicherheit

Der Zutritt zu IBM Rechenzentren und Rechenzentren, die IBM von Dritten bereitgestellt werden, ist auf autorisierte Personen beschränkt. Der Zugang zur IBM Cloud-Service-Umgebung ist durch Mehrfaktorauthentifizierung gesichert. Dies schließt einen eindeutigen Zugangscode sowie biometrische Prüfung, Sicherheitspersonal rund um die Uhr (24x7), einen Wachdienst und Videoüberwachung ein. Das unbefugte Anzeigen, Kopieren, Ändern oder Entfernen von Medien, auf denen sich Kundendaten befinden, ist untersagt. Austauschbare Medien, auf denen Kundendaten gespeichert sind (einschließlich Thumb-Drives, CDs und DVDs) werden mit mindestens 256-Bit-AES-Verschlüsselung (oder einem gleichwertigen Verfahren) verschlüsselt. Auf den von IBM ausgegebenen Laptops und Workstations muss Festplattenverschlüsselung (PGP) eingerichtet sein und für den Zugriff auf sensitive Daten oder Kundendaten sind ggf. besondere Zugriffsberechtigungen erforderlich. Austauschbare Medien und mobile Einheiten (wie z. B. Datenträger, USB-Laufwerke, DVDs, Sicherungsbänder, Drucker und Laptops), auf denen sich Kundendaten befinden, werden von IBM vernichtet, oder die auf solchen physischen Medien befindlichen Kundendaten werden vor der Wiederverwendung der Medien unleserlich gemacht und sind mit technischen Mitteln nicht wiederherstellbar. Damit Papierabfall nicht gelesen werden kann, wird er geschreddert und auf sichere und vertrauliche Weise entsorgt.

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 (früher SAS 70) 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. Sicherheitsprüfungen, das regelmäßige Einspielen von Sicherheitspatches sowie Kennwortmanagement und -kontrolle sind Bestandteil der Sicherheitsrichtlinien. Sowohl IBM Mitarbeiter als auch externe Mitarbeiter müssen einmal pro Jahr an Sicherheitsschulungen und Sensibilisierungstrainings teilnehmen. Die Mitarbeiter werden an ihre Zielvorgaben erinnert und auf ihre Verantwortung zur Einhaltung der Unternehmensethik, der Vertraulichkeit und der IBM Sicherheitsverpflichtungen hingewiesen.

3. Service-Level-Ziele

IBM ist bestrebt, den Cloud-Service mit einer Verfügbarkeit von 99 Prozent bereitzustellen. Service-Level-Ziele stellen keine vertragliche Verpflichtung dar, sondern sind lediglich Zielsetzungen, die das IBM Customer-Support-Team versucht, durch seine Prozesse, Technologien und Mitarbeiter zu erreichen oder zu übertreffen.

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. „Eine Million Serveraufrufe“ (Million Server Calls = MSCs) ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Serveraufruf umfasst Daten, die infolge eines markierten („getaggten“) Ereignisses, das von einem zurückverfolgten Besucher ausgelöst wird, für eine einzige Entitäts-ID zur Verarbeitung an den Cloud-Service übergeben werden. Von unterschiedlichen Entitäts-IDs verarbeitete Serveraufrufe werden jeweils als separate Serveraufrufe gezählt. Eine Entitäts-ID trennt und/oder steuert die Zugriffsrechte auf die Daten im Cloud-Service, die verarbeitete Daten einer einzelnen oder mehrerer Websites des Kunden umfassen können. Jede MSC-Berechtigung

entspricht einer (1) Million Serveraufrufe. Der Kunde muss ausreichende MSC-Berechtigungen erwerben, um die Anzahl der Serveraufrufe abzudecken, die während des im Auftragsdokument angegebenen Abrechnungszeitraums verarbeitet werden.

4.2 Gebühren und Abrechnung

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

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 an einen 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, das 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 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, in dem die Beendigung wirksam wurde, berechnet.

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 das Cloud-Service-Angebot und die Aktivierungssoftware erbracht. Die technische Unterstützung ist Bestandteil des Cloud-Service und nicht als separates Angebot erhältlich.

Informationen zur technischen Unterstützung sind auf der folgenden Website zu finden: http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

7. Aktivierungssoftware

a. Dieses Cloud-Service-Angebot kann Aktivierungssoftware enthalten. Die Aktivierungssoftware darf nur in Verbindung mit dem Cloud-Service während der Laufzeit des Cloud-Service verwendet werden. Falls die Aktivierungssoftware Beispielcode enthält, hat der Kunde außerdem das Recht, abgeleitete Werke des Beispielcodes zu erstellen und in Übereinstimmung mit den hierunter gewährten Berechtigungen zu nutzen. Die Aktivierungssoftware wird entsprechend dem Service-Level-Agreement (sofern vorhanden) als Komponente des Cloud-Service bereitgestellt, aber ohne Wartung (auf „as-is“-Basis).

8. Zusätzliche Informationen

8.1 Berechtigungsdetails

Folgendes ist Bestandteil der Subscription-Gebühr für IBM Digital Data Exchange:

a. Es wird eine einzige Instanz von IBM Digital Data Exchange zur Verfügung gestellt.

b. Standardmäßig werden bis zu fünf (5) Stunden remote geleisteter Implementierungsservices für das erstmalige Onboarding des Kunden in IBM Digital Data Exchange bereitgestellt. Die Services enden 90 Tage nach dem Datum, an dem der Kunde von IBM darüber benachrichtigt wird, dass sein Zugriff auf den Cloud-Service freigeschaltet ist, unabhängig davon, ob das Stundenkontingent ausgeschöpft wurde.

8.2 Datenschutzhinweis und -richtlinien

Der Kunde erklärt sich damit einverstanden, (i) einen deutlich sichtbaren Link zu den für seine Website geltenden Nutzungsbedingungen und Datenschutzrichtlinien bereitzustellen, einschließlich eines Links zu den von ihm angewendeten Datenerfassungs- und Nutzungspraktiken sowie zu denjenigen von IBM (http://www.ibm.com/software/marketing-solutions/privacy/index.html); (ii) darauf hinzuweisen, dass auf dem Computer des Besuchers von IBM im Namen des Kunden Cookies sowie Clear GIFs bzw. Web-Beacons abgelegt werden, und eine Erklärung über den Zweck und die Verwendung solcher Technologien mitzuliefern; und (iii) vom Besucher der Website dessen Zustimmung einzuholen, bevor Cookies sowie Clear GIFs bzw. Web-Beacons vom Kunden oder von IBM im Namen des Kunden auf den Geräten des Website-Besuchers abgelegt werden, soweit dies gesetzlich gefordert wird.

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für die Cloud-Services über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der Nutzung der Cloud-Services im Zusammenhang stehen. Auf diese Weise kann IBM statistische Daten und Informationen über die Effektivität der Cloud-Services 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 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.

8.3 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.