IBM Trusteer Rapport

Diese Servicebeschreibung beschreibt den Cloud-Service. Die anwendbaren Auftragsdokumente enthalten Preisangaben und weitere Einzelheiten zur Bestellung des Kunden.

1. Cloud-Service

IBM Trusteer Rapport ist eine innovative Lösung zum Schutz von Endpunkten, um Benutzer vor Malware- und Phishing-Attacken zu schützen.

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl.

1.1.1 IBM Trusteer Rapport for Retail und/oder IBM Trusteer Rapport for Business („Trusteer Rapport“)

Trusteer Rapport bietet Schutz vor Phishing-Attacken und Man-in-the-Browser-Attacken (MitB). Mit einem globalen Netzwerk bestehend aus mehreren zehn Millionen Endpunkten erfasst IBM Trusteer Rapport weltweit relevante Informationen über aktive Phishing- und Malware-Attacken auf Unternehmen. IBM Trusteer Rapport wendet Verhaltensalgorithmen an, die darauf abzielen, Phishing-Attacken zu blockieren sowie die Installation und Ausführung von MitB-Malware-Stämmen zu verhindern.

Dieser Cloud-Service ist mit der Gebührenmetrik erhältlich, die auf berechtigten Teilnehmern basiert. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern verkauft.

Dieses Cloud-Service-Angebot beinhaltet Folgendes:

a. Trusteer Management Application („TMA“):

   Die TMA wird über die in der Cloud gehostete IBM Trusteer-Umgebung zur Verfügung gestellt, über die der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) (i) bestimmte Ereignisdatenberichte und Risikobewertungen anzeigen und herunterladen sowie (ii) die Konfiguration der Client-Software für Kontoinhaber (wie nachstehend definiert) anzeigen kann. Die Client-Software für Kontoinhaber darf vom Kunden nur über den Trusteer Splash oder die Rapport-API weitergegeben werden. Die Nutzung dieser Software für unternehmensinterne Zwecke des Kunden oder zur Verwendung durch Mitarbeiter des Kunden (außer zum persönlichen Gebrauch der Mitarbeiter) ist nicht zulässig. Für die Zwecke dieser Servicebeschreibung bezieht sich der Begriff „Kontoinhaber“ auf den Endbenutzer des Kunden, der die Clientaktivierungssoftware installiert, die Endbenutzerlizenzvereinbarung („EULA“) akzeptiert und sich mindestens einmal bei der Retail- oder Business-Anwendung authentifiziert hat, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat. Der Begriff „Client-Software für Kontoinhaber“ bezieht sich auf die Clientaktivierungssoftware von IBM Trusteer Rapport oder jede andere Clientaktivierungssoftware, die mit einigen Cloud-Services für die Installation auf dem Gerät des Endbenutzers bereitgestellt wird. IBM Trusteer Pinpoint Detect und IBM Trusteer Pinpoint Verify werden als Teil der TMA-Anmeldung verwendet. IBM kann den Kunden auf Online-Support-Portalen von IBM öffentlich bekannt geben, um den Endbenutzern des Kunden das ordnungsgemäße Herunterladen und Installieren der Client-Software für Kontoinhaber, die im Rahmen des Cloud-Service verfügbar ist, zu ermöglichen.

b. Web-Script:

   Für den Zugriff auf eine Website zum Aufruf oder zur Verwendung des Cloud-Service.

c. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die von der Client-Software für Kontoinhaber infolge der Online-Interaktionen der Kontoinhaber mit der Business- oder Retail-Anwendung generiert werden, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat. Die Ereignisdaten werden von der Client-Software für Kontoinhaber übertragen, die auf den Geräten der berechtigten Teilnehmer ausgeführt wird, die die EULA akzeptiert und sich mindestens einmal bei der Business- oder Retail-Anwendung des Kunden authentifiziert haben, und sofern die Konfiguration des Kunden die betreffenden Benutzer-IDs enthält.

d. Trusteer Splash:

Über die Trusteer Splash-Marketing-Plattform wird den berechtigten Teilnehmern, die auf die Business- und/oder Retail-Anwendungen zugreifen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, die Client-Software für Kontoinhaber zum Download angeboten. Der Kunde kann eine Splash-Vorlage aus einer Reihe verfügbarer Vorlagen auswählen. Eine Splash-Anpassung kann unter einem separaten Vertrag oder einer Leistungsbeschreibung vereinbart werden.

Der Kunde kann seine Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA und dem Trusteer Splash bereitstellen, damit diese in der Client-Software für Kontoinhaber und/oder auf den von IBM im Auftrag des Kunden gehosteten Landing-Pages dargestellt werden. Die Marken, Logos oder Symbole werden von IBM ausschließlich in den vom Kunden angegebenen Kontexten verwendet.

Der Kunde muss eine Subscription für den Cloud-Service „IBM Trusteer Rapport Mandatory Service“ erwerben, wenn er die Bereitstellung der Client-Software für Kontoinhaber in irgendeiner Form erzwingen möchte.

Als zwingende Bereitstellung der Client-Software für Kontoinhaber werden alle Arten der Bereitstellung durch Mechanismen oder Verfahren angesehen, die einen berechtigten Teilnehmer direkt oder indirekt zum Download der Client-Software für Kontoinhaber zwingen, sowie alle Methoden, Tools, Prozeduren, Vereinbarungen oder Mechanismen, die die Umgehung der Lizenzierungsanforderungen für die zwingende Bereitstellung der Client-Software für Kontoinhaber ermöglichen und von IBM weder erstellt noch genehmigt wurden.

1.2 Optionale Services

1.2.1 Zusätzliche Cloud-Services für IBM Trusteer Rapport

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Rapport II for Business:

- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Additional Applications for Business

b. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Rapport II for Retail:

- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail

Für jedes der Business- und Retail-Add-ons zu den IBM Trusteer Rapport-Cloud-Services, mit Ausnahme der IBM Trusteer Rapport Mandatory Service-Add-ons, ist ein zugehöriges Premium-Support-Produkt gegen Zahlung einer zusätzlichen Gebühr erhältlich.

Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind, ist eine Subscription für IBM Trusteer Rapport II for Business oder IBM Trusteer Rapport II for Retail.

1.2.2 Optionale zusätzliche Cloud-Services für IBM Trusteer Rapport II for Business und/oder IBM Trusteer Rapport II for Retail

Voraussetzung für die im Folgenden aufgelisteten zusätzlichen Cloud-Services ist eine Subscription für die IBM Trusteer Rapport II-Cloud-Services. Ist der Cloud-Service als „for Business“ gekennzeichnet, dann müssen die zusätzlich erworbenen Cloud-Services ebenfalls als „for Business“ gekennzeichnet sein. Ist der Cloud-Service als „for Retail“ gekennzeichnet, dann müssen die zusätzlich erworbenen Cloud-Services ebenfalls als „for Retail“ gekennzeichnet sein. Der Kunde erhält Ereignisdaten von den berechtigten Teilnehmern oder den Clienteinheiten, die die Client-Software für Kontoinhaber ausführen, wenn diese die EULA akzeptiert, sich mindestens einmal bei der Business- und/oder Retail-Anwendung des Kunden authentifiziert haben und die Konfiguration des Kunden Benutzer-IDs erfasst.

1.2.3 IBM Trusteer Rapport Fraud Feeds for Business und/oder IBM Trusteer Rapport Fraud Feeds for Retail

Bei Erwerb einer Subscription für diesen Add-on-Cloud-Service kann der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) die TMA verwenden, um die vom Cloud-Service Trusteer Rapport generierten Bedrohungsdaten (Threat Feeds) anzuzeigen, zu subskribieren und deren Zustellung zu konfigurieren. Die Bedrohungsdaten können per E-Mail an bestimmte E-Mail-Adressen oder über SFTP als Textdateien gesendet werden.

Für dieses Angebot kommt nur die Gebührenmetrik zur Anwendung, die auf berechtigten Teilnehmern basiert.

1.2.4 IBM Trusteer Rapport Phishing Protection for Business und/oder IBM Trusteer Rapport Phishing Protection for Retail

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Benachrichtigungen über Ereignisdaten zu empfangen, die sich auf die Eingabe der Anmeldeinformationen eines Kontoinhabers auf mutmaßlichen Phishing-Sites oder potenziell betrügerischen Sites beziehen. Wenn seriöse Online-Anwendungen (URLs) fälschlicherweise als Phishing-Sites markiert sind, warnt der Cloud-Service die Kontoinhaber ggf. vor einer Phishing-Site, obwohl es sich um eine seriöse Site handelt. In solchen Fällen muss der Kunde IBM den Fehler melden, woraufhin der Fehler von IBM behoben wird. Diese Maßnahme ist der einzige Abhilfeanspruch des Kunden für einen solchen Fehler.

Für diesen Cloud-Service kommen die Gebührenmetriken zur Anwendung, die auf berechtigten Teilnehmern oder auf Clienteinheiten basieren. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verkauft.

Für diese Cloud-Services kann Premium Support unter den Gebührenmetriken erworben werden, die auf berechtigten Teilnehmern oder auf Clienteinheiten basieren. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verkauft.

1.2.5 IBM Trusteer Rapport Mandatory Service for Business und/oder IBM Trusteer Rapport Mandatory Service for Retail

Der Kunde kann eine Instanz der Trusteer Splash-Marketing-Plattform verwenden, um den Download der Client-Software für Kontoinhaber für berechtigte Teilnehmer zu erzwingen, die auf die Business- und/oder Retail-Anwendungen zugreifen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

IBM Trusteer Rapport Premium Support for Business ist die Voraussetzung für IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail ist die Voraussetzung für IBM Security Rapport Mandatory Service for Retail.

Der Kunde kann die zusätzliche Funktionalität des IBM Trusteer Rapport Mandatory Service nur implementieren, wenn dieser Service für die Nutzung mit der Retail- oder Business-Anwendung bestellt und konfiguriert wurde, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

Für diesen Cloud-Service kommt die Gebührenmetrik zur Anwendung, die auf berechtigten Teilnehmern basiert. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern verkauft.

1.2.6 IBM Trusteer Rapport Additional Applications for Business und/oder IBM Trusteer Rapport Additional Applications for Retail

Soll IBM Trusteer Rapport II for Business nach der Bereitstellung für eine einzelne Business-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für den Cloud-Service IBM Trusteer Rapport Additional Applications for Business erworben werden. Soll IBM Trusteer Rapport II for Retail nach der Bereitstellung für eine einzelne Retail-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für den Cloud-Service IBM Trusteer Rapport Additional Applications for Retail erworben werden.

1.3 Acceleration Services

1.3.1 IBM Trusteer Rapport Large Redeployment und/oder IBM Trusteer Rapport Small Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und infolgedessen Änderungen an ihrer Bereitstellung von IBM Trusteer Rapport II benötigen, müssen den Cloud-Service IBM Trusteer Rapport Redeployment erwerben.

Eine erneute Bereitstellung kann erforderlich sein, wenn der Kunde die Domäne oder Host-URL der Anwendung geändert hat, Änderungen an der Splash-Konfiguration vorgenommen hat oder auf eine neue Online-Banking-Plattform umzieht.

Während der 6-monatigen Übergangszeit für die erneute Bereitstellung hat der Kunde auf Eins-zu-eins-Basis Anspruch auf zusätzliche Anwendungen, die neben den bereits per Subscription erworbenen Anwendungen ausgeführt werden können.

IBM Trusteer Rapport Large Redeployment gilt für Umgebungen mit mehr als 20.000 Benutzern und IBM Trusteer Rapport Small Redeployment für Umgebungen mit bis zu 20.000 Benutzern.

2. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung von IBM unter http://ibm.com/dpa (EB-AV) und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet(s), nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Datenschutzinformationen für die Cloud-Services und deren Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungstätigkeiten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Die EB-AV finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) oder ii) eines der unter http://ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

Dazu ist anzumerken, dass in den Datenblättern im Allgemeinen alle Standorte aufgelistet werden, an denen IBM (sowie die externen Unterauftragsverarbeiter) personenbezogene Daten hosten und verarbeiten, ungeachtet des Rechenzentrums, von dem die Services erbracht werden. Eine Liste der Hosting- und Verarbeitungsstandorte, die dem Rechenzentrum zugeordnet sind, von dem die Services erbracht werden, ist in Abschnitt 5.2 (Zusätzliche Informationen über den Verarbeitungsstandort) zu finden.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

3. Service-Levels und technische Unterstützung

3.1 Service-Level-Agreement

IBM stellt dem Kunden das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) bereit. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service anwenden (siehe die nachstehende Tabelle). Der Prozentsatz der Verfügbarkeit wird berechnet als Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Serviceausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die Definition von Serviceausfall, der Prozess zur Bearbeitung von Ansprüchen und die Kontaktaufnahme mit IBM bei Problemen mit der Serviceverfügbarkeit sind im IBM Cloud Service-Supporthandbuch unter https://www.ibm.com/software/support/saas_support_overview.html enthalten.

Verfügbarkeit	Gutschrift (in Prozent (%) der monatlichen Subscription-Gebühr*)
Unter 99,9 %	2 %
Unter 99,0 %	5 %
Unter 95,0 %	10 %

* Die Subscription-Gebühr ist der vertraglich vereinbarte Preis für den Monat, der Gegenstand des Anspruchs ist.

3.2 Technische Unterstützung

Eine Beschreibung der technischen Unterstützung für den Cloud-Service, einschließlich Support-Kontaktinformationen, Fehlerklassen, Unterstützungszeiten, Reaktionszeiten und sonstiger Unterstützungsinformationen und -prozesse, finden Sie durch Auswahl des Cloud-Service im IBM Support Guide, der unter https://www.ibm.com/support/home/pages/support-guide/ verfügbar ist.

Premium Support:

Eine Premium Support-Subscription ist gegen Aufpreis für den Cloud-Service verfügbar und umfasst Folgendes:

- Unterstützung rund um die Uhr (24x7) für alle Fehlerklassen
- Der Support ist direkt per Telefon und Rückrufanfrage erreichbar
- Die Kunden und ihre berechtigten Teilnehmer können Support-Tickets elektronisch einreichen, wie im Software as a Service [SaaS] Support Handbook ausführlich beschrieben
- Über das Kundenunterstützungsportal unter http://www.ibm.com/software/security/trusteer/support/ haben die Kunden Zugriff auf Meldungen, Dokumente, Fallberichte und häufig gestellte Fragen (FAQs).

4. Gebühren

4.1 Gebührenmetriken

Die Gebührenmetriken für den Cloud-Service sind im Auftragsdokument angegeben.

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit den Cloud-Services.
- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „Clienteinheit“ ist jede Einheit, die Ausführungsbefehle, Prozeduren oder Anwendungen von einer Serverumgebung, die auf die Cloud-Services zugreift, anfordert oder empfängt.
- „Anwendung“ ist ein eindeutig benanntes Softwareprogramm, das von den Cloud-Services entwickelt oder für den Zugriff auf die Cloud-Services und zu ihrer Verwendung zur Verfügung gestellt wurde.

4.2 Gebühren für Remote Services

Ein Remote Service endet 90 Tage nach dem Erwerb, unabhängig davon, ob er in Anspruch genommen wurde.

5. Zusätzliche Bedingungen

Für Vereinbarungen für Cloud-Services (oder vergleichbare Cloud-Basisvereinbarungen), die vor dem 1. Januar 2019 unterzeichnet wurden, finden die Bedingungen unter https://www.ibm.com/acs Anwendung.

5.1 EULA und die Grundlage für die Verarbeitung von Daten betroffener Personen

Für IBM Trusteer Rapport-Cloud-Services (einschließlich Rapport Remediation oder Rapport for Mitigation, wenn die Bereitstellung in Verbindung mit den Pinpoint-Cloud-Services erfolgt): Sofern nicht abweichend vereinbart und gemäß der Verarbeitungsgrundlage, die der Kunde selbst festgelegt hat, erteilt der Kunde IBM die Berechtigung, die unter https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA verfügbare Endbenutzerlizenzvereinbarung bereitzustellen.

In Bezug auf IBM Trusteer-Cloud-Services berechtigt der Kunde IBM, als Auftragsverarbeiter des Sponsorunternehmens, das Programm für die Erfassung von Malware und Malware-Artefakten, d. h. Dateien, die mit böswilligen Aktivitäten oder mit einer ungewöhnlichen Fehlfunktion des Programms in Zusammenhang stehen, zu nutzen. IBM verwendet das Programm nicht, um Dateien mit personenbezogenen Daten des Endbenutzers abzugreifen; es könnte jedoch sein, dass die erfassten Dateien personenbezogene Daten enthalten, die von der Malware ohne die Genehmigung des Endbenutzers erfasst wurden. IBM wird 1) alle Dateien unverzüglich löschen, die für eine solche Analyse

nicht relevant sind, und 2) relevante Dateien nur für die Dauer der Analyse und auf keinen Fall länger als drei Monate aufbewahren.

5.2 Zusätzliche Informationen zum Verarbeitungsstandort

Alle personenbezogenen Daten werden an den nachstehend angegebenen Standorten gehostet und verarbeitet, auch wenn das Hosting und die Verarbeitung von den im Datenblatt angegebenen externen Unterauftragsverarbeitern durchgeführt wird:

Bei allen Services, die über das Rechenzentrum in Deutschland erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Deutschland, Israel, Irland und die Niederlande.

Bei allen Services, die über das Rechenzentrum in Japan erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Japan, Israel und Irland.

Bei allen Services, die über das Rechenzentrum in den USA erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: USA, Israel, Irland, Singapur und Australien.

Hinsichtlich aller Services, die über Rechenzentren in Deutschland, Japan und den USA erbracht werden, können zusätzlich zu den obigen Standorten unterstützende Daten in Deutschland und Frankreich von Salesforce.Com als externem Unterauftragsverarbeiter von IBM gehostet und verarbeitet werden.

IBM Trusteer-Support- und Kontowartungsservices können bei Bedarf ebenfalls erbracht werden und richten sich nach der Verfügbarkeit der entsprechenden IBM Mitarbeiter, dem Standort des Kunden und dem Rechenzentrum, in dem die Daten gehostet sind.

5.3 Daten des Kontoinhabers

Zur Erläuterung: Falls mehr als ein IBM Kunde mit der Client-Software für Kontoinhaber eines bestimmten Kontoinhabers verbunden ist (solche IBM Kunden werden als „Verbundene Kunden“ (Affiliated Customers) bezeichnet) und die Services unter dieser Servicebeschreibung von IBM für diese verbundenen Kunden über Rechenzentren in anderen Regionen erbracht werden, dann können die Daten des Kontoinhabers an allen Standorten verarbeitet werden, die den einzelnen in Abschnitt 5.2 angegebenen Rechenzentren zugeordnet sind.

5.4 Integrierte Lösungen

Es wird ausdrücklich darauf hingewiesen, dass die verschiedenen Angebote der Marke Trusteer als integrierte Lösung implementiert sein können. Selbst wenn der Kunde einen dieser Cloud-Services kündigt, kann IBM Kundendaten aufbewahren, damit sowohl die übrigen Cloud-Services, die durch diese Servicebeschreibung abgedeckt sind, als auch andere Trusteer-Services gemäß den für sie anwendbaren Servicebeschreibungen erbracht werden können.

5.5 Aktivierungssoftware

Der Cloud-Service enthält die folgende Aktivierungssoftware:

- IBM Rapport Agents

5.6 Prüfung

Der Kunde wird i) Aufzeichnungen und Ausgaben von Systemtools aufbewahren und auf Anforderung bereitstellen, soweit dies für IBM und ihre beauftragten externen Prüfer erforderlich ist, um die Einhaltung der Vereinbarung durch den Kunden zu überprüfen, und ii) unverzüglich alle erforderlichen Berechtigungen bestellen und zu den zum jeweiligen Zeitpunkt gültigen Preisen von IBM bezahlen und andere Verbindlichkeiten, die sich aufgrund der Prüfung ergeben und in einer Rechnung von IBM angegeben sind, begleichen. Die Verpflichtungen im Rahmen dieses Abschnitts bleiben während der Laufzeit des Cloud-Service und eines Zeitraums von zwei Jahren danach in Kraft.

5.7 Datenerfassung im Rahmen der Bereitstellung

Bei der Bereitstellung des Cloud-Service können bestimmte Daten des Kunden an IBM weitergegeben werden. Richtlinien für Daten, die im Rahmen der Bereitstellung an IBM weitergegeben werden, sind in den Trusteer Deployment Guidelines zu finden, die dem Kunden zur Verfügung gestellt werden müssen.

6. Übergeordnete Bedingungen

6.1 Nutzung von Daten

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen im Abschnitt „Inhalte und Datenschutz“ der Basisbedingungen für Cloud-Services zwischen den Vertragsparteien: IBM wird die Ergebnisse, die sich aus der Nutzung des Cloud-Service durch den Kunden ergeben und sich eindeutig auf Kundeninhalte beziehen (Erkenntnisse) oder den Kunden anderweitig identifizieren, weder verwenden noch offenlegen. IBM ist jedoch berechtigt, Inhalte und andere Informationen, die sich im Rahmen des Cloud-Service aus den Inhalten ergeben, zu verwenden, sofern persönliche Kennungen entfernt wurden, sodass personenbezogene Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können. IBM wird diese Daten ausschließlich für Forschungs- und Testzwecke sowie für die Angebotsentwicklung verwenden.