IBM Trusteer Pinpoint Assure

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

1. Cloud-Service

IBM Trusteer Pinpoint Assure ist eine sichere mehrstufige Lösung, die darauf spezialisiert ist, zu verhindern, dass Personen mit betrügerischen Absichten gestohlene Identitäten verwenden, falsche Daten echten Identitäten hinzufügen oder synthetische Identitäten erstellen, die es ermöglichen, eine Gasttransaktion durchzuführen, ein ganz neues Konto zu eröffnen oder ein neues digitales Konto im Namen eines bestehenden Kunden zu eröffnen.

1.1 Angebote

1.1.1 IBM Trusteer Pinpoint Assure

Dieser Service markiert verdächtige Aktivitäten und generiert Warnungen während des Erstellungs-/Registrierungsprozesses eines neuen Kontos. Der Service überwacht den Kontoregistrierungsprozess, um betrügerische Aktivitäten aufzudecken und durch eine Frühwarnung anzuzeigen, dass es sich bei dem neuen Konto möglicherweise um einen „Mule Account“ oder um ein Konto handelt, das für Betrügereien benutzt wird. Entsprechende Nutzungsberichte sind in der Trusteer Management Application (TMA) verfügbar. IBM Trusteer Pinpoint Detect und IBM Trusteer Pinpoint Verify werden als Teil der TMA-Anmeldung verwendet.

IBM Trusteer Pinpoint Assure ist in Paketen mit 100 Verbindungen pro Jahr verfügbar.

1.2 Optionale Services

1.2.1 IBM Trusteer Pinpoint Assure Application

Wenn IBM Trusteer Pinpoint Assure für eine Anwendung bereitgestellt werden soll, muss eine Berechtigung für IBM Trusteer Pinpoint Assure Application erworben werden.

IBM Trusteer Pinpoint Assure kann pro Anwendung erworben werden.

1.2.2 IBM Trusteer Mobile Carrier Intelligence

Der Kunde muss über eine aktuelle Subscription für IBM Trusteer Pinpoint Assure verfügen, bevor er eine Subscription für diesen Cloud-Service erwirbt.

Dieser Cloud-Service erweitert IBM Trusteer Pinpoint Assure. Er bietet zusätzliche Informationen und Kontext zu Mobiltelefonnummern, die diesem Cloud-Service zur Verfügung gestellt werden, und trägt so dazu bei, das Betrugsrisiko einer bestimmten Sitzung zu ermitteln. Der Kunde kann durch eine Abfrage des Cloud-Service Merkmale einer bestimmten Mobiltelefonnummer herausfinden, z. B. Informationen über den Mobilfunkanbieter, zu dem diese Nummer gehört.

Die von diesem Cloud-Service bereitgestellten Daten zu Mobiltelefonnummern (nachfolgend „Mobile-Intelligence-Daten“ genannt) dürfen vom Kunden nur zu internen Zwecken verwendet und nur dreißig (30) Tage lang aufbewahrt werden. Nach diesem Zeitraum muss der Kunde eine erneute Abfrage des Cloud-Service bezüglich derselben Mobiltelefonnummer durchführen, um Mobile-Intelligence-Daten zu dieser Nummer zu erhalten, und kann nicht einfach die bei einer früheren Abfrage erhaltenen Mobile-Intelligence-Daten wiederverwenden. Der Kunde darf Mobile-Intelligence-Daten weder ganz noch teilweise zwischenspeichern (ausgenommen wie oben erlaubt), wiederverwenden oder in Verbindung mit Data-Mining nutzen oder archivieren.

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 5.1 (Zusätzliche Informationen über den Verarbeitungsstandort) zu finden.

IBM Trusteer Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

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 Technischer Support

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.

4. Gebühren

4.1 Gebührenmetriken

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

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Verbindung“ ist die Anbindung oder Zuordnung einer Datenbank, einer Anwendung, eines Servers oder einer anderen Art von Einheit, die für die Cloud-Services verfügbar gemacht wurden oder werden.

- „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.

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 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 (1) unterstützende Daten in Deutschland und Frankreich von Salesforce.Com als externem Unterauftragsverarbeiter von IBM gehostet und verarbeitet werden und (2) für Kunden, die es bevorzugen, Daten an Mobile Carrier Intelligence-Provider zu senden, personenbezogene Daten in den Ländern der jeweiligen externen Unterauftragsverarbeiter, die im Datenblatt aufgeführt sind, gehostet und verarbeitet werden. Ungeachtet gegenteiliger Angaben im Datenblatt haben die in Klausel (2) des unmittelbar vorangehenden Satzes angegebenen externen Unterauftragsverarbeiter unter Umständen keine Compliance-Zertifizierung für ISO 27001 oder SOC2.

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.

5.2 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.

5.3 Datenerfassung im Rahmen der Bereitstellung

Bei der Bereitstellung des Cloud-Service können bestimmte Daten des Kunden an IBM weitergegeben werden. Diese Daten dürfen keine Informationen enthalten, die es ermöglichen, bestimmte Personen zu identifizieren, oder die bestimmten Personen zugeordnet werden können. Weitere Richtlinien zu 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 (ausgenommen Erkenntnissen) ergeben, für die

Verbesserung des Cloud-Service zu verwenden. Des Weiteren ist IBM berechtigt, Bedrohungs-IDs und weitere Sicherheitsinformationen, die in Inhalten eingebettet sind, zum Zweck der Erkennung von Sicherheitsbedrohungen und zum Schutz vor Sicherheitsbedrohungen weiterzugeben.