IBM Financial Crimes Insight

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

1. Cloud-Service

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl.

1.1.1 IBM Financial Crimes Insight Basic

Dieser Cloud-Service stellt eine gemeinsame Infrastruktur und eine Reihe gemeinsamer Services bereit, auf denen die Financial Crimes Insights-Angebote basieren. IBM Financial Crimes Insight ermöglicht die erforderliche Integration zwischen Angeboten, damit die Kunden die Vorteile der integrierten Angebote zur Bekämpfung von Finanzkriminalität nutzen können.

1.1.2 IBM Financial Crimes Insight Advanced

Dieser Cloud-Service stellt dieselben Leistungen wie IBM Financial Crimes Insight Basic bereit und enthält darüber hinaus die in IBM Financial Crimes Insight – Data Science enthaltenen Leistungen.

IBM Financial Crimes Insight Basic oder IBM Financial Crimes Insight Advanced ist eine erforderliche Komponente, die die Instanz des Cloud-Service bereitstellt.

1.1.3 IBM Financial Crimes Insight Basic Non-Production

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Financial Crimes Insight Basic Non-Production als Cloudangebot.

1.1.4 IBM Financial Crimes Insight Advanced Non-Production

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Financial Crimes Insight Advanced Non-Production als Cloudangebot.

1.1.5 IBM Financial Crimes Insight Advanced BYOL

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Financial Crimes Insight Advanced als Cloudangebot. Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben. Das IBM Programm, das für das Angebot IBM Financial Crimes Insight Advanced BYOL benötigt wird, ist IBM Cloud Pak for Data Financial Crimes Insight.

1.1.6 IBM Financial Crimes Insight Advanced Non-Production BYOL

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Financial Crimes Insight Advanced Non-Production als Cloudangebot. Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben. Das IBM Programm, das für das Angebot IBM Financial Crimes Insight Advanced Non-Production BYOL benötigt wird, ist IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment.

1.1.7 IBM Financial Crimes Insight for Entity Research Negative News API

Dieser Cloud-Service nutzt Cognitive-Computing-Technologie und Advanced Analytics, um unstrukturierte Nachrichten und Medien zu dem Zweck zu durchsuchen, zu analysieren und zu priorisieren, das potenzielle Risiko von Finanzkriminalität durch eine Entität aufzudecken, indem eine Liste gefilterter und klassifizierter Artikel ausgegeben wird. Das Angebot wird für Unternehmen als API zum Aufrufen oder Einbetten in deren Workflows und Prozesse bereitgestellt.

1.1.8 IBM Financial Crimes Insight for Entity Research Enrichment API

Dieser Cloud-Service nutzt Cognitive-Computing-Technologie, um Daten aus strukturierten Quellen zu aggregieren, die Unternehmen dabei helfen, mehr über eine Entität zu verstehen, Entitäts- oder Kundendatensätze auf dem aktuellen Stand zu halten und das potenzielle Risiko von Finanzkriminalität durch eine Entität zu erkennen. Entitäten können Kunden, Kontrahenten oder Lieferanten sein. Das

Angebot wird für Unternehmen als API zum Aufrufen oder Einbetten in deren Workflows und Prozesse bereitgestellt.

1.2 Optionale Services

Zusätzlich zur Subscription für IBM Financial Crimes Insight oder IBM Financial Crimes Insight Non-Production muss der Kunde außerdem eine Subscription für einen der folgenden Cloud-Services erwerben:

1.2.1 IBM Financial Crimes Insight Data Science

Dieser Cloud-Service bietet Leistungen für die Aufbereitung von Daten und für die Erstellung, das Training und die Governance von Modellen sowie einen Datenkatalog für das Management von Unternehmensdaten und die Governance, Qualität und gemeinsame Bearbeitung von KI-Modellen.

1.2.2 IBM Financial Crimes Insight for Anti-Money Laundering

Bei IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML) werden die Ebenen der Advanced Analytics für die Überwachung von Finanzaktivitäten und die Unterstützung des Kunden bei der Identifizierung von Entitäten mit der Bereitschaft zur Durchführung von Geldwäsche eingesetzt. Anhand von demografischen, Verhaltens- und Beziehungsdaten unterstützt FCI for AML den Prozess zur Überprüfung der Kunden auf bekannte Risiken und kann zudem die Risikoabsicherung durch erklärbare Erkenntnisse über verborgene Risiken verbessern.

1.2.3 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring

Dieser Cloud-Service nutzt Daten historischer Fälle, Datenerfassung und -zusammenfassung von Nachweisen im Kontext und die Techniken des maschinellen Lernens mit dem Ziel, den Triageprozess für Alerts zu optimieren, Fehlmeldungen (False Positives) zu reduzieren, die Alertklassifizierung zu beschleunigen und die Entscheidungsfindung durch ein besseres Verständnis für Entitätsrisiken zu verbessern. Der Service ist eine zusätzliche Komponente, die zwischen die vorhandenen Transaktionsüberwachungs- und Fallmanagementsysteme der Kundeninstitution integriert werden kann.

1.2.4 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening

Dieser Cloud-Service erweitert vorhandene Systeme zur Prüfung von Sanktionslisten durch die Analyse von als verdächtig gemeldeten Transaktionen über eine konfigurierbare, erweiterbare, API-gesteuerte Pipeline. Die Transaktionsdaten werden bereinigt, syntaktisch analysiert, aufbereitet und anschließend mit heuristischen Methoden und Cognitive-Computing-Verfahren verarbeitet. Die Ergebnisse werden verwendet, um Treffer zu finden, Falschmeldungen (False Positives) festzustellen und informative, anpassbare Erkenntnisse zurückzuliefern.

1.2.5 IBM Financial Crimes Insight for Entity Research

Dieser Cloud-Service nutzt Cognitive-Computing-Technologie, um relevante Inhalte in strukturierten und unstrukturierten Datenquellen zu prüfen, zu extrahieren und zu verknüpfen, mit dem Ziel, ein besseres Verständnis der Entitäten und/oder der Risiken zu erreichen, die sich aus der Geschäftsbeziehung mit diesen ergeben, und die zur Durchführung von „KYC-Aktivitäten (KYC = Know Your Customer) erforderliche Zeit zu verringern. Die Lösung unterstützt die Automatisierung und Standardisierung der Recherche und Analyse von Kundeninformationen durch Zusammenfassen einer Vielzahl von Datenquellen. Ziel des Service ist eine höhere Qualität der KYC-Dokumente und ein verbessertes Kundenerlebnis durch Optimierung von Recherche- und Due-Diligence-Aktivitäten.

Folgende Berechtigungsoptionen stehen für den Kunden zur Wahl:

- IBM Financial Crimes Insight for Entity Research – Enterprise – jedes Ereignis ermöglicht die Untersuchung von mehr als 5 beteiligten Parteien.
- IBM Financial Crimes Insight for Entity Research – Advanced – jedes Ereignis ermöglicht die Untersuchung von bis zu 5 beteiligten Parteien.
- IBM Financial Crimes Insight for Entity Research – Basic – jedes Ereignis ermöglicht die Untersuchung von bis zu 2 beteiligten Parteien.

Eine beteiligte Partei ist jede Entität (Unternehmen/Organisation oder Person), die im Rahmen der Prüfung einer Parent Investigation gemäß der Definition in Abschnitt 4.1 untersucht werden muss. Üblicherweise kann es sich dabei um Unterschriftsberechtigte, Führungskräfte, wirtschaftliche Eigentümer (Ultimate Beneficial Owners), Mutter- oder Tochtergesellschaften innerhalb des Organigramms handeln.

Wenn die beteiligte Partei eine Entität ist, bei der jedes einzelne oder assoziierte Mitglied untersucht werden muss, dann zählt jedes einzelne oder assoziierte Mitglied als beteiligte Partei.

1.2.6 IBM Financial Crimes Insight for Entity Research with Material Change

Dieser Cloud-Service nutzt Cognitive-Computing-Technologie, um relevante Inhalte in strukturierten und unstrukturierten Datenquellen zu prüfen, zu extrahieren und zu verknüpfen, mit dem Ziel, ein besseres Verständnis der Entitäten und/oder der Risiken zu erreichen, die sich aus der Geschäftsbeziehung mit diesen ergeben, und die zur Durchführung von „KYC-Aktivitäten (KYC = Know Your Customer) erforderliche Zeit zu verringern. Die Lösung unterstützt die Automatisierung und Standardisierung der Recherche und Analyse von Kundeninformationen durch Zusammenfassen einer Vielzahl von Datenquellen. Ziel des Service ist eine höhere Qualität der KYC-Dokumente und ein verbessertes Kundenerlebnis durch Optimierung von Recherche- und Due-Diligence-Aktivitäten. Dazu gehört die Material-Change-Funktionalität, welche die planmäßige Überwachung von Entitäten auf wesentliche Unterschiede und die Benachrichtigung des Analysten ermöglicht, wenn eine Überprüfung erforderlich ist.

Folgende Berechtigungsoptionen stehen für den Kunden zur Wahl:

- IBM Financial Crimes Insight for Entity Research – Enterprise – jedes Ereignis ermöglicht die Untersuchung von mehr als 5 beteiligten Parteien.
- IBM Financial Crimes Insight for Entity Research – Advanced – jedes Ereignis ermöglicht die Untersuchung von bis zu 5 beteiligten Parteien.
- IBM Financial Crimes Insight for Entity Research – Basic – jedes Ereignis ermöglicht die Untersuchung von bis zu 2 beteiligten Parteien.

Eine beteiligte Partei ist jede Entität (Unternehmen/Organisation oder Person), die im Rahmen der Prüfung einer Parent Investigation gemäß der Definition in Abschnitt 4.1 untersucht werden muss. Üblicherweise kann es sich dabei um Unterschriftsberechtigte, Führungskräfte, wirtschaftliche Eigentümer (Ultimate Beneficial Owners), Mutter- oder Tochtergesellschaften innerhalb des Organigramms handeln. Wenn die beteiligte Partei eine Entität ist, bei der jedes einzelne oder assoziierte Mitglied untersucht werden muss, dann zählt jedes einzelne oder assoziierte Mitglied als beteiligte Partei.

1.2.7 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty

Dieser Cloud-Service unterstützt Organisationen bei der Analyse von Daten, um Risiken aufzudecken, die aus betrügerischen Forderungen resultieren, die von ihren Kunden, medizinischen Dienstleistern oder anderen Entitäten eingereicht werden, und um den kompletten Untersuchungslebenszyklus zu steuern und Ergebnisberichte zu erstellen.

1.2.8 IBM Financial Crimes Insight for Claims Fraud – Investigation

Dieser Cloud-Service unterstützt Organisationen dabei, den kompletten Untersuchungslebenszyklus von verdächtigen Aktivitäten und potenziellen Betrugsfällen zu steuern.

1.2.9 IBM Electronic Communication Surveillance Analytics on Cloud

Dieser Cloud-Service ist ein Tool, das Finanzdienstleistungsinstitute bei der effektiven Analyse und Überwachung der Interaktionsdaten von Mitarbeitern über mehrere Kanäle unterstützt, um verschiedene Muster verdächtiger Kommunikationen aufzudecken. Das Tool unterstützt das Erkennen verschiedener Muster für verdächtiges Verhalten im Bereich des Marktmissbrauchs und der Marktmanipulation. Das Tool nutzt Funktionen zur Verarbeitung natürlicher Sprache, um Textdaten zu verstehen und mehrdeutige Begriffe anhand des Kontextes zu unterscheiden. Es arbeitet außerdem mit Funktionen für die Stimmungs- und Emotionsanalyse, die zum Analysieren der Kommunikation eingesetzt werden können. Diese Funktionen sind nicht dazu bestimmt, die Persönlichkeitsmerkmale von Personen festzustellen, und führen keine entsprechende Prüfung durch. Diese Analyse fließt in die allgemeine Reasoning-Engine ein, die verschiedene Erkenntnisse miteinander verknüpft und Compliance-Managern eine Risikoeinschätzung liefert.

1.2.10 IBM Voice Surveillance Analytics on Cloud

Dieser Cloud-Service ist ein Tool, das Finanzdienstleistungsinstitute bei der Analyse und Überwachung der Sprachkommunikation von Mitarbeitern über mehrere Kanäle unterstützt, um verdächtige Aktivitäten aufzudecken. Das Tool arbeitet mit Speech-to-Text-Technologie und konvertiert menschliche Stimme in geschriebenen Text, indem maschinelles Lernen zum Erkennen von grammatikalischen und Sprachstrukturen eingesetzt wird. Es verknüpft die Speech-to-Text-Ausgabe mit den komplexen Metadaten, die vom Telefonsystem generiert werden, und wendet Sprecheridentifizierung auf den Text

an, um eine schnelle und einfache Suche nach relevanten Gesprächen und deren Wiedergabe zu ermöglichen. Die Speech-to-Text-Ausgabe wird dem Kunden zusammen mit den Metadaten in einem klar strukturierten Format verfügbar gemacht. Optional kann das Tool Funktionen zur Verarbeitung natürlicher Sprache nutzen, um semantische Metadaten aus Inhalten zu extrahieren, und linguistische Analyse, um Themen, Untertöne, Stimmungen und Emotionen zu erkennen. Diese Funktionen sind nicht dazu bestimmt, die Persönlichkeitsmerkmale von Personen festzustellen, und führen keine entsprechende Prüfung durch. Die gesamte Speech-to-Text-Konvertierung findet im Hauptspeicher („In Memory“) statt, um die Speicherung doppelter Dateien und Transkripte zu verringern. Nach der Verarbeitung bleiben keine Sprachdaten in der Cloud gespeichert.

1.2.11 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics

Dieser Cloud-Service ermöglicht Unternehmen das Identifizieren, Aggregieren und Kategorisieren von Beschwerden, Verdachtsmeldungen und anderen Aktivitäten. Er bietet Einblicke in aufkommende Fragen bezüglich des Umgangs mit ständig zunehmenden regulatorischen Anforderungen. Das Tool nutzt Advanced Analytics, um Beschwerden zu identifizieren und zu analysieren, die ansonsten von konventionellen Systemen nicht erfasst würden. Es kann strukturierte und unstrukturierte Daten aufnehmen, wie beispielsweise Kundendaten, E-Mails, Wartungshinweise, Beschwerden in Social Media und Sprachaufzeichnungen. Anschließend werden kognitive Fähigkeiten angewendet, um Beschwerdedaten zu aggregieren und aufzubereiten, um systemische Risiken zu erkennen. Das Tool arbeitet außerdem mit dynamischer Segmentierung und Zeitreihenprofilen, um Änderungen und Trends zu überwachen und vorwegzunehmen.

Um IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics verwenden zu können, muss der Kunde außerdem eine Subscription für entweder IBM Electronic Communication Surveillance Analytics on Cloud oder IBM Voice Surveillance Analytics on Cloud erwerben.

1.2.12 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Electronic Communication Surveillance Analytics on Cloud als Cloudangebot. Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben. Das IBM Programm, das für das Angebot IBM Electronic Communication Surveillance Analytics on Cloud BYOL benötigt wird, ist IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication.

1.2.13 IBM Voice Surveillance Analytics on Cloud BYOL

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Voice Surveillance Analytics on Cloud als Cloudangebot. Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben. Das IBM Programm, das für das Angebot IBM Voice Surveillance Analytics on Cloud BYOL benötigt wird, ist IBM Financial Crimes Insight for Conduct Surveillance Software – Voice.

1.2.14 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL

Dieser Cloud-Service ermöglicht dem Kunden den Zugriff auf die Funktionalität von IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics als Cloudangebot. Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben. Das IBM Programm, das für das Angebot IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL benötigt wird, ist IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics.

1.3 Acceleration Services

1.3.1 IBM Financial Crimes Insight Set-up

Die folgenden Setup-Services sind die Voraussetzung dafür, dass die jeweiligen Cloud-Services für den Kunden zur Nutzung bereitgestellt werden können:

- IBM Financial Crimes Insight for Anti-Money Laundering Set-up
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up
- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up

- IBM Financial Crimes Insight for Entity Research – Basic Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up
- IBM Financial Crimes Insight for Entity Research Negative News API Set-up
- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up
- IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up
- IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up
- IBM Surveillance Insight for Financial Services on Cloud Set-up

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://www.ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

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.

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.
- „Instanz“ ist jeder Zugriff auf eine bestimmte Konfiguration der Cloud-Services.
- „Ereignis“ ist das Auftreten eines bestimmten Vorkommnisses, das von den Cloud-Services verarbeitet wird oder mit der Nutzung der Cloud-Services in Zusammenhang steht.
    - Bei IBM Financial Crimes Insight for Anti-Money Laundering ist ein Ereignis definiert als 10 Millionen Finanztransaktionen in einem Kalendermonat.
    - Bei IBM Financial Crimes Insight for Claims Fraud – Property and Casualty und IBM Financial Crimes Insight for Claims – Investigation ist ein Ereignis definiert als das Einreichen einer Forderung. Eine „Forderung“ ist ein formeller bei einer Organisation eingereichter Antrag auf Kostenübernahme oder Entschädigung für einen abgedeckten Verlust oder Schadensfall.
    - Bei IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring ist ein Ereignis definiert als einzelner Alert oder Vorfall, der in einem Kalendermonat aus dem Ursprungssystem in den Cloud-Service aufgenommen wird. Das Ursprungssystem ist üblicherweise ein Transaktionsüberwachungssystem oder ein Fallmanagementsystem.
    - Bei IBM Financial Crimes Insight for Alert Triage – Transaction List Screening ist ein Ereignis definiert als bis zu 1.000 einzelne Alerts, die in einem Kalendermonat aus dem Ursprungssystem in den Cloud-Service aufgenommen werden. Das Ursprungssystem ist üblicherweise ein Transaktionsüberwachungssystem oder ein Fallmanagementsystem.
    - Bei IBM Financial Crimes Insight for Entity Research und IBM Financial Crimes Insight for Entity Research with Material Change ist ein Ereignis definiert als eine vom Cloud-Service in einem Kalendermonat durchgeführte Parent Investigation, einschließlich identischer wiederholter Suchvorgänge. Eine Parent Investigation ist jeder Datensatz, der nicht als Child mit einer anderen Untersuchung verknüpft ist. Ein Child ist eine beteiligte Partei (wie in Abschnitt 1.2.5 beschrieben), die nicht auf andere Weise einer Parent Investigation unterliegt.
- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „Element“ ist das Vorkommen eines bestimmten Objekts, das vom Cloud-Service verwaltet oder verarbeitet wird bzw. mit der Nutzung des Cloud-Service in Zusammenhang steht.
    - Bei IBM Voice Surveillance Analytics on Cloud entspricht ein Element einem einstündigen Voice Stream, der vom Cloud-Service an einem Kalendertag verarbeitet wird. Ein Voice Stream ist die Erfassung einer Audiokommunikation entweder in Echtzeit oder in einem Aufzeichnungsformat.
- „API-Aufruf“ ist der Aufruf der Cloud-Services über eine programmierbare Schnittstelle.
- „Entitäts-ID“ ist eine eindeutige Kennung für eine innerhalb des Cloud-Service identifizierte Entität.
- „Digitale Nachricht“ ist eine elektronische Mitteilung, die von den Cloud-Services verwaltet oder verarbeitet wird.

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 Unterstützungsprogramme

IBM Financial Crimes Insight und IBM Financial Crimes Insight Non-Production schließen den Zugriff auf bestimmte Programme („Unterstützungsprogramme“) ein, die in der Cloudumgebung implementiert werden. Der Kunde darf diese Unterstützungsprogramme nur verwenden, um Betrug, Finanzkriminalität und falsche Zahlungen abzuwenden oder anderweitige Maßnahmen zu deren Aufdeckung und/oder Verhinderung zu ergreifen.

5.1.1 Nutzungsbeschränkungen bei bestimmten Unterstützungsprogrammen

Die folgenden Unterstützungsprogramme werden mit den aufgeführten Beschränkungen zur Verfügung gestellt:

- IBM Watson Studio – Berechtigung: 5 gleichzeitig angemeldete Benutzer
- IBM Watson Machine Learning – Berechtigung: 50 Modelle
- IBM Openscale – Berechtigung: 50 Modelle
- IBM SPSS Modeler Premium – Berechtigung: 4 berechtigte Benutzer
- IBM SPSS Statistics Standard – Berechtigung: 4 berechtigte Benutzer
- Watson Explorer Advanced Edition – Berechtigung: auf der Basis von X Gigabyte wie nachstehend definiert

  Der Kunde darf Folgendes analysieren:

  - Alle im Repository des Cloud-Service gespeicherten Inhalte für die Nutzung mit Nicht-Analyseobjektgruppen (Non-Analytics Collections)
  - Bis zu 10 Gigabyte an Inhalten, die nicht im Repository des Cloud-Service gespeichert sind, für die Nutzung mit Nicht-Analyseobjektgruppen (Non-Analytics Collections)
  - 100 Gigabyte an Inhalten, die im Repository des Cloud-Service gespeichert sind, für die Nutzung mit Analyseobjektgruppen (Analytics Collections)

    Analyseobjektgruppen (Analytics Collections) sind Objektgruppen, die in der Watson Explorer Annotation Administration Console, in der Watson Explorer Content Analytics Administration Console oder über die API des Typs „Content Analytics“ oder „Analytics“ erstellt werden.

    Zu Nicht-Analyseobjektgruppen (Non-Analytics Collections) zählen alle anderen vom Cloud-Service analysierten Inhalte.
- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer – Berechtigung: 2 berechtigte Benutzer
- IBM Operational Decision Manager – Berechtigung: 1 Million Regelentscheidungen pro Monat und 1000 verwaltete Entscheidungsartefakte pro Monat

Berechtigungsdefinitionen

a. „Gleichzeitig angemeldeter Benutzer“ ist eine Person, die zu einem beliebigen Zeitpunkt auf das Unterstützungsprogramm zugreift. Ungeachtet dessen, ob die Person mehrmals zur gleichen Zeit auf das Unterstützungsprogramm zugreift, zählt sie nur als ein einziger gleichzeitig angemeldeter Benutzer.

b. „Modell“ ist ein mathematisches Modell oder ein mathematischer Algorithmus, der auf die zugrunde liegenden Daten oder den Datengenerierungsprozess für die Simulation, Erklärung oder Erstellung von Vorhersagen angewendet wird.

c. „Berechtigter Benutzer“ ist ein bestimmter Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) Zugriff auf das Unterstützungsprogramm erteilt wird.

d. „Gigabyte (GB)“ entspricht 2 hoch 30 Byte an Daten, die im Unterstützungsprogramm verarbeitet, analysiert, verwendet, gespeichert oder konfiguriert werden.

e. „Regelentscheidungen pro Monat“ ist das Ergebnis des Aufrufs eines Regelsatzes von einem Rule Execution Server, der vom Unterstützungsprogramm in einem Kalendermonat ausgeführt oder verarbeitet wird.

f. „Verwaltete Entscheidungsartefakte pro Monat“ ist ein Objekt, das vom Unterstützungsprogramm in einem Kalendermonat verwaltet wird.

5.2 Besondere Bedingungen für IBM Financial Crimes Insight BYOL

Als Voraussetzung für BYOL-Angebote (BYOL = Bring your Own Licenses) muss der Kunde zuvor entsprechende Lizenzberechtigungen für das in der folgenden Tabelle angegebene zugehörige IBM Programm erworben haben. Die Berechtigungen des Kunden für BYOL SaaS können seine Berechtigungen für das zugehörige IBM Programm in Bezug auf das nachstehend angegebene Berechtigungsverhältnis nicht überschreiten.

Im BYOL-Angebot ist Subscription und Support (S&S) für das zugehörige IBM Programm nicht eingeschlossen. Der Kunde versichert, dass er (1) die erforderlichen Lizenzberechtigungen sowie (2) S&S für das zugehörige IBM Programm erworben hat. Während der Subscription-Laufzeit des BYOL-Angebots muss der Kunde S&S für die IBM Programmberechtigungen aufrechterhalten, die in Verbindung mit den Berechtigungen für das BYOL-Angebot genutzt werden. Falls entweder die Lizenz des Kunden oder sein S&S-Vertrag für das zugehörige IBM Programm ausläuft, erlischt auch sein Recht zur Nutzung des BYOL-Angebots.

Der Kunde kann die Berechtigungen für das zugehörige IBM Programm, die der Nutzung des BYOL-Angebots zugeordnet werden, weiterhin nutzen, um das zugehörige IBM Programm gleichzeitig mit dem BYOL-Angebot für den folgenden Zeitraum bereitzustellen („Zeitraum der gleichzeitigen Nutzung“ genannt): bei Kunden mit einer Subscription-Laufzeit unter (3) Jahren darf der Zeitraum der gleichzeitigen Nutzung neunzig (90) Tage ab Beginn der erstmaligen Subscription des Kunden für das BYOL-Angebot nicht überschreiten; bei Kunden mit einer Subscription-Laufzeit von mehr als drei (3) Jahren darf der Zeitraum der gleichzeitigen Nutzung ein (1) Jahr ab Beginn der erstmaligen Subscription des Kunden für das BYOL-Angebot nicht überschreiten. Nach Ablauf des Zeitraums der gleichzeitigen Nutzung werden die Berechtigungen des Kunden für das zugehörige IBM Programm, die dem BYOL-Angebot zugeordnet sind, für die Dauer seiner Nutzung des BYOL-Angebots ausgesetzt und dürfen nicht mehr für die Bereitstellung des zugehörigen IBM Programms verwendet werden (vorbehaltlich eventuell bestehender Ausnahmen).

In der folgenden Tabelle ist angegeben, wie viele Berechtigungen für das zugehörige IBM Programm vorhanden sein müssen, damit das BYOL-Angebot unter der jeweils genannten Berechtigung genutzt werden kann. Sobald der Kunde das BYOL-Angebot erworben hat und während seiner Nutzung des BYOL-Angebots sind seine Berechtigungen für das zugehörige IBM Programm, die dem BYOL-Angebot zugeordnet sind, ausgesetzt und dürfen nicht mehr für die Bereitstellung des zugehörigen IBM Programms verwendet werden (vorbehaltlich eventuell bestehender Ausnahmen).

Zugehöriges IBM Programm	BYOL-Angebot	Verhältnis n/m*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL	Verhältnis: 1 Installation / 1 Instanz
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL	Verhältnis: 1 Installation / 1 Instanz
IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication	IBM Electronic Communication Surveillance Analytics on Cloud BYOL	Kumulative Verhältnisse: Stufe 1 (1–100 RVUs): ● 1 RVU / 1 berechtigter Teilnehmer Stufe 2 (101–235 RVUs): ● 0,9 RVUs / 1 berechtigter Teilnehmer Stufe 3 (236–435 RVUs): ● 0,8 RVUs / 1 berechtigter Teilnehmer Stufe 4 (436–585 RVUs): ● 0,6 RVUs / 1 berechtigter Teilnehmer Stufe 5 (586–835 RVUs): ● 0,5 RVUs / 1 berechtigter Teilnehmer Stufe 6 (836–1.135 RVUs): ● 0,4 RVUs / 1 berechtigter Teilnehmer Stufe 7 (1.136 und mehr RVUs): ● 0,3 RVUs / 1 berechtigter Teilnehmer
IBM Financial Crimes Insight for Conduct Surveillance Software – Voice	IBM Voice Surveillance Analytics on Cloud BYOL	Kumulative Verhältnisse: Stufe 1 (1–100 RVUs): ● 1 RVU / 1 Element Stufe 2 (101–235 RVUs): ● 0,9 RVUs / 1 Element Stufe 3 (236–435 RVUs): ● 0,8 RVUs / 1 Element Stufe 4 (436–585 RVUs): ● 0,6 RVUs / 1 Element Stufe 5 (586–835 RVUs): ● 0,5 RVUs / 1 Element Stufe 6 (836–1.135 RVUs): ● 0,4 RVUs / 1 Element

Zugehöriges IBM Programm	BYOL-Angebot	Verhältnis n/m*
		Stufe 7 (1.136 und mehr RVUs): ● 0,3 RVUs / 1 Element
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics	IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL	Kumulative Verhältnisse: Stufe 1 (1–100 RVUs): ● 5.000 RVUs / 1 digitale Nachricht Stufe 2 (101–235 RVUs): ● 4.500 RVUs / 1 digitale Nachricht Stufe 3 (236–435 RVUs): ● 4.000 RVUs / 1 digitale Nachricht Stufe 4 (436–585 RVUs): ● 3.000 RVUs / 1 digitale Nachricht Stufe 5 (586–835 RVUs): ● 2.500 RVUs / 1 digitale Nachricht Stufe 6 (836–1.135 RVUs): ● 2.000 RVUs / 1 digitale Nachricht Stufe 7 (1.136 und mehr RVUs): ● 1.500 RVUs / 1 digitale Nachricht

* „Verhältnis n/m“ bedeutet, dass der Kunde für jeweils ('n') Berechtigungen der angegebenen Metrik für das zugehörige IBM Programm die angegebene Anzahl ('m') an Berechtigungen der angegebenen Metrik für das BYOL-Angebot zuordnen kann. Falls das Ergebnis der Umrechnung von einem zugehörigen IBM Programm in ein BYOL-Angebot keine Ganzzahl ist, wird auf die nächste Ganzzahl aufgerundet.

Beispiel 1:

710 RVUs zu berechtigten Teilnehmern (BT)

(anwendbar auf IBM Trade Surveillance Analytics und IBM Electronic Communication Surveillance Analytics)

Stufe 1: wenn 710>100, dann 100/1 = 100 BT

Stufe 2: wenn 710>235, dann (235-100)/0,9 = +150 BT

Stufe 3: wenn 710>435, dann (435-235)/0,8 = +250 BT

Stufe 4: wenn 710>585, dann (585-435)/0,6 = +250 BT

Stufe 5: wenn 710>835 → nein, dann (710-585)/0,5 = +250 BT

Berechtigte Teilnehmer insgesamt: 100 + 150 + 250 + 250 + 250 = 1000

Beispiel 2:

500.000 RVUs zu digitalen Nachrichten (Paket mit 5.000)

(Anwendbar für IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics)

Stufe 1: wenn 500.000>100, dann 100/5.000 = 0,02 digitale Nachrichten

Stufe 2: wenn 500.000>235, dann (235-100)/4.500 = + 0,03 digitale Nachrichten

Stufe 3: wenn 500.000>435 → dann (435-235)/4.000 = + 0,05 digitale Nachrichten

Stufe 4: wenn 500.000>585 → dann (585-435)/3.000 = + 0,05 digitale Nachrichten

Stufe 5: wenn 500.000>835 → dann (835-585)/2.500 = + 0,1 digitale Nachrichten

Stufe 6: wenn 500.000>1.135 → dann (1.135-835)/2.000 = + 0,15 digitale Nachrichten

Stufe 7: wenn 500.000>1.135 → dann (500.000-1.135)/1.500 = + 99,6 digitale Nachrichten

Digitale Nachrichten insgesamt: 0,02 + 0,03 + 0,05 + 0,1 + 0,15 + 99,6 = 100 digitale Nachrichten

5.3 Suchergebnisse

Der Kunde bestätigt, dass die in den Berichten, die im Rahmen der hierin beschriebenen Cloud-Services generiert werden, enthaltenen oder referenzierten Suchergebnisse („Suchergebnisse“) Daten oder Inhalte enthalten können, die Dritten gehören, und dass IBM diese Suchergebnisse oder Inhalte weder verkauft noch diesbezügliche Lizenzen oder andere Rechte erteilt. Bei diesen Cloud-Services werden Suchergebnisse als Inhalte betrachtet.

5.4 Ablauf des Cloud-Service

Vor Ablauf oder Beendigung des Cloud-Service können Daten vom Kunden über die vom Cloud-Service bereitgestellten Berichterstellungs- oder Exportfunktionen extrahiert werden. Kundenspezifische Datenextraktionsservices werden unter einer separaten Vereinbarung zur Verfügung gestellt.

Wenn IBM innerhalb von 30 Tagen nach dem Ablauf- oder Beendigungsdatum des Cloud-Service eine entsprechende Unterstützungsanfrage des Kunden erhält, wird IBM dem Kunden eine elektronische Kopie seiner Inhalte im nativen Anwendungsformat zukommen lassen.