IBM Security Trusteer Fraud Protection

Die Nutzungsbedingungen bestehen aus diesen IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen (nachfolgend „SaaS-spezifische Angebotsbedingungen“ genannt) und einem Dokument mit dem Titel IBM Nutzungsbedingungen – Allgemeine Bedingungen (nachfolgend „Allgemeine Bedingungen“ genannt), das unter der folgende Adresse zu finden ist: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Im Falle eines Widerspruchs haben die SaaS-spezifischen Angebotsbedingungen Vorrang vor den Allgemeinen Bedingungen. Durch die Bestellung von IBM SaaS, den Zugriff darauf oder die Nutzung von IBM SaaS erklärt der Kunde sein Einverständnis mit diesen Nutzungsbedingungen.

Die Nutzungsbedingungen unterliegen dem IBM International Passport Advantage Vertrag, dem IBM International Passport Advantage Express Vertrag oder dem IBM Internationalen Vertrag über ausgewählte IBM SaaS-Angebote (nachfolgend „Vertrag“ genannt) und bilden zusammen mit dem jeweils anwendbaren Vertrag die vollständige Vereinbarung.

1. IBM SaaS

Diese SaaS-spezifischen Angebotsbedingungen gelten für die folgenden IBM SaaS-Angebote:

1.1 IBM SaaS-Angebote für Rapport

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 IBM SaaS-Angebote für Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 IBM SaaS-Angebote für Mobile

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Gebührenmetriken

Die IBM SaaS-Angebote werden unter einer der folgenden Gebührenmetriken entsprechend der Angabe im Auftragsdokument verkauft:

a. **Berechtigter Teilnehmer** ist eine Maßeinheit für den Erwerb von IBM SaaS. Jede Einzelperson oder Entität, die zur Teilnahme an einem von IBM SaaS verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist, ist ein berechtigter Teilnehmer. Der Kunde muss ausreichende Berechtigungen erwerben, um alle berechtigten Teilnehmer abzudecken, die während des Abrechnungszeitraums, der im Auftragsdokument angegeben ist, innerhalb von IBM SaaS verwaltet oder überwacht werden.

   Die einzelnen von IBM SaaS verwalteten Servicebereitstellungsprogramme werden separat analysiert und anschließend addiert. Alle Einzelpersonen oder Entitäten, die für mehrere Servicebereitstellungsprogramme berechtigt sind, benötigen separate Berechtigungen.

   Im Rahmen dieser Angebote umfasst ein Servicebereitstellungsprogramm eine einzelne Business- oder Retail-Anwendung des Kunden mit einer Hauptanmeldeseite und den zugehörigen Seiten für die jeweilige Business- oder Retail-Anwendung. Ein berechtigter Teilnehmer ist ein Endbenutzer eines Kunden, der über Anmeldeinformationen für die Business- oder Retail-Anwendung verfügt.

b. **Clienteinheit** ist eine Maßeinheit für den Erwerb von IBM SaaS. Eine Clienteinheit ist eine Datenverarbeitungseinheit eines einzelnen Benutzers, ein Spezialsensor oder ein Telemetriegerät, das eine Reihe von Befehlen, Prozeduren oder Anwendungen zur Ausführung an ein anderes Computersystem, das üblicherweise als Server bezeichnet wird, übergibt oder von diesem zur Ausführung empfängt, Daten für den Server bereitstellt oder vom Server verwaltet wird. Mehrere Clienteinheiten können gemeinsam auf einen Server zugreifen. Eine Clienteinheit kann über gewisse Verarbeitungsfunktionen verfügen oder programmierbar sein, sodass ein Benutzer Arbeiten ausführen kann. Der Kunde muss für jede Clienteinheit Berechtigungen erwerben, die in Verbindung mit IBM SaaS ausgeführt wird, Daten an IBM SaaS liefert, von IBM SaaS bereitgestellte Services nutzt oder auf andere Weise während des Abrechnungszeitraums, der im Auftragsdokument angegeben ist, auf IBM SaaS zugreift.

3. Gebühren und Abrechnung

Der für IBM SaaS zu bezahlende Betrag ist im Auftragsdokument angegeben.

3.1 Anteilige Monatsgebühren

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

4. Compliance und Prüfung

Der Zugriff auf die IBM Security Trusteer Fraud Protection-Angebote ist auf die maximale Anzahl der berechtigten Teilnehmer oder Clienteinheiten begrenzt, die im Auftragsdokument angegeben ist. Der Kunde ist dafür verantwortlich, sicherzustellen, dass die im Auftragsdokument angegebene maximale Anzahl nicht überschritten wird.

Im Rahmen eines Audits kann geprüft werden, ob die maximale Anzahl der berechtigten Teilnehmer oder Clienteinheiten eingehalten wird.

5. Verlängerungsoptionen für die IBM SaaS-Subscription-Laufzeit

Im Auftragsdokument des Kunden ist durch folgende Optionen geregelt, ob sich das IBM SaaS-Angebot am Ende der Subscription-Laufzeit verlängert:

5.1 Automatische Verlängerung

Ist im Auftragsdokument des Kunden angegeben, dass sich die IBM SaaS-Subscription-Laufzeit automatisch verlängert, kann der Kunde die ablaufende IBM SaaS-Subscription-Laufzeit kündigen, indem er den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner mindestens neunzig (90) Tage vor dem im Auftragsdokument genannten Ablaufdatum durch schriftliche Mitteilung davon in Kenntnis setzt. Wenn IBM oder der IBM Business Partner kein solches Kündigungsschreiben vor dem Ablaufdatum erhält, wird die ablaufende Subscription-Laufzeit automatisch entweder um ein (1) Jahr oder um die im Auftragsdokument genannte ursprüngliche Subscription-Laufzeit verlängert.

5.2 Fortlaufende Abrechnung

Wird die Laufzeit gemäß dem Auftragsdokument des Kunden fortlaufend verlängert, bedeutet dies, dass der Kunde kontinuierlichen Zugriff auf IBM SaaS hat und die IBM SaaS-Nutzung fortlaufend in Rechnung gestellt wird. Um die IBM SaaS-Nutzung 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 von IBM SaaS beantragen. Bei Einstellung des Zugriffs werden dem Kunden evtl. ausstehende Zugriffsgebühren für den Monat berechnet, in dem die Beendigung wirksam wurde.

5.3 Verlängerung erforderlich

Ist im Auftragsdokument des Kunden eine befristete Laufzeit angegeben, wird IBM SaaS zum Ende der Subscription-Laufzeit abgeschaltet und der Zugriff des Kunden auf IBM SaaS entfernt. Um IBM SaaS 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

Für das IBM SaaS-Angebot steht technische Unterstützung zur Verfügung, um dem Kunden und seinen berechtigten Teilnehmern Hilfestellung bei der Nutzung von IBM SaaS zu leisten.

Bei allen Angeboten ist Standard Support in der Subscription eingeschlossen. Der Trusteer Rapport Mandatory Service ist ein Add-on zu Trusteer Rapport und setzt voraus, dass Premium Support im Rahmen der Basis-Subscription für Trusteer Rapport erworben wird.

Für jedes IBM SaaS-Angebot ist eine Premium-Support-Subscription gegen Zahlung einer zusätzlichen Gebühr erhältlich, mit Ausnahme der IBM Security Trusteer Mobile SDK-Angebote und der IBM Security Trusteer Rapport Mandatory Service-Angebote.

Standard Support:

- Unterstützung von 08:00 Uhr bis 17:00 Uhr Ortszeit
- Die Kunden und ihre berechtigten Teilnehmer können Support-Tickets elektronisch einreichen, wie im Software as a Service [SaaS] Support Handbook ausführlich beschrieben
- Die Kunden können über das Kundenunterstützungsportal unterhttp://www-01.ibm.com/software/security/trusteer/support/ auf Meldungen, Dokumente, Fallberichte und häufig gestellte Fragen (FAQs) zugreifen

- Informationen über Unterstützungsoptionen und weitere Einzelheiten sind im IBM Software as a Service [SaaS] Support Handbook unter http://www-01.ibm.com/software/support/handbook.html zu finden

Premium Support:

- Unterstützung rund um die Uhr (24x7) für alle Fehlerklassen
- Der Support ist per Telefon direkt erreichbar
- Die Kunden und ihre berechtigten Teilnehmer können Support-Tickets elektronisch einreichen, wie im Software as a Service [SaaS] Support Handbook ausführlich beschrieben
- Die Kunden können über das Kundenunterstützungsportal unterhttp://www-01.ibm.com/software/security/trusteer/support/ auf Meldungen, Dokumente, Fallberichte und häufig gestellte Fragen (FAQs) zugreifen
- Informationen über Unterstützungsoptionen und weitere Einzelheiten sind im IBM Software as a Service [SaaS] Support Handbook unter http://www-01.ibm.com/software/support/handbook.html zu finden

7. Zusätzliche Bedingungen für die IBM SaaS-Angebote

7.1 Einhaltung des Safe-Harbor-Abkommens

IBM hält sich an die Safe-Harbor-Bestimmungen, welche die Zusammenarbeit zwischen den USA und der Europäischen Union regeln und vom Handelsministerium der Vereinigten Staaten in Zusammenarbeit mit der Europäischen Kommission erarbeitet wurden. Die IBM Security Trusteer-Produkte sind in die Safe-Harbor-Zertifizierung von IBM im Rahmen des Safe-Harbor-Abkommens zwischen den USA und der EU eingeschlossen. Weitere Informationen über Safe Harbor und die Liste der an Safe Harbor beteiligten Unternehmen kann unter http://export.gov/safeharbor/ eingesehen werden.

7.2 Erhöhung der jährlichen Subscription-Gebühr des Kunden

IBM behält sich das Recht vor, die Subscription-Gebühr für die IBM SaaS-Angebote einmal innerhalb von zwölf (12) Monaten um einen von IBM festzulegenden Prozentsatz, maximal jedoch um 3 %, zu erhöhen. Die Anpassung der Subscription-Gebühr wird am Jahrestag des Startdatums der Erstlaufzeit des Vertrags wirksam. Die Gebührenanpassung hat keine Auswirkung auf die Berechtigung des Kunden für IBM SaaS oder die Gebührenmetrik, mit der IBM SaaS erworben wurde. IBM Business Partner sind von IBM unabhängig und entscheiden allein über ihre Preise und Bedingungen.

7.3 Premium Support

Premium Support darf nur für die IBM SaaS-Angebote in Anspruch genommen werden, für die der Kunde eine Subscription für das zugehörige Premium-Support-Angebot erworben hat.

7.4 Rechtmäßige Nutzung und Zustimmung

Ermächtigung zur Erfassung und Verarbeitung von Daten

Die IBM SaaS-Angebote sind dazu ausgelegt, den Kunden bei der Verbesserung seiner Sicherheitsumgebung und -daten zu unterstützen. Dabei werden von IBM SaaS Informationen über berechtigte Teilnehmer und Clienteinheiten erfasst, die mit den Business- oder Retail-Anwendungen interagieren, die der Kunde als IBM SaaS-Angebote erworben hat. Die von den IBM SaaS-Angeboten erfassten Informationen können allein oder in Kombination in einigen Rechtsordnungen als personenbezogene Daten gelten. Personenbezogene Daten sind sämtliche Informationen, die zur Identifizierung einer bestimmten Person dienen, wie z. B. Name, E-Mail-Adresse, Privatadresse oder Telefonnummer, und IBM zur Speicherung, Verarbeitung oder Übertragung im Auftrag des Kunden zur Verfügung gestellt werden.

Die Datenerfassungs- und Datenverarbeitungsverfahren können aktualisiert werden, um die Funktionalität von IBM SaaS zu verbessern. Das Dokument mit einer vollständigen Beschreibung der Datenerfassungs- und Datenverarbeitungsverfahren wird bei Bedarf aktualisiert und dem Kunden auf Anfrage zur Verfügung gestellt. Der Kunde ermächtigt IBM zur Erfassung dieser Informationen und zu deren Verarbeitung gemäß den Bestimmungen der Abschnitte „Grenzüberschreitende Datenübermittlung“ und „Datenschutz“ dieser Nutzungsbedingungen sowie des Abschnitts „Datenschutz und Datensicherheit“ der IBM Nutzungsbedingungen – Allgemeine Bedingungen.

Für IBM Security Trusteer Pinpoint-Angebote:

Folgende Daten können erfasst werden: IP-Adressen von Benutzern, verschlüsselte oder mittels Einweg-Hashfunktion verschlüsselte Benutzer-IDs, domänenweite Cookies, sofern keine Filterung erfolgt, Zugriffe auf geschützte Anwendungen und Phishing-Sites, Standorte und die auf Phishing-Sites eingegebenen Anmeldeinformationen.

Für IBM Security Trusteer Mobile SDK-Angebote und IBM Security Trusteer Mobile Browser-Angebote:

Folgende Daten können erfasst werden: IP-Adressen von Benutzern, verschlüsselte oder mittels Einweg-Hashfunktion verschlüsselte Benutzer-IDs, Standorte, Zugriffe auf geschützte Anwendungen, SIM-Karteninformationen, Gerätenamen und Informationen zur Kundenbeziehung.

Für IBM Security Trusteer Rapport-Angebote:

Folgende Daten können erfasst werden: IP-Adressen von Benutzern, verschlüsselte oder mittels Einweg-Hashfunktion verschlüsselte Benutzer-IDs, Sicherheitsereignisse, Benutzernamen und E-Mail-Adressen, die zur Kontaktaufnahme mit der IBM Kundenunterstützung angegeben wurden, Informationen zur Kundenbeziehung, verschlüsselte Kennwörter, die auf geschützten Sites eingegeben wurden, Zugriffe auf geschützte Anwendungen und Phishing-Sites, verschlüsselte Zahlungskartennummern sowie Dateien und Daten, die per Fernzugriff vom IBM Personal erfasst wurden, um vermutete Malware, schädliche Aktivitäten oder Störungen zu untersuchen.

Einverständniserklärung der betroffenen Personen:

Bei der Nutzung dieser IBM SaaS-Angebote können mehrere Gesetze oder Bestimmungen zur Anwendung kommen. Die IBM SaaS-Angebote dürfen nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde willigt ein, die IBM SaaS-Angebote gemäß den anwendbaren Gesetzen, Bestimmungen und Richtlinien zu verwenden, und übernimmt die gesamte Verantwortung für deren Einhaltung.

Für IBM Security Trusteer Pinpoint-Angebote und IBM Security Trusteer Mobile SDK-Angebote:

Der Kunde versichert, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen eingeholt hat oder einholen wird, die für die rechtmäßige Nutzung der IBM SaaS-Angebote sowie die Erfassung und Verarbeitung der Informationen durch IBM über die IBM SaaS-Angebote erforderlich sind.

Für IBM Security Trusteer Rapport-Angebote und/oder IBM Security Trusteer Mobile Browser-Angebote:

Der Kunde ermächtigt IBM, die Einverständniserklärungen einzuholen, die für die rechtmäßige Nutzung der IBM SaaS-Angebote sowie die Erfassung und Verarbeitung der Informationen gemäß der Beschreibung in der Endbenutzerlizenzvereinbarung erforderlich sind, die unter https://www.trusteer.com/support/end-user-license-agreement verfügbar ist. Falls der Kunde den Schriftverkehr mit den Endbenutzern zur Einholung der Zustimmungen selbst erledigt (und nicht IBM überlässt), versichert er, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen eingeholt hat oder einholen wird, die für die rechtmäßige Nutzung der IBM SaaS-Angebote sowie die Erfassung und Verarbeitung der Informationen durch IBM als Auftragsverarbeiter des Kunden über die IBM SaaS-Angebote erforderlich sind.

7.5 Grenzüberschreitende Datenübermittlung

Der Kunde willigt ein, dass IBM die Inhalte, einschließlich personenbezogener Daten, unter Einhaltung der einschlägigen Gesetze und Anforderungen grenzüberschreitend durch Auftragsverarbeiter und Unterauftragsverarbeiter in den folgenden Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) und in Ländern, die von der Europäischen Kommission als Länder mit einem angemessenen Schutzniveau eingestuft werden, verarbeiten lassen kann: in den USA.

7.6 Datenschutz

Wenn der Kunde personenbezogene Daten in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen oder in der Schweiz in IBM SaaS verfügbar macht oder wenn sich berechtigte Teilnehmer oder Clienteinheiten des Kunden in diesen Ländern befinden, beauftragt der Kunde als alleiniger Verantwortlicher IBM als Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten (gemäß der Definition dieser Begriffe in der EU-Richtlinie 95/46/EG). IBM wird personenbezogene Daten nur in dem Umfang verarbeiten, der zur Bereitstellung des IBM SaaS-Angebots gemäß den von IBM veröffentlichten Beschreibungen der IBM SaaS-Angebote erforderlich ist, und der Kunde stimmt zu, dass eine solche Verarbeitung seinen Anweisungen entspricht. IBM wird wesentliche Änderungen in Bezug auf den Verarbeitungsstandort oder den Schutz personenbezogener Daten im Rahmen von IBM SaaS durch

rechtzeitige Benachrichtigung bekannt geben. Der Kunde kann die derzeitige Subscription-Laufzeit für das betroffene IBM SaaS-Angebot durch schriftliche Mitteilung an IBM innerhalb von dreißig (30) Tagen nach Erhalt der Benachrichtigung über die Änderung kündigen. Der Kunde willigt ein, dass IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort*
IBM Vertragspartei	Auftragsverarbeiter	Laut Auftragsdokument
Amazon Web Services LLC	Unterauftragsverarbeiter	410 Terry Ave. N Seattle, WA 98109 Vereinigte Staaten von Amerika
Connectria Corp.	Unterauftragsverarbeiter	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Vereinigte Staaten von Amerika
IBM Israel Ltd.	Unterauftragsverarbeiter	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corporation	Unterauftragsverarbeiter	1 New Orchard Rd. Armonk, NY 10504 Vereinigte Staaten von Amerika

Der Kunde erklärt sich damit einverstanden, dass IBM nach vorheriger Mitteilung diese Länderliste ändern kann, wenn dies zur Erbringung von IBM SaaS für notwendig erachtet wird.

Der Kunde willigt ein, dass bei Services, für die während des Bereitstellungsprozesses ein Rechenzentrum in Deutschland als Verarbeitungsstandort bestimmt wurde, IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort*
IBM Vertragspartei	Auftragsverarbeiter	Laut Auftragsdokument
Amazon Web Services (Deutschland)	Unterauftragsverarbeiter	München, Deutschland
IBM Israel Ltd.	Unterauftragsverarbeiter	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Der Kunde willigt ein, dass bei Services, für die während des Bereitstellungsprozesses ein Rechenzentrum in Japan als Verarbeitungsstandort bestimmt wurde, IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort*
IBM Vertragspartei	Auftragsverarbeiter	Laut Auftragsdokument
Amazon Web Services (Japan)	Unterauftragsverarbeiter	Tokio, Japan
IBM Israel Ltd.	Unterauftragsverarbeiter	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* Die in den obigen Tabellen angegebenen Standorte enthalten die Adressen der Corporate Offices des Auftragsverarbeiters oder Unterauftragsverarbeiters. Die Rechenzentren befinden sich jeweils im angegebenen Land.

Die Vertragsparteien oder ihre verbundenen Unternehmen können in ihren jeweiligen Rollen separate Vereinbarungen basierend auf den EU-Standardvertragsklauseln gemäß dem EU-Beschluss 2010/87/EU unter Ausschluss der optionalen Klauseln abschließen. Alle Rechtsstreitigkeiten oder Verbindlichkeiten, die aus diesen Vereinbarungen entstehen, selbst wenn die Vereinbarungen zwischen verbundenen Unternehmen geschlossen wurden, werden von den Vertragsparteien so behandelt, als seien sie unter den Bedingungen der vorliegenden Vereinbarung entstanden.

Anhang A

1. IBM SaaS-Angebote

IBM bietet diese Services als eigenständige Services und Angebote oder als zusätzliche Services und Angebote an. Die vom Kunden bestellten IBM SaaS-Angebote sind in seinem Berechtigungsnachweis angegeben.

1.1 Begriffsbestimmung von Business- und Retail-Anwendung

Die IBM Security Trusteer Fraud Protection-Produkte werden für die Nutzung mit bestimmten Anwendungsarten lizenziert. Eine Anwendung ist entweder als „Retail“ oder als „Business“ definiert. Für Retail-Anwendungen und Business-Anwendungen stehen jeweils unterschiedliche Angebote zur Verfügung.

- Eine Retail-Anwendung ist eine Online-Banking-Anwendung, mobile Anwendung oder E-Commerce-Anwendung, die speziell für Endverbraucher ausgelegt ist. Nach der Richtlinie des Kunden können bestimmte kleinere Unternehmen so klassifiziert werden, dass sie zur Nutzung von Retail-Anwendungen berechtigt sind.
- Eine Business-Anwendung ist eine Online-Banking-Anwendung, mobile Anwendung oder E-Commerce-Anwendung, die für Unternehmen, institutionelle oder vergleichbare Einrichtungen ausgelegt ist, oder jede andere Anwendung, die nicht zur Kategorie der Retail-Anwendungen gehört.

1.2 IBM SaaS-Basis-Subscription-Angebote

Business-Angebote:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Retail-Angebote:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Für jedes der Business- und Retail-Angebote, mit Ausnahme der IBM Security Trusteer Mobile SDK-Angebote, ist ein zugehöriges Premium-Support-Produkt gegen Zahlung einer zusätzlichen Gebühr erhältlich.

1.3 Zusätzliche IBM SaaS-Subscription-Angebote für IBM Security Trusteer Rapport-Angebote

Zusätzlich verfügbare Angebote für IBM Security Trusteer Rapport for Business:

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

Zusätzlich verfügbare Angebote für IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

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

Eine Subscription für IBM Security Trusteer Rapport for Business oder IBM Security Trusteer Rapport for Retail ist die Voraussetzung für die zugehörigen zusätzlichen IBM SaaS-Subscription-Angebote, die in diesem Abschnitt aufgelistet sind.

1.4 Zusätzliche IBM SaaS-Subscription-Angebote für IBM Security Trusteer Pinpoint Malware Detection-Angebote

Zusätzlich verfügbare Angebote für IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition oder IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Zusätzlich verfügbare Angebote für IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition oder IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

Für alle zusätzlichen IBM SaaS-Angebote, die in diesem Abschnitt aufgelistet sind, ist eine Premium-Support-Subscription gegen Zahlung einer zusätzlichen Gebühr erhältlich.

Eine Subscription für IBM Security Trusteer Pinpoint Malware Detection for Business-Angebote oder IBM Security Trusteer Pinpoint Malware Detection for Retail-Angebote ist die Voraussetzung für die zugehörigen zusätzlichen IBM SaaS-Subscription-Angebote, die in diesem Abschnitt aufgelistet sind.

1.5 Weitere zusätzliche IBM SaaS-Subscriptions

Alle zusätzlichen IBM SaaS-Subscriptions für die obigen Basis-Subscriptions, die hierin nicht aufgelistet sind, unabhängig davon, ob sie derzeit verfügbar sind oder sich in der Entwicklung befinden, gelten nicht als Update und müssen separat erworben werden.

1.6 Begriffsbestimmungen

Kontoinhaber bezieht sich auf den Endbenutzer des Kunden, der die clientfähige Software installiert, die Endbenutzerlizenzvereinbarung („EULA“) akzeptiert und sich mindestens einmal bei der Retail- oder Business-Anwendung authentifiziert hat, die der Kunde als IBM SaaS-Angebot erworben hat.

Client-Software für Kontoinhaber bezieht sich auf die clientfähige IBM Security Trusteer Rapport-Software, die clientfähige IBM Security Trusteer Mobile Browser-Software oder jede andere clientfähige Software, die mit einigen IBM SaaS-Subscriptions zur Installation auf dem Gerät des Endbenutzers bereitgestellt wird.

Trusteer Splash bezieht sich auf den Splash, der dem Kunden basierend auf den verfügbaren Splash-Vorlagen bereitgestellt wird.

Landing-Page bezieht sich auf die von IBM gehostete Seite, die dem Kunden zusammen mit dem Kunden-Splash und der für den Download verfügbaren Client-Software für Kontoinhaber bereitgestellt wird.

2. IBM Security Trusteer Rapport-Angebote

2.1 IBM Security Trusteer Rapport for Retail und/oder IBM Security 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 Security Trusteer Rapport weltweit relevante Informationen über aktive Phishing- und Malware-Attacken auf Unternehmen. IBM Security Trusteer Rapport wendet Verhaltensalgorithmen an, die darauf abzielen, Phishing-Attacken zu blockieren sowie die Installation und Ausführung von MitB-Malware-Stämmen zu verhindern.

Dieses IBM SaaS-Angebot 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 IBM SaaS-Angebot beinhaltet Folgendes:

a. Trusteer Management Application („TMA“):

   Die TMA wird über die Cloud-Umgebung von IBM Security Trusteer zur Verfügung gestellt und bietet dem Kunden (und einer unbegrenzten Zahl seiner autorisierten Mitarbeiter) folgende Funktionen: (i) Erhalt von Ereignisdatenberichten und Risikobewertungen, (ii) Anzeigen, Konfigurieren und Definieren von Richtlinien zur Erstellung von Berichten aus Ereignisdaten sowie (iii) Anzeigen der Konfiguration der kostenlosen clientfähigen Software, die unter einer Endbenutzerlizenzvereinbarung („EULA“) frei lizenziert und zum Download auf die Desktops oder Geräte (PC/MACs) der berechtigten Teilnehmer zur Verfügung gestellt wird. Sie wird auch als Trusteer Rapport-Softwaresuite bezeichnet („Client-Software für Kontoinhaber“). 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.

b. Web-Script:

   Für den Zugriff auf eine Website zum Aufruf oder zur Verwendung der IBM SaaS-Angebote.

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, die der Kunde als IBM SaaS-Angebot erworben hat. Die Ereignisdaten werden von der Client-Software für Kontoinhaber übertragen, die auf den Geräten der berechtigten Teilnehmer ausgeführt wird, sofern diese den 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 beim Zugriff auf die Business- und/oder Retail-Anwendungen, die der Kunde als IBM SaaS-Angebote erworben hat, die Client-Software für Kontoinhaber zum Download angeboten. Der Kunde kann eine Splash-Vorlage aus einer Reihe verfügbarer Vorlagen auswählen. Unter einem separaten Vertrag oder einer separaten Leistungsbeschreibung kann eine Splash-Anpassung vereinbart werden.

Der Kunde kann Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA zur Verfügung stellen, die im Trusteer Splash und in der Client-Software für Kontoinhaber oder auf den von IBM gehosteten Landing-Pages sowie auf der IBM Security Trusteer-Website angezeigt werden können. Der Umgang mit den vom Kunden bereitgestellten Marken, Logos und Symbolen erfolgt gemäß den IBM Richtlinien für Werbung und die Nutzung von Marken.

Der Kunde muss eine Subscription für das SaaS-Angebot „IBM Security 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.

2.2 Optionale zusätzliche IBM SaaS-Angebote für IBM Security Trusteer Rapport for Business und/oder IBM Security Trusteer Rapport for Retail

Subscriptions für IBM Security Trusteer Rapport-Angebote sind die Voraussetzung für die Subscription für eines der folgenden zusätzlichen IBM SaaS-Angebote. Ist das IBM SaaS-Angebot als „for Business“ gekennzeichnet, dann muss das zusätzlich erworbene IBM SaaS-Angebot ebenfalls als „for Business“ gekennzeichnet sein. Ist das IBM SaaS-Angebot als „for Retail“ gekennzeichnet, dann muss das

zusätzlich erworbene IBM SaaS-Angebot ebenfalls als „for Retail“ gekennzeichnet sein. Der Kunde kann Ereignisdaten von den berechtigten Teilnehmern empfangen, die die Client-Software für Kontoinhaber ausführen, sofern diese den EULA akzeptiert und sich bei mindestens einer Business- und/oder Retail-Anwendung des Kunden authentifiziert haben und sofern die Konfiguration des Kunden die betreffenden Benutzer-IDs enthält.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business und/oder IBM Security Trusteer Rapport Fraud Feeds for Retail

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten über Malware-Infektionen und sonstige Endpunkt-Schwachstellen auf dem Desktop eines bestimmten Kontoinhabers zu empfangen.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business und/oder IBM Security Trusteer Rapport Phishing Protection for Retail

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Benachrichtigungen in Form von 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 IBM SaaS 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.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business und/oder IBM Security 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, die der Kunde als IBM SaaS-Angebote erworben hat.

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

IBM Security 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 Security Trusteer Rapport Mandatory Service nur implementieren, wenn dieser Service für die Nutzung mit der Retail- oder Business-Anwendung bestellt und konfiguriert wurde, die der Kunde als IBM SaaS-Angebot erworben hat.

3. IBM Security Trusteer Pinpoint-Angebote

IBM Security Trusteer Pinpoint ist ein cloudbasierter Service, der eine zusätzliche Schutzstufe bietet und dafür ausgelegt ist, Malware- und Phishing-Attacken sowie Attacken zur Kontoübernahme zu erkennen und abzuwehren. Trusteer Pinpoint kann in die Business- und/oder Retail-Anwendungen, die der Kunde als IBM SaaS-Angebote erworben hat, und in die Prozesse zur Betrugsprävention integriert werden.

Dieses IBM SaaS-Angebot beinhaltet Folgendes:

a. TMA:

   Die TMA wird über die Cloud-Umgebung von IBM Security Trusteer zur Verfügung gestellt und bietet dem Kunden (und einer unbegrenzten Zahl seiner autorisierten Mitarbeiter) folgende Funktionen: (i) Erhalt von Ereignisdatenberichten und Risikobewertungen sowie (ii) Anzeigen, Konfigurieren und Definieren von Sicherheitsrichtlinien und Richtlinien zur Erstellung von Berichten aus Ereignisdaten.

b. Web-Script und/oder APIs:

   Für die Bereitstellung auf einer Website zum Aufruf oder zur Verwendung der IBM SaaS-Angebote.

3.1 IBM Security Trusteer Pinpoint Malware Detection und IBM Security Trusteer Pinpoint Criminal Detection

Im Falle einer Malware-Erkennung durch die IBM Security Trusteer Pinpoint Malware Detection-Angebote oder der Erkennung einer Kontoübernahme durch die IBM Security Trusteer Pinpoint Criminal Detection-Angebote müssen die Anweisungen im Pinpoint Best Practices Guide befolgt werden. Der Kunde darf die IBM Security Trusteer Pinpoint Malware Detection-Angebote oder die IBM Security Trusteer Pinpoint

Criminal Detection-Angebote nicht in einer Weise verwenden, die sich auf das Verhalten des berechtigten Teilnehmers unmittelbar nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme auswirkt und beispielsweise Dritte vermuten lässt, dass die Maßnahmen des Kunden mit der Verwendung der IBM Security Trusteer Pinpoint-Angebote in Verbindung stehen (z. B. durch Meldungen, Nachrichten, Blockieren von Geräten oder Zugangssperren auf die Business- und/oder Retail-Anwendung sofort nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business und/oder IBM Security Trusteer Pinpoint Criminal Detection for Retail

Clientlose Erkennung verdächtiger Kontoübernahmeaktivitäten von Browsern, die unter Verwendung einer Geräte-ID eine Verbindung zu einer Business- oder Retail-Anwendung herstellen, Phishing-Erkennung und Erkennung des Diebstahls von Zugangsdaten durch Malware. Die IBM Security Trusteer Pinpoint Criminal Detection-Angebote bieten eine zusätzliche Schutzstufe und sind für das Erkennen von Kontoübernahmeversuchen ausgelegt. Sie übermitteln Risikobewertungen von Browsern oder mobilen Geräten (über den nativen Browser oder über die mobile Anwendung des Kunden), die auf eine Business- oder Retail-Anwendung zugreifen, direkt an den Kunden.

a. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die infolge der Online-Interaktionen der berechtigten Teilnehmer mit den Business- und/oder Retail-Anwendungen generiert werden, die der Kunde als IBM SaaS-Angebote erworben hat. Die Ereignisdaten können auch von einer Back-End-API an den Kunden übermittelt werden.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile und/oder IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile-Angebote (PPCD Mobile) bieten eine zusätzliche Schutzstufe und sind dazu ausgelegt, vor Kontoübernahme- und betrügerischen Aktivitäten zu schützen, indem sie Kontozugriffe mit krimineller Absicht erkennen und eine Empfehlung für den Kunden bereitstellen. Dieses IBM SaaS-Angebot erfasst über die PPCD Mobile-API Informationen, die sowohl von den Business- und/oder Retail-Anwendungen des Kunden als auch von den mobilen Geräten der berechtigten Teilnehmer stammen. Die IBM Security Trusteer PPCD Mobile-Angebote sind dazu ausgelegt, komplexe Informationen im Zusammenhang mit den mobilen Geräten der berechtigten Teilnehmer mit anderen Datenquellen zu korrelieren, wie beispielsweise Malware-Infizierungen und Phishing-Vorfälle in Echtzeit, die über andere in diesen Nutzungsbedingungen genannte IBM SaaS-Angebote von IBM Security Trusteer integriert sind.

Der Kunde kann in der Cloud-Umgebung von IBM Security Trusteer auf die IBM Security Trusteer PPCD Mobile-Angebote zugreifen und diese nutzen sowie Risikobewertungsdaten von den mobilen Geräten der berechtigten Teilnehmer empfangen, die infolge der Online-Interaktionen dieser mobilen Geräte mit der Business- oder Retail-Anwendung generiert werden, die der Kunde als IBM SaaS-Angebot erworben hat. Für die Zwecke dieser Angebote schließt der Begriff „mobile Geräte“ nur unterstützte Mobiltelefone und Tablets ein, aber keine PCs oder Mac-Computer.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Clientlose Erkennung von Browsern, die durch Man-in-the-Browser-Attacken (MitB) mit Finanz-Malware infiziert sind und eine Verbindung zu einer Business- und/oder Retail-Anwendung herstellen. Die IBM Security Trusteer Pinpoint Malware Detection-Angebote bieten eine zusätzliche Schutzstufe und ermöglichen es den Unternehmen, sich auf Prozesse zur Betrugsprävention zu konzentrieren, die auf der Erkennung von Malwarerisiken basieren, indem bei einer Infizierung mit MitB-Finanz-Malware Risikobewertungen und Benachrichtigungen an den Kunden gesendet werden.

a. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die infolge der Online-Interaktionen der berechtigten Teilnehmer mit den Business- und/oder Retail-Anwendungen des Kunden generiert werden.

b. Advanced Edition:

Die Advanced Editions for Business und/oder for Retail bieten zusätzliche Schutz- und Erkennungsstufen, die an die Struktur und den Ablauf der Business- und/oder Retail-Anwendungen des Kunden angepasst sind und auf die Bedrohungslandschaft, der das Unternehmen des Kunden ausgesetzt ist, abgestimmt werden können. Sie können an verschiedenen Standorten in die Business- und/oder Retail-Anwendungen des Kunden integriert werden.

Die Advanced Edition wird mit einer Mindestbestellmenge von 100.000 berechtigten Teilnehmern im Retail-Bereich und 10.000 berechtigten Teilnehmern im Business-Bereich angeboten. Dies entspricht 1.000 Paketen mit jeweils 100 berechtigten Teilnehmern für Retail-Angebote und 1.000 Paketen mit jeweils 10 berechtigten Teilnehmern für Business-Angebote.

c. Standard Edition:

Die Standard Edition for Business oder die Standard Edition for Retail ist eine Lösung, die in kurzer Zeit einsatzbereit ist und die hierin beschriebene Kernfunktionalität dieses IBM SaaS-Angebots bereitstellt.

3.2 Optionale zusätzliche IBM SaaS-Angebote für IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition und/oder IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Als Voraussetzung für die IBM Security Trusteer Rapport Remediation for Retail-Angebote muss die IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition oder die IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition erworben werden.

Als Voraussetzung für IBM Security Trusteer Pinpoint Carbon Copy for Retail muss die IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition oder die IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition erworben werden. Als Voraussetzung für IBM Security Trusteer Pinpoint Carbon Copy for Business muss die IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition oder die IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition erworben werden.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business und/oder IBM Security Trusteer Pinpoint Carbon Copy for Retail

Die IBM Security Trusteer Pinpoint Carbon Copy-Angebote bieten eine zusätzliche Schutzstufe und einen Überwachungsservice, der dabei hilft, Anmeldeinformationen berechtigter Teilnehmer zu identifizieren, die durch Phishing-Attacken auf die Retail- oder Business-Anwendungen beschädigt wurden, die der Kunde als IBM SaaS-Angebote erworben hat.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail ist dazu ausgelegt, Malware-Infizierungen durch Man-in-the-Browser-Attacken (MitB) auf betroffenen Geräten (PC/MACs) der berechtigten Teilnehmer des Kunden, die auf Ad-hoc-Basis auf die Retail-Anwendung des Kunden zugreifen, zu untersuchen, zu beheben, zu blockieren und zu entfernen, sofern die MitB-Malware-Infizierungen anhand der Ereignisdaten von IBM Security Trusteer Pinpoint Malware Detection festgestellt wurden. Der Kunde muss über eine aktuelle Subscription für den IBM Security Trusteer Pinpoint Malware Detection-Service verfügen und der Service muss derzeit für die Retail-Anwendung des Kunden ausgeführt werden. Der Kunde darf dieses IBM SaaS-Angebot nur für berechtigte Teilnehmer nutzen, die auf seine Retail-Anwendung zugreifen, und ausschließlich als Tool zum Untersuchen und Wiederherstellen eines bestimmten infizierten Geräts (PC/MAC) auf Ad-hoc-Basis verwenden. IBM Security Trusteer Rapport Remediation for Retail muss derzeit auf dem betroffenen Gerät (PC/MAC) des berechtigten Teilnehmers ausgeführt werden und der berechtigte Teilnehmer muss den EULA akzeptiert und sich mindestens einmal bei der Retail-Anwendung des Kunden authentifiziert haben und in der Konfiguration des Kunden müssen die betreffenden Benutzer-IDs enthalten sein. Dieses IBM SaaS-Angebot berechtigt den Kunden weder zur Verwendung des Trusteer Splash noch dazu, die Client-Software für Kontoinhaber auf irgendeine andere Weise allen seinen berechtigten Teilnehmern verfügbar zu machen.

4. IBM Security Trusteer Mobile-Angebote

4.1 IBM Security Trusteer Mobile Browser for Business und/oder IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser bietet eine zusätzliche Schutzstufe und sicheren Onlinezugriff über die mobilen Geräte der berechtigten Teilnehmer auf die Business- oder Retail-Anwendungen, die der Kunde als IBM SaaS-Angebote erworben hat, sowie Risikobewertungen von mobilen Geräten und Phishing-Schutz. Die Erkennung sicherer WiFi-Umgebungen ist nur für Android-Plattformen verfügbar. Für die Zwecke dieses IBM SaaS-Angebots schließt der Begriff „mobile Geräte“ Mobiltelefone und Tablets ein, aber keine Laptops oder Mac-Computer.

Über die TMA kann der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) Ereignisdaten sowie Analyse- und Statistikdaten empfangen, die sich auf Geräte beziehen, deren berechtigte Teilnehmer (i) die Client-Software für Kontoinhaber heruntergeladen haben (eine kostenlose Anwendung, die unter einer Endbenutzerlizenzvereinbarung (EULA) frei lizenziert und zum Download auf die mobilen Geräte der berechtigten Teilnehmer zur Verfügung gestellt wird) sowie (ii) die EULA akzeptiert und sich mindestens einmal bei Business- oder Retail-Anwendungen authentifiziert haben, die der Kunde als IBM SaaS-Angebote erworben hat. Der Kunde darf die Client-Software für Kontoinhaber nur über den Trusteer Splash weitergeben. Die Nutzung dieser Software für unternehmensinterne Zwecke des Kunden ist nicht zulässig.

a. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die infolge der Online-Interaktionen der mobilen Geräte mit den Business- oder Retail-Anwendungen generiert werden, die der Kunde als IBM SaaS-Angebote erworben hat.

b. Trusteer Splash:

   Über die Trusteer Splash-Marketing-Plattform wird den berechtigten Teilnehmern beim Zugriff auf die Business- und/oder Retail-Anwendungen, die der Kunde als IBM SaaS-Angebote erworben hat, die Client-Software für Kontoinhaber zum Download angeboten. Der Kunde kann eine Splash-Vorlage aus einer Reihe verfügbarer Vorlagen auswählen. Unter einem separaten Vertrag oder einer separaten Leistungsbeschreibung kann eine Splash-Anpassung vereinbart werden.

Der Kunde kann Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA zur Verfügung stellen, die im Trusteer Splash und in der Client-Software für Kontoinhaber oder auf den von IBM gehosteten Landing-Pages oder auf der IBM Security Trusteer-Website angezeigt werden können. Der Umgang mit den vom Kunden bereitgestellten Marken, Logos und Symbolen erfolgt gemäß den IBM Richtlinien für Werbung und die Nutzung von Marken.

4.2 IBM Security Trusteer Mobile SDK for Business und/oder IBM Security Trusteer Mobile SDK for Retail

Die IBM Security Trusteer Mobile SDK-Angebote sorgen für zusätzlichen Schutz, indem sie sicheren Webzugriff auf die Business- und/oder Retail-Anwendungen ermöglichen, die der Kunde als IBM SaaS-Angebote erworben hat, und bieten Risikobewertungen für Geräte sowie Pharming-Schutz. Die Erkennung sicherer WiFi-Umgebungen ist nur für Android-Plattformen verfügbar.

Die IBM Security Trusteer Mobile SDK-Angebote enthalten ein proprietäres Mobile Software Developer Kit („SDK“) (dabei handelt es sich um ein Softwarepaket, das Dokumentation, proprietäre Softwareprogrammierbibliotheken sowie weitere zugehörige Dateien und Elemente enthält, die sogenannte IBM Security Trusteer Mobile Library) sowie die „Run-time-Komponente“ oder „weiterverteilbare Komponente (Redistributable)“, einen proprietären Code, der vom IBM Security Trusteer Mobile SDK generiert wird und in die geschützten eigenständigen mobilen iOS- oder Android-Anwendungen eingebettet und integriert werden kann, die der Kunde als IBM SaaS-Angebote erworben hat („Integrierte mobile App des Kunden“).

IBM Security Trusteer Mobile SDK for Retail ist in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verfügbar und IBM Security Trusteer Mobile SDK for Business ist in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verfügbar.

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdatenberichte und Einschätzungen zu Risikobewertungen zu erhalten. Über die integrierte mobile App kann der Kunde Risikoanalyseinformationen und Informationen empfangen, die sich auf die mobilen

Geräte der berechtigten Teilnehmer beziehen, die die integrierte mobile App des Kunden heruntergeladen haben. Diese Informationen ermöglichen dem Kunden die Definition einer Betrugspräventionsrichtlinie, um Maßnahmen zur Minderung dieser Risiken durchzusetzen. Für die Zwecke dieses Angebots schließt der Begriff „mobile Geräte“ nur unterstützte Mobiltelefone und Tablets ein, aber keine PCs oder Mac-Computer.

Der Kunde darf:

a. das IBM Security Trusteer Mobile SDK ausschließlich intern für die Entwicklung der integrierten mobilen App des Kunden nutzen.

b. die weiterverteilbare Komponente (nur in Objektcodeformat) als festen, untrennbaren Bestandteil in seine integrierte mobile App einbetten. Jeder bearbeitete oder eingefügte Bestandteil der weiterverteilbaren Komponente unterliegt gemäß dieser Lizenz den Bestimmungen dieser Nutzungsbedingungen.

c. die weiterverteilbare Komponente zum Download auf die mobilen Geräte der berechtigten Teilnehmer oder des Inhabers der Clienteinheit vertreiben und weitergeben, sofern folgende Bedingungen eingehalten werden:

   - Soweit nicht ausdrücklich in dieser Vereinbarung vorgesehen, ist es dem Kunden untersagt, (1) das SDK zu verwenden, zu kopieren, zu ändern oder weiterzugeben, (2) das SDK rückumzuwandeln (reverse assemble, reverse compile), in anderer Weise zu übersetzen oder rückzuentwickeln, sofern eine solche Umwandlung nicht durch ausdrückliche gesetzliche Regelung unabdingbar vorgesehen ist, (3) das SDK zu vermieten, zu verleasen oder diesbezügliche Unterlizenzen zu erteilen; (4) Copyright- oder Notice-Dateien zu entfernen, die in der weiterverteilbaren Komponente enthalten sind, (5) dieselben Pfadnamen wie für die Dateien/Module der ursprünglichen weiterverteilbaren Komponente zu verwenden und (6) die Namen oder Marken von IBM, ihren Lizenzgebern oder Distributoren ohne ihre vorherige schriftliche Zustimmung in Verbindung mit der Vermarktung seiner integrierten mobilen App zu verwenden.
   - Die weiterverteilbare Komponente muss als fester, untrennbarer Bestandteil in die integrierte mobile App des Kunden eingebettet bleiben. Sie darf nur in Objektcodeformat vorhanden sein und muss allen Anweisungen, Instruktionen und Spezifikationen im SDK und der zugehörigen Dokumentation entsprechen. In der Endbenutzerlizenzvereinbarung für die integrierte mobile App des Kunden muss ein Hinweis für den Endbenutzer enthalten sein, dass die weiterverteilbare Komponente i) nur zur Aktivierung der integrierten mobilen App des Kunden verwendet werden darf, ii) nicht kopiert werden darf (außer für Sicherungszwecke), iii) nicht weitergegeben oder übertragen werden darf und iv) nicht rückumgewandelt (reverse assemble, reverse compile) oder in anderer Weise übersetzt werden darf, soweit nicht durch gesetzliche Regelung etwas anderes zwingend vorgeschrieben ist. Die Lizenzvereinbarung des Kunden muss die Rechte von IBM in mindestens demselben Maße schützen, wie sie durch die Bedingungen dieser Vereinbarung geschützt werden.
   - Das SDK darf nur für interne Entwicklungszwecke und Komponententests auf den angegebenen mobilen Testgeräten des Kunden eingesetzt werden. Der Kunde ist nicht berechtigt, das SDK zur Verarbeitung oder Simulation von Produktionsworkloads oder zum Testen der Skalierbarkeit von Code, Anwendungen oder Systemen zu nutzen. Er ist ferner nicht berechtigt, Teile des SDK für andere Zwecke zu verwenden.

Der Kunde trägt die Verantwortung für die gesamte technische Unterstützung seiner integrierten mobilen App sowie für sämtliche von ihm durchgeführten Bearbeitungen der weiterverteilbaren Komponenten, die gemäß diesem Dokument zulässig sind.

Der Kunde darf die weiterverteilbare Komponente und das IBM Security Mobile SDK nur zur Unterstützung seiner Nutzung des IBM SaaS-Angebots installieren und verwenden.

IBM hat Beispielanwendungen getestet, die mit den zum Lieferumfang des IBM Security Trusteer Mobile SDK gehörenden Tools für mobile Geräte („Mobile Tools“) erstellt wurden, um festzustellen, ob diese auf bestimmten Versionen von Betriebssystemplattformen für mobile Geräte von Apple (iOS), Google (Android) und anderen (gemeinsam „OS-Plattformen für mobile Geräte“ genannt) ordnungsgemäß ausgeführt werden. Die OS-Plattformen für mobile Geräte werden jedoch von Drittherstellern angeboten, befinden sich nicht unter der Kontrolle von IBM und können ohne Mitteilung an IBM geändert werden. Aus diesem Grund und ungeachtet gegenteiliger Aussagen gewährleistet IBM nicht, dass mit den Mobile Tools erstellte Anwendungen oder sonstige damit erstellte Ausgaben auf OS-Plattformen für mobile

Geräte oder auf mobilen Endgeräten ordnungsgemäß ausgeführt werden, mit diesen zusammenarbeiten oder mit diesen kompatibel sind.

Der Kunde verpflichtet sich, korrekte schriftliche Aufzeichnungen, Ausgaben von Systemtools und sonstige Systemdaten zu erstellen, aufzubewahren und IBM sowie ihren Prüfern bereitzustellen, um prüffähige Nachweise dafür zu erbringen, dass seine Nutzung des IBM Security Trusteer Mobile SDK in Übereinstimmung mit den Bestimmungen dieser Nutzungsbedingungen erfolgt.

5. Bereitstellung von IBM SaaS Fraud Protection-Angeboten

Die Basis-Subscription des Kunden umfasst die Maßnahmen, die für das Setup und die erstmalige Bereitstellung erforderlich sind, sowie die erstmalige Inbetriebnahme, die Konfiguration und die Splash-Vorlage einschließlich Testen und Schulungen.

Weitere Services können gegen Zahlung einer zusätzlichen Gebühr unter einem separaten Vertrag vereinbart werden.

Anhang B

Das folgende Service-Level-Agreement („SLA“) von IBM beinhaltet Angaben zur Verfügbarkeit von IBM SaaS und kommt zur Anwendung, sofern es im Auftragsdokument des Kunden angegeben ist.

Für den Kunden kommt die Version des SLA zur Anwendung, die bei Beginn oder bei Verlängerung seiner Subscription-Laufzeit aktuell ist. Der Kunde nimmt zur Kenntnis, dass das SLA keine Gewährleistung darstellt.

1. Begriffsbestimmungen

a. **Berechtigte Kontaktperson** ist diejenige Person, die der Kunde IBM als Ansprechpartner genannt hat und die zur Einreichung von Ansprüchen im Rahmen dieses SLA autorisiert ist.

b. **Gutschrift für Ausfallzeiten** ist der Schadensersatz, den IBM für einen bestätigten Anspruch leistet. Die Gutschrift für Ausfallzeiten wird in Form einer Gutschrift oder eines Nachlasses gewährt und mit einer zukünftigen Rechnung über Subscription-Gebühren für das IBM SaaS-Angebot verrechnet.

c. **Anspruch** ist ein von der berechtigten Kontaktperson des Kunden gemäß diesem SLA bei IBM eingereichter Anspruch, der besagt, dass ein Service-Level während eines Vertragsmonats nicht erfüllt wurde.

d. **Vertragsmonat** ist jeder volle Monat während der IBM SaaS-Laufzeit, der um 00:00 Uhr MEZ am ersten Kalendertag des Monats beginnt und um 23:59 Uhr MEZ am letzten Kalendertag des Monats endet.

e. **Kunde** ist eine juristische Person, die IBM SaaS direkt von IBM bezieht und keine wesentlichen Verpflichtungen, einschließlich Zahlungsverpflichtungen, aus ihrem Vertrag mit IBM für IBM SaaS verletzt hat.

f. **Ausfallzeit** ist ein Zeitraum, in dem die Verarbeitung auf dem Produktionssystem für den Service gestoppt ist und die Benutzer des Kunden nicht in der Lage sind, alle Aspekte des Service zu nutzen, für die sie berechtigt sind. Ausfallzeiten umfassen nicht den Zeitraum, in dem der Service aus einem der folgenden Gründe nicht verfügbar ist:

- Geplante Systemausfallzeiten
- Höhere Gewalt
- Probleme mit Anwendungen, Geräten oder Daten des Kunden oder Dritter
- Handlungen oder Unterlassungen des Kunden oder Dritter (einschließlich der Personen, die sich mithilfe von Kennwörtern oder Geräten des Kunden Zugriff auf IBM SaaS verschaffen)
- Nichtbeachtung erforderlicher Systemkonfigurationen und unterstützter Plattformen für den Zugriff auf IBM SaaS
- Unterbrechungen, die dadurch verursacht werden, dass IBM Entwürfe, Spezifikationen oder Anweisungen des Kunden oder eines in seinem Auftrag handelnden Dritten zu beachten hat

g. **Vorfall** ist ein Umstand oder eine Reihe von Umständen, die zur Nichteinhaltung eines Service-Levels geführt haben.

h. **Höhere Gewalt** sind unabwendbare Ereignisse, Terrorismus, Streiks, Brände, Überflutungen, Erdbeben, Unruhen, Kriege, staatliche Maßnahmen, Anordnungen und Beschränkungen, Viren, Denial-of-Service-Attacken sowie arglistiges Verhalten, Strom- und Netzausfälle oder sonstige Ursachen für die Nichtverfügbarkeit von IBM SaaS, die außerhalb des angemessenen Einflussbereichs von IBM liegen.

i. **Geplante Systemausfallzeiten** sind vorab geplante Unterbrechungen von IBM SaaS zur Durchführung von Wartungsarbeiten.

j. **Service-Level** ist der nachstehend erläuterte Standard, nach dem IBM den Level des Service misst, den sie in diesem SLA bereitstellt.

2. Gutschriften für Ausfallzeiten

a. Damit der Kunde berechtigt ist, einen Anspruch in Bezug auf einen Vorfall geltend zu machen, muss er beim IBM Help-Desk für Kundenunterstützung anhand des von IBM festgelegten

Verfahrens zum Melden von Problemen der Fehlerklasse 1 ein Support-Ticket für den betroffenen IBM SaaS-Service geöffnet haben. Der Kunde muss alle erforderlichen Einzelheiten zu dem Vorfall zur Verfügung stellen und IBM bei der Diagnose des Vorfalls und der Problemlösung in dem Umfang unterstützen, der für Support-Tickets der Fehlerklasse 1 erforderlich ist. Ein solches Ticket muss innerhalb von 24 Stunden, nachdem der Kunde zum ersten Mal festgestellt hat, dass der Vorfall die Nutzung von IBM SaaS beeinträchtigt, geöffnet werden.

b. Die berechtigte Kontaktperson des Kunden muss den Anspruch auf eine Gutschrift für Ausfallzeiten spätestens drei (3) Arbeitstage nach Ablauf des Vertragsmonats geltend machen, in dem der Vorfall auftrat, der Gegenstand des Anspruchs ist.

c. Die berechtigte Kontaktperson des Kunden muss IBM alle angemessenen Einzelheiten zu dem Anspruch zur Verfügung stellen, einschließlich, aber nicht beschränkt auf detaillierte Beschreibungen aller relevanten Vorfälle und des Service-Levels, der angeblich nicht erfüllt worden ist.

d. IBM wird die insgesamt während jedes einzelnen Vertragsmonats aufgelaufene Ausfallzeit gemäß dem anwendbaren Service-Level in der nachstehenden Tabelle intern messen. Die Gutschriften für Ausfallzeiten 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. Wenn der Kunde eine Anwendungsausfallzeit und eine Ausfallzeit bei der Eingangsdatenverarbeitung meldet und beide Vorfälle gleichzeitig aufgetreten sind, behandelt IBM die sich überschneidenden Ausfallzeiten als eine einzige Ausfallzeit, und nicht als zwei separate Ausfallzeiten. Für jeden gültigen Anspruch wird IBM die höchstmögliche Gutschrift für Ausfallzeiten basierend auf dem während jedes einzelnen Vertragsmonats erreichten Service-Level anwenden (siehe nachstehende Tabellen). IBM gewährt keine Mehrfachgutschriften für Ausfallzeiten für den gleichen Vorfall/die gleichen Vorfälle in ein und demselben Vertragsmonat.

e. Bei einem Bundled Service (einzelne IBM SaaS-Angebote, die in einem Paket zusammengefasst sind und zu einem Gesamtpreis verkauft werden) wird die Gutschrift für Ausfallzeiten basierend auf dem Gesamtpreis des Bundled Service pro Monat, und nicht basierend auf der monatlichen Subscription-Gebühr für jedes einzelne IBM SaaS-Angebot berechnet. Der Kunde darf innerhalb eines Vertragsmonats Ansprüche nur in Bezug auf ein einziges IBM SaaS-Angebot in einem Bundle geltend machen. IBM übernimmt keine Verpflichtung zur Gewährung von Gutschriften für Ausfallzeiten in Bezug auf mehrere IBM SaaS-Angebote in einem Bundle innerhalb eines einzigen Vertragsmonats.

f. Hat der Kunde das IBM SaaS-Angebot bei einem offiziellen IBM Reseller im Rahmen eines Weiterverkaufs erworben, in dem IBM die Hauptverantwortung für die Erbringung der IBM SaaS-Leistungen und für die Verpflichtungen unter diesem SLA übernimmt, dann basiert die Gutschrift für Ausfallzeiten auf dem zum jeweiligen Zeitpunkt für das IBM SaaS-Angebot gültigen RSVP (Relationship Suggested Value Price), der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%).

g. Die Gesamtsumme der Gutschriften für Ausfallzeiten, die für einen beliebigen Vertragsmonat gewährt wird, wird unter keinen Umständen zehn Prozent (10 %) von einem Zwölftel (1/12) der Jahresgebühr überschreiten, die der Kunde IBM für IBM SaaS bezahlt hat.

h. IBM wird Ansprüche nach bestem Wissen und Gewissen anhand der in IBM Aufzeichnungen verfügbaren Informationen prüfen, wobei die IBM Aufzeichnungen im Falle eines Widerspruchs mit den Daten in den Kundenaufzeichnungen Vorrang haben.

i. Die Gutschriften für Ausfallzeiten, die dem Kunden im Rahmen dieses SLA gewährt werden, stellen den einzigen und ausschließlichen Abhilfeanspruch des Kunden im Hinblick auf einen Anspruch dar.

3. Service-Levels

IBM SaaS-Verfügbarkeit in einem Vertragsmonat

Erreichter Service-Level (in einem Vertragsmonat)	**Gutschrift für Ausfallzeiten (in Prozent (%) der monatlichen Subscription-Gebühr für den Vertragsmonat, der Gegenstand des Anspruchs ist)**
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	10 %

Der Prozentsatz des „erreichten Service-Levels“ wird wie folgt berechnet: (a) Gesamtzahl der Minuten in einem Vertragsmonat, minus (b) der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch (c) die Gesamtzahl der Minuten in einem Vertragsmonat.

Beispiel: 250 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 250 Minuten Ausfallzeit = 42.950 Minuten _____ 43.200 Minuten insgesamt	= Gutschrift für Ausfallzeiten in Höhe von 2 % bei einem erreichten Service-Level von 99,4 % in einem Vertragsmonat

3.1 Ausschlüsse

Dieses SLA wird nur IBM Kunden zur Verfügung gestellt und gilt nicht:

- für Beta- und Testservices;
- für Nicht-Produktionsumgebungen, einschließlich, aber nicht beschränkt auf Tests, Disaster-Recovery, Qualitätssicherung oder Entwicklung;
- für Ansprüche, die von Benutzern, Gästen, Teilnehmern und eingeladenen Personen eines IBM Kunden, die IBM SaaS nutzen, geltend gemacht werden;
- wenn der Kunde wesentliche Verpflichtungen aus den Nutzungsbedingungen, einschließlich, aber nicht beschränkt auf die Verletzung von Zahlungsverpflichtungen, nicht erfüllt hat.