IBM MobileFirst Protect (SaaS)

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:

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Management Suite (SaaS)

- IBM MobileFirst Protect – Management Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Secure Mail (SaaS)
- IBM MobileFirst Protect – Secure Mail (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

2. Gebührenmetriken

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

a. **Berechtigter Benutzer** ist eine Maßeinheit für den Erwerb von IBM SaaS. Der Kunde muss für jeden einzelnen berechtigten Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) Zugriff auf IBM SaaS erteilt wird, eine separate, dedizierte Berechtigung erwerben. Es müssen ausreichende Berechtigungen erworben werden, um die Anzahl der berechtigten Benutzer abzudecken, denen während des Messzeitraums, der im Berechtigungsnachweis (Proof of Entitlement = PoE) oder Auftragsdokument angegeben ist, Zugriff auf IBM SaaS erteilt wird.

b. **Gigabyte** ist eine Maßeinheit für den Erwerb von IBM SaaS. Ein Gigabyte entspricht 2 hoch 30 Byte (1.073.741.824 Byte). Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Gigabyte abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, von IBM SaaS verarbeitet werden.

c. **Verwaltete 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, die während des im Berechtigungsnachweis (PoE) oder Auftragsdokument angegebenen Messzeitraums von IBM SaaS verwaltet wird, eine Berechtigung für eine verwaltete Clienteinheit erwerben.

d. **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, die während des im Berechtigungsnachweis (PoE) oder Auftragsdokument angegebenen Messzeitraums in Verbindung mit IBM SaaS ausgeführt wird, Daten an IBM SaaS liefert, von IBM SaaS bereitgestellte Services nutzt oder auf andere Weise auf IBM SaaS zugreift, eine Berechtigung erwerben.

3. Gebühren und Abrechnung

Der für IBM SaaS zu bezahlende Betrag ist in einem Auftragsdokument angegeben.

3.1 Anteilige Monatsgebühren

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

3.2 Zusatzgebühren

Wenn die tatsächliche IBM SaaS-Nutzung durch den Kunden während des Messzeitraums die im Berechtigungsnachweis festgelegte Berechtigung überschreitet, wird dem Kunden die Nutzungsüberschreitung gemäß dem Auftragsdokument in Rechnung gestellt.

4. Verlängerungsoptionen für die IBM SaaS-Subscription-Laufzeit

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

4.1 Automatische Verlängerung

Ist im Berechtigungsnachweis 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 Berechtigungsnachweis 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 Berechtigungsnachweis genannte ursprüngliche Subscription-Laufzeit verlängert.

Die Anzahl oder das Volumen der Verlängerungsberechtigungen entspricht der ursprünglichen Bestellmenge oder der monatlichen Nutzung, die für den Monat vor der Erstellung der Rechnung für die Verlängerung gemeldet wird (es gilt der höhere Wert), es sei denn, IBM erhält eine Mitteilung mit abweichenden Angaben zur Verlängerung der Berechtigungen.

Verlängerungsberechtigungen für Step-up-Angebote basieren auf der ursprünglichen Bestellmenge.

4.2 Fortlaufende Abrechnung

Wird die Laufzeit gemäß dem Berechtigungsnachweis 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.

4.3 Verlängerung erforderlich

Ist im Berechtigungsnachweis 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.

5. Technische Unterstützung

Die technische Unterstützung für IBM SaaS ist als Second-Level-Support für das Betriebsteam des Kunden, nicht als Endbenutzerunterstützung strukturiert und steht während der Subscription-Laufzeit zur Verfügung.

Die Unterstützung wird über mehrere Kanäle rund um die Uhr (24x7) bereitgestellt. Informationen über die Unterstützung für die IBM SaaS-Lösung sind im Produktportal zu finden.

Übersicht der angestrebten Reaktionszeiten:

Fehlerklasse	Definition der Fehlerklasse	Angestrebte Reaktionszeiten Angestrebte Reaktionszeiten	Deckungszeiten
1	**Kritische Auswirkung auf den Geschäftsbetrieb/Serviceausfall:** Geschäftskritische Funktionen sind nicht funktionsfähig oder eine kritische Schnittstelle ist ausgefallen. Dies betrifft normalerweise eine Produktionsumgebung und weist darauf hin, dass der Zugriff auf die Services nicht möglich ist, mit kritischen Auswirkungen auf betriebliche Abläufe. In diesem Fall ist eine sofortige Lösung erforderlich.	30 Minuten	24x7
2	**Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines geschäftsrelevanten Service-Features oder einer Servicefunktion ist stark eingeschränkt, oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann.	1 Stunde während der Geschäftszeiten	24 x 7
3	**Mittlere Auswirkung auf den Geschäftsbetrieb:** Der Service oder die Funktionalität kann genutzt werden und das Problem hat keine kritische Auswirkung auf betriebliche Abläufe.	2 Stunden während der Geschäftszeiten	24 x 7
4	**Geringe Auswirkung auf den Geschäftsbetrieb:** Eine Anfrage oder eine Frage nicht technischer Art.	3 Stunden während der Geschäftszeiten	24 x 7

6. Zusätzliche Bedingungen für die IBM SaaS-Angebote

6.1 Step-up-Beschränkung

Als Voraussetzung für die als „Step up for existing Customers“ (nachfolgend „Step-up SaaS“ genannt) gekennzeichneten IBM SaaS-Angebote muss der Kunde zuvor oder gleichzeitig entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben, das im Namen des Step-up SaaS-Angebots angegeben ist. Wenn der Kunde beispielsweise „IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers“ erwirbt, muss er über Lizenzberechtigungen für das zugehörige IBM MobileFirst Protect-Programm verfügen. Die Berechtigungen des Kunden für das Step-up SaaS-Angebot dürfen seine Berechtigungen für das zugehörige IBM Programm nicht überschreiten.

Wenn der Kunde das Step-up SaaS-Angebot erwirbt, darf er die Lizenzberechtigungen für das zugehörige IBM Programm, die er in Verbindung mit den Step-up SaaS-Berechtigungen nutzt, nicht mehr innerhalb seiner On-Premise-Umgebung einsetzen. Angenommen, der Kunde verfügt über 250 Berechtigungen für verwaltete Clienteinheiten für das zugehörige IBM Programm und erwirbt 100 Step-up SaaS-Berechtigungen für verwaltete Clienteinheiten, dann beziehen sich die 100 Step-up SaaS-Berechtigungen auf die Verwaltung der Clienteinheiten in der IBM SaaS-Umgebung und 150 Clienteinheiten können weiterhin über die vor Ort installierte Software verwaltet werden.

Der Kunde versichert, dass er (1) die erforderlichen Lizenzberechtigungen und (2) Subscription und Support für das zugehörige IBM Programm erworben hat. Während der Subscription-Laufzeit für das Step-up SaaS-Angebot muss der Kunde seinen laufenden Subscription- und Support-Vertrag für die IBM Programmberechtigungen aufrechterhalten, die in Verbindung mit den Step-up SaaS-Berechtigungen genutzt werden. Falls entweder die Lizenz des Kunden oder sein Subscription- und Support-Vertrag für das jeweilige zugehörige IBM Programm ausläuft, erlischt auch sein Recht zur Nutzung des Step-up SaaS-Angebots.

6.2 Cookies

Der Kunde stimmt zu, dass IBM gemäß der IBM Datenschutzrichtlinie unter http://www-01.ibm.com/software/info/product-privacy/index.html Cookies und Tracking-Technologien zur Erfassung personenbezogener Daten für die Erstellung von Nutzungsstatistiken und -informationen verwenden darf, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder Interaktionen mit Benutzern anzupassen.

6.3 Grenzüberschreitende Datenübermittlung

Wenn der Kunde personenbezogene Daten innerhalb der IBM SaaS-Angebote in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen, in der Schweiz, in der Türkei und in anderen europäischen Ländern, die nationale Datenschutzbestimmungen eingeführt haben, verfügbar macht, willigt er ein, dass IBM die Inhalte, einschließlich der personenbezogenen 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:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort
IBM Corporation	Unterauftragsverarbeiter	1 New Orchard Rd. Armonk, NY 10504, USA
IBM India Private Limited	Unterauftragsverarbeiter	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Indien

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.

6.4 EU-Datenschutz

Wenn der Kunde personenbezogene Daten innerhalb der IBM SaaS-Angebote in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen, in der Schweiz, in der Türkei und in anderen europäischen Ländern, die nationale Datenschutzbestimmungen eingeführt haben, verfügbar macht oder wenn sich berechtigte Benutzer oder Geräte des Kunden in diesen Ländern befinden, beauftragt der Kunde als alleiniger Verantwortlicher IBM als Auftragsverarbeiter mit der Verarbeitung der personenbezogenen 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.

6.5 Einhaltung des Safe-Harbor-Abkommens

Die IBM SaaS-Angebote sind in die Safe-Harbor-Zertifizierung der Fiberlink Communications Corporation (IBM Tochtergesellschaft) im Rahmen des Safe-Harbor-Abkommens zwischen den USA und der Europäischen Union eingeschlossen. Sowohl IBM als auch Fiberlink halten die vom United States Department of Commerce verabschiedeten und die Zusammenarbeit zwischen den USA und der Europäischen Union regelnden Safe-Harbor-Grundsätze ein, welche für das Erheben, Verwenden und Speichern von Informationen gelten, die in der Europäischen Union erhoben wurden. Weitere Informationen über das Safe-Harbor-Abkommen oder das Zertifizierungsdokument von Fiberlink sind unter http://www.export.gov/safeharbor/ zu finden.

Wenn die Safe-Harbor-Grundsätze, die die Zusammenarbeit zwischen den USA und der Europäischen Union regeln, für die Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum (EWR) nicht zum Tragen kommen, können die Vertragsparteien oder ihre verbundenen Unternehmen in ihren jeweiligen Rollen stattdessen Vereinbarungen basierend auf den EU-Standardvertragsklauseln gemäß dem EU-Beschluss 2010/87/EU unter Ausschluss der optionalen Klauseln abschließen. Alle Rechtsstreitigkeiten oder Verbindlichkeiten, die sich aus diesen Vereinbarungen ergeben, 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.

6.6 Bevorzugte Standorte

Soweit möglich, orientieren sich die Steuern an dem Standort/den Standorten, für den/die IBM SaaS erbracht wird. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung von IBM SaaS als primärer Standort angegeben wird, es sei denn, der Kunde stellt IBM zusätzliche Informationen bereit. Der Kunde ist dafür verantwortlich, diese Informationen auf dem aktuellen Stand zu halten und IBM über Änderungen zu informieren.

6.7 Normative Daten

Ungeachtet gegenteiliger Regelungen darf IBM Daten, welche die individuellen Erfahrungen der berechtigten Benutzer des Kunden mit dem IBM SaaS-Angebot widerspiegeln, nur für normative Recherche sowie für Analyse-, Demonstrations- und Berichtszwecke in einem aggregierten, anonymen Format aufbewahren und verwenden (d. h., der Kunde oder die berechtigten Benutzer des Kunden können nicht als Quelle der Daten identifiziert werden und persönliche Informationen, die eine Identifizierung des Kunden oder der berechtigten Benutzer des Kunden ermöglichen, wurden entfernt).

6.8 Rechtmäßige Nutzung und Zustimmung

6.8.1 Ermächtigung zur Erfassung und Verarbeitung von Daten

Die IBM SaaS-Angebote sind für die Einrichtung, Verwaltung, Absicherung, Überwachung und Kontrolle von Mobilgeräten ausgelegt. Sie erfassen Informationen von Benutzern und Geräten, die vom Kunden zur Interaktion mit dem jeweiligen IBM SaaS-Angebot berechtigt wurden, das er per Subscription erworben hat. Die von den IBM SaaS-Angeboten erfassten Informationen können allein oder in Kombination in einigen Rechtsordnungen als personenbezogene Daten gelten. Zu den erfassten Informationen können der Name des berechtigten Benutzers, seine Telefonnummer, seine registrierte E-Mail-Adresse und der Gerätestandort, seine Benutzer-ID und der Browserverlauf, Informationen über die Gerätehardware, die Software und die Einstellungen sowie von dem Gerät generierte Informationen gehören. Der Kunde ermächtigt IBM, diese Informationen gemäß den Bestimmungen dieser Nutzungsbedingungen zu erfassen, zu verarbeiten und zu verwenden.

6.8.2 Einverständniserklärung der betroffenen Personen

Bei der Nutzung von IBM SaaS können mehrere Gesetze und 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.

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 als Auftragsverarbeiter des Kunden über die IBM SaaS-Angebote erforderlich sind. Der Kunde ermächtigt hiermit IBM, die Einverständniserklärungen einzuholen, die für die rechtmäßige Nutzung von IBM SaaS sowie die Erfassung und Verarbeitung der Informationen gemäß der Beschreibung in der Endbenutzerlizenzvereinbarung erforderlich sind, die unter http://www.ibm.com/software/sla/sladb.nsf/ verfügbar ist.

6.9 Datenaufbewahrung

IBM wird alle erfassten Informationen, einschließlich der ggf. enthaltenen personenbezogenen Daten, nach Beendigung dieser Nutzungsbedingungen löschen, außer den Informationen, die für die vorstehend genannten Zwecke oder per Gesetz, Vorschrift oder Verordnung aufbewahrt werden müssen. In einem solchen Fall wird IBM die erfassten Informationen für die zu diesem Zweck erforderliche oder für die per Gesetz, Vorschrift oder Verordnung vorgeschriebene Frist aufbewahren.

Anhang A

MobileFirst Protect ist eine benutzerfreundliche Cloudplattform mit allen wesentlichen Funktionen für das End-to-End-Management moderner Mobilgeräte wie iPhones, iPads, Android- und Kindle Fire-Geräte, Windows Phone-Geräte und BlackBerry-Smartphones. Im Folgenden werden die IBM SaaS-Angebote in einer Kurzbeschreibung vorgestellt:

1. IBM MobileFirst Protect – Devices (SaaS)

Zu den zentralen Mobility Device Management-Funktionen (MDM) gehören Geräteregistrierung, Konfiguration, Verwaltung von Sicherheitsrichtlinien und Aktionen für Geräte wie das Senden von Nachrichten und das Lokalisieren, Sperren und Löschen von Geräten. Die Advanced MDM-Features bieten automatisierte Konformitätsregeln, Datenschutzeinstellungen für Bring Your Own Device (BYOD) sowie Mobility Intelligence-Dashboards und Berichterstellung.

2. IBM MobileFirst Protect – Applications (SaaS)

MobileFirst Protect Applications ermöglicht das Hinzufügen von Anwendungen und deren Verteilung an unterstützte Geräte, die von MobileFirst Protect verwaltet werden. Bestandteil dieses Angebots ist der MobileFirst Protect App-Katalog, eine auf dem Gerät vorhandene Anwendung für Benutzer zum Anzeigen und Installieren verwalteter Anwendungen, die außerdem auf Updates für verwaltete Anwendungen aufmerksam macht.

3. IBM MobileFirst Protect – Application Security (SaaS)

MobileFirst Protect Application Security bietet zusätzlichen Datenschutz für Unternehmensanwendungen, wenn bei der Entwicklung das WorkPlace SDK verwendet wird, die Möglichkeit zum Hochladen von iOS-Apps als Anwendung (.ipa) sowie ein Bereitstellungsprofil und die automatische Integration eines Signaturzertifikats. Mobile Application Security integriert die App mit der Secure Productivity Suite. Auf diese Weise werden Single Sign-on, Intranetzugang über das Mobile Enterprise Gateway und die Durchsetzung der Datensicherheitseinstellungen ermöglicht.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

MobileFirst Protect Gateway for Apps ermöglicht Benutzern außerhalb des Unternehmensnetzes einen sicheren und nahtlosen Zugriff auf die internen Anwendungsressourcen, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist.

5. IBM MobileFirst Protect – Content (SaaS)

MobileFirst Protect Content ermöglicht dem Administrator das Hinzufügen und Verteilen von Dokumenten an die unterstützten Geräte, die von IBM MobileFirst Protect Devices verwaltet werden. Bestandteil dieses Angebots ist der IBM MobileFirst Protect Doc Catalogue, ein auf dem Gerät befindlicher, kennwortgeschützter Container, der Benutzern auf sichere und einfache Weise den Zugriff auf Dokumente sowie das Anzeigen und Teilen von Dokumenten ermöglicht. Dieses Angebot bietet einen nahtlosen Zugriff auf verteilte Inhalte und Repositorys wie SharePoint, Box und Google Drive. Der Zugriff auf private SharePoint- und Windows-Dateifreigaben erfolgt über das MobileFirst Protect Mobile Enterprise Gateway. Für Dokumente, die über MobileFirst Protect verwaltet werden, kann eine Versionssteuerung erfolgen, sie können geprüft und mit Richtlinienoptionen zum Schutz vor Datenverlusten (Data Loss Prevention, DLP) abgesichert werden, wie Authentifizierungsanforderung, Einschränkung der Kopier- und Einfügefunktion und Blockierung von Inhalten, damit sie nicht in anderen Anwendungen geöffnet oder geteilt werden können.

6. IBM MobileFirst Protect – Document Sync (SaaS)

MobileFirst Protect Document Sync bietet Benutzern die Möglichkeit, Benutzerinhalte über verwaltete Mobilgeräte hinweg einfach und sicher zu synchronisieren. Die Administratoren können sicherstellen, dass Richtlinien, die beispielsweise das Ausschneiden, Kopieren und Einfügen von Inhalten einschränken oder verhindern, dass Inhalte in anderen Apps geöffnet oder geteilt werden, für sämtliche Benutzerinhalte auf allen Geräten aktiviert sind. Inhalte werden sowohl in der Cloud als auch auf dem Gerät sicher gespeichert; der Zugriff kann nur über den MobileFirst Protect Doc Catalogue erfolgen.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor ist eine leistungsfähige Office-Suite, mit der Geschäftsdokumente auch unterwegs bearbeitet werden können. Der MobileFirst Protect Secure Editor:

- ermöglicht die Erstellung und Bearbeitung von DOC-, PPT- und XLS-Dateien
- verfügt über einen Präsentationsmodus für Folien
- ermöglicht die problemlose Bearbeitung von E-Mail-Anhängen und anderen Dateien aus MobileFirst Protect for iOS

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

Unternehmen können MobileFirst Protect Content in Verbindung mit dem MobileFirst Protect Gateway for Documents einsetzen, um auch Geräten außerhalb des Unternehmensnetzes einen sicheren und nahtlosen Zugriff auf interne Connections-Sites, SharePoint-Sites, Windows File Shares und andere Dateispeicher anzubieten, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist. Für die Nutzung des MobileFirst Protect Gateway for Documents muss MobileFirst Protect Content erworben werden. Unterstützt werden iOS 5.0 und Android 4.0 oder höhere Versionen.

9. IBM MobileFirst Protect – Email Management (SaaS)

MobileFirst Protect Email Management enthält Schlüsselfunktionen zur Unterstützung von Microsoft Exchange ActiveSync und Lotus Traveler.

- Exchange ActiveSync: Bietet Unterstützung für Mobilgeräte, die über das ActiveSync-Protokoll eine Verbindung zu Microsoft Exchange herstellen. Zu den Features gehören zentrale Managementfunktionen für Mobilgeräte wie das Konfigurieren von Geräten, das Erstellen und Durchsetzen von ActiveSync-Richtlinien (Passcode, Zugriff auf E-Mail sperren oder zulassen), das Durchführen von Aktionen für Geräte wie Sperren und Löschen sowie detaillierte Berichte über Geräteattribute.
- Lotus Traveler: Bietet Unterstützung für Mobilgeräte, die über das Lotus Traveler-Protokoll eine Verbindung zu IBM Lotus Notes® herstellen. Zu den Features gehören das Konfigurieren von Geräten, das Sperren oder Freigeben von Geräten, das Durchsetzen von Passcoderichtlinien, das Löschen von Geräten und das Erstellen detaillierter Berichte über Geräteattribute.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser ist ein mit vielen Funktionen ausgestatteter Web-Browser, der den sicheren Zugriff auf die Intranet-Sites des Unternehmens ermöglicht und die Einhaltung der Inhaltsrichtlinien durchsetzt. Dazu werden Richtlinien für Website-Filterung und Sicherheitsrichtlinien definiert, um sicherzustellen, dass nur genehmigte Webinhalte zugänglich sind und eine Reihe von Inhaltskategorien, wie beispielsweise Social-Networking-Sites, Sites mit bestimmten Inhalten oder Malware-Sites, ausgeschlossen werden können. Dazu gehört auch die Möglichkeit ein, native Web-Browser und Web-Browser anderer Anbieter bei der Nutzung in Verbindung mit MobileFirst Protect Devices entweder durch eine Anwendungsrichtlinie oder durch Blacklisting zu inaktivieren. Whitelist-Ausnahmen in Bezug auf bestimmte Websites, die Inaktivierung von Cookies sowie der Funktionen Kopieren, Einfügen und Drucken und die Aktivierung des Kiosk-Modus sind weitere mögliche Optionen.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser ermöglicht unterstützten Geräten den Zugriff auf genehmigte interne Websites, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist.

12. IBM MobileFirst Protect for Blackberry (SaaS)

Bietet über BlackBerry-APIs Unterstützung für Mobilgeräte, die mit einem BlackBerry Enterprise Server (BES) verbunden sind. Zu den Features gehören fern ausgeführte Aktionen, wie das Senden von Nachrichten, das Zurücksetzen des Passcodes, die Zuordnung einer BES-Richtlinie und die Löschung eines Geräts sowie die Erstellung detaillierter Berichte über Geräteattribute. Die Installation von MobileFirst Protect Cloud Extender ist erforderlich. Diese Unterstützung ist nur für Geräte verfügbar, die mit MobileFirst Protect über BES 5.0 angezeigt oder verwaltet werden.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses ermöglicht dem Administrator die Erstellung von Datennutzungsrichtlinien und deren Zuordnung zu unterstützten Geräten, die über MobileFirst Protect verwaltet werden. Diese Richtlinien können auf Geräte-, Gruppen- oder globaler Ebene zugeordnet werden, und es können Schwellenwerte für Warnhinweise und Benachrichtigungen sowohl für die Nutzung innerhalb des Netzes auch für Daten-Roaming konfiguriert werden.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Produkt-Suite/Produkt-Bundle bestehend aus MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content und MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Produkt-Suite/Produkt-Bundle bestehend aus MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content und MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail stellt Benutzern eine separate und sichere Officeproduktivitätsanwendung für den Zugriff auf E-Mail, Kalender und Kontakte bereit, mit der Möglichkeit zur Kontrolle von E-Mails und Anhängen, um das Ausspähen von Daten (Datenlecks) zu verhindern, indem das Weiterleiten oder Verschieben von Inhalten in andere Anwendungen eingeschränkt, die Authentifizierung erzwungen sowie die Berechtigungen zum Ausschneiden, Kopieren und Einfügen von Inhalten über Einstellungen gesteuert werden und E-Mail-Anhänge nur im Ansichtsmodus aufrufbar sind.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

Die MobileFirst Protect Gateway Suite ermöglicht unterstützten Apps auf iOS und Android die sichere und nahtlose Kommunikation mit Ressourcen im internen Netz des Unternehmens.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Produkt-Suite/Produkt-Bundle bestehend aus MobileFirst Protect Content, MobileFirst Protect Document Editor und MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

MobileFirst Protect Threat Management verbessert die mobile Sicherheit durch das Erkennen mobiler Malware und die erweiterte Erkennung von Jailbreak/Rooting. Mit MobileFirst Protect Threat Management ist der Kunde in der Lage, Konformitätsrichtlinien im Zusammenhang mit erkannter Malware und anderen Sicherheitslücken festzulegen und zu verwalten.

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) ermöglicht Benutzern den Upload von Anwendungspaketen und Dokumenten in das Content-Distribution-System von MobileFirst Protect.

Kunden, die den MobileFirst Protect Content Service nutzen, müssen sowohl für MobileFirst Protect Content Service Storage (SaaS) als auch für MobileFirst Protect Content Service Bandwidth (SaaS) jeweils mindestens eine Berechtigung erwerben.

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) ermöglicht Benutzern den Erwerb des gesamten Datenspeichers, der für die Nutzung mit dem MobileFirst Protect Content Service (SaaS) verfügbar ist.

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) ermöglicht Benutzern den Erwerb der gesamten Bandbreite, die für die Nutzung mit dem MobileFirst Protect Content Service (SaaS) verfügbar ist.

23. IBM MobileFirst Protect – Professional (SaaS)

Bietet kleinen und mittelständischen Unternehmen eine schnelle und einfache Möglichkeit, Smartphones und Tablets über Fernzugriff zu konfigurieren, Sicherheitsrichtlinien durchzusetzen, Apps und Dokumente mit Push-Operationen zu übertragen sowie die Daten auf Unternehmensgeräten und privaten Geräten zu

schützen. Dieses Angebot ermöglicht dem Kunden schnellen, einfachen und bezahlbaren Zugriff auf die für sein Unternehmen geeigneten Mobilitätsmanagementfunktionen.

24. IBM MobileFirst Protect – Laptop (SaaS)

Bietet dem Kunden die Möglichkeit, OS X- und Windows-basierte PCs sowie Smartphones und Tablets zu konfigurieren, zu verwalten und abzusichern sowie Berichte zu erstellen. Unternehmen können konsistente Sicherheitsrichtlinien und Profile sowohl für unternehmenseigene als auch für mitarbeitereigene Geräte über dieselbe MobileFirst Protect-Managementkonsole verwalten.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) für Windows-basierte PCs ermöglicht die Registrierung über eine Funkschnittstelle (Over the Air = OTA) sowie Bestandsmanagementberichte mit Informationen über Hardware, Betriebssysteme und Software. Das Berichterstellungsmodul für Endpunktsicherheit bietet interaktive Berichterstellung und Datenanalyse für vom Kunden bereitgestellte Anwendungen, wie beispielsweise Virenschutz, Backup/Recovery, Datenverschlüsselung, persönliche Firewall und fehlende Betriebssystempatches. Das Datenschutzmodul bietet interaktive Berichterstellung und Analyse für Sicherheitsservices, einschließlich Datenverschlüsselung, Vermeidung von Datenlecks (Data Leak Prevention), Backup/Recovery und weitere integrierte Anwendungen. Unterstützt werden XP SP3, Windows Vista, Windows 7, Windows 8+ und Windows 8+ Pro (sofern zutreffend, die 32-Bit- als auch die 64-Bit-Version).

Zu den für die Geräte ausführbaren Aktionen gehören:

- Senden einer Nachricht an ein Gerät
- Sperren eines Geräts
- Lokalisieren eines Geräts (dazu ist MobileFirst Protect Laptop Location erforderlich)
- Stoppen/Starten/Erneutes Starten von Services
- Herunterfahren/Warmstart
- Löschen der Daten auf der Festplatte
- Konfigurieren der Patcheinstellungen
- Verteilen der Software

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) für Mac OS X ermöglicht die Registrierung über eine Funkschnittstelle (Over the Air = OTA) sowie Bestandsmanagementberichte mit Informationen über Hardware, Betriebssysteme und Software. Das Berichterstellungsmodul für Endpunktsicherheit bietet interaktive Berichterstellung und Datenanalyse für vom Kunden bereitgestellte Anwendungen, wie beispielsweise Virenschutz, Backup/Recovery, Datenverschlüsselung, persönliche Firewall und fehlende Betriebssystempatches. Das Datenschutzmodul bietet interaktive Berichterstellung und Analyse für Datensicherheitsservices, einschließlich Datenverschlüsselung. Das Konfigurationsmanagementmodul ermöglicht die Fernverwaltung einer Reihe von Geräte- und Benutzereinstellungen, einschließlich Kennwort, E-Mail, VPN und WiFi. Unterstützt wird Mac OS X Version 10.7.3 oder eine höhere Version.

Zu den für die Geräte ausführbaren Aktionen gehören:

- Sperren eines Geräts
- Löschen der Daten auf der Festplatte
- Ändern der Geräterichtlinie

25. IBM MobileFirst Protect – Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) ermöglicht das Lokalisieren unterstützter Laptops und Tablets. MobileFirst Protect meldet die Position der Wifi- oder IP-Adresskoordinaten und übersetzt diese Daten in eine leicht erkennbare Adresse. Wenn ein Gerät online ist, kann die aktuelle Position abgerufen werden. Die gemeldeten Daten werden von MobileFirst Protect gespeichert, sodass im Laufe der Zeit ein Protokoll aufgebaut wird, das zu Prüfungszwecken verfügbar ist. Voraussetzung dafür ist IBM MobileFirst Protect Laptop (SaaS) for Windows. Unterstützt werden XP SP3, Windows Vista, Windows 7, Windows 8+ und Windows 8+ Pro (sofern zutreffend, die 32-Bit- als auch die 64-Bit-Version).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Enthält die Funktionalität des Angebots MobileFirst Protect – Laptop (SaaS) und bietet darüber hinaus die folgenden Funktionen:

- Ermöglicht den Upload von Paketen auf die MobileFirst Protect Content Service (SaaS)-Plattform und die Planung der Nutzdatenverteilung an die Geräte, die vom MobileFirst Protect Laptop (SaaS)-Service für Microsoft Windows verwaltet werden. Die Steuerung sämtlicher Aspekte der Verteilung, einschließlich der Installationsanweisungen, und die Verteilung auf Geräte-, Gruppen- oder globaler Ebene liegt beim Kunden. Der Kunde trägt die gesamte Verantwortung für das Paketierung und die Erstellung der Installationsdatei. IBM leistet keine Unterstützung bei der Erstellung des Installationspakets.

27. IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)

Ermöglicht Unternehmen die Verwaltung konsistenter Sicherheitsrichtlinien und Profile sowohl für unternehmenseigene als auch für mitarbeitereigene Geräte über dieselbe Managementkonsole.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

Zu den zentralen Mobility Device Management-Funktionen (MDM) gehören Geräteregistrierung, Konfiguration, Verwaltung von Sicherheitsrichtlinien und Aktionen für Geräte wie das Senden von Nachrichten und das Lokalisieren, Sperren und Löschen von Geräten. Die Advanced MDM-Features bieten automatisierte Konformitätsregeln, Datenschutzeinstellungen für Bring Your Own Device (BYOD) sowie Mobility Intelligence-Dashboards und Berichterstellung.

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Ermöglicht den sicheren Zugriff auf E-Mail, die sichere Speicherung, Verteilung und Verwaltung von Anwendungen sowie die Bereitstellung des Zugriffs auf die Intranet-Site über den Secure Browser.

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Ermöglicht die Verwaltung und Konfiguration von Smartphones und Tablets über Fernzugriff, die Durchsetzung von Sicherheitsrichtlinien, die Verteilung von Daten und die Erstellung von Berichten über die Wifi-Nutzung, die zur Überwachung der Datennutzung und Kosten herangezogen werden kann, sowie die Inhaltsspeicherung und Verteilung von Anwendungen und Dokumenten.

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Bietet kleinen und mittelständischen Unternehmen die Möglichkeit, Smartphones und Tablets über Fernzugriff zu konfigurieren, Sicherheitsrichtlinien durchzusetzen, Apps und Dokumente mit Push-Operationen zu übertragen sowie die Daten auf Unternehmensgeräten und privaten Geräten zu schützen.

32. IBM MaaS360 Educational Bundle Prime (SaaS)

Ermöglicht Bildungseinrichtungen die Verwaltung und Konfiguration von Smartphones und Tablets über Fernzugriff, die Durchsetzung von Sicherheitsrichtlinien, die Verteilung von Daten sowie die Inhaltsspeicherung und die Verteilung und Verwaltung von Anwendungen.

33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Ermöglicht Unternehmen die Verwaltung, Aktualisierung, Lokalisierung und Verteilung von Software an Laptops mit konsistenten Sicherheitsrichtlinien für alle Laptops/Desktops, die an die MaaS360-Managementkonsole berichten.

Anhang B

Das folgende Service-Level-Agreement („SLA“) von IBM beinhaltet Angaben zur Verfügbarkeit von IBM SaaS und kommt zur Anwendung, sofern es im Berechtigungsnachweis oder 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 per Subscription direkt von IBM bezieht und keine wesentlichen Verpflichtungen, einschließlich Zahlungsverpflichtungen, aus ihrem Vertrag mit IBM für IBM SaaS verletzt hat.

f. **Ausfallzeit** ist die Anwendungsausfallzeit und/oder die Ausfallzeit bei der Eingangsverarbeitung gemäß dem anwendbaren Service-Level in der nachstehenden Tabelle. Ausfallzeiten umfassen nicht den Zeitraum, in dem das IBM SaaS-Angebot 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 notwendigen 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, bei dem IBM die Hauptverantwortung für die Erbringung der IBM SaaS-Leistungen und die Verpflichtungen unter dem 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)**
Unter 99,8 %	2 %
Unter 98,8 %	5 %
Unter 95,0 %	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: 50 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 50 Minuten Ausfallzeit = 43.150 Minuten _____ 43.200 Minuten insgesamt	= Gutschrift für Ausfallzeiten in Höhe von 2 % bei einem erreichten Service-Level von 99,8 % in einem Vertragsmonat

4. 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 des Kunden, Gästen, Teilnehmern und zugelassenen eingeladenen Personen, die IBM SaaS nutzen, geltend gemacht werden;
- für Aktivierungssoftware.