IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen

IBM Watson Health Core

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 folgenden 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 Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Gebührenmetriken

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

a. **Zugriff** ist eine Maßeinheit für den Erwerb von IBM SaaS. Unter „Zugriff“ versteht man die Rechte zur Nutzung von IBM SaaS. Der Kunde muss eine einzelne Zugriffsberechtigung erwerben, um IBM SaaS während des Messzeitraums nutzen zu können, der im Berechtigungsnachweis (Proof of Entitlement = PoE) oder Auftragsdokument angegeben ist.

b. **Individuum** ist eine Maßeinheit für den Erwerb von IBM SaaS. Ein Individuum ist ein einzelnes Ding oder ein Mensch. Der Kunde muss ausreichende Berechtigungen erwerben, um jedes Individuum abzudecken, das während des Messzeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, über IBM SaaS verarbeitet oder verwaltet wird.

   Für die Zwecke dieses IBM SaaS-Angebots zählen Personen, Geräte oder mobile Anwendungen als Individuen, deren Daten von IBM SaaS verwaltet werden.

c. **Instanz** ist eine Maßeinheit für den Erwerb von IBM SaaS. Eine Instanz ermöglicht den Zugriff auf eine bestimmte IBM SaaS-Konfiguration. Der Kunde muss ausreichende Berechtigungen für alle IBM SaaS-Instanzen erwerben, die während des Messzeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, zum Zugriff und zur Nutzung bereitgestellt werden.

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. Laufzeit und Verlängerungsoptionen

Die IBM SaaS-Laufzeit beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf die Pilotbetriebsumgebung von IBM SaaS gemäß der Angabe im Auftragsdokument freigeschaltet ist. Die Subscription-Laufzeit der Berechtigungen für ein Individuum beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf die Produktionsbetriebsumgebung freigeschaltet ist. Im Auftragsdokument ist festgelegt, ob sich IBM SaaS automatisch verlängert, auf fortlaufender Basis genutzt werden kann oder am Ende der Laufzeit abläuft.

Bei automatischer Verlängerung wird IBM SaaS automatisch um die im Berechtigungsnachweis angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM mindestens 90 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht.

Bei fortlaufender Nutzung steht IBM SaaS auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 90 Tagen schriftlich kündigt. IBM SaaS bleibt nach Ablauf der 90-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

5. Technische Unterstützung

IBM stellt das IBM Software as a Service Support Handbook zur Verfügung, das Kontaktinformationen für die technische Unterstützung, Wartungszeiten sowie weitere Informationen und Prozesse enthält. Die Kontaktinformationen für die technische Unterstützung sowie weitere Einzelheiten in Bezug auf die Abwicklung der Unterstützung sind unter „IBM SaaS Support Handbook“ auf https://support.ibmcloud.com zu finden.

Anfragen an die technische Unterstützung und einfache Konfigurationsanfragen für IBM SaaS können durch elektronische Übermittlung gestellt werden. Die technische Unterstützung ist Bestandteil von IBM SaaS und nicht als separates Angebot erhältlich.

Dokumente oder Informationen, die bei der Meldung eines Problems oder Vorfalls weitergegeben werden, dürfen keine personenbezogenen Daten, geschützten Gesundheitsdaten oder sensiblen personenbezogenen Daten enthalten.

6. Begriffsbestimmungen

Geltende Gesetze bezeichnet alle Gesetze, Statuten oder gesetzlichen Regelungen, Regeln, Verordnungen, Richtlinien, Verfügungen, Erlässe oder sonstigen Vorschriften einer Regierungsbehörde oder alle allgemein anerkannten Branchenstandards, die bei der Erfüllung dieser Nutzungsbedingungen zur Anwendung kommen.

API bezeichnet eine Anwendungsprogrammierschnittstelle (Application Program Interface), die aus einer Reihe von Routinen, Protokollen und Tools für die Erstellung von Softwareanwendungen besteht. APIs legen fest, wie Softwarekomponenten interagieren sollen, und werden bei der Programmierung der Komponenten grafischer Benutzerschnittstellen (Graphical User Interface = GUI) verwendet.

Berechtigter Administrator ist ein Mitarbeiter des Kunden oder ein vom Kunden autorisierter Auftragnehmer, ein Individuum oder eine Gruppe, die für die Wartung und den zuverlässigen Betrieb der Plattform verantwortlich ist. Zu den Zuständigkeiten können die Konfiguration, die Unterstützung sowie das Benutzer- und Kontomanagement gehören. Der Administrator kann auch ein klinischer Prüfer sein, der für die Durchführung einer Studie im Watson Health-System verantwortlich ist.

Berechtigtes Individuum ist eine authentifizierte Person, eine mobile Anwendung oder ein Gerät, dem die Zugriffsberechtigung zum Senden von Daten an Watson Health Core erteilt wurde. Dazu können der Kunde, Studienteilnehmer, Endkunden oder Patienten des Kunden gehören.

Für den Kunden geltende Datengesetze sind die Datengesetze, die bei der Erfüllung der Verpflichtungen des Kunden unter dem Vertrag, den zugehörigen Dokumenten und anwendbaren Servicebeschreibungen, Auftragsdokumenten und Leistungsbeschreibungen zwischen den Vertragsparteien zur Anwendung kommen.

Kundendaten sind Daten, die vom Kunden oder für den Kunden in IBM SaaS eingestellt werden. Dabei kann es sich um kundeneigene Daten handeln oder um Daten, die vom Endkunden des Kunden oder von einem Dritten bzw. in deren Auftrag eingestellt werden, sowie um Daten, die vom Wellness- oder Medizingerät eines Drittanbieters stammen.

Datengesetze sind alle anwendbaren Gesetze, die sich auf den Datenschutz, den Schutz der Privatsphäre oder die Sicherheit beziehen.

Betroffene Person bezeichnet eine bestimmte oder bestimmbare natürliche Person, auf die sich die personenbezogenen Daten beziehen.

Bestimmtes Rechenzentrum bezeichnet das Rechenzentrum (oder die Rechenzentren), das im Auftragsdokument als primäres Rechenzentrum oder Rechenzentrum für Disaster-Recovery angegeben ist, in dem die IBM SaaS-Instanz des Kunden ausgeführt wird.

Gesundheitsdaten sind alle Daten oder Informationen, einschließlich Bildmaterial, bei denen es sich um gesundheitsrelevante personenbezogene Daten handelt.

Für Gesundheitsdaten geeignet bedeutet in Bezug auf IBM SaaS, dass IBM SaaS die geltenden Sicherheits- und Datenschutzstandards, -gesetze und -bestimmungen im Rahmen der Gesetzgebung für Gesundheitsdaten einhält, einschließlich der Durchführungsbestimmungen (Implementation Specifications) in Teil (Part) 164, Abschnitte (Subparts) A und C der Regelungen zur Umsetzung des HIPAA (geändert durch den HITECH Act) und anderer geltender Gesetze, die sich auf Gesundheitsdaten beziehen; es bedeutet aber nicht, dass IBM als Business Associate (Geschäftspartner) oder als Verantwortlicher für die Verarbeitung von Daten handelt.

HIPAA bezeichnet den Health Insurance Portability and Accountability Act aus dem Jahr 1996, einschließlich der durch den Health Information Technology for Economic & Clinical Health Act des American Recovery and Reinvestment Act aus dem Jahr 2009 („HITECH Act“) geänderten Fassung, sowie bestimmte Vorschriften, die vom Ministerium für Gesundheitspflege und Soziale Dienste der Vereinigten Staaten unter dem HIPAA in 45 C.F.R. Teil (Part) 160 und 164 veröffentlicht wurden, und bestimmte Vorschriften, die gemäß dem HITECH Act veröffentlicht wurden.

Für IBM geltende Datengesetze sind die Datengesetze, die bei der Erfüllung der Verpflichtungen von IBM unter dem Vertrag, den zugehörigen Dokumenten und anwendbaren Servicebeschreibungen, Auftragsdokumenten und Leistungsbeschreibungen zwischen den Vertragsparteien zur Anwendung kommen.

IBM Personal bezieht sich auf (a) IBM, ihre verbundenen Unternehmen und Unterauftragnehmer sowie die Mitarbeiter der Vorgenannten und (b) alle Lieferanten, die Services im Auftrag von IBM gemäß dem Vertrag und der anwendbaren zugehörigen Dokumente erbringen oder die von IBM auf andere Weise zum Zugriff auf die personenbezogenen Daten des Kunden berechtigt werden.

Beteiligte Länder sind die 28 Mitgliedstaaten der Europäischen Union und die Schweiz sowie alle Länder, die von IBM im Laufe der Zeit in diese Liste aufgenommen werden.

Personenbezogene Daten oder **Persönliche Daten** sind Informationen auf einem beliebigen Medium oder in einem beliebigen Format, einschließlich elektronischer und Papieraufzeichnungen, über eine bestimmte oder bestimmbare natürliche Person; als „bestimmbare natürliche Person“ wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Verarbeitung (in Groß- oder Kleinschreibung) bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

Verarbeitete Daten sind jegliche Daten, vertrauliche oder urheberrechtlich geschützte Informationen oder Materialien, einschließlich Gesundheitsdaten und personenbezogener Daten, die von IBM gemäß dem Vertrag, einem zugehörigen Dokument und/oder einer Servicebeschreibung, einem Auftragsdokument und/oder einer Leistungsbeschreibung verarbeitet werden.

Sicherheitsvorfall hat die im Anhang für Sicherheit und Business-Continuity festgelegte Bedeutung.

7. Kontomanagement

Nur berechtigte Benutzer des Kunden („**Berechtigte Administratoren**“ oder „**Berechtigte Individuen**“) haben Zugriff auf IBM SaaS. Der Kunde kontrolliert die Konten, die zum Zugriff auf IBM SaaS berechtigt sind, wozu berechtigte Anwendungen, das Kundenpersonal, externe Service-Provider und Auftragnehmer gehören können, und ist allein dafür verantwortlich, (i) alle berechtigten Benutzer zu kontrollieren, einschließlich, aber nicht beschränkt auf die Prüfung der Identität jedes berechtigten Benutzers, und (ii) sicherzustellen, dass nur berechtigte Benutzer auf IBM SaaS zugreifen.

Berechtigte Individuen, bei denen es sich um Endkunden, Patienten oder Studienteilnehmer des Kunden handelt, dürfen ausschließlich zum Zweck des Datenuploads in IBM SaaS Zugriff erhalten; andere Zugriffsberechtigungen für IBM SaaS werden den berechtigten Individuen in diesem Fall nicht erteilt.

8. Datenschutz

8.1 Allgemeine Anforderungen

Im Hinblick auf das Verhältnis zwischen den Vertragsparteien ist der Kunde der alleinige Verantwortliche für seine personenbezogenen Daten und beauftragt IBM als Auftragsverarbeiter. Der Kunde hat gemäß den geltenden Datengesetzen das Recht, IBM in Bezug auf die Verarbeitung seiner personenbezogenen Daten Anweisungen zu erteilen.

Soweit IBM die Verarbeitung der personenbezogenen Daten des Kunden übernimmt, wird IBM:

a. alle für IBM geltenden Datengesetze einhalten und

b. die personenbezogenen Daten des Kunden nicht mit Daten aus anderen Quellen in Verbindung bringen, außer:

   - wenn dies zur Bereitstellung von IBM SaaS erforderlich ist, aber nicht für andere Zwecke, es sei denn, der Kunde hat ausdrücklich anderslautende Anweisungen erteilt, oder
   - gemäß den Bestimmungen dieser Nutzungsbedingungen und des Anhangs für Sicherheit und Business-Continuity.

Soweit IBM die Verarbeitung der personenbezogenen Daten des Kunden übernimmt, wird der Kunde:

a. alle für ihn geltenden Datengesetze einhalten,

b. die Kommunikation mit seinen verbundenen Unternehmen, Patienten, Endbenutzern und betroffenen Personen und/oder anderen Dritten übernehmen,

c. Vereinbarungen zur Auftragsdatenverarbeitung mit seinen Verantwortlichen (controllers) schließen, die erforderlich sind, damit IBM als Auftragsverarbeiter und die Unterauftragsverarbeiter von IBM personenbezogene Daten des Kunden verarbeiten dürfen, und

d. als einziger Ansprechpartner für IBM fungieren und die alleinige Verantwortung für die interne Koordination, Prüfung und Erteilung von Anweisungen oder Anforderungen durch seine verbundenen Unternehmen übernehmen, die andere Verantwortliche (controllers) für IBM sind. IBM wird von ihrer Verpflichtung befreit, die verbundenen Unternehmen des Kunden, die als Verantwortliche (controllers) anzusehen sind, zu informieren oder zu benachrichtigen, wenn die entsprechende Information oder Benachrichtigung bereits an den Kunden übermittelt wurde. IBM kann direkte Anweisungen eines verbundenen Unternehmen des Kunden, das zwar ein Verantwortlicher (controller), aber nicht der Kunde ist, verweigern.

Keine der Vertragsparteien darf gezwungen sein, gegen die für sie geltenden Datengesetze zu verstoßen.

8.2 Rechte an Kundendaten

Der Kunde versichert und gewährleistet, (a) dass er der Eigentümer der Daten ist, die von ihm in IBM SaaS eingestellt werden, oder (b) dass er alle erforderlichen Rechte, Genehmigungen, Einwilligungserklärungen und Berechtigungen eingeholt hat und für deren Aufrechterhaltung verantwortlich ist, um IBM die Zugriffs-, Nutzungs- und Veröffentlichungsrechte für die Kundendaten gemäß den Bestimmungen dieser Nutzungsbedingungen oder des Vertrags oder sonstige Rechte, die IBM für die Bereitstellung von IBM SaaS benötigt, zu erteilen. Der Kunde versichert und gewährleistet des Weiteren, dass sich die Kundendaten (a) nur auf Personen beziehen, die in den USA ansässig sind, und nur in einem Rechenzentrum in den USA in IBM SaaS eingestellt werden, oder (b) auf Personen beziehen, die in einem oder mehreren der beteiligten Länder ansässig sind, und in diesen Fällen nur in den bestimmten Rechenzentren in IBM SaaS eingestellt werden.

8.3 Datenservices und Verantwortlichkeiten

a. Der Kunde versichert, dass er nur im Zusammenhang mit seinen Aktivitäten, die entweder „Gesundheitsdienstleistungen“ oder „Forschungsaktivitäten“ gemäß der Definition im HIPAA und/oder in ähnlichen Regelwerken unter anderen geltenden Gesetzen darstellen, Analysen durchführen oder IBM mit der Durchführung von Analysen beauftragen wird, und dass er die Kundendaten nur gemäß allen einschlägigen Anforderungen (z. B. Festlegung durch ein Prüfungsgremium (Institution Review Board, IRB) oder aufgrund einer Ausnahmeregelung) unter diesen und anderen für den Kunden geltenden Datengesetzen verwenden oder IBM zu deren Verwendung anweisen wird.

b. Der Kunde ist allein dafür verantwortlich, alle Registrierungen, Einwilligungserklärungen, Berechtigungen und Genehmigungen einzuholen, die nach den für den Kunden geltenden Gesetzen in jedem beteiligten Land erforderlich sind, einschließlich, aber nicht beschränkt auf den HIPAA und andere geltende Datenschutz- und Datensicherheitsgesetze, -regeln und -vorschriften, damit die Kundendaten, so wie es im Rahmen dieser Nutzungsbedingungen und des Vertrags vorgesehen ist, vom Kunden und von IBM sowie ihren zugelassenen Unterauftragnehmern in IBM SaaS eingestellt, verwendet und offengelegt werden können. IBM ist nicht dafür zuständig, zu kontrollieren, wann diese Registrierungen, Einwilligungserklärungen, Berechtigungen und Genehmigungen erteilt wurden oder erforderlich sind.

c. Der Kunde ist allein dafür verantwortlich, sicherzustellen, dass alle in IBM SaaS eingestellten Daten sich nur auf Personen beziehen, die in den USA oder in einem beteiligten Land ansässig sind.

d. IBM verfügt über Support Centers, deren Mitarbeiter in Bezug auf die HIPAA-Richtlinien und andere für IBM geltende Datengesetze hinsichtlich der Daten aus beteiligten Ländern geschult sind.

8.4 Sicherheitsmaßnahmen und Sicherheitsvorfälle

a. IBM wird die technischen und organisatorischen Maßnahmen umsetzen, ausführen und einhalten (einschließlich der organisatorisch notwendigen Prozesse und Abläufe sowie aller spezifischen Sicherheitspflichten, die in diesen Nutzungsbedingungen oder im Anhang für Sicherheit und Business-Continuity festgelegt sind oder auf die dort verwiesen wird), um die personenbezogenen Daten des Kunden vor unbefugter Nutzung oder unbefugtem Zugriff, zufälligem Untergang, Beschädigung, Veränderung, Vernichtung, Diebstahl oder nicht autorisierter Offenlegung zu schützen.

b. Falls IBM Kenntnis von einem Sicherheitsvorfall (gemäß der Definition im Anhang für Sicherheit und Business-Continuity) erhält, der sich auf verarbeitete Daten des Kunden auswirkt, wird IBM den Kunden gemäß den Bedingungen des Anhangs für Sicherheit und Business-Continuity und der für IBM geltenden Datengesetze benachrichtigen, und diese Benachrichtigung wird Informationen über bekannte Auswirkungen des Sicherheitsvorfalls auf den Kunden oder andere betroffene Personen (sofern dies der Fall ist) sowie über Abhilfemaßnahmen enthalten, die von IBM getroffen wurden oder vorgeschlagen werden.

8.5 Anfragen und Beschwerden

IBM wird den Kunden unverzüglich und in dem nach den für IBM geltenden Datengesetzen zulässigen Umfang nicht später als fünf (5) Arbeitstage schriftlich benachrichtigen, wenn von IBM erhaltene Anfragen, Mitteilungen oder Beschwerden beim IBM Watson Health Data Privacy Officer in Bezug auf personenbezogene Daten des Kunden eingereicht wurden, die:

a. von einer betroffenen Person stammen und sich auf die von IBM verarbeiteten personenbezogenen Daten dieser Person beziehen. Der Kunde wird die Anfragen der betroffenen Personen beantworten und IBM wird allen angemessenen Anweisungen des Kunden zur Unterstützung bei der Beantwortung dieser Anfragen Folge leisten. Falls nach den für IBM geltenden Gesetzen erforderlich, wird IBM diese Anfragen direkt beantworten, sofern IBM den Kunden vorab darüber informiert und die Antwort in Form und Inhalt mit dem Kunden in sinnvoller Weise koordiniert, wenn dies nach den für IBM geltenden Gesetzen zulässig oder anderweitig möglich ist.

b. von einer Justiz- oder Regulierungsbehörde stammen und sich auf die Verarbeitung personenbezogener Daten des Kunden durch IBM beziehen, sofern IBM den von einer Behörde in einer Vorladung (Subpoena) oder einem vergleichbaren rechtsgültigen Dokument erhaltenen Aufforderungen zur Offenlegung von Unterlagen nachkommen darf oder soweit dies nach dem geltenden Datengesetz erforderlich ist und sofern IBM den Kunden vorab über die Offenlegung informiert und die Antwort in Form und Inhalt mit dem Kunden in sinnvoller Weise koordiniert, wenn dies nach den für IBM geltenden Gesetzen zulässig oder anderweitig möglich ist.

8.6 Verarbeitung der personenbezogenen Daten des Kunden

IBM wird die Offenlegung personenbezogener Daten des Kunden auf die IBM Mitarbeiter beschränken, die an der Bereitstellung der Services beteiligt sind.

IBM wird allen angemessenen Anforderungen des Kunden im Rahmen des geltenden Gesetzes nachkommen, in denen IBM aufgefordert wird, personenbezogene Daten des Kunden zu ändern, zu korrigieren, zu löschen oder zu blockieren.

Auf Antrag einer der beiden Parteien werden IBM, der Kunde oder ihre verbundenen Unternehmen Standardvereinbarungen schließen, die nach dem Gesetz zum Schutz der personenbezogenen Daten des Kunden erforderlich sind. Die Parteien kommen überein (und werden dafür sorgen, dass ihre jeweiligen verbundenen Unternehmen zustimmen), dass diese Vereinbarungen bei gegenseitigen Ansprüchen der Parteien den Haftungsbegrenzungen und -ausschlüssen in diesem Vertrag unterliegen. Die Parteien werden zusammenarbeiten, um weitere einvernehmlich festgelegte Bedingungen oder Vereinbarungen abzuschließen (oder dafür sorgen, dass ihre verbundenen Unternehmen solche Bedingungen oder Vereinbarungen abzuschließen) und einzuhalten, soweit dies nach den geltenden Datengesetzen erforderlich ist.

8.7 Rückgabe der personenbezogenen Daten des Kunden

Bei Ablauf oder Kündigung des Vertrags wird IBM die Nutzung oder Verarbeitung aller proprietären Informationen und aller personenbezogenen Daten des Kunden einstellen und allen IBM Mitarbeitern entsprechende Anweisungen erteilen sowie nach Wahl und Aufforderung durch den Kunden:

a. alle von IBM gespeicherten proprietären Informationen und personenbezogenen Daten unverzüglich in einem vom Kunden in angemessener Weise angeforderten Format und auf Speichermedien zurückzugeben und nach der Empfangsbestätigung des Kunden alle proprietären Informationen und personenbezogenen Daten löschen, vernichten oder auf andere Weise unleserlich und nicht entschlüsselbar machen, einschließlich Kopien und Sicherungen. IBM kann die Kosten für die Speichermedien und bestimmte auf Anforderung des Kunden durchgeführte Aktivitäten (z. B. Bereitstellung der proprietären Informationen und personenbezogenen Daten in einem speziellen Format oder deren Vernichtung auf eine bestimmte Art und Weise) in Rechnung stellen; und

b. die proprietären Informationen und personenbezogenen Daten direkt löschen, vernichten oder auf andere Weise unleserlich und nicht entschlüsselbar machen, einschließlich Kopien und Sicherungen.

8.8 Business-Associate-Vereinbarung

Soweit nach dem HIPAA angemessen und erforderlich, werden IBM und der Kunde eine Business-Associate-Vereinbarung abschließen, in der die Verpflichtungen von IBM als Business Associate (Geschäftspartner) des Kunden im Rahmen der Bereitstellung von IBM SaaS geregelt sind. Ohne die ausdrücklichen Verpflichtungen von IBM unter dem Vertrag und der Business-Associate-Vereinbarung, sofern anwendbar, einzuschränken, bestätigt der Kunde und erklärt sich damit einverstanden, dass er allein dafür verantwortlich ist, festzustellen, welche geltenden Gesetze und Lizenzvoraussetzungen bei seiner Nutzung von IBM SaaS oder anderen Aktivitäten in Bezug auf IBM SaaS (einschließlich der Nutzung oder anderer Aktivitäten durch seine berechtigten Benutzer) zur Anwendung kommen, und diese einzuhalten.

8.9 Vertragszusatz zur Verarbeitung von Daten aus der Europäischen Union

Wenn der Kunde IBM mit der Verarbeitung personenbezogener Daten aus der Europäischen Union beauftragt, werden IBM und der Kunde einen Vertragszusatz zur Datenverarbeitung, einschließlich, bei Bedarf, der EU-Modellklauseln unter Ausschluss der optionalen Klauseln abschließen.

9. Zusätzliche Bedingungen für die IBM SaaS-Angebote

9.1 Sicherheit

Diese IBM SaaS-Angebote orientieren sich an den unter http://www.ibm.com/cloud/data-security verfügbaren IBM Datensicherheits- und Datenschutzrichtlinien für IBM SaaS sowie den zusätzlichen Bedingungen, die nachstehend und im Anhang für Sicherheit und Business-Continuity dieser Nutzungsbedingungen aufgeführt sind. Änderungen der IBM Datensicherheits- und Datenschutzrichtlinien führen nicht zu einer Beeinträchtigung der Sicherheit von IBM SaaS.

Bei IBM Watson Health Core werden Sicherheitsrichtlinien, Standards und Prozesse umgesetzt, die auf dem Regelwerk von ISO 27001 basieren und in der Sicherheitsbeschreibung weiter erläutert werden. Zu den im Rahmen der Lösung umgesetzten Sicherheitsfunktionen gehören:

a. Sichere Betriebszonen

   IBM Watson Health Core implementiert eine tiefengestaffelte Sicherheitsstrategie mit mehreren Sicherheitszonen, um Cloudintegrationspunkte, wie Daten-Onboarding und die Entwicklung angepasster Anwendungen, zu steuern.

b. Verschlüsselung

   Alle Kundendaten im Ruhezustand und alle In-Flight-Kundendaten werden verschlüsselt. Ebenso werden alle Daten bei der Übertragung in und aus IBM Watson Health Core verschlüsselt. Ein gemeinsam genutzter Service bietet Verschlüsselung mit Schlüsselmanagement. Der Kunde trägt die Verantwortung für die gesamte Netzkonnektivität und -qualität zwischen dem IBM Watson Health Service und seinem Proxy-Server.

c. Überwachung von Sicherheitsereignissen

   IBM nutzt ihre Security Intelligence Platform für das Management von Sicherheitsinformationen und Ereignissen, für Protokollmanagement, Incident Forensics, die Erkennung von Bedrohungen und für das Schwachstellenmanagement.

d. Identitätsmanagement

   - Watson Health Core unterstützt Open-Standard-Identitätsprovider bei umfangreichen Patienten- und Benutzerpopulationen mithilfe von OpenID Connect.
   - Ist IBM der Identitätsprovider der Benutzerpopulationen, nutzt Watson Health Core entsprechende Directory Services und Identitätsmanagementfunktionen für die Authentifizierung.

e. Strikte Authentifizierung und rollenbasierter Zugriff

   - Watson Health Core unterstützt die Authentifizierung über SAML als Mechanismus für Kunden zur Integration ihrer Single-Sign-On-Services (SSO) oder Directory Services.
   - Watson Health Core nutzt eine Zugriffsmanagementlösung und zugehörige Komponenten zur Verwaltung von Sicherheitsrichtlinien, soweit erforderlich.
   - Watson Health Core unterstützt softwarebasierte Zwei-Faktor-Authentifizierung.
   - Watson Health Core bietet eine grundlegende rollenbasierte Zugriffssteuerung, soweit erforderlich, und unterstützt die Konfiguration von Studien, Benutzerprofilen, Rollen und Benutzergruppen über Anwendungsprogrammierschnittstellen („"API“ oder „APIs“), die einen rollenbasierten Zugriff ermöglichen.

9.2 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für IBM SaaS über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der IBM SaaS-Nutzung in Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität von IBM SaaS zusammenstellen, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder Interaktionen mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholen wird oder eingeholt hat, damit IBM die erfassten personenbezogenen Daten für die vorstehenden Zwecke innerhalb von IBM, durch andere IBM Unternehmen und durch ihre Unterauftragnehmer in allen Ländern, in denen wir und unsere Unterauftragnehmer geschäftlich tätig sind, in Übereinstimmung mit der geltenden Gesetzgebung verarbeiten darf. IBM wird den Weisungen der Mitarbeiter und Auftragnehmer des Kunden nachkommen,

die sich auf den Zugriff auf ihre erfassten personenbezogenen Daten, deren Aktualisierung, Korrektur oder Löschung beziehen.

9.3 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.

9.4 Continuous Delivery

Der Kunde hat Anspruch auf Funktionen und Erweiterungen, die in die Lösung eingebaut und von IBM in einem Continuous-Delivery-Modell in der Cloud bereitgestellt werden.

9.5 Sicherung und Wiederherstellung

IBM Watson Health Core ermöglicht die Sicherung der Kundendaten in der Produktionsumgebung (einschließlich Data-Lake- und Data-Reservoir-Repositorys) mit dem letzten als funktionierend bekannten Zustand, um den Service im Falle eines Systemausfalls wiederherstellen zu können.

9.6 Hochverfügbarkeit

Die IBM Watson Health Core-Komponenten in der Produktionsumgebung werden in Hochverfügbarkeitskonfigurationen implementiert, wobei Datenbankserver zur Redundanz in Clustern zusammengefasst werden, um die Workload zu verteilen und Single Points of Failure zu vermeiden.

9.7 Disaster-Recovery

Das IBM Disaster-Recovery-Konzept besteht in der Nutzung mehrerer geografisch verteilter Rechenzentren, um die folgenden Business-Continuity-Ziele für die Produktionsumgebung zu erreichen:

- RTO – innerhalb von 36 Stunden nach der Meldung einer Katastrophe
- RPO – maximal 24 Stunden Verlust von Kundeninhalten

9.8 Messtools

IBM SaaS verwendet eine synthetische Überwachungslösung für die Überwachung, Messung und Meldung der Verfügbarkeit oder von Betriebsunterbrechungen für den Abgleich mit zugesagten Service-Levels. Diese Lösung simuliert und überwacht Benutzeraktionen und Benutzererfahrungen auf globaler Ebene sowohl im Hinblick auf die statische Verfügbarkeit als im Hinblick auf Transaktionen.

IBM SaaS wird auch als internes Überwachungssystem für Metriken, Ereignisse und Alerts innerhalb der gesamten Lösung eingesetzt.

9.9 Kundenreferenz

Der Kunde erklärt sich damit einverstanden, dass IBM in Werbe- oder Marketingmaterial öffentlich auf den Kunden als Subskribenten von IBM SaaS verweisen darf.

Anhang A

1. IBM Watson Health Core

IBM Watson Health Core ist eine für Gesundheitsdaten geeignete Platform-as-a-Service (PaaS), eine Entwicklungsplattform und ein operatives Subsystem, um im HIPAA definierte geschützte Gesundheitsdaten und andere Gesundheitsdaten, die sich in einem IBM eigenen oder von IBM kontrollierten Rechenzentrum befinden, gemäß den für IBM geltenden Datengesetzen zu speichern, zu pflegen und zu verarbeiten. Der Kunde muss entsprechende Berechtigungen für IBM Watson Health Core und IBM Watson Health Core Access erwerben, um die nachfolgend beschriebenen Features und Funktionen zu aktivieren.

1.1 Betriebsumgebungen von Watson Health Core

Die Watson Health Core-Berechtigung beinhaltet drei für Gesundheitsdaten geeignete Cloudbetriebsumgebungen, die dazu ausgelegt sind, dem Kunden die Verarbeitung von Gesundheitsdaten zu ermöglichen:

- Pilotumgebung

  Bietet eine Sandboxumgebung, in der die Kunden Anwendungen mithilfe von IBM SaaS entwickeln und testen können. In der Pilotumgebung sind alle HIPAA-Sicherheitsmaßnahmen implementiert, außer für Disaster-Recovery, Hochverfügbarkeit und Sicherung der Systems of Record.

- Produktionsumgebung

  Bietet eine umfassende Umgebung für die Verarbeitung von Gesundheitsdaten-Workloads. Die Produktionsumgebung ist eine hoch verfügbare Umgebung mit Lastausgleich und kann ein Failover an einen Disaster-Recovery-Standort durchführen.

- Disaster-Recovery

  Stellt eine spiegelgleiche Replik der Produktionsumgebung zur Verfügung, die sich in einem räumlich getrennten Rechenzentrum befindet.

1.2 Anwendungsentwicklung

IBM Watson Health Core ermöglicht die Anwendungsentwicklung und sichere Datenerfassung von Kundengeräten oder Geräten der berechtigten Benutzer des Kunden. Über APIs werden Programmschnittstellen und Dokumentation bereitgestellt, die von den berechtigten Benutzern und externen Service-Providern des Kunden für die Entwicklung von Anwendungen und den Datenaustausch mit IBM SaaS verwendet werden können. Die Nutzung der APIs durch den Kunden oder seine Entwickler ist an die Einhaltung der API Developer Requirements gebunden.

- REST-APIs

  Watson Health Core stellt eine Reihe von REST-APIs und Services für die Watson Health Core-Plattform bereit. Die API-Funktionen schließen unter anderem Verfahren für den Zugriff auf die Datenrepositorys, einen Datenpflegeservice, Benutzermanagement und Auditprotokolle ein.

- Apple HealthKit und Apple ResearchKit

  Watson Health Core unterstützt die Integration mit Forschungsstudien, die auf dem Apple ResearchKit API-Framework für iOS basieren, und mit dem Apple HealthKit zur Erfassung von Wellnessdaten.

1.3 Datengovernance

- Management der Einwilligungserklärungen

  Watson Health Core bietet ein Framework für die Erfassung der von Patienten oder Studienteilnehmern erteilten Einwilligungserklärungen und ist in der Lage, eine Aufzeichnung der Einwilligungserklärungen getrennt von den Nutzlastdaten sicher zu speichern, wenn sich Personen über eine Kundenanwendung registrieren, von der sie zur Erteilung einer Einwilligungserklärung aufgefordert werden.

- Datenmaskierung

  Watson Health Core bietet die Möglichkeit, Namenskennungen von strukturierten Nutzlastdaten zu trennen. Watson Health Core empfängt Daten in der Cloud über Programm-APIs. Die APIs ermöglichen die Trennung der Namenskennungen von Patienten oder Personen von den restlichen Nutzlastdaten, um sie in einem separaten verschlüsselten Datenspeicher zu speichern. Den Nutzlastdaten wird ein anonymisiertes Token zugeordnet, das zukünftig für die Herkunftsverfolgung verwendet werden kann.

1.4 Services für Gesundheitsdaten

Watson Health Core ermöglicht die Erfassung, Speicherung und Synchronisierung von Daten, einschließlich exogener Gesundheitsdaten und anderer personenbezogener Daten sowohl in strukturierter als auch in unstrukturierter Form.

- Datenaufnahme

  Watson Health Core ermöglicht das Einpflegen von Daten aus Patientenanwendungen oder Geräten über Programm-APIs. Zu diesem Zweck ist es jedem berechtigten Individuum des Kunden gestattet, bis zu 25 MB an Daten jährlich während der Vertragslaufzeit in Health Core hochzuladen. Der Service ist für bis zu 10 Uploads pro Individuum und Tag ausgelegt.

- Operativer Data Lake (Datensee)

  Rohdaten über Kunden oder Patienten werden in nativer Form in Watson Health Core gespeichert, bis sie für die Analyse und Modellierung benötigt werden.

- Extract Transform Load (ETL)

  Die Daten werden innerhalb des operativen Subsystems in ein normalisiertes Format umgesetzt. Ein auf Branchenstandards basierender Enterprise Service Bus für das Gesundheitswesen ermöglicht die Integration über mehrere verschiedene Kundenanwendungen und Protokolle.

- Data Reservoir (Datenreservoir)

  Nach der Aufbereitung werden die Daten in das Data Reservoir übertragen. Watson Health Core nutzt Aspekte des IBM Unified Data Model for Healthcare, um geschäftliche und technische Gesundheitsdaten für die Verwendung in Analysen zu normalisieren.

- Master Person Index

  Watson Health bietet Tools für die Stammdatenverwaltung, um Daten aus mehreren Quellen für die Erstellung einer longitudinalen Patientenakte (Longitudinal Patient Record = LPR) zu konsolidieren.

2. Optionale Features

2.1 IBM Watson Health Core Terminology Service

Dieser Add-on-Service vereinfacht die Datenintegration und -interoperabilität zwischen unterschiedlichen Gesundheitssystemen, indem konsistente klinische Terminologie für alle Watson Health Cloud-Anwendungen bereitgestellt wird. Dieser Service verfügt über eine funktionale Plattform für alle Aufgaben, bei denen Terminologien, Codesysteme und strukturierte Inhalte eine Rolle spielen, wie beispielsweise:

- die Erstellung neuer Codesysteme,
- die Übersetzung internationaler Codesysteme und
- der Abgleich zwischen nationalen Codelisten und internationalen Standards.

Anhang B

Das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) wird von IBM, so wie im Berechtigungsnachweis angegeben, für IBM SaaS bereitgestellt. Das SLA stellt keine Gewährleistung dar. Es wird nur Kunden zur Verfügung gestellt und gilt ausschließlich für Produktionsumgebungen.

1. Gutschriften für Ausfallzeiten

Rückvergütungen bei Nichtverfügbarkeit des Service kommen nur bei Subscription-Gebühren für Berechtigungen auf der Basis von Individuen zur Anwendung.

Der Kunde muss innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass ein Vorfall die Verfügbarkeit von IBM SaaS beeinträchtigt, ein Support-Ticket der Fehlerklasse 1 beim IBM Help-Desk für technische Unterstützung öffnen. Der Kunde ist verpflichtet, IBM in angemessener Weise bei der Diagnose und Lösung des Problems zu unterstützen.

Der Anspruch aus einem Support-Ticket aufgrund der Nichteinhaltung eines SLA muss innerhalb von drei (3) Arbeitstagen nach Ablauf des Vertragsmonats geltend gemacht werden. Die Entschädigung für einen berechtigten Anspruch aus einem SLA wird als Gutschrift gewährt und mit einer künftigen Rechnung für IBM SaaS verrechnet. Sie basiert auf dem Zeitraum, in dem das Produktionssystem nicht zur Verarbeitung von IBM SaaS zur Verfügung stand („Ausfallzeit“). Die Erfassung der Ausfallzeit beginnt mit der Meldung des Vorfalls durch den Kunden und endet, wenn IBM SaaS wiederhergestellt ist. Als Ausfallzeit zählen nicht: Zeiten für vorab geplante oder angekündigte Unterbrechungen zur Durchführung von Wartungsarbeiten; Gründe, die IBM nicht zu vertreten hat; Probleme mit dem Inhalt, der Technologie, den Entwürfen oder den Anweisungen des Kunden oder Dritter; nicht unterstützte Systemkonfigurationen und Plattformen oder andere Fehler des Kunden; vom Kunden verursachte Sicherheitsvorfälle oder vom Kunden durchgeführte Sicherheitstests. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit von IBM SaaS während jedes einzelnen Vertragsmonats anwenden (siehe die nachstehende Tabelle). Die Gesamtentschädigung für einen beliebigen Vertragsmonat wird 20 Prozent von einem Zwölftel (1/12) der Jahresgebühr für IBM SaaS nicht überschreiten.

2. Service-Levels

IBM SaaS-Verfügbarkeit in einem Vertragsmonat

Verfügbarkeit in einem Vertragsmonat	**Entschädigung (in Prozent (%) der monatlichen Subscription-Gebühr* für Berechtigungen auf der Basis von Individuen für den Vertragsmonat, der Gegenstand des Anspruchs ist)**
< 99,95 %	10 %
< 99,0 %	20 %

* Wurde das IBM SaaS-Angebot von einem IBM Business Partner erworben, so wird die monatliche Subscription-Gebühr auf der Basis des zum jeweiligen Zeitpunkt gültigen Listenpreises für IBM SaaS berechnet, der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%). Eine eventuelle Rückvergütung von IBM wird direkt an den Kunden geleistet.

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in einem Vertragsmonat.

Beispiel: 108 Minuten Gesamtausfallzeit in einem Vertragsmonat

43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 108 Minuten Ausfallzeit = 43.092 Minuten _____ 43.200 Minuten insgesamt	= Gutschrift für Ausfallzeiten in Höhe von 10 % bei einer Verfügbarkeit von 99,75 % in einem Vertragsmonat

3. Ausschlüsse

Dieses SLA gilt nicht:

- abgesehen von der Serverüberwachung, für gehostete virtuelle Maschinen, die angepasste oder Kundenanwendungen unterstützen.
- wenn der Kunde wesentliche Verpflichtungen im Rahmen der aktuellen Verpflichtungen aus dem Vertrag nicht erfüllt hat.

Anhang C

In diesem Anhang für Sicherheit und Business-Continuity sind bestimmte Anforderungen und Verpflichtungen von IBM bei der Bereitstellung von IBM SaaS für den Kunden festgelegt. Diese Anforderungen und Verpflichtungen ergänzen diejenigen, die in der Beschreibung der Grundsätze der Datensicherheit für IBM SaaS festgelegt sind, die unter http://www.ibm.com/cloud/data-security zur Verfügung stehen. Alle Begriffe, die in diesem Anhang nicht definiert sind, haben die im Vertrag oder in den Nutzungsbedingungen festgelegte Bedeutung.

1. Informationssicherheitsprogramm

IBM verfügt über interne Sicherheitsrichtlinien, Standards und Prozesse, die auf dem Regelwerk und den Kontrollbereichen von ISO 27001 basieren. Neben den Grundsätzen der Unternehmensführung (Governance) der IBM Corporate Security Organization werden diese Richtlinien, Standards und Prozesse regelmäßig internen Audits unterzogen.

Das Informationssicherheitsprogramm von IBM umfasst organisatorische, operative, administrative, physische und technische Sicherheitsvorkehrungen, die für die Verarbeitung, Speicherung und Übertragung von Kundeninhalten gelten und mindestens die Anforderungen in diesem Anhang abdecken.

IBM wird dem Kunden auf Anfrage Informationen über das Informationssicherheitsprogramm von IBM Watson Health zur Verfügung stellen, damit sich der Kunde ein Bild von der fortdauernden Eignung, Angemessenheit und Effektivität des Programms machen kann. Das Informationssicherheitsprogramm von IBM Watson Health wird regelmäßig aktualisiert, um mit den allgemein anerkannten branchenspezifischen Verfahren und den für IBM geltenden Gesetzen Schritt zu halten.

2. Zugriffskontrollen

IBM wird Kundeninhalte nur Mitarbeitern, Unterauftragnehmern oder Dritten offenlegen, die aus legitimen geschäftlichen Gründen Zugriff auf die Kundeninhalte haben müssen, um IBM bei der Erfüllung ihrer Verpflichtungen gegenüber dem Kunden oder anderen Personen zu unterstützen, soweit dies zur Bereitstellung von IBM SaaS gemäß den geltenden Gesetzen, dem Vertrag oder einem zugehörigen Dokument, sofern anwendbar, erforderlich ist. Ist IBM ein Business Associate (Geschäftspartner) des Kunden, so werden IBM und der Kunde persönliche Gesundheitsdaten nur in Übereinstimmung mit den Bedingungen einer gültigen Business-Associate-Vereinbarung zwischen den Vertragsparteien offenlegen.

IBM hat einen formalen internen Zugriffsmanagementprozess für Benutzer etabliert, nach dem der Benutzerzugriff formal angefordert, nach der Identitätsprüfung genehmigt und abhängig vom begründeten Informationsbedarf unter Anwendung des Prinzips der geringsten Rechte erteilt wird. Der Zugriff auf Kundeninhalte ist auf aktive Benutzer und aktive Benutzerkonten beschränkt. Im Rahmen eines formalen Prozesses findet regelmäßig eine interne Revalidierung der Zugriffe aktiver Benutzerkonten statt.

IBM verwendet sichere Benutzerauthentifizierungsprotokolle; aktiven Benutzerkonten auf Systemen, die zur Bereitstellung von Services für Kunden dienen, werden eindeutige Kennungen und sichere Kennwörter nach den IBM Sicherheitsstandards und -richtlinien zugeordnet:

a. Kennwörter dürfen keine voreingestellten Kennwörter des Herstellers sein und müssen an Orten und/oder in Formaten aufbewahrt werden, die die Sicherheit der Daten, die sie schützen sollen, nicht gefährden.

b. Kennwörter müssen beim Anzeigen und Drucken maskiert, unterdrückt oder auf andere Weise unkenntlich gemacht werden, sodass unbefugte Dritte diese nicht erspähen oder später wiederherstellen können. Kennwörter dürfen bei der Eingabe nicht protokolliert oder erfasst werden. Benutzerkennwörter dürfen nicht als Klartext gespeichert werden.

c. Kennwörter werden für jede Technologie, einschließlich IBM SaaS, so gewählt, dass Risiken im Zusammenhang mit bekannten Schwachstellen bei der Kennwortlänge begrenzt werden, und müssen dokumentiert werden.

d. Wenn aus betrieblichen Gründen die Verwendung interner, privilegierter, gemeinsam genutzter Funktions-IDs erforderlich ist, übernimmt IBM die Verwaltung der gemeinsam genutzten Funktions-IDs und/oder System-IDs, indem Kennwörter ausgescheckt werden müssen, um die persönliche Verantwortlichkeit zu wahren.

Für alle Systeme und Anwendungen, die Kundeninhalte speichern, werden Inaktivitätszeitlimits festgelegt.

Falls erforderlich, erhalten Kunden auf Anforderung und nach ausdrücklicher Zustimmung von IBM Remotezugriff auf das Netz, die Systeme und Anwendungen von IBM, in denen Kundendaten gespeichert sind. Alle dazu verwendeten Fernverbindungen sind durch strikte Authentifizierungs- und Verschlüsselungsprotokolle abgesichert. Remotezugriffsaktivitäten werden protokolliert und überwacht.

Falls IBM im Rahmen der Bereitstellung von IBM SaaS remote auf ein System innerhalb der internen Netze des Kunden zugreifen muss, erfolgen alle Remotezugriffe ausschließlich über sichere Kundensysteme und Protokolle für den Remotezugriff und unter Verwendung der vom Kunden bereitgestellten Zugriffsberechtigungsnachweise. Der Remotezugriff auf das Netz des Kunden wird nur auf Anforderung von IBM und nach der Zustimmung des Kunden sowie in Übereinstimmung mit den zum jeweiligen Zeitpunkt gültigen Richtlinien des Kunden eingerichtet, die IBM vorab zur Verfügung gestellt werden. Die Nutzung der internen Netze des Kunden durch IBM unterliegt den IT-Nutzungs- und Sicherheitsrichtlinien des Kunden, die IBM vorab zur Verfügung gestellt werden.

Innerhalb von IBM werden Aufgaben im Zusammenhang mit der Verwaltung von Sicherheitsfunktionen, der Zugriffsprüfung und der Untersuchung von Sicherheitsverstößen strikt getrennt.

Die Speicherung, das Hosting und die Verarbeitung kundenspezifischer Inhalte sind logisch von den Inhalten anderen Kunden, die von IBM betreut werden, getrennt. In Fällen, in denen ein gemeinsamer Arbeitsbereich für die Speicherung, das Hosting und die Verarbeitung vom Kunden genehmigt wird, hat IBM Verfahren und Sicherungsmaßnahmen eingerichtet, die den in diesem Anhang für Sicherheit und Business-Continuity festgelegten Anforderungen entsprechen, um die unbefugte Offenlegung der Kundeninhalte zu verhindern.

IBM etabliert Clean-Desk/Clear-Screen-Richtlinien, um sicherzustellen, dass Kundeninhalte zu keiner Zeit an öffentlich zugänglichen Orten unbeaufsichtigt sind.

3. Übertragung und Verschlüsselung

IBM wird geeignete Vorsichtsmaßnahmen bei der Übertragung von Kundeninhalten (per Fax, E-Mail, Kurier usw.) ergreifen, um sicherzustellen, dass die korrekten Kontaktinformationen für den Empfänger verwendet werden, und den vorgesehenen Empfänger vorab informieren, damit dieser vorab Vorkehrungen für einen sicheren Erhalt der Informationen treffen kann.

IBM verwendet jederzeit geeignete Formen der Verschlüsselung oder andere sichere Technologien bei der Verarbeitung von Kundeninhalten sowie der Übertragung, der Kommunikation, dem Remotezugriff oder der Speicherung (einschließlich Backup-Speicherung) der Kundeninhalte und wird dafür Sorge tragen, dass die IBM Mitarbeiter sich ebenso verhalten. Beispielsweise werden alle Datensätze und Dateien, die Kundeninhalte enthalten, mit einem geeigneten Standardverschlüsselungsverfahren verschlüsselt. Dies gilt für Kundendaten:

a. die auf IBM Laptops, mobilen Geräten oder mobilen elektronischen Medien, wie beispielsweise Sicherungsbändern, gespeichert sind und zur Aufbewahrung an einen externen Speicherort gebracht werden;

b. die außerhalb der physisch gesicherten Büroräume und Einrichtungen des Kunden oder von IBM gespeichert oder transportiert werden, mit Ausnahme von Papierdokumenten;

c. während der Übertragung durch IBM über öffentliche Netze;

d. während der Übertragung von IBM Systemen an den Kunden;

e. während der drahtlosen Übertragung durch IBM und

f. die von IBM auf Servern und in Datenbanken gespeichert werden.

4. Netzsicherheit

IBM verwendet hinreichend aktuelle Versionen von Systemsicherheitssoftware, wie Firewalls, Proxys, Webanwendungsfirewalls und Schnittstellen. Diese Software muss Malwareschutz und hinreichend aktuelle Patches und Virusdefinitionen enthalten. Gemäß den Unternehmensstandards muss Antivirensoftware, sofern technisch möglich, auf Workstations, Servern und zugehörigen Endpunkten installiert werden, und die Software wird nach der unternehmensinternen Richtlinie mit internen Managementlösungen verwaltet.

IBM überwacht IBM SaaS, um Sicherheitsvorfälle so früh wie möglich zu erkennen und aufzudecken. Dabei wird IBM mindestens dem Branchenstandard entsprechende Intrusion-Detection- und Prevention-

Tools sowie Überwachungs- und Rückmeldungsprozesse auf eine Art und Weise einsetzen, dass sowohl interne als auch externe Sicherheitslücken und Risiken aufgedeckt werden, die eine unbefugte Offenlegung, missbräuchliche Verwendung, Änderung oder Vernichtung von Kundeninhalten oder Informationssystemen, die zur Bereitstellung von Services für den Kunden verwendet werden, zur Folge haben könnten.

IBM nutzt Vulnerability-Intelligence-Services oder Mitteilungsdienste zur Informationssicherheit und andere einschlägige Quellen, die aktuelle Informationen über Sicherheitslücken in Systemen bereitstellen. IBM führt regelmäßig Schwachstellenanalysen und Korrekturen am IBM Netz durch.

IBM überwacht IBM SaaS, um Sicherheitsvorfälle zu erkennen, aufzudecken, einzudämmen und zu beheben.

IBM prüft die Verfügbarkeit, Integrität und Effektivität der Netzsicherheitsinfrastruktur, auf deren Basis IBM SaaS über die Freigabemanagementprozesse von IBM zur Verfügung gestellt wird.

5. Vorfallmanagement und Benachrichtigung

Die IBM Watson Health-Teams arbeiten mit dem IBM Cybersecurity Incident Response-Team, einem globalen Team, zusammen, das im Zusammenhang mit IBM Angeboten aufgetretene Sicherheitsvorfälle untersucht und intern koordiniert, um vorbeugende Maßnahmen zur Verringerung softwarebezogener Sicherheitsprobleme umzusetzen. Ein „Sicherheitsvorfall“ ist der erfolgreiche unbefugte Zugriff oder die erfolgreiche unbefugte Nutzung, Offenlegung, Änderung oder Beeinträchtigung von Systemoperationen oder Daten in einem Informationssystem, das von IBM für die Bereitstellung von IBM SaaS verwendet wird. Sobald ein Sicherheitsvorfall aufgedeckt wird (durch Routine-Scans, Alerts, Schwellenwertereignisse usw.), wird IBM:

a. den Kunden über jeden bestätigten Sicherheitsvorfall, von dem Kundeninhalte betroffen sind, so früh wie möglich, aber keinesfalls später als 2 Arbeitstage nach der Untersuchung und Bestätigung des Sicherheitsvorfalls informieren;

b. den Kunden unverzüglich nach der Aufforderung durch eine staatliche Stelle (einschließlich einer Datenschutz- oder Strafverfolgungsbehörde), die Zugriff auf oder Informationen über Kundeninhalte verlangt, informieren, es sei denn, dass dies IBM kraft Gesetz oder aufgrund einer Anordnung untersagt ist; und

c. den Kunden vorab über Offenlegungen, Übertragungen oder Zugriffe auf Kundeninhalte durch Dritte informieren, außer wenn diese gemäß dem Abschnitt „Zugriffskontrollen“ dieses Anhangs für Sicherheit und Business-Continuity zulässig sind.

6. Protokollierung

IBM hat gemäß den IBM Richtlinien und Verfahren sowie den allgemein anerkannten Branchenstandards Maßnahmen eingeführt, um Systeme hinreichend auf unbefugte Zugriffe auf verarbeitete Kundendaten und deren unbefugte Verwendung zu überwachen. Tatsächliche unbefugte Anmeldungen und Anmeldeversuche sowie Zugriffsverletzungen werden protokolliert.

IBM bewahrt Aufzeichnungen aller Zugriffsanforderungen und Protokolle der Zugriffsaktivitäten für alle Systeme, auf denen Kunden- und Gesundheitsdaten gespeichert, aufgerufen, verarbeitet und übertragen werden, so lange auf, wie dies vom HIPAA und anderen für IBM geltenden Gesetzen gefordert wird.

Die Protokolle und Berichte enthalten mindestens (i) alle erfolgreichen und nicht erfolgreichen Anmeldeversuche, einschließlich angemessener Identifikationsinformationen; (ii) alle System- und Netzkonfigurationsänderungen, einschließlich der Anwendungsinstallationen sowie der Änderungen des Benutzermanagements und der Dateizugriffsberechtigungen; (iii) erfolgreiche und nicht erfolgreiche Zugriffsversuche auf Ressourcen, einschließlich der versuchten Zugriffe auf Dateien, gemeinsam genutzte Netzbereiche, Protokolle oder andere Ressourcen, sowie (iv) Datendownloads, einschließlich der Inhaltstypen der Daten und der zum Download verwendeten Zugriffsprotokolle.

7. Entwicklung von Softwareanwendungen und Change-Management

IBM befolgt sichere Anwendungsentwicklungs- und Programmiertechniken, die die Integrität von Produktionsanwendungen und des zugehörigen Quellcodes vor unbefugten und nicht getesteten Änderungen schützen.

IBM orientiert sich an einem Change-Management-Prozess, der (a) die Aufzeichnung und ausdrückliche Genehmigung von Änderungen sowie Rücksetzungsverfahren und (b) entsprechende Tests für solche Änderungen, einschließlich gegebenenfalls Benutzerabnahmetests, sowie Sicherheitstests einschließt.

IBM folgt einem Patch-Management-Prozess, der das Testen der Patches vorsieht, bevor sie auf allen Systemen installiert werden, die für die Speicherung, den Zugriff und die Übertragung von Kundeninhalten oder für die Bereitstellung von Services für den Kunden, einschließlich IBM SaaS, verwendet werden.

IBM verlangt, dass Systemadministratoren vollständige, korrekte und aktuelle Informationen über die Konfiguration aller Informationssysteme vorhalten, die für die Speicherung, den Zugriff und die Übertragung von Kundeninhalten eingesetzt werden.

8. Physische und umgebungsbezogene Sicherheit

Die IBM Watson Health Core-Plattform wird auf der IBM SoftLayer-Dateninfrastruktur bereitgestellt. IBM SoftLayer gewährleistet physische und umgebungsbezogene Sicherheit, Zugriffskontrolle sowie Kontrollmechanismen und Prozesse, um die Kundendaten vor Verletzungen und Einflüssen durch den Menschen, die Umwelt und die Technik zu schützen.

Der allgemeine Zugang zu den Einrichtungen, in denen IBM SaaS gehostet ist, wird über ein Kartenzutrittssystem gesteuert. An allen Standorten sind Videoüberwachungsanlagen installiert, die vom Sicherheitspersonal überwacht werden. Ausgewählte Zugangstüren sind alarmgesichert und die Alarmanlagen werden vom Sicherheitspersonal überwacht.

Der Zutritt zu kontrollierten Bereichen wird durch die Verwendung von Zutrittskarten und/oder zusätzliche biometrische Prüfung eingeschränkt. Alle Personen ohne Zutrittsberechtigung zu den kontrollierten Bereichen müssen sich anmelden und werden von einer Person mit Zutrittsgenehmigung zu den kontrollierten Bereichen begleitet. Alle Notausgänge der kontrollierten Bereiche sind mit akustischen Alarmanlagen ausgerüstet, die vom Sicherheitspersonal überwacht werden. Die Alarmanlagen werden regelmäßig auf ihre Funktionstüchtigkeit hin überprüft und die Prüfergebnisse werden dokumentiert und aufbewahrt. Die Zutrittsrechte zu kontrollierten Bereichen werden vierteljährlich neu überprüft. Bei Beendigung oder Kündigung des Arbeitsverhältnisses wird der Zutritt zu den kontrollierten Bereichen entzogen.

Die Einrichtungen werden vor Umwelteinflüssen wie Feuer, Wasser und Hitze mithilfe von Feuer- und Rauchmeldern, Feuerlöschern sowie Feuerschutz- und Feuerlöschanlagen geschützt. Der Schutz der Einrichtungen vor Stromunterbrechungen oder Stromausfällen erfolgt über unterbrechungsfreie Stromversorgungsanlagen und Notstromaggregate, die regelmäßig gewartet und getestet werden.

Informationen und Berichte zur Compliance bei IBM SoftLayer sind unter http://www.softlayer.com/compliance zu finden.

9. Unterbrechungsfreier Geschäftsbetrieb

IBM verfügt über Business-Continuity- und Disaster-Recovery-Pläne, die dazu ausgelegt sind, einen Service-Level entsprechend den Verpflichtungen von IBM unter dem Vertrag aufrechtzuerhalten. Die Business-Continuity- und Disaster-Recovery-Pläne werden laufend aktualisiert und getestet (mindestens einmal pro Jahr). IBM wird alle angemessenen Änderungen an den Business-Continuity- und Disaster-Recovery-Plänen durchführen, die erforderlich sind, um die Einhaltung allgemein anerkannter Branchenstandards sicherzustellen, ohne dabei IBM SaaS oder die vom Kunden genutzte Produktionsumgebung übermäßig zu beeinträchtigen.

Falls sich eine Katastrophe abzeichnet, die dazu führt, dass IBM SaaS nicht mehr verfügbar ist, wird IBM den Kunden unverzüglich benachrichtigen und den Business-Continuity- und Disaster-Recovery-Plan aktivieren. Ist der Katastrophenfall eingetreten, so soll der Zugriff des Kunden auf IBM SaaS gemäß dem Business-Continuity-Ziel wie folgt wiederhergestellt werden: Bei einem Ausfall der IBM Watson Health-Produktionsumgebung besteht die Zielsetzung für die Wiederherstellungszeit (Recovery Time Objective = RTO) darin, die Produktionsumgebung innerhalb von 36 Stunden nach der Meldung des Katastrophenfalls wiederherzustellen. Die Zielsetzung für den Wiederherstellungspunkt (Recovery Point Objective = RPO) beträgt maximal 24 Stunden in Bezug auf den Verlust von Kundeninhalten innerhalb der Produktionsumgebung. Die Business-Continuity-Ziele für bestimmte Watson Health-Lösungen können unterschiedlich sein.

Das IBM Disaster-Recovery-Konzept besteht in der Nutzung mehrerer geografisch verteilter Rechenzentren.

Alle IBM SoftLayer-Rechenzentren verfügen über mehrere Stromzuführungen, Glasfaserverbindungen, dedizierte Generatoren und Notstromversorgung. Sie basieren auf branchenführenden Hardwarelösungen und Bauteilen, um höchste Leistung, Zuverlässigkeit und Interoperabilität

sicherzustellen. Alle Komponenten der Rechenzentren, einschließlich zum Beispiel der redundanten n+1 Stromversorgungs- und Kühlungsressourcen, werden überprüft, um die Stabilität innerhalb der Rechenzentren zu gewährleisten.

10. Compliance

Die Sicherheitsverfahren von IBM basieren auf ISO 27001-27002. Diese Verfahren bieten die Kontrollstrukturen für Risikoanalyse, physische Sicherheit, Notfallplanung, Untersuchungen, Informationsschutz, Schulung, Datenschutz und Operationen und vieles mehr.

IBM überprüft alle Aktivitäten im Zusammenhang mit Sicherheit und Datenschutz auf Einhaltung der IBM Sicherheitsverfahren.

IBM hält alle für IBM geltenden Datengesetze in den beteiligten Ländern ein.

Des Weiteren ist nach den Geschäftsgrundsätzen (Business Conduct Guidelines) von IBM die ordnungsgemäße Handhabung der vertraulichen Informationen des Kunden unerlässlich. Die Geschäftsgrundsätze müssen von allen Mitarbeitern jährlich überprüft werden (und die Überprüfung muss von ihnen bestätigt werden).

11. Sonstiges

IBM wird sicherstellen, dass alle Vereinbarungen mit Unterauftragnehmern und/oder Dritten, die an der Bereitstellung von IBM SaaS beteiligt sind, Bedingungen enthalten, durch die die Kundeninhalte in mindestens dem gleichen Maße geschützt werden wie durch die Bedingungen dieses Anhangs für Sicherheit und Business-Continuity und etwaiger zur Anwendung kommender zugehöriger Dokumente, soweit solche Bedingungen für die Services anwendbar sind, die von den Unterauftragnehmern und/oder Dritten ausgeführt werden sollen.