Zuletzt überarbeitet am: 1. März 2018

Anlage zur Sicherheit von Citrix Diensten

In dieser Anlage zur Sicherheit von Citrix Diensten (der Anlage) werden die technischen und organisatorischen Sicherheitskontrollen beschrieben, die im Zusammenhang mit Citrix Cloud Diensten, technischen Supportdiensten oder Beratungsdiensten im Rahmen einer Lizenz, eines Abonnements oder einer Dienstvereinbarung von Citrix verwendet werden. Diese Anlage wird durch Bezugnahme in diese Dienstvereinbarungen (die „Vereinbarungen“) aufgenommen. Diese Anlage gilt nicht für Beta-, Technology Preview- oder Labs-Dienste, einschließlich Citrix Cloud Labs.
Definierte Begriffe haben die in der Vereinbarung oder hierin, einschließlich Artikel 7 „Begriffsbestimmungen“ unten, definierte Bedeutung.

Artikel 1. Citrix Sicherheitskontrollen

In diesem Artikel werden die physischen, logischen und administrativen Kontrollen beschrieben, die Citrix einsetzt, um die Dienste zu sichern, sowie die zugehörigen Sicherheitsverpflichtungen der Kunden. Citrix nutzt ISO/IEC 27002 als Grundlage für das Dienstsicherheitsprogramm.

Die in Artikel 1.A angegebenen Kontrollen beziehen sich auf alle Dienste. Die zusätzlichen, in Abschnitt 1.B angegebenen Kontrollen gelten für alle allgemein verfügbaren Citrix Cloud Services (zusammen auch „Cloud-Dienste“).

Citrix behält sich das Recht vor, die in diesem Artikel 1 angegebenen Kontrollen zu ändern, vorausgesetzt, die während einer Dienstlaufzeit, für die der Kunde gezahlt hat, verwendeten Kontrollen schützen die Kundeninhalte mindestens ebenso gut wie die in diesem Artikel 1 zum Tag des Intrafttretens der Laufzeit angegebenen.

1.A. Unternehmenssicherheitskontrollen – Alle Dienste

Gebiet	Kontrolle(n)
Sicherheitsprogramm-Management	**Sicherheitsbesitz**. Citrix hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitskontrollen für die Dienste zuständig sind. **Sicherheitsrollen und Zuständigkeiten**. Citrix Mitarbeiter mit Zugriff auf Kundeninhalte unterliegen Geheimhaltungspflichten. **Dienstsicherheitsrichtlinien.** Citrix unterhält ein umfassendes Global Security Framework (GSF), das die übergeordneten Sicherheitsprinzipien bereitstellt, die von der Citrix Geschäftsführung festgelegt und genehmigt wurden. Richtlinien fassen

Gebiet	Kontrolle(n)
	Sicherheitsanforderungen klar und knapp zusammen. Standards definieren den Prozess oder die Methodik zum Erfüllen der Richtlinienanforderungen. Das GSF-Sicherheitsprogramm wird regelmäßig überprüft und ausgewertet. Citrix pflegt eine Zusammenfassung des GSF-Programms, die den Kunden auf Anfrage bereitgestellt wird. **Produktrisiko-Management** Citrix führt Beurteilungen für wichtige Risikobereiche durch, die den Diensten zugeordnet sind, darunter beispielsweise und wie zutreffend Datenschutzrisikobewertungen, Open Source-Überprüfungen und Exportkontrollanalysen.
Asset-Management	**Asset-Bestand**. Citrix pflegt einen Bestand der von Citrix verwalteten Ausrüstung, die zur Erbringung der Dienste verwendet wird („Assets“). Identifizierte Systembesitzer sind für die Pflege und Aktualisierung des Bestands wie erforderlich zuständig. **Umgang mit Assets und Daten** Citrix identifiziert und klassifiziert Kundeninhalte, um sicherzustellen, dass der Zugriff angemessen eingeschränkt wird. Citrix legt Einschränkungen für das Drucken von Kundeninhalten und das Entsorgen von Druckmaterial mit Kundeninhalten fest. Citrix Mitarbeiter müssen vor dem Speichern von Kundeninhalten auf portablen Geräten, dem Remotezugriff auf Kundeninhalte oder dem Verarbeiten von Kundeninhalten außerhalb der von Citrix oder seinen Dienstanbietern verwalteten Geschäftsräume eine Autorisierung erhalten.
Zugriffsmanagement	**Zugriffsrichtlinie.** Citrix pflegt einen Datensatz der Sicherheitsberechtigungen von Personen, die Zugriff auf Kundeninhalte haben, und befolgt das Prinzip der niedrigsten Berechtigung. **Zugriffsautorisierung** Citrix pflegt und aktualisiert einen Datensatz der Mitarbeiter, die Zugriff auf Citrix Systeme mit Kundeninhalten haben. Ein Neuzugriff auf Systeme wird vor der Gewährung von der Geschäftsführung überprüft und genehmigt. Citrix führt regelmäßig Überprüfungen von Benutzerkonten und zugewiesenen Berechtigungen für wichtige Systeme durch. Citrix identifiziert die Mitarbeiter, die autorisierte Zugriffsrechte auf Daten und Ressourcen gewähren, ändern oder stornieren dürfen.

Gebiet	Kontrolle(n)
	Citrix stellt für den Fall, dass mehr als eine Person Zugriff auf Systeme mit Kundeninhalt hat, sicher, dass die einzelnen Personen getrennte IDs bzw. Anmeldeinformationen haben. **Niedrigste Berechtigung** Citrix schränkt den Zugriff auf Kundeninhalte auf nur diejenigen Personen ein, die den Zugriff zur Ausübung der Funktionen ihrer Stelle benötigen. **Integrität und Vertraulichkeit** Citrix verlangt, dass Benutzer Computer und Daten sichern, während diese unbeaufsichtigt sind. Citrix verlangt, dass Kenntwörter während des Lebenszyklus nicht erkennbar bleiben. **Authentifizierung** Citrix verwendet Branchenstandardpraktiken, um Benutzer, die auf Informationssysteme zugreifen, zu identifizieren und zu authentifizieren. Im Fall von auf Kennwörter gestützten Authentifizierungsmechanismen befolgt Citrix Branchenstandardpraktiken für den Umgang mit und die Verwaltung von Kennwörtern. Dazu zählen Folgende: Kennwörter werden regelmäßig geändert, wie von den Systemanforderungen und Citrix Standards vorgeschrieben. Kennwörter müssen den Längen- und Komplexitätsanforderungen entsprechen, darunter einer Mindestlänge von 8 Zeichen. Die Mitarbeiter dürfen keine Kennwörter weitergeben. Deaktivierte oder abgelaufene IDs werden nicht an andere Personen vergeben. Citrix pflegt Verfahren zum Deaktivieren von Kennwörtern, die fehlerhaft sind oder versehentlich offengelegt wurden. Citrix überwacht wiederholte Versuche, mit einem ungültigen Kennwort Zugriff auf die Dienste zu erhalten. Citrix verwendet Praktiken, die darauf ausgerichtet sind, die Vertraulichkeit und Integrität der Kennwörter zu schützen, die zugewiesen, verteilt und gespeichert werden.

Gebiet	Kontrolle(n)
Verlustverhinderung	**Schadsoftware**. Citrix verwendet Antivirensoftware und andere Kontrollen, um zu verhindern, dass Schadsoftware unberechtigten Zugriff auf Kundeninhalte erhält, darunter Schadsoftware aus öffentlichen Netzwerken. **Medienentsorgung.** Citrix entsorgt nicht mehr benötigte Medien entsprechend ihrer Klassifizierung und verwendet sichere Löschprozesse.
Physische und Umgebungssicherheit (Zugangskontrolle, Verfügbarkeitskontrolle)	**Physischer Zugang zu Citrix Einrichtungen**. Citrix beschränkt den Zugang zu Einrichtungen auf autorisierte Personen. Mitarbeiter, Vertragnehmer und Gäste benötigen ID-Badges, die während des Aufenthalts in der Einrichtung jederzeit sichtbar getragen werden müssen. Citrix überwacht die Eingänge zu den Einrichtungen mit verschiedenen Methoden, darunter Wachpersonal, Eindringmeldesysteme und Überwachungskameras. **Schutz vor Unterbrechungen**. Citrix verwendet Systeme für den Schutz vor Datenverlust wegen Stromausfall oder Leitungsstörungen, darunter eine globale und redundante Dienstinfrastruktur, die mit Notfallwiederherstellungs-Sites eingerichtet ist. Datencenter und Internetdienstanbieter (ISPs) werden ausgewertet, um die Leistung hinsichtlich der Bandbreite, Latenz und Isolierung bei der Notfallwiederherstellung zu optimieren. Datencenter werden in sicheren Einrichtungen untergebracht, die unabhängig von den ISPs sind und physische Sicherheit, redundante Stromversorgung und redundante Infrastruktur aufweisen. Mit den wichtigsten Anbietern werden Betriebszeitvereinbarungen abgeschlossen. **Gehostete Datencenter.** Wenn Citrix Datencenter von Dritten mit gemeinsamem Standort für die Bereitstellung der Dienste verwendet, verlangt Citrix, dass der Dienstanbieter die physischen und Umgebungssicherheitsanforderungen für von Citrix verwaltete Einrichtungen erfüllt oder übertrifft. Zu den Mindestsicherheitsanforderungen zählen u. a.: • Beschränkungen und Schutz des physischen Zugangs (Authentifizierung, Protokolle, Überwachung usw.) • Angemessene Trennung der Umgebungen • Mechanismen zur Unterdrückung, Entdeckung und Verhütung von Bränden • Klimakontrollsysteme (Temperatur, Luftfeuchtigkeit usw.) **Cloud Computing.** Wenn Citrix XaaS [Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)] zur Bereitstellung von Diensten verwendet, so stellt Citrix XasS-Anbieter ein, die im Wesentlichen vergleichbare physische Zugangskontrollen für ihre gehosteten Datencenter bereitstellen.

Gebiet	Kontrolle(n)
Anwendungs- und Entwicklungssicherheit	**Systementwicklung und -instandhaltung.** Citrix verwendet einen Prozess namens Secure by Design (bauartbestimmte Sicherheit). Dazu zählen Standards und Änderungskontrollverfahren, die dafür ausgelegt sind, Sicherheitsanforderungen für Informationssysteme, Codeüberprüfung und Tests sowie Sicherheit bei der Verwendung von Testdaten zu erfüllen. Dieser Prozess wird von einem spezialisierten Sicherheitstechnikerteam verwaltet und überwacht, das auch für die Designüberprüfung, Bedrohungsmodellierung, manuelle Codeüberprüfung und Stichprobenprüfungen sowie Durchdringungstests zuständig ist. **Open-Source-Management**. Citrix verwendet ein softwarebasiertes System für die Verwaltung von Open-Source-Prüfungen und -Genehmigungen. Zudem führt Citrix regelmäßig Scans und Prüfungen seiner Softwareprodukte durch, um die Einhaltung der Open-Source-Bestimmungen zu bestätigen. **Änderungsmanagement.** Citrix verwendet Änderungskontrollverfahren, die dafür ausgelegt sind, Sicherheitsanforderungen für Informationssysteme, Tests, Akzeptanz von Tests sowie Sicherheit bei der Verwendung von Testdaten zu erfüllen. Software- und Konfigurationsänderungen werden anhand von Standardticketsystemen verwaltet und verfolgt.
Sichere Vorgänge	**Netzwerkdesign**. Citrix implementiert Mechanismen, die dafür ausgelegt sind, Zugriffsmanagementrichtlinien und -standards über die Dienste hinweg durchzusetzen, darunter Netzwerkkontrollen bezüglich des Zugriffs auf Kundeninhalte. Dazu zählen wie zutreffend: Konfigurieren einer nicht vertrauenswürdigen Zwischenzone zwischen dem Internet und dem internen Netzwerk, die einen Sicherheitsmechanismus umfasst, um den Zugriff und unautorisierten Datenverkehr einzuschränken; sowie die Trennung von Web- und Anwendungsservern von den entsprechenden Datenbankservern in einer geschichteten Struktur, die den Datenverkehr zwischen den Schichten einschränkt.
Vorfallmanagement	**Vorfallreaktion**. Citrix unterhält ein Vorfallreaktions-Programm, in dessen Rahmen Sicherheitsvorfälle eingegrenzt, analysiert, behoben und mitgeteilt werden, die die verwalteten Netzwerke und/oder Systeme von Citrix oder Kundeninhalte betreffen. **Vorfallbenachrichtigung**. Wenn Citrix entscheidet, dass Kundeninhalte unter seiner Kontrolle Gegenstand eines Sicherheitsvorfalls waren, wird der Kunde innerhalb des gesetzlich vorgeschriebenen Zeitraums benachrichtigt. **Vorfallaufzeichnung**. Citrix pflegt einen Datensatz bekannter Sicherheitsvorfälle mit einer Beschreibung des Vorfalls, dem Zeitraum, den Folgen des Vorfalls, dem Namen des Berichtenden, der Person, der der Vorfall gemeldet wurde und dem Verfahren zur Wiederherstellung der Daten und Dienste wie zutreffend.

Gebiet	Kontrolle(n)
Lieferantenmanagement	**Neuaufnahmen**. Citrix führt Sicherheitsbeurteilungen für Dienstanbieter durch, die Zugriff auf Kundeninhalte und/oder Komponenten der Dienste, die Kundeninhalte verarbeiten, erhalten sollen. Citrix verlangt von den Dienstanbietern im Zusammenhang mit den Diensten, dass sie für die von ihnen angebotenen Dienste mindestens das in diesem Abschnitt beschriebene Sicherheitsniveau einhalten. Dienstanbieter, die möglicherweise Zugriff auf Kundeninhalte im Rahmen der Gesetze der Europäischen Union erhalten, müssen eine Selbstzertifizierung für die Privacy Shield-Programme EU-US bzw. EU-Schweiz durchführen oder Standardvertragsklauseln umsetzen. **Fortlaufende Instandhaltung.** Dienstanbieter werden regelmäßig beurteilt, gestützt auf die Vertraulichkeit und das Risiko im Zusammenhang mit ihren Diensten. **Ausscheiden.** Bei Beendigung einer Anbieterbeziehung muss der Dienstanbieter alle Kundeninhalte in seinem Besitz zurückgeben oder bescheinigen, dass jegliche Kundeninhalte auf sichere Weise vernichtet wurden.
Geschäftskontinuität und Notfallwiederherstellung	**Geschäftskontinuität.** Citrix pflegt Notfall- und Ausweichpläne für die Einrichtungen, in denen sich die Citrix Informationssysteme, die Kundeninhalte verarbeiten, befinden. **Notfallwiederherstellung.** Der redundante Speicher von Citrix und seine Verfahren für die Datenwiederherstellung sind dafür ausgelegt, zu versuchen, Kundeninhalte in seinem ursprünglichen bzw. zuletzt replizierten Zustand wiederherzustellen.
Sicherheitsverpflichtungen des Kunden.	Der Kunde ist für die Verwaltung der Sicherheitselemente verantwortlich, die nicht ausdrücklich als Bestandteil in die Dienste eingeschlossen sind. Dazu zählt u. a.: • die Beschränkung des Zugriffs von Citrix auf Kundeninhalte auf den erforderlichen Umfang, damit der Kunde die Dienste erhalten kann. • der Schutz seiner Netzwerke und Dienstkomponenten vor Störungen, einschließlich Überwachung und Sicherung seiner Netzwerke und Computerausrüstung. • das Herunterladen von Kundeninhalten nach Bedarf, sowohl während der Dienstlaufzeit als auch bei deren Beendigung. • Citrix verschlüsselt die Daten während der Übertragung standardmäßig oder stellt den Kunden die Mittel zur Verschlüsselung dieser Daten bereit. Weitere Einzelheiten sind der Produktdokumentation für die Dienste zu entnehmen. Der Kunde ist dafür verantwortlich sicherzustellen, dass die Daten während der Übertragung angemessen geschützt sind.

1.B. Zusätzliche Sicherheitskontrollen für Cloud-Dienste

Gebiet	Kontrolle(n)
Datenschutz (Verfügbarkeitskontrolle, Übertragungskontrolle, Datenlöschung)	**Failover-Verfahren**. Citrix implementiert Mechanismen, um dem Verfügbarkeitsverlust von Kundeninhalten zu begegnen. Dazu zählt das Speichern von Kopien der Kundeninhalte an einem anderen Standort als dem der primären Computerausrüstung, die die Kundeninhalte verarbeitet. **Daten über Grenzen hinweg**. Citrix verschlüsselt Kundeninhalte bzw. ermöglicht dem Kunden dessen Verschlüsselung, wenn Kundeninhalte im Rahmen des Dienstes über öffentliche Netzwerke übertragen werden. **Aufbewahrung.** Citrix kann Kundeninhalte nach dem Dienstzeitraum aufbefahren und für Kundenzugriffe archivieren, wenn dies für gesetzliche Zwecke erforderlich ist. Citrix hält alle Anforderungen dieser Anlage ein, bis diese Kundeninhalte dauerhaft gelöscht wurde. Vorbehaltlich der Rückgabe wie unmittelbar nachfolgend beschrieben ist Citrix in keiner Weise verpflichtet, die Kundeninhalte nach Beendigung des Dienstes aufzubewahren. **Rückgabe.** Vorbehaltlich der Verfügbarkeit und der anwendbaren Dienstbeschreibung hat der Kunde dreißig (30) Tage Zeit, die Kundeninhalte nach dem Ablauf herunterzuladen. **Datenlöschung**. Citrix löscht Kundeninhalte auf sichere Weise, wenn sie nicht mehr für rechtmäßige Zwecke benötigt werden.
Sichere Vorgänge	**Ereignisprotokollierung**. Bei bestimmten Diensten erfasst Citrix Protokolle. Protokolle können die Zugriffs-ID, Uhrzeit, gewährte oder verweigerte Autorisierung, Diagnosedaten wie Verfolgungs- oder Absturzdateien und andere relevante Aktivität umfassen. Protokolle werden verwendet, (**i**) um die Dienste und zugehörigen Analysen bereitzustellen, zu sichern, zu verwalten, zu messen und zu verbessern, (**ii**) wie vom Kunden und seinen Benutzern angewiesen und/oder (**iii**) um die Citrix Richtlinien, anwendbaren Gesetze, Vorschriften oder behördlichen Aufforderungen einzuhalten. Dazu kann die Überwachung der Leistung, Stabilität, Nutzung und Sicherheit der Dienste und zugehörigen Komponenten zählen. Der Kunde darf diese Überwachung weder blockieren noch behindern. Citrix kann Protokolle zu den oben aufgeführten Zwecken mit von Dritten erfassten Daten ergänzen. Protokolle dürfen für nicht in diesem Anhang angegebene Zwecke nur in zusammengefasster Form verwendet werden.

Gebiet	Kontrolle(n)
Geschäftskontinuität und Notfallwiederherstellung	**Sicherungen.** Außer wenn in der entsprechenden Dienstbeschreibung anders angegeben, werden Dienste auf hochverfügbaren, aktiv-aktiven Clustern über mehrere physische Standorte hinweg gepflegt. Systeme, die nicht in einer aktiv-aktiven Konfiguration gepflegt werden, werden entsprechend den spezifischen Zielen des Servicelevels des Dienstes gesichert.

Artikel 2. **Behandlung von personenbezogenen Daten**

Personenbezogene Daten sind Informationen über eine identifizierte oder identifizierbare Person. Der Kunde legt fest, welche personenbezogenen Daten in Kundeninhalte aufgenommen werden. Bei der Durchführung der Dienste handelt Citrix als Auftragsverarbeiter der Daten, und der Kunde bleibt der Verantwortliche für alle personenbezogenen Daten, die in Kundeninhalten enthalten sind. Citrix handelt nach Anweisung des Kunden hinsichtlich der Verarbeitung dieser personenbezogenen Daten, wie in der Vereinbarung angegeben.

Weitere Informationen hinsichtlich der Verarbeitung von personenbezogenen Daten, die den allgemeinen Datenschutzbestimmungen unterliegen, darunter die Mechanismen für die internationale Übertragung derartiger Daten, sind in Anlage I, Allgemeine Datenschutzbestimmungen, enthalten.

Artikel 3. **Speicherort der Dienste**

Kundeninhalte können in die USA oder andere Länder, in denen Citrix und/oder seine Dienstanbieter tätig sind, übertragen, dort gespeichert und/oder verarbeitet werden. Die Anforderungen dieser Anlage gelten weiter, unabhängig davon, wo Citrix Kundeninhalte speichert oder verarbeitet.

Die Parteien können in gutem Glauben alle weiteren Datenverarbeitungs- oder Datenübertragungsvereinbarungen verhandeln, die benötigt werden, um die rechtmäßige internationale Datenübertragung im Zusammenhang mit der Bereitstellung der Dienste durch Citrix zu gewährleisten.

Artikel 4. **Offenlegung von Kundeninhalten**

Der Kunde stimmt zu, dass Citrix Kundeninhalte wie in diesem Abschnitt bestimmt offenlegen kann.
Citrix kann Untervertragnehmer und Agenten zur Durchführung der Dienste einsetzen. Alle Unterauftragnehmer und Agenten sind nur in dem Umfang, der zur Erbringung der Dienste erforderlich ist, zum Zugriff auf Kundeninhalte berechtigt, und sind an schriftliche Vereinbarungen gebunden, in denen sie verpflichtet werden, mindestens wie zutreffend das Datenschutzniveau bereitzustellen, das Citrix in dieser Anlage verlangt. Citrix bleibt jederzeit wie zutreffend für die Einhaltung der Bestimmungen der Vereinbarung seitens seiner Unterauftragnehmer und Agenten verantwortlich.

Citrix kann Kundeninhalte auch wie folgt offenlegen: (a) an verbundene Unternehme zu Zwecken wie mit dieser Vereinbarung vereinbar, (b) im Zusammenhang mit voraussichtlichen oder tatsächlichen Fusionen, Akquisitionen, Verkäufen, Bankrott oder einer anderen Neuorganisation eines Teils oder des ganzen Geschäfts, vorbehaltlich der Verpflichtung zum Schutz der Kundeninhalte gemäß den Bestimmungen dieser Vereinbarung; oder (c) zu rechtlichen Zwecken, darunter Rechtedurchsetzung, Feststellung oder Verhinderung von Betrug, Schutz vor

Schäden an Rechten oder Eigentum von Citrix, Kunden, Benutzern oder der Öffentlichkeit; und (c) wie gesetzlich vorgeschrieben, auch in Beantwortung einer Vorladung, einer gerichtlichen oder behördlichen Anweisung oder eines anderen bindenden Instruments (jeweils eine „Aufforderung“). Außer in Fällen, in denen dies gesetzlich verboten ist, wird Citrix den Kunden umgehend über jede Aufforderungen verständigen und den Kunden angemessene Utnerstützung leisten, damit der Kunde zeitnah auf die Aufforderung antworten kann.

Artikel 5. Verpflichtungen des Kunden

1. Allgemeine Bestimmungen. Der Kunde kann die Dienste nur im Rahmen der Bestimmungen der Vereinbarung nutzen und darauf zugreifen. Der Kunde muss alle anwendbaren Gesetze im Zusammenhang mit seiner Nutzung der Dienste einhalten.

2. Berechtigungen. Der Kunde ist für den Erhalt aller erforderlichen Berechtigungen verantwortlich, damit Citrix die Dienste ausführen kann, einschließlich der Bereitstellung aller Benachrichtigungen und des Erhalts aller Zustimmungen oder Lizenzen, die benötigt werden, damit Citrix auf Kundeninhalte wie in dieser Anlage dargelegt zugreifen und sie verarbeiten kann.

3. Bestimmungen. Der Kunde ist dafür verantwortlich zu bestimmen, ob Kundeninhalte weiteren Bestimmungen oder Sicherheitsanforderungen über die in der Vereinbarung, einschließlich dieser Anlage, angegeben hinaus entsprechen müssen. Der Kunde darf keine Kundeninhalte zulassen, die den US-amerikanischen International Traffic in Arms Regulations (ITAR) oder vergleichbaren Vorschriften eines Landes unterliegen, welche den Import oder Export von Verteidigungsmaterialien oder -dienstleistungen einschränken. Des weiteren darf der Kunde keine Kundeninhalte bereitstellen oder speichern, die weiteren Bestimmungen unterliegen, wie geschützte Gesundheitsinformationen, Zahlungskarteninformationen oder Daten mit kontrollierter Verteilung gemäß behördlichen Vorschriften, es sei denn, im Auftrag des Kunden und in der anwendbaren Dienstbeschreibung ist dies angegeben und die Parteien haben in Voraus weitere Vereinbarungen abgeschlossen (z. B. eine Geschäftspartnervereinbarung), wie von Citrix zur Verarbeitung derartiger Daten verlangt. Kunden des ShareFile-Dienstes können sich unter privacy@sharefile.com an Citrix wenden, um eine Geschäftspartnervereinbarung zu beantragen.

4. Kunden-Sicherheitsumgebung. Die Dienste sind so konzipiert, dass sie nur innerhalb einer größeren Kunden-Sicherheitsumgebung bereitgestellt werden. Der Kunde muss für die entsprechende Sicherheitsfunktionalität für alle Komponenten sorgen, die nicht ausdrücklich von Citrix verwaltet werden, einschließlich, aber nicht beschränkt auf Zugriffssteuerungen, Firewalls, Anwendungen und Netzwerke, die in Verbindung mit den Diensten verwendet werden. Siehe Abschnitt 1.A., Sicherheitsverpflichtungen des Kunden, oben.

5. Sicherheitsbenachrichtigung. Der Kunde ist dafür verantwortlich, Citrix umgehend über alle Sicherheitsvorfälle zu benachrichtigen, die die Dienste und/oder Kundeninhalte betreffen, wie in Artikel VI, Citrix Kontakte, unten beschrieben.

6. Benutzereinhaltung. Der Kunde ist für die Einhaltung der Bestimmungen des Auftrags und der Vereinbarung durch seine Benutzer verantwortlich.

Artikel 6. **Citrix Kontakte**

FUNKTION	KONTAKT
Kundensupport	https://www.citrix.com/contact/technical-support.html
Melden eines Vorfalls	secure@citrix.com
Vermutete Schwachstellen in Citrix Produkten	secure@citrix.com

Artikel 7. **Begriffsbestimmungen**

Die entsprechenden Begriffe in der Anlage haben die in der Vereinbarung oder unten angegebene Bedeutung. Im Fall eines Konflikts zwischen den verbleibenden Bestimmungen der Vereinbarung und jeglichen Begriffsbestimmungen unten gilt die Begriffsbestimmung unten für diese Anlage.

Kundeninhalte beziehen sich auf alle Daten, die zur Speicherung an das Kundenkonto hochgeladen wurden, oder auf Daten in der Rechenumgebung des Kunden, auf die Citrix zur Erbringung von Diensten Zugriff erhält.

Protokoll bezieht sich auf eine Aufzeichnung von Ereignissen im Zusammenhang mit den Diensten, darunter Aufzeichnungen zum Messen von Leistung, Stabilität, Nutzung, Sicherheit und Support.

Sicherheitsvorfall bezieht sich auf nicht autorisierten Zugriff auf Kundeninhalte, der zum Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit führt.