RINGCENTRAL SECURITY ADDENDUM

1. Umfang

Dieses Dokument beschreibt die Maßnahmen zur Informationssicherheit (**„Maßnahmen“**), die RingCentral bei der Verarbeitung Geschützter Daten durch RingCentral-Dienste einsetzt.

2. Definitionen

Nur für die Zwecke dieses Sicherheitsnachtrags haben großgeschriebene Begriffe, die hier nicht anderweitig definiert sind, die jeweils im Vertrag festgelegte Bedeutung.

A. **„RingCentral Dienste“** oder **„Dienste“** bezeichnet die von RingCentral angebotenen und vom Kunden erworbenen Dienste.

B. **„Kunde“** bezeichnet das Unternehmen, das den Vertrag mit RingCentral abgeschlossen hat.

C. **„Geschützte Daten“** sind Kunden- und Partnerdaten, die von den RingCentral-Diensten verarbeitet werden, wie in dem geltenden RingCentral-DPA oder dem Vertrag definiert, einschließlich “personenbezogener Daten” und “persönlicher Informationen” im Sinne der geltenden Datenschutzgesetze, vertraulicher Daten im Sinne des Vertrags, Kontodaten, Konfigurationsdaten, Kommunikationsinhalte einschließlich Nachrichten, Voicemail und Videoaufzeichnungen.

D. **„Vertrag“** bezeichnet die zwischen RingCentral und dem Kunden bestehende Vereinbarung über die Bereitstellung der Dienste.

E. **„Personal“** bedeutet Mitarbeiter von RingCentral, Auftragnehmer oder unterbeauftragte Professional Services Mitarbeiter.

3. Management der Informationssicherheit

A. Sicherheitsprogramm

RingCentral unterhält ein schriftliches Informationssicherheitsprogramm, das:

i. Dokumentierte Richtlinien oder Standards beinhaltet, die geeignet sind, den Umgang mit geschützten Daten in Übereinstimmung mit dem Vertrag und dem geltenden Recht zu regeln.

ii. Von einem leitenden Mitarbeiter geleitet wird, der für die Überwachung und Umsetzung des Programms verantwortlich ist.

iii. Administrative, technische und physische Schutzmaßnahmen beinhaltet, die angemessen gestaltet sind, um die Vertraulichkeit, Integrität und Verfügbarkeit Geschützter Daten zu schützen.

iv. Im Hinblick auf die Art, Größe und Komplexität des Geschäftsbetriebs von RingCentral angemessen ist.

B. Verwaltung von Sicherheitsrichtlinien

Die Sicherheitsrichtlinien, -standards und -verfahren von RingCentral:

i. Entsprechen den etablierten Industriestandards für Informationssicherheit.

ii. Unterliegen einer laufenden Überprüfung.

iii. Können überarbeitet werden, um Änderungen in den anerkannten Verfahren der Branche zu berücksichtigen.

C. Risikomanagement

RingCentral:

i. Führt mindestens einmal jährlich eine Bewertung der Cybersecurity-Risiken durch, um Bedrohungen für das Unternehmen oder den Betrieb zu identifizieren.

ii. Aktualisiert RingCentral-Richtlinien, -Verfahren und -Standards soweit notwendig, im Hinblick auf Bedrohungen für das Geschäft oder den Betrieb von RingCentral.

4. Unabhängige Sicherheitsbewertungen

A. Externe Prüfung

RingCentral:

i. Setzt qualifizierte unabhängige Drittprüfer ein, um Sicherheitsaudits für Systeme, Umgebungen und Netzwerke durchzuführen, in denen Geschützte Daten verarbeitet werden, einschließlich.

a. SOC2 Typ II.

b. IES/ISO 27001.

ii. Unterhält zusätzliche Audits und Compliance-Zertifizierungen, wie sie für das Geschäft von RingCentral angemessen sind und wie unter www.ringcentral.com/trust-center.html angegeben.

B. Weitergabe von Berichten

Kopien relevanter Prüfberichte und Zertifizierungen:

i. Werden dem Kunden auf Anfrage zur Verfügung gestellt.

ii. Unterliegen einer Geheimhaltungsvereinbarung.

C. Jährlicher Fragebogen zur Risikobewertung

Der Kunde kann einmal (1) innerhalb eines Zeitraums von zwölf (12) Monaten verlangen, dass RingCentral einen Fragebogen zur Risikobewertung durch Dritte innerhalb eines angemessenen Zeitrahmens ausfüllt.

Im Falle eines Konflikts zwischen diesem Abschnitt und dem entsprechenden Abschnitt in dem RingCentral DPA hat das DPA Vorrang.

5. Sicherheit im Personalwesen

A. Hintergrund-Checks

RingCentral verlangt von allen Mitarbeitern vor der Einstellung eine Überprüfung. RingCentral stellt kriminelle Hintergrundüberprüfungen seiner Mitarbeiter sicher, soweit dies gesetzlich zulässig ist. Jede Hintergrundüberprüfung in den USA umfasst:

i. Eine Identitätsüberprüfung (SSN-Trace).

ii. Strafrechtliche Überprüfungen für bis zu sieben (7) Jahre auf Verbrechen und Vergehen auf lokaler, staatlicher und bundesstaatlicher Ebene, wo dies angemessen ist.

iii. Eine Suche in der Terroristenliste (OFAC), soweit es das Gesetz erlaubt.

Im Ausland werden Überprüfungen der Vorstrafen entsprechend der lokalen Gesetzgebung durchgeführt.

Hintergrundprüfungen werden von einem Mitglied der National Association of Professional Background Screeners oder einem kompetenten, von der Industrie anerkannten Unternehmen im lokalen Rechtsraum durchgeführt.

B. Ausbildung

RingCentral stellt sicher, dass alle Mitarbeiter, einschließlich Auftragnehmer:

i. Eine jährliche Schulung absolvieren, um nachzuweisen, dass Sie mit den Sicherheitsrichtlinien von RingCentral vertraut sind.

ii. Jährliche Schulungen für Sicherheits- und Datenschutzanforderungen, einschließlich Cyberecurity Awareness, GDPR und CCPA absolvieren.

iii. Über angemessene Fähigkeiten und Erfahrungen verfügen, die für eine Anstellung und eine Position des Vertrauens innerhalb von RingCentral geeignet sind.

C. Sicherheit am Arbeitsplatz

RingCentral stellt das sicher, dass:

i. RingCentral-Mitarbeiter entweder RingCentral-eigene und verwaltete Geräte bei der Erfüllung ihrer Aufgaben oder Bring Your Own Device (BYOD) Geräte verwenden.

ii. Alle Geräte, ob RingCentral-eigene und verwaltete oder Bring Your Own Device (BYOD)-Geräte, im umfassenden RingCentral-Managed-Device-Programm eingeschrieben sind.

D. Schutz vor Datenverlust

RingCentral setzt ein umfassendes System ein, um die versehentliche oder absichtliche Beschädigung oder Verlust von RingCentral-Daten und Geschützten Daten zu verhindern.

E. Due Diligence in Bezug auf Subunternehmer

RingCentral wird:

i. Einen Sicherheitsprozess unterhalten, um vor der Beauftragung von Subunternehmern eine angemessene Due Diligence durchzuführen.

ii. Die Sicherheitsfähigkeiten solcher Subunternehmer regelmäßig bewerten, um sicherzustellen, dass die Subunternehmer in der Lage sind, die in diesem Dokument beschriebenen Maßnahmen einzuhalten.

iii. Schriftliche Informationssicherheitsanforderungen anwenden, die Subunternehmer dazu verpflichten, die wichtigsten Richtlinien und Standards von RingCentral betreffend Informationssicherheit einzuhalten, die mit diesen Maßnahmen übereinstimmen und nicht weniger Schutz bieten wie diese.

F. Geheimhaltung

RingCentral stellt sicher, dass Mitarbeiter und Auftragnehmer/Subunternehmer, die Geschützte Daten verarbeiten, schriftlich zur Vertraulichkeit verpflichtet werden.

6. Physische Sicherheit

A. Allgemein

RingCentral:

i. Schränkt den Zugang zu allen physischen Bereichen, in denen RingCentral-Dienste Geschützte Daten verarbeiten (**„Sichere Bereiche“**), ein, steuert und überwacht diese.

ii. Unterhält angemessene physische Sicherheitskontrollen auf einer 24-Stunden-pro-Tag, 7-Tage-pro-Woche Basis („24/7“).

iii. Widerruft den physischen Zugang zu den Sicherheitsbereichen unverzüglich, wenn die Notwendigkeit des Zugangs zu den Gebäuden und dem/den System(en) entfallen ist.

iv. Führt mindestens einmal jährlich eine Überprüfung der Zugriffsrechte durch.

B. Zugriffs- und Berechtigungsprozesse

RingCentral unterhält einen dokumentierten Zugriffsberechtigungs- und Protokollierungsprozess. Der Autorisierungs- und Protokollierungsprozess umfasst mindestens Folgendes:

i. Berichte mit detaillierten Angaben zu allen Zugriffen auf die Sicherheitsbereiche, einschließlich der Identitäten sowie Datum und Uhrzeit des Zugriffs.

ii. Die Berichte müssen mindestens ein Jahr lang aufbewahrt werden, wie es das Gesetz gestattet.

iii. Videoüberwachungsgeräte zur Überwachung und Aufzeichnung von Aktivitäten an allen Ein- und Ausgängen der Sicherheitsbereiche rund um die Uhr, soweit dies nach den geltenden Gesetzen und Vorschriften zulässig ist.

iv. Die Videoaufzeichnung muss mindestens 30 Tage lang oder gemäß den Richtlinien des Anbieters des physischen Standorts aufbewahrt werden.

C. Rechenzentren

Sofern RingCentral ein Rechenzentrum betreibt oder nutzt, stellt RingCentral sicher, dass die physischen Sicherheitskontrollen mit Industriestandards wie ISO 27001 und SSAE 16 oder ISAE 3402 oder ähnlichen Standards übereinstimmen:

i. Sicherheit der Gebäude (Perimetersicherheit) einschließlich Umzäunung/Absperrung und Videoüberwachung.

ii. Sicherer Zugang inklusive Wachmann/Empfang.

iii. Innenraumzugang kontrolliert durch RFID-Karten, 2FA, Anti-Tailgating-Kontrollen.

iv. Redundante Versorgungseinspeisungen und Unterstützung für kontinuierliche Bereitstellung durch Backup-Systeme.

v. Redundante Netzwerkverbindung von mehreren Anbietern.

7. Logische Sicherheit

A. Benutzeridentifikation und -authentifizierung

RingCentral:

i. Unterhält einen dokumentierten Prozess zur Verwaltung des Lebenszyklus der Benutzerverwaltung, der manuelle und/oder automatisierte Prozesse für die genehmigte Erstellung von Konten, die Entfernung von Konten und die Änderung von Konten für alle Informationsressourcen und über alle Umgebungen hinweg umfasst.

ii. Stellt sicher, dass RingCentral-Benutzer ein individuelles Konto für eine eindeutige Rückverfolgbarkeit haben.

iii. Stellt sicher, dass RingCentral-Benutzer keine gemeinsamen Konten verwenden; wo gemeinsame Konten technisch erforderlich sind, sind Kontrollen vorhanden, um die Rückverfolgbarkeit sicherzustellen.

iv. RingCentral-Benutzerpasswörter werden gemäß den aktuellen NIST-Richtlinien konfiguriert.

Für die kundenorientierten Anwendungen kann der Kunde die Integration mit SSO (Single Sign on) wählen, so dass der Kunde die Kontrolle über seine erforderlichen Passworteinstellungen behält, einschließlich der bestehenden MFA/2FA-Lösungen des Kunden.

B. Benutzerautorisierung und Zugriffskontrolle

RingCentral:

i. Konfiguriert den Fernzugriff auf alle Netzwerke, die Geschützte Daten speichern oder übertragen, so, dass für diesen Zugriff eine Multi-Faktor-Authentifizierung erforderlich ist.

ii. Widerruft den Zugriff auf Systeme und Anwendungen, die Geschützte Daten enthalten oder verarbeiten, unverzüglich nach Beendigung der Notwendigkeit des Zugriffs auf das/die System(e) oder die Anwendung(en).

iii. Hat die Fähigkeit, Zugriffe auf das System und das Netzwerk oder Versuche, die Sicherheit des Systems oder des Netzwerks zu verletzen, zu erkennen, zu protokollieren und zu melden.

RingCentral setzt Mechanismen zur Zugriffskontrolle ein, die dazu dienen:

i. Den Zugriff auf Geschützte Daten auf diejenigen Mitarbeiter zu beschränken, die einen angemessenen Bedarf für den Zugriff auf diese Daten haben, damit RingCentral seine Verpflichtungen aus dem Vertrag erfüllen kann.

ii. Den unbefugten Zugriff auf Geschützte Daten zu verhindern.

iii. Den Zugriff auf Benutzer zu beschränken, die das Wissen geschäftlich benötigen.

iv. Das Prinzip des geringsten Privilegs zu befolgen und nur den Zugriff auf die Informationen und Ressourcen zu erlauben, die notwendig sind.

v. Mindestens einmal jährlich eine Überprüfung der Zugriffskontrollen für alle Systeme von RingCentral durchzuführen, die Geschützte Daten übertragen, verarbeiten oder speichern.

8. Telekommunikation und Netzwerksicherheit

A. Netzwerk-Management

RingCentral:

i. Pflegt ein Netzwerksicherheitsprogramm, das einen Firewall-Schutz nach Industriestandard und eine Zwei-Faktor-Authentifizierung für den Zugriff auf die Netzwerke von RingCentral umfasst.

ii. Setzt ein Intrusion Detection System (IDS) und/oder Intrusion Prevention System (IPS) ein, um Alarme zu generieren, zu überwachen und darauf zu reagieren, die auf eine potenzielle Gefährdung des Netzwerks und/oder des Hosts hinweisen könnten.

iii. Überwacht den Web-Verkehr aus dem Internet und aus internen Quellen, um Cyber-Attacken, einschließlich Distributed Denial of Service (DDoS)-Attacken gegen Websites / Dienste, zu erkennen und um böswilligen Verkehr zu blockieren.

B. Netzwerk-Segmentierung

RingCentral:

i. Implementiert die Netzwerksegmentierung zwischen dem Unternehmensnetzwerk und den Hosting-Einrichtungen für Services.

ii. Gewährleistet die Trennung zwischen Umgebungen für Entwicklung, Staging und Produktion.

iii. Schränkt den Zugriff auf autorisierte Geräte zwischen Umgebungen ein.

iv. Kontrolliert die Konfiguration und das Management von Netzwerktrennung und Firewall-Regeln durch einen formalen Antrags- und Genehmigungsprozess.

C. Scannen von Sicherheitslücken im Netzwerk

RingCentral:

i. Führt mindestens vierteljährlich interne und externe Netzwerk-Schwachstellen-Scans gegen informationsverarbeitende Systeme durch.

ii. Bewertet die Ergebnisse auf der Grundlage (falls zutreffend) des CVSS-Scores und der Bewertung von Auswirkungen, Wahrscheinlichkeit und Schweregrad.

iii. Behebt Befunde nach branchenüblichen Zeitplänen.

9. Betriebssicherheit

A. Vermögensverwaltung

RingCentral:

i. Führt ein genaues und aktuelles Anlagenregister, das Hardware- und Software umfasst, die für die Erbringung von Dienstleistungen verwendet werden.

ii. Erfüllt die Rechenschaftspflicht für Vermögensgegenstände (Assets) während ihres gesamten Lebenszyklus.

iii. Verfügt über Prozesse, um Gegenstände vor ihrer Entsorgung zu löschen oder physisch zu zerstören.

B. Konfigurationsmanagement

RingCentral:

i. Verwaltet Basiskonfigurationen von Informationssystemen und Anwendungen auf der Grundlage von anerkannten Verfahren der Branche, einschließlich:

a. Entfernen aller vom Hersteller bereitgestellten Passwörter.

b. Entfernen/Deaktivieren nicht verwendeter Dienste und Einstellungen.

c. Anti-Malware/Endpunkt-Schutz, soweit technisch machbar.

ii. Setzt Sicherheitskonfigurationseinstellungen für Systeme durch, die für die Bereitstellung der Dienste verwendet werden.

iii. Stellt sicher, dass die Uhren aller informationsverarbeitenden Systeme auf eine oder mehrere Referenzzeitquelle/n synchronisiert werden.

C. Schutz vor Bösartigem Code

i. Soweit praktikabel, hat RingCentral einen Endpunktschutz in Form von Endpoint Detection and Response (EDR) und/oder Antivirensoftware auf Servern und Workstations installiert und ausgeführt.

ii. EDR-Warnungen werden überwacht und es werden sofort Maßnahmen ergriffen, um jedes abnormale Verhalten zu untersuchen und zu beheben.

iii. Sofern verwendet, ist die Antivirensoftware auf Windows-Servern und -Workstations auf dem neuesten Stand und wird ausgeführt, um Viren und andere Malware zu suchen und umgehend zu entfernen oder in Quarantäne zu stellen.

D. Schwachstelle, Sicherheits-Patching

RingCentral:

i. Überwacht öffentlich bekannt gewordene Schwachstellen und Gefährdungen auf Auswirkungen auf die Informationssysteme und Produkte des Lieferanten.

ii. Stellt Qualitätssicherungstests für Patches vor der Bereitstellung sicher.

iii. Stellt sicher, dass alle Ergebnisse von Netzwerk-Gefährdungs-Scans und relevante, öffentlich bekannt gegebene Schwachstellen und Gefährdungen gemäß branchenüblicher, anerkannter Verfahren behoben

werden, einschließlich CVSS-Score und Bewertung von Auswirkung, Wahrscheinlichkeit und Schweregrad, und dass die Behebung nach branchenüblichen Zeitplänen erfolgt.

E. Protokollierung und Überwachung

RingCentral muss sicherstellen, dass:

i. Alle Systeme, Geräte oder Anwendungen, die mit dem Zugriff, der Verarbeitung, der Speicherung, der Kommunikation und/oder der Übertragung Geschützter Daten zusammenhängen, Audit-Protokolle erzeugen.

ii. Der Zugriff auf Geschützte Daten protokolliert wird.

iii. Die Protokolle so detailliert sind, dass sie zur Erkennung signifikanter unautorisierter Aktivitäten verwendet werden können.

iv. Die Protokolle vor unberechtigtem Zugriff, Änderung und Löschung geschützt sind.

v. Die Protokolle zur Sammlung und Überwachung an einen zentralen Ort gesendet werden.

10. Software-Entwicklung und -Wartung

A. Sicherer Entwicklungslebenszyklus

RingCentral:

i. Wendet Praktiken des sicheren Entwicklungslebenszyklus an, einschließlich während der Design-, Entwicklungs- und Testzyklen.

ii. Stellt sicher, dass Produkte einer Überprüfung des Sicherheitsdesigns unterzogen werden, einschließlich Überlegungen zu Bedrohungen und Praktiken der Datenverarbeitung.

iii. Stellt sicher, dass Services einer sicheren Freigabeprüfung unterzogen werden, bevor sie in die Produktion gehen.

B. Sicherheitstests

Als Teil des sicheren Entwicklungslebenszyklus wird RingCentral:

i. Strenge Sicherheitstests durchführen, einschließlich, soweit technisch machbar:

a. Statische Code-Analyse.

b. Quellcode-Peer-Reviews.

c. Dynamische und interaktive Sicherheitstests.

d. Sicherheitslogik, oder Sicherheits-”QA”-Tests.

ii. Sicherstellen, dass Anwendungen, die mit dem Internet verbunden sind, einer Bewertung der Anwendungssicherheit unterzogen und getestet werden, um übliche Sicherheitsschwachstellen zu identifizieren, die von branchenweit anerkannten Organisationen ermittelt wurden (z. B. OWASP Top 10 Vulnerabilities, CWE/SANS Top 25 Vulnerabilities).

iii. Führt für alle mobilen Anwendungen (d. h. unter Android, Blackberry, iOS, Windows Phone), die Geschützte Daten erfassen, übertragen oder anzeigen, eine Überprüfung der Anwendungssicherheit durch, um branchenweit anerkannte Schwachstellen speziell für mobile Anwendungen zu identifizieren und zu beheben.

iv. Verwendet die Geschützten Daten NICHT zum Testen.

v. Unternimmt alle angemessenen Anstrengungen, um Software-Schwachstellen vor der Freigabe zu identifizieren und zu beheben.

C. Jährliche Penetrationstests

RingCentral:

i. Beauftragt qualifizierte, unabhängige externe Tester mit der Durchführung jährlicher Penetrationstests für seine Produkte und Umgebungen, in denen Geschützte Daten gehostet werden.

ii. Verlangt von den Unter-Datenverarbeitern (sub-processors), ähnliche Penetrationstests gegen ihre Systeme, Umgebungen und Netzwerke durchzuführen.

iii. Stellt sicher, dass alle Feststellungen in einem wirtschaftlich angemessenen Zeitraum behoben werden.

D. Produkt-Schwachstellen-Management

RingCentral:

i. Verwendet wirtschaftlich angemessene Anstrengungen, um regelmäßig Software-Sicherheitslücken in RingCentral-Diensten zu identifizieren.

ii. Stellt relevante Updates, Upgrades und Bugfixes für bekannte Softwaresicherheitslücken zur Verfügung, für jede Software, die bereitgestellt wird oder in der Geschützte Daten verarbeitet werden.

iii. Stellt sicher, dass alle Feststellungen, die aus internen und externen Tests resultieren, gemäß branchenüblichen, anerkannten Verfahren bewertet werden, einschließlich CVSS-Score und Bewertung von Auswirkung, Wahrscheinlichkeit und Schweregrad, und dass sie gemäß branchenüblichen Zeitplänen behoben werden.

E. Open Source und Software von Drittanbietern

RingCentral:

i. Führt ein Bestandsverzeichnis aller Software von Drittanbietern (TPS) und Open-Source-Software (OSS), die in die Dienste integriert sind.

ii. Verwendet wirtschaftlich angemessene Anstrengungen, um die sichere Entwicklung und Sicherheit von Open-Source-Software und Software von Drittanbietern zu gewährleisten, die von RingCentral verwendet wird.

iii. Verwendet wirtschaftlich angemessene Anstrengungen, um Schwachstellen von Open-Source-Software (OSS) und anderen Software Bibliotheken von Drittanbietern, die in die Dienste integriert sind, zu bewerten, zu verfolgen und zu beheben.

11. Datenverarbeitung

A. Daten-Klassifizierung

RingCentral unterhält Standards zur Datenklassifizierung, einschließlich:

i. Öffentliche Daten, Daten, die allgemein verfügbar sind oder von denen erwartet wird, dass sie der Öffentlichkeit bekannt sind.

ii. Vertrauliche Daten, Daten, die der Allgemeinheit nicht zugänglich sind.

Geschützte Daten werden als vertrauliche Daten von RingCentral eingestuft.

B. Datentrennung

RingCentral:

i. Stellt die physische oder logische Trennung der Geschützten Daten von den Daten anderer Kunden sicher.

ii. Stellt die physische Trennung und Zugriffskontrolle sicher, um die Geschützten Daten von den RingCentral-Daten zu trennen.

C. Verschlüsselung von Daten

RingCentral:

i. Muss die Verschlüsselung Geschützter Daten in elektronischer Form bei der Übertragung über alle öffentlichen drahtgebundenen Netzwerke (z. B. Internet) und alle drahtlosen Netzwerke (mit Ausnahme der Kommunikation über öffentliche Telefonwählnetze) sicherstellen.

ii. Mit Ausnahme der Engage-Communities-Funktion von Engage Digital muss die Verschlüsselung Geschützter Daten in elektronischer Form sichergestellt werden, wenn sie in Ruhe gespeichert werden.

iii. Verwendet branchenübliche Verschlüsselungsalgorithmen und Schlüsselstärken zur Verschlüsselung Geschützter Daten bei der Übertragung über alle öffentlichen kabelgebundenen Netzwerke (z. B. Internet) und alle drahtlosen Netzwerke.

D. Vernichtung von Daten

RingCentral soll:

i. Für die sichere Löschung von Daten sorgen, wenn sie nicht mehr benötigt werden.

ii. Sicherstellen, dass elektronische Medien, die bei der Erbringung von Dienstleistungen für den Kunden verwendet wurden, vor der Entsorgung oder Wiederverwendung einem Reinigungsprozess unterzogen werden, der die Löschung von Daten sicherstellt und verhindert, dass Daten rekonstruiert oder gelesen werden können.

iii. Alle Geräte (Equipment)*, die* Geschützte Daten *enthalten* zerstören werden*., wenn sie beschädigt oder nicht funktionsfähig sind.*

12. Reaktion auf Vorfälle

Die Fähigkeit von RingCentral, auf Vorfälle zu reagieren, ist so konzipiert, dass sie den gesetzlichen und behördlichen Verpflichtungen zur Reaktion auf Vorfälle entspricht. Als solches,

A. Unterhält RingCentral eine Incident-Response-Fähigkeit, um auf Ereignisse zu reagieren, die möglicherweise die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Diensten und/oder Daten, einschließlich Geschützter Daten, beeinträchtigen.

B. Verfügt RingCentral über einen dokumentierten Plan zur Reaktion auf Vorfälle, der auf branchenüblichen, anerkannten Verfahren basiert.

C. Verfügt RingCentral über einen Prozess für den Umgang mit Beweismaterial, der die Integrität der gesammelten Beweise sicherstellt, einschließlich der Erkennung von unbefugtem Zugriff auf und

D. Ergreift RingCentral geeignete Schritte und Maßnahmen, um die gesetzlichen und behördlichen Verpflichtungen zur Reaktion auf Vorfälle einzuhalten.

Wenn RingCentral von einem Sicherheitvorfall erfährt oder ihn entdeckt, das sich auf Geschützte Daten auswirkt, wird RingCentral den Kunden ohne unangemessene Verzögerung benachrichtigen und wird wirtschaftlich angemessene Schritte unternehmen, um ein solches Ereignis zu isolieren, abzuschwächen und/oder zu beheben.

13. Geschäftskontinuität und Disaster Recovery

A. Geschäftskontinuität

RingCentral:

i. Stellt sicher, dass die Verantwortlichkeiten für die Service Continuity klar definiert und dokumentiert sind und einer Person mit ausreichender Autorität zugewiesen wurden.

ii. Verfügt über einen Business Continuity Plan (BCP), der die fortlaufende Bereitstellung der Dienste für den Kunden gewährleisten soll.

iii. Entwickelt, implementiert und pflegt ein Business-Continuity-Management-Programm, um die Anforderungen des Unternehmens und der dem Kunden bereitgestellten Dienste zu erfüllen. Zu diesem Zweck führt RingCentral ein Mindestmaß an Business-Impact-Analyse, Krisenmanagement, Business-Continuity- und Disaster-Recovery-Planung durch.

iv. Stellt sicher, dass der Geltungsbereich des BCP alle relevanten Standorte, Mitarbeiter und Informationssysteme umfasst, die für die Erbringung der Services verwendet werden.

v. Stellt sicher, dass der BCP unter anderem Elemente wie Standort-Workarounds, Anwendungs-Workarounds, Anbieter-Workarounds und Personal-Workarounds umfasst, die mindestens einmal jährlich trainiert werden.

vi. Überprüft, aktualisiert und testet die BCPs mindestens einmal jährlich.

B. Wiederherstellung im Katastrophenfall

RingCentral:

i. Unterhält einen Notfallwiederherstellungsplan (Disaster-Recovery-Plan), der unter anderem Details zu Infrastruktur, Technologie und System(en) sowie Wiederherstellungsaktivitäten enthält und die für eine solche Wiederherstellung erforderlichen Personen/Teams identifiziert und mindestens einmal jährlich geübt wird.

ii. Stellt sicher, dass der Disaster-Recovery-Plan Maßnahmen vorsieht, die RingCentral im Falle eines längeren Ausfalls des Dienstes ergreifen wird.

iii. Stellt sicher, dass seine Pläne die Maßnahmen und Ressourcen berücksichtigen, die erforderlich sind, um (i) den kontinuierlichen Betrieb von RingCentral, und (ii) im Falle einer Unterbrechung, die

Wiederherstellung der Funktionen zu gewährleisten, die erforderlich sind, um RingCentral in die Lage zu versetzen, die Dienste bereitzustellen, einschließlich der erforderlichen Systeme, Hardware, Software, Ressourcen, Mitarbeiter und Daten, die diese Funktionen unterstützen.