Technische und organisatorische Maßnahmen
GoTo Connect

Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für GoTo Connect dargelegt. Insbesondere unterhält GoTo robuste globale Datenschutz- und Sicherheitsprogramme sowie organisatorische, administrative und technische Schutzmaßnahmen, um: (i) die Vertraulichkeit, Integrität und Verfügbarkeit von Kundeninhalten sicherzustellen; (ii) vor Bedrohungen und Gefahren für die Sicherheit von Kundeninhalten zu schützen; (iii) vor Verlust, Missbrauch, unbefugtem Zugriff, Offenlegung, Veränderung und Zerstörung von Kundeninhalten zu schützen; und (iv) die Einhaltung geltender Gesetze und Vorschriften, einschließlich Datenschutzgesetzen, zu gewährleisten. Solche Maßnahmen umfassen:

- **Verschlüsselung:**
  - *Während der Übertragung* Transport Layer Security (TLS)
  - *Im Ruhezustand* Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte.
- **Rechenzentren:** Standorte in den USA, Brasilien, Deutschland, Australien, Singapur und im Vereinigten Königreich, um Redundanz und Stabilität zu gewährleisten.
- **Physische Sicherheit:** Geeignete physische Sicherheits- und Umgebungskontrollen sind vorhanden und darauf ausgelegt, den physischen Zugang zu Systemen und Servern mit Kundeninhalten zu schützen, zu kontrollieren und einzuschränken, um die Verpflichtungen hinsichtlich Betriebszeit, Leistung und Skalierbarkeit einhalten zu können.
- **Compliance-Audits:** GoTo Connect ist nach SOC 2 Typ II, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy sowie APEC CBPR und PRP zertifiziert.
- **Einhaltung gesetzlicher/behördlicher Vorschriften:** GoTo unterhält ein umfassendes Datenschutzprogramm mit Prozessen und Richtlinien, die sicherstellen sollen, dass Kundeninhalte in Übereinstimmung mit den geltenden Datenschutzgesetzen, einschließlich DSGVO, CCPA/CPRA und LGPD, behandelt werden.
- **Sicherheitsprüfungen**: GoTo führt nicht nur interne Tests durch, sondern beauftragt zusätzlich externe Firmen mit der regelmäßigen Durchführung von Sicherheitsprüfungen und/oder Penetrationstests.
- **Logische Zugriffskontrollen:** Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollen soll die Bedrohung des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden.
- **Datentrennung**: GoTo verwendet eine Multi-Tenant-Architektur und trennt Kundenkonten logisch auf der Datenbankebene.
- **Perimeterabwehr und Erkennung von Eindringversuchen**: Tools, Techniken und Dienste zum Schutz des Perimeters sollen verhindern, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung.
- **Datenaufbewahrung:**
  - Kunden von GoTo Connect können jederzeit einen Antrag auf Rückgabe oder Löschung von Kundeninhalten stellen, der innerhalb von dreißig (30) Tagen nach Antragstellung des Kunden bearbeitet wird.
  - Kundeninhalte werden dreißig (30) Tage nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht. Während der Laufzeit des Abonnements werden Anrufaufzeichnungen und Anrufberichte ab dem Datum ihrer Erstellung dreizehn (13) Monate lang aufbewahrt.

Inhalt

Klicken Sie auf die Seitenzahlen unten, um zum entsprechenden Abschnitt der TOMs zu gelangen.

Zusammenfassung 1

Inhalt 2

1 *Produkteinführung* 3

2 *Technische Maßnahmen* 3

3 *Produktarchitektur* 4

4 *Technische Sicherheitskontrollen* 5

5 *Aktualisierungen des Sicherheitsprogramms* 6

6 *Daten-Backup, Notfallwiederherstellung und Verfügbarkeit* 6

7 *Rechenzentren* 7

8 *Einhaltung von Standards* 7

9 *Anwendungssicherheit* 8

10 *Protokollierung, Überwachung und Warnmeldungen* 8

11 *Endpoint Detection and Response (EDR)* 8

12 *Bedrohungsmanagement* 8

13 *Sicherheits- und Schwachstellenscans sowie Patch-Management* 9

14 *Logische Zugriffskontrolle* 9

15 *Datentrennung* 9

16 *Perimeterabwehr und Erkennung von Eindringversuchen* 9

17 *Sicherheitsmaßnamen und Incident-Management* 10

18 *Löschung und Rückgabe von Inhalten* 10

19 *Organisatorische Kontrollen* 10

20 *Datenschutzpraktiken* 11

21 *Kontrollen der Sicherheits- und Datenschutzpraktiken von Drittanbietern* 14

22 *Kontaktaufnahme mit GoTo* 14

1 Produkteinführung

GoTo Connect ist eine Unified Communications as a Service (UCaaS)-Komplettlösung für Unternehmen und Betriebe. Die Lösung kombiniert cloudbasierte VoIP-Telefonsysteme (Voice-over-Internet Protocol) mit den Web-, Audio- und Videokonferenzdiensten von GoTo Meeting* in einer einfachen, zuverlässigen und flexiblen Collaboration-Lösung (der „Dienst“).

Der Dienst umfasst die folgenden Funktionen und Angebote:

- Der cloudbasierte Telefondienst von GoTo Connect wurde als Ersatz für herkömmliche On-Premise-PBX-Telefonanlagen (Private Branch Exchange) entwickelt. Das PBX-Administrationsportal ermöglicht es Benutzern mit Administratorberechtigungen, die Systemeinstellungen von jedem Gerät mit einer Internetverbindung aus anzuzeigen und allgemeine Änderungen daran vorzunehmen.
- Die Ersatzdienste für das öffentliche Telefonnetz (Public Switch Telephone Network, PSTN) (einschließlich Telefonnummern, Minuten und zugehörige Dienste) werden über Partnerschaften mit einigen der weltweit führenden Telekommunikationsanbieter bereitgestellt.
- Der visuelle Wählplan-Editor ist ein Tool zur Bearbeitung des Anrufablaufs, mit dem Sie Anrufe an bestimmte Voicemailboxen, automatische Telefonzentralen oder Rufgruppen weiterleiten oder Wartezeiten einrichten können.
- GoTo Connect Business Continuity (früher bekannt als „JBC“) ist ein optionales Premiumangebot aus Diensten und Hardware, das in den Räumlichkeiten einer Person, die den Dienst nutzt („Benutzer“), installiert wird und im Fall eines Netzwerkausfalls einen lokalen Telefondienst über einen unabhängigen Drittanbieter bereitstellt, dessen Dienste von einem Benutzer separat bezogen werden.

*Weitere Informationen über den GoTo Meeting-Dienst und seine technischen und organisatorischen Maßnahmen finden Sie in den GoTo Meeting-TOMs unter https://www.goto.com/company/trust/resource-center.

In diesem Dokument verwendete Begriffe, die nicht im Text definiert sind, werden in den Nutzungsbedingungen erklärt.

2 Technische Maßnahmen

Die Produkte von GoTo sind so konzipiert, dass sie Lösungen bieten, die sicher, zuverlässig und privat sind. Die im Folgenden definierten technischen Maßnahmen beschreiben, wie GoTo dieses Konzept umsetzt und in der Praxis anwendet.

2.1 Schutzmaßnahmen

Die Implementierung von Schutzmaßnahmen, Funktionen und Praktiken durch GoTo beinhaltet Folgendes:

I. Entwicklung von Produkten, bei denen Sicherheit und Datenschutz standardmäßig integriert sind, und Einbeziehung zusätzlicher Sicherheitsebenen zum Schutz von Kundeninhalten

II. Durchführung organisatorischer Kontrollen, die interne Richtlinien und Verfahren in Bezug auf die Einhaltung von Standards, Incident-Management, Anwendungssicherheit, Personalsicherheit und regelmäßige Schulungsprogramme operationalisieren

III. Sicherstellung, dass Datenschutzpraktiken vorhanden sind, die den Umgang mit und die Verwaltung von Daten in Übereinstimmung mit geltenden Gesetzen, einschließlich DSGVO, CCPA/CPRA, LGPD, sowie mit unserem eigenen Datenverarbeitungsnachtrag (DVN) und den geltenden Richtlinien und Verpflichtungen von GoTo regeln.

Durch Einbau von Sicherheitsvorkehrungen in das Produkt bemühen wir uns, GoTo-Kundeninhalte vor Bedrohungen zu schützen und sicherzustellen, dass die Sicherheitskontrollen der Art und dem Umfang der Dienste angemessen sind. Die konfigurierbaren Sicherheitsfunktionen von GoTo können Administratoren dabei helfen, Bedrohungen und Risiken, die von Benutzern der GoTo-Dienste ausgehen, für Systeme und Netzwerke zu minimieren.

3 Produktarchitektur

Das folgende Diagramm (Abbildung 1) zeigt die Netzwerkarchitektur von GoTo Connect.

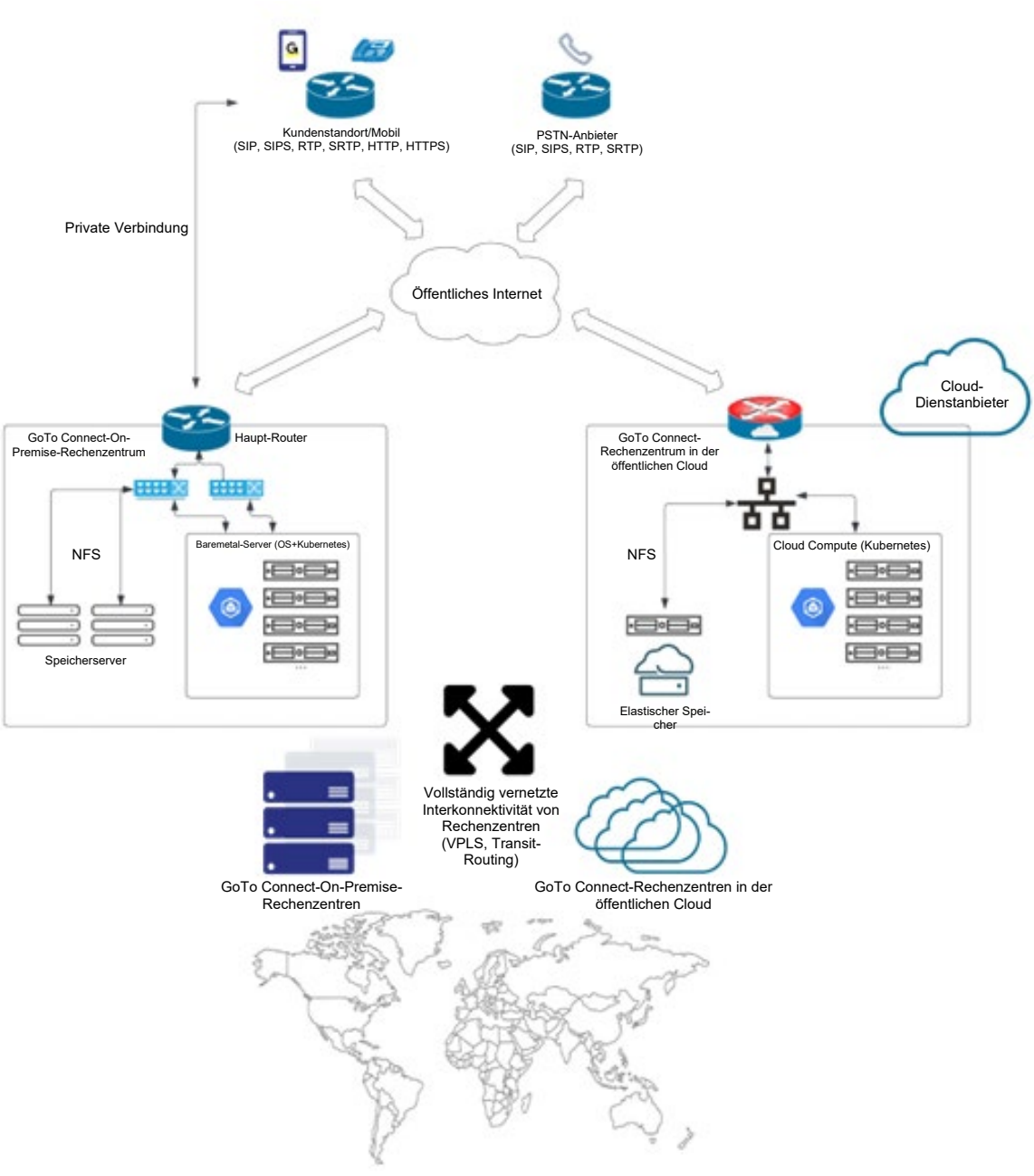

Abbildung 1: GoTo Connect-Architektur

4 Technische Sicherheitskontrollen

GoTo setzt technische Sicherheitskontrollen ein, die dafür entwickelt wurden, die Dienstinfrastruktur und die darin enthaltenen Daten zu schützen.

4.1 Verschlüsselung

GoTo überprüft regelmäßig seine Verschlüsselungsstandards und aktualisiert gegebenenfalls die verwendeten Verschlüsselungsverfahren und/oder Technologien entsprechend der Risikobewertung und der Marktakzeptanz neuer Standards.

4.2 Verschlüsselung während der Übertragung

Der Dienst ist mit End-to-End-Sicherheitsmaßnahmen zum Schutz von Daten ausgestattet, um sicherzustellen, dass Kommunikationsdaten während der Übertragung über öffentliche oder private Netzwerke oder zu Kommunikationsservern nicht unverschlüsselt offenliegen.

Zum Schutz der Kommunikation zwischen Endpunkten werden TLS-Standardprotokolle der Internet Engineering Task Force (IETF) verwendet. Der gesamte Netzwerk-Datenverkehr, der in Rechenzentren ein- und ausgeht, in denen GoTo-Daten gespeichert sind, wird während der Übertragung verschlüsselt. Dies schließt auch alle Kundeninhalte ein.

Beim Aufbau von TLS-Verbindungen nutzen GoTo-Server Zertifikate mit öffentlichem Schlüssel, um sich bei Clients (d. h. Workstations oder Geräten) zu authentifizieren. Wenn TLS von Benutzergeräten unterstützt wird, wird dieses Protokoll zur Absicherung des Datenverkehrs zwischen den Benutzergeräten und der Infrastruktur des Diensts verwendet. TLS sichert auch die Übertragung zur Bereitstellung von Informationen (darunter die Zugangsdaten des Telefons) von der Infrastruktur des Diensts an die Telefone ab. Medien werden mit dem Secure Real-time Transport Protocol (SRTP) übertragen, während Audiodatenverkehr mit vorinstallierten Schlüsseln abgesichert wird, die über Session Initiation Protocol Secure (SIPS) übertragen werden.

4.3 Verschlüsselung ruhender Daten

Voicemail-Aufzeichnungen, Voicemail-Begrüßungen und Anrufaufzeichnungen werden im Ruhezustand mit 256-Bit-AES-Verschlüsselung verschlüsselt, wenn sie im Cloud-Speicher von GoTo gespeichert sind.

4.4 Benutzerauthentifizierung

GoTo Connect verwaltet den Benutzerzugriff über die GoTo-eigene Identitätsverwaltungsplattform, nutzt Security Assertion Markup Language (SAML), um Single Sign-On (SSO) anzubieten, und kann über eine API direkt in die GoTo-Plattform integriert werden. Die Identitätsverwaltungsplattform unterstützt Administrationskontrollen im Zusammenhang mit der Benutzerauthentifizierung, darunter die Konfiguration von Passwort-Richtlinien, die Erzwingung der Zurücksetzung von Passwörtern und die Verwendung von SAML für die Anmeldung.

PBX-Dienstadministratoren (Superadministratoren) können im PBX-Administrationsportal bestimmte Berechtigungen gewähren oder verweigern. Diese Berechtigungen umfassen die Möglichkeit, die PBX-Anlage zu konfigurieren, Notrufadressen/-standorte zu bearbeiten, Berichte anzuzeigen, Rechnungen anzuzeigen und zu bezahlen sowie Einstellungen und Konten für folgende Elemente zu aktualisieren und zu löschen:

- Benutzer
- Benutzergruppen
- Durchwahlen
- Geräte

- Hardware
- Standorte
- Telefonnummern (das Löschen und Erstellen von Telefonnummern wird über den Bestellvorgang für Telefonnummern verwaltet)

Weitere Einzelheiten zu Gruppenberechtigungen in der PBX-Administration finden Sie im Leitfaden mit ersten Schritten für Administratoren.

5 Aktualisierungen des Sicherheitsprogramms

Mindestens einmal jährlich überprüft und aktualisiert GoTo unser Sicherheitsprogramm und beauftragt unabhängige Dritte mit der Bewertung unserer maßgeblichen Sicherheitskontrollen, um sicherzustellen, dass wir uns an die aktuelle Bedrohungslage anpassen und mit den relevanten Rahmenwerken, Branchenstandards, Kundenverpflichtungen und ggf. Änderungen von Gesetzen und Vorschriften in Bezug auf die Sicherheit der GoTo-Daten konform sind.

6 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo Connect ist so konzipiert, dass eine Replikation in nahezu Echtzeit an geografisch verteilten Standorten erfolgt. Datenbanken werden mit einer rollierenden inkrementellen Backup-Strategie gesichert. Im Notfall oder bei einem Totalausfall an einem der zahlreichen aktiven Standorte sind die verbleibenden Standorte so konzipiert, dass sie die Anwendungslast ausgleichen. Die Notfallwiederherstellung für diese Systeme wird regelmäßig getestet.

Um eine hohe Verfügbarkeit zu gewährleisten, betreibt GoTo ein Netzwerk von Rechenzentren, die vollständig miteinander vernetzt sind. Diese Rechenzentren arbeiten mit einer Kapazität von N+1-Rechenzentren, d. h., der Dienst ist so konzipiert, dass er den Kapazitätsverlust bei Ausfall eines Rechenzentrums verkraften und den Betrieb aufrechterhalten kann, indem der Datenverkehr automatisch an andere Rechenzentrumsstandorte weitergeleitet wird.

Insbesondere verwendet der Dienst eine containerisierte Microservice-Plattform, die eine schnelle Bereitstellung und Skalierung von Diensten ermöglicht und den Benutzern Redundanz, Anruf-Failover, Skalierbarkeit und hohe Verfügbarkeit bietet. Dank dieses vollständig vernetzten Designs können sich Microservices bei einem Ausfall in einem bestimmten Rechenzentrum oder im Fall eines geografisch begrenzten Problems im öffentlichen Internet selbst erkennen und wiederherstellen. Der Dienst ist so konzipiert, dass ein automatischer Failover zwischen Rechenzentren möglich ist.

Die Infrastruktur ist zwischen Rechenzentren in Form von „Clustern“ verbunden, mit der Interkonnektivität eines vernetzten Virtual Private LAN Service (VPLS)-Netzwerks und Transit-Routing. Falls die primären Verbindungen getrennt werden, können VPLS-Verbindungen über Internetlinks auf ein verschlüsseltes Dynamic Multipoint Virtual Private Network (DMVPN) ausweichen. Rechenzentren in der Cloud sind über verschlüsselte Tunnel mit Standorten regionaler Cloud-Anbieter verbunden. Diese Tunnel schützen die Daten, indem sie sie so lange wie möglich vom öffentlichen Internet fernhalten. Alle Produktionsrechenzentren sind miteinander verbunden, damit interne Anwendungen von jedem Standort aus auf die Dienste zugreifen können. GoTo Connect-Daten werden vor Ort in privater Hardware (Racks und Blades) oder in Rechenzentren von Cloud-Hosting-Anbietern gehostet, die eine ähnliche, aber angepasste Architektur aufweisen. Jeder Rechenzentrumsstandort ist über SIP-Trunks (Session Initiation Protocol) über das öffentliche Internet mit mehreren PSTN-Partnern/Anbietern verbunden.

7 Rechenzentren

Die GoTo-Infrastruktur setzt auf die folgenden Komponenten, um die Zuverlässigkeit des Diensts zu erhöhen und das Risiko von Ausfallzeiten aufgrund eines Single Point of Failure zu verringern:

a) redundante, aktiv-aktive Rechenzentren oder
b) Rechenzentren von Cloud-Hosting-Anbietern

Die Hosting-Rechenzentren befinden sich in den USA, Brasilien, Deutschland, Australien, Singapur und im Vereinigten Königreich.

In allen Rechenzentren werden die Umgebungsbedingungen überwacht und Daten rund um die Uhr durch die nachfolgend erläuterten physischen Sicherheitsvorkehrungen geschützt.

7.1 Physische Sicherheit im Rechenzentrum

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungskontrollen für Systeme und Server mit Kundeninhalten zu gewährleisten. Zu diesen Kontrollen gehören die folgenden:

- Videoüberwachung und -aufzeichnung
- HLK-Temperaturregelung (Heizung, Lüftung und Klimatisierung)
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung
- Doppelböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen natürlichen und vom Menschen verursachten Katastrophen, je nach Geografie und Standort des jeweiligen Rechenzentrums
- Planmäßige Wartung und Validierung aller kritischen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu den Produktionsdatenzentren auf autorisierte Personen. Um Zugang zu einem On-Premise-Serverraum oder zu einer Hosting-Einrichtung eines Drittanbieters zu erhalten, muss ein Antrag über das entsprechende Ticketsystem gestellt werden, der vom zuständigen Manager genehmigt und vom technischen Betriebsteam von GoTo überprüft und genehmigt werden muss. Der gesamte physische Zugang zu Rechenzentren und Serverräumen wird protokolliert, und die Protokolle werden vom GoTo-Management mindestens vierteljährlich überprüft. Darüber hinaus wird die Autorisierung für den physischen Zugang zum Rechenzentrum bei einem Rollenwechsel (wenn ein solcher Zugang nicht mehr erforderlich ist) oder bei Kündigung oder Austritt eines zuvor autorisierten Mitarbeiters umgehend aufgehoben. Für hochsensible Bereiche, zu denen auch Rechenzentren gehören, ist eine Multifaktor-Authentifizierung (z. B. Biometrie, Ausweis und Tastatur) erforderlich, um Zugang zu erhalten.

8 Einhaltung von Standards

GoTo prüft regelmäßig die Einhaltung der geltenden rechtlichen, sicherheitstechnischen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen. Die Datenschutz- und Sicherheitsprogramme von GoTo erfüllen strenge und international anerkannte Standards, wurden nach umfassenden externen Audit-Standards bewertet und haben wichtige Zertifizierungen erhalten, darunter:

- **TRUSTe Enterprise Privacy- und Data Governance Practices-Zertifizierung** für betriebliche Datenschutz- und Datensicherheitskontrollen, die mit den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzrahmenwerken übereinstimmen. Um mehr zu erfahren, besuchen Sie unseren Blogbeitrag.

- **TRUSTe APEC CBPR- und PRP-Zertifizierungen** für die Übertragung von Kundeninhalten zwischen APEC-Mitgliedsländern, erworben und unabhängig validiert von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für Datenschutz-Compliance. Um mehr über unsere APEC-Zertifizierungen zu erfahren, klicken Sie hier.
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Typ II** Zertifizierungsbericht inkl. **BSI Cloud Computing Katalog (C5)**.
- **Payment Card Industry Data Security Standard (PCI DSS)**-Compliance für die E-Commerce- und Zahlungsumgebungen von GoTo.
- Bewertung der internen Kontrollen, wie im Rahmen einer Jahresabschlussprüfung des **Public Company Accounting Oversight Board (PCAOB)** erforderlich.

9 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo folgt dem Microsoft Security Development Lifecycle (SDL), um den Produktcode zu abzusichern. Das Microsoft SDL-Programm umfasst manuelle Codeprüfungen, Bedrohungsmodellierung, statische Codeanalyse, dynamische Analyse und Systemhärtung. GoTo-Teams führen außerdem regelmäßig dynamische und statische Schwachstellenprüfungen von Anwendungen und Penetrationstests für bestimmte Umgebungen durch.

10 Protokollierung, Überwachung und Warnmeldungen

GoTo unterhält Richtlinien und Verfahren für Protokollierung, Überwachung und Warnmeldungen, in denen die Grundsätze und Kontrollen festgelegt werden, die implementiert wurden, um unsere Fähigkeit zur Erkennung verdächtiger Aktivitäten und zur rechtzeitigen Reaktion darauf zu verbessern. GoTo sammelt identifizierten anomalen oder verdächtigen Datenverkehr in den entsprechenden Sicherheitsprotokollen der jeweiligen Produktionssysteme.

11 Endpoint Detection and Response (EDR)

EDR-Software (Endpoint Detection and Response) mit Audit-Protokollierung wird auf allen GoTo-Servern eingesetzt, um Unterbrechungen oder Auswirkungen auf die Leistung des Diensts zu minimieren. Wenn verdächtige Aktivitäten entdeckt werden, werden Sicherheitsuntersuchungen gemäß unseren Verfahren zur Reaktion auf Vorfälle eingeleitet, sofern dies angemessen und notwendig ist. In Abschnitt 17 finden Sie weitere Informationen über das GoTo Security Operations Center und die Verfahren zur Reaktion auf Vorfälle.

12 Bedrohungsmanagement

Das Cyber Security Incident Antwort-Team („CSIRT“) von GoTo besteht aus mehreren Teams und ist für den Schutz vor Cyberbedrohungen zuständig. Speziell das Cyber Threat Intelligence-Team innerhalb des CSIRT sammelt, prüft und verbreitet Informationen über aktuelle und neu auftretende Bedrohungen. Durch ständige Überprüfung von Open- und Closed-Source-Software und sowie die Teilnahme an Austauschgruppen und Mitgliedschaft in Branchenverbänden (IT-ISAC, FIRST.org usw.) hält sich GoTo über Bedrohungsforschung und -abwehr auf dem Laufenden.

13 Sicherheits- und Schwachstellenscans sowie Patch-Management

GoTo unterhält ein formelles Patch-Management-Programm und führt mindestens vierteljährlich Patch-Management-Aktivitäten für alle relevanten Systeme, Geräte, Firmware, Betriebssysteme, Anwendungen und andere Software durch, die Kundeninhalte verarbeiten. Mindestens einmal im Monat sowie nach jeder wesentlichen Änderung dieser Systeme führt GoTo Bewertungen durch und sucht nach Schwachstellen auf Systemebene sowie in internen und externen Hosts/Netzwerken („Systeme“) und behebt die betreffenden entdeckten Schwachstellen in Übereinstimmung mit dokumentierten Richtlinien, die die Abhilfemaßnahmen auf Basis des Risikos priorisieren.

14 Logische Zugriffskontrolle

Verfahren zur logischen Zugriffskontrolle sollen das Risiko eines unbefugten Anwendungszugriffs und des Datenverlusts in Unternehmens- und Produktionsumgebungen verringern. Mitarbeitern wird der Zugriff auf bestimmte GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte nach dem Prinzip der geringsten Rechte gewährt. Benutzerberechtigungen werden auf der Grundlage der funktionalen Rolle (rollenbasierte Zugriffskontrolle) und der Umgebung unter Verwendung von Kontrollen, Prozessen und/oder Verfahren zur Aufgabentrennung getrennt.

15 Datentrennung

GoTo hat Kontrollen implementiert, um zu verhindern, dass Benutzer die Daten anderer Benutzer sehen können. GoTo nutzt zum Beispiel eine logisch auf Datenbankebene getrennte Multi-Tenant- (und Multi-PBX-)Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Die Parteien müssen sich authentifizieren, um Zugriff auf ein Konto zu erhalten.

16 Perimeterabwehr und Erkennung von Eindringversuchen

GoTo verwendet Tools, Techniken und Dienste zum Schutz des Perimeters, um zu verhindern, dass unbefugter Netzwerkdatenverkehr in die Produktinfrastruktur von GoTo gelangt. Zu diesen Maßnahmen zählen unter anderem:

- Systeme zur Erkennung von Eindringversuchen, die Systeme, Dienste, Netzwerke und Anwendungen auf unbefugten Zugriff überwachen
- Überwachung kritischer System- und Konfigurationsdateien
- Web Application Firewall (WAF) und DDoS-Präventionsdienste auf der Anwendungsschicht, die als Proxy für den GoTo-Datenverkehr fungieren
- Eine lokale Anwendungs-Firewall, die als zusätzlicher Schutz vor den OWASP Top Ten und anderen Schwachstellen in Webanwendungen sowie vor bösartigem Datenverkehr dient
- Host-basierte Firewalls auf GoTo-Webservern, die eingehende und ausgehende Verbindungen filtern, darunter auch interne Verbindungen zwischen GoTo-Systemen

17 Sicherheitsmaßnamen und Incident-Management

Das GoTo Security Operations Center ist für die Erkennung von und die Reaktion auf Sicherheitsereignisse zuständig. Das Security Operations Center verwendet Sicherheitssensoren und Analysesysteme, um potenzielle Probleme zu identifizieren, und hat Verfahren zur Reaktion auf Vorfälle entwickelt, einschließlich eines dokumentierten Notfallplans.

Der GoTo-Notfallplan ist auf unsere Prozesse, Richtlinien und Standardbetriebsverfahren für kritische Kommunikation abgestimmt. Er wurde entwickelt, um relevante mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten des Unternehmens (einschließlich GoTo Connect) zu verwalten, zu identifizieren und zu beheben. Im Notfallplan sind Mechanismen festgelegt, mit denen Mitarbeiter mutmaßliche Sicherheitsereignisse melden können, sowie Eskalationswege, die gegebenenfalls zu befolgen sind. Mutmaßliche Ereignisse werden dokumentiert und ggf. über standardisierte Ereignistickets eskaliert und nach ihrer Kritikalität eingestuft.

18 Löschung und Rückgabe von Inhalten

Löschung und/oder Rückgabe: Kunden können die Rückgabe und/oder Löschung ihrer Kundeninhalte anfordern, indem sie einen Antrag über das Portal zur Verwaltung individueller Rechte (Individual Rights Management Portal, IRM) von GoTo stellen, und zwar über support.goto.com oder per E-Mail an privacy@goto.com. Anträge werden innerhalb von dreißig (30) Tagen nach Eingang bei GoTo bearbeitet. Sollten wir jedoch mehr Zeit benötigen, werden wir Sie so schnell wie möglich über die voraussichtliche Verzögerung und den neuen Abschlusstermin informieren.

Zeitplan für die Aufbewahrung von Kundeninhalten: Sofern das geltende Recht nichts anderes vorschreibt, werden Kundeninhalte dreißig (30) Tage nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden automatisch gelöscht. Während der Laufzeit des Kundenabonnements werden Anrufaufzeichnungen und Anrufberichte rollierend gelöscht und ab dem Datum ihrer Erstellung dreizehn (13) Monate lang aufbewahrt. Auf schriftliche Anfrage kann GoTo die Löschung von Inhalten schriftlich bestätigen/bescheinigen.

19 Organisatorische Kontrollen

19.1 Sicherheitsrichtlinien und -verfahren

GoTo unterhält einen umfassenden Satz von Sicherheitsrichtlinien und -verfahren, die regelmäßig überprüft und bei Bedarf aktualisiert werden, um den Sicherheitszielen von GoTo, Änderungen der geltenden Gesetze, Branchenstandards und Compliance-Bemühungen zu entsprechen.

19.2 Änderungsmanagement

GoTo unterhält ein geeignetes Änderungsmanagement-Verfahren. Änderungen an GoTo-Systemen werden vor der Implementierung bewertet, getestet und genehmigt, um das Risiko einer Unterbrechung der GoTo-Dienste zu verringern.

19.3 Programme für Sicherheitssensibilisierung und -schulung

Das GoTo-Programm zur Sensibilisierung für Datenschutz und Sicherheit beinhaltet die Schulung der Mitarbeiter über die Bedeutung eines ethisch korrekten, verantwortungsvollen, gesetzeskonformen und sorgfältigen Umgangs mit personenbezogenen Daten und

vertraulichen Informationen. Neu eingestellte Mitarbeiter, Vertragspartner und Praktikanten werden beim Onboarding über die Sicherheitsrichtlinien und den betrieblichen Verhaltenskodex und die ethischen Grundsätze von GoTo informiert. GoTo-Mitarbeiter absolvieren mindestens einmal jährlich eine Schulung zum Thema Datenschutz und Sicherheit. Sensibilisierungsmaßnahmen finden das ganze Jahr über statt und können Kampagnen zum Datenschutztag, zum Cybersecurity Awareness Month, Webinare mit dem Chief Information Security Officer und ein Programm für Sicherheits-Champions umfassen.

Gegebenenfalls müssen die Mitarbeiter auch rollenspezifische Schulungen absolvieren. Darüber hinaus müssen alle Mitarbeiter, Vertragspartner und Tochtergesellschaften von GoTo die Richtlinien von GoTo in Bezug auf Sicherheit und Datenschutz lesen und befolgen.

20 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten unserer Kunden und Benutzer sehr ernst und verpflichtet sich, relevante Praktiken zur Datenverarbeitung und -verwaltung offen und transparent darzulegen.

20.1 Datenschutzprogramm

GoTo unterhält ein umfassendes Datenschutzprogramm, für das Koordination mehrerer Funktionen innerhalb des Unternehmens erforderlich ist, darunter Datenschutz, Sicherheit, Governance, Risiko und Compliance (GRC), Recht, Produkt, Technik und Marketing. Dieses Datenschutzprogramm konzentriert sich auf die Einhaltung von Vorschriften und umfasst die Implementierung und Pflege interner und externer Richtlinien, Standards und Ergänzungen zur Regelung der Praktiken des Unternehmens.

20.2 Einhaltung behördlicher Vorschriften

20.3 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) bzgl. des Schutzes der Daten und der Privatsphäre aller Personen in der EU. GoTo unterhält ein umfassendes Programm zur Sicherstellung der DSGVO-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die der DSGVO unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen der DSGVO tun. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

20.4 CCPA

Der California Consumer Privacy Act in der Fassung des California Privacy Rights Act (gemeinsam als „CCPA“ bezeichnet), gewährt den kalifornischen Bürgern zusätzliche Rechte und zusätzlichen Schutz in Bezug auf die Verwendung ihrer persönlichen Informationen durch Unternehmen. GoTo unterhält ein umfassendes Programm zur Sicherstellung der CCPA-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die dem CCPA unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen des CCPA tun. Weitere Informationen über die Einhaltung des CCPA finden Sie in der Datenschutzrichtlinie von GoTo und den Ergänzenden Offenlegungen nach dem California Consumer Privacy Act.

20.5 LGPD

Das brasilianische Datenschutzgesetz (LGPD) regelt die Verarbeitung personenbezogener Daten in Brasilien und/oder von Personen, die sich zum Zeitpunkt der Datenerfassung in Brasilien befinden. GoTo unterhält ein umfassendes Programm zur Sicherstellung der

LGPD-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die dem LGPD unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen des LGPD tun. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

20.6 Datenverarbeitungsnachtrag

GoTo bietet einen globalen Datenverarbeitungsnachtrag (DVN) an, der auf Englisch und Deutsch verfügbar ist. Dieser DVN erfüllt die Anforderungen von DSGVO, CCPA, LGPD und anderen geltenden Vorschriften und regelt die Verarbeitung von Kundeninhalten durch GoTo.

Unser DVN enthält mehrere auf die DSGVO ausgerichtete Datenschutzmaßnahmen, darunter:

(a) Details zur Datenverarbeitung und Offenlegungen der Unterauftragsverarbeiter unter Artikel 28
(b) überarbeitete (2021) Standardvertragsklauseln (auch bezeichnet als EU-Musterklauseln) und
(c) produktspezifische technische und organisatorische Maßnahmen von GoTo.

Um den Anforderungen des CCPA Rechnung zu tragen, umfasst unser globaler DVN außerdem:

(a) überarbeitete Definitionen, die dem CCPA zugeordnet sind
(b) Zugriffs- und Löschrechte
(c) Garantien, dass GoTo die persönlichen Informationen unserer Kunden oder Benutzer nicht verkauft

Unser globaler DVN enthält außerdem Bestimmungen zu folgenden Punkten:

(a) Einhaltung des LGPD durch GoTo
(b) Unterstützung der rechtmäßigen Übertragung personenbezogener Daten nach/aus Brasilien
(c) Sicherstellung, dass unsere Benutzer die gleichen Vorteile beim Datenschutz genießen wie unsere anderen Benutzer in aller Welt.

20.7 Abkommen zur Datenübertragung

GoTo unterstützt die rechtmäßige internationale Übertragung von Daten im Rahmen der folgenden Abkommen:

20.8 Standardvertragsklauseln

Die Standardvertragsklauseln (Standard Contractual Clauses, SCCs), die manchmal auch als EU-Musterklauseln bezeichnet werden, sind standardisierte Vertragsbedingungen, die von der Europäischen Kommission anerkannt und übergenommen wurden, um sicherzustellen, dass alle personenbezogenen Daten, die den Europäischen Wirtschaftsraum (EWR) verlassen, in Übereinstimmung mit dem EU-Datenschutzrecht übertragen werden. Die 2021 überarbeiteten und herausgegebenen SCCs wurden in den globalen DVN von GoTo integriert, um GoTo-Kunden die Übertragung von Daten aus dem EWR in Übereinstimmung mit der DSGVO zu ermöglichen.

20.9 Zertifizierung nach APEC CBPR und PRP

GoTo ist gemäß APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft) CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) zertifiziert. Die APEC CBPR- und PRP-Rahmenwerke wurden als erste ihrer Art für die Übertragung personenbezogener Daten zwischen APEC-Mitgliedsländern

genehmigt und von TrustArc, einem von der APEC anerkannten Drittanbieter für Datenschutz-Compliance, erworben und unabhängig validiert.

20.10 Ergänzende Maßnahmen

Zusätzlich zu den in diesen TOMs genannten Maßnahmen hat GoTo eine FAQ erstellt, die die zusätzlichen Maßnahmen zur Unterstützung rechtmäßiger Übertragungen gemäß Kapitel 5 der DSGVO darlegt und alle vom Europäischen Gerichtshof in Verbindung mit der Verwendung der SCCs empfohlenen Einzelfallanalysen behandelt und leitet.

20.11 Datenanfragen

GoTo unterhält umfassende Prozesse, um die Entgegennahme von datenschutz- und sicherheitsbezogenen Anfragen zu erleichtern. Dazu gehören das IRM-Portal, die Datenschutz-E-Mail-Adresse (privacy@goto.com) und der Kundensupport unter https://support.goto.com.

20.12 Offenlegungen der Unterauftragsverarbeiter und Rechenzentren

GoTo veröffentlicht die Offenlegungen der Unterauftragsverarbeiter in seinem Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Diese Offenlegungen enthalten die Namen, Standorte und Verarbeitungszwecke von Datenhosting-Anbietern und anderen Drittanbietern, die Kundeninhalte im Rahmen der Bereitstellung des Diensts für GoTo-Kunden verarbeiten.

20.13 Einschränkungen bei der Verarbeitung sensibler Daten

Die folgenden Arten von sensiblen Daten dürfen nicht in GoTo Connect hochgeladen oder GoTo auf andere Weise zur Verfügung gestellt werden, es sei denn, GoTo hat dies ausdrücklich verlangt oder der Kunde hat eine anderweitige schriftliche Genehmigung von GoTo erhalten:

- Von der Regierung ausgestellte Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen, die sich auf die Gesundheit einer Person beziehen, einschließlich, aber nicht beschränkt auf geschützte Gesundheitsinformationen (Protected Health Information, PHI) gemäß Definition im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) sowie anderen einschlägigen geltenden Gesetzen und Vorschriften.
- Informationen im Zusammenhang mit Finanzkonten und Zahlungsinstrumenten, einschließlich, aber nicht beschränkt auf, Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung bezieht sich auf ausdrücklich gekennzeichnete Zahlungsformulare und -seiten, die von GoTo verwendet werden, um Zahlungen für den Dienst einzuziehen.
- Alle Informationen, die durch geltende Gesetze und Vorschriften besonders geschützt sind, insbesondere Informationen über Rasse, ethnische Zugehörigkeit, religiöse oder politische Überzeugung, Mitgliedschaften einer Person in Organisationen usw.

20.14 Compliance in regulierten Umgebungen

Es liegt in der Verantwortung der Kunden, angemessene Richtlinien, Verfahren und andere Schutzmaßnahmen in Bezug auf die Verwendung von GoTo Connect in regulierten Umgebungen einzuführen.

21 Kontrollen der Sicherheits- und Datenschutzpraktiken von Drittanbietern

Vor der Beauftragung von Drittanbietern, die Kundeninhalte oder vertrauliche, sensible oder Mitarbeiterdaten verarbeiten, überprüft und analysiert GoTo die Sicherheits- und Datenschutzpraktiken des Anbieters über die entsprechenden Beschaffungskanäle. Gegebenenfalls holt GoTo in regelmäßigen Abständen Compliance-Dokumente oder -Berichte von Anbietern ein und wertet diese aus, um sicherzustellen, dass das Kontrollumfeld und die Standards der Anbieter weiterhin ausreichend sind.

GoTo schließt mit allen Drittanbietern schriftliche Vereinbarungen ab und verwendet entweder von GoTo genehmigte Beschaffungsvorlagen oder verhandelt die Standardbedingungen dieser Drittanbieter, um die von GoTo akzeptierten Datenschutz- und Sicherheitsstandards zu erfüllen, sofern dies für erforderlich gehalten wird. Die Teams für Finanzen, Recht, Datenschutz und Sicherheit sind an der Überprüfung der Anbieter beteiligt und verifizieren, ob die Anbieter die spezifischen obligatorischen Anforderungen für den Umgang mit Daten und die vertraglichen Anforderungen erfüllen, sofern dies erforderlich und/oder angemessen ist. Die GoTo-Richtlinien in Bezug auf Drittanbieterrisiken regeln die Anforderungen an den Datenschutz und die Sicherheit von Anbietern m Hinblick auf Art und Dauer der Datenverarbeitung und der Zugriffsebene. Gegebenenfalls (z. B. wenn Kundeninhalte verarbeitet oder gespeichert werden) beinhalten die Vereinbarungen mit Anbietern Anforderungen zur „Einhaltung der geltenden Gesetze“, einen DVN oder ein ähnliches Dokument, das Themen wie DSGVO, CCPA, LGPD sowie Nutzungs- und Verkaufsbeschränkungen behandelt, je nach Bedarf. Der GoTo-DVN für Lieferanten enthält beispielsweise Beschränkungen bzgl. des „Verkaufs“ von Daten gemäß der Definition des CCPA. Entsprechend werden ergänzende Sicherheitsmaßnahmen mit geeigneten Kontrollen und Systemanforderungen mit den betreffenden Anbietern vereinbart.

22 Kontaktaufnahme mit GoTo

Für allgemeine Fragen können Kunden GoTo unter support.goto.com kontaktieren. Bei Fragen oder Anfragen in Bezug auf personenbezogene Daten oder Datenschutz besuchen Sie bitte unser IRM-Portal oder senden Sie eine E-Mail an privacy@goto.com.