# Technische und organisatorische Maßnahmen
## Rescue und Rescue Lens

## Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für Rescue und Rescue Lens 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) Version 1.2.
  - *Im Ruhezustand* Transparent Data Encryption (TDE) mit Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte.
- **Rechenzentren:**[1] Standorte in den USA, Deutschland und Irland, 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:** Rescue ist nach ISO/IEC 27001:2013, SOC 2 Typ II, 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:**
  - Rescue-Kunden 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 innerhalb von 140 Tagen nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht.

[1] Die Hosting-Standorte können variieren (d. h. abhängig von der Wahl des Datenspeicherorts verschieden sein). Weitere Informationen finden Sie in der Offenlegungen der Unterauftragsverarbeiter (Rescue Sub-Processor Disclosure) für Rescue, die Sie im Abschnitt „Product Resources“ (Produktressourcen) im GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center) finden.

# Inhalt

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

# 1 Produkteinführung

**Rescue** ist ein Online-Remotesupportdienst, mit dem Techniker ohne vorinstallierte Software über das Internet Remotesupport leisten können. Mit Genehmigung des Benutzers oder einer anderen Person, die Rescue nutzt bzw. Support von einem Techniker erhält (Endbenutzer), ermöglicht es Rescue einem Techniker, auf den Computer eines Endbenutzers zuzugreifen und ihn einzusehen und/oder die Kontrolle über den Computer zu übernehmen. Der Techniker kommuniziert über ein Chat-Fenster und kann Computerprobleme untersuchen, diagnostizieren und beheben sowie den Endbenutzer bei Problemen mit dem Betriebssystem und Softwareanwendungen unterstützen.

Mit **Rescue Lens** können Endbenutzer das Videobild ihrer Mobilgerätkamera (über die mobile Lens-App) an einen externen Techniker übertragen, damit dieser sich die fehlerhafte Hardware wie etwa einen falsch konfigurierten Router oder eine beschädigte Fahrzeugkomponente ansehen kann. Rescue Lens ist eine optionale Funktion von Rescue und kann im Rescue Admin Center aktiviert werden. Weitere Informationen zu Rescue Lens finden Sie im Benutzerhandbuch für Rescue Lens.

*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 für Rescue und Rescue Lens 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

Rescue ist eine Software-as-a-Service (SaaS)-basierte Remotesupport-Lösung, die aus drei zentralen Komponenten besteht: der Technikerkonsole, der mobilen Endbenutzer-App oder dem Desktop-Applet und dem Administrationscenter.

Die Technikerkonsole ist die Benutzeroberfläche, über die die Techniker Remotesupport-Sitzungen ausführen. Dabei können die Techniker neue Sitzungen entweder selbst starten oder auf Endbenutzeranfragen aus dem Internet reagieren, die in einer gemeinsamen Warteschlange gespeichert sind. Techniker kommunizieren mit den Endbenutzern über die mobile App von Rescue (Android oder iOS) oder das Desktop-Applet (Windows, macOS oder Linux) und leisten ihnen darüber Support. Das Applet wird auf den Remote-PC des Endbenutzers heruntergeladen und ist so konzipiert, dass es sich nach Beendigung der Sitzung selbst entfernt.

Die Rescue-Technikerkonsole interagiert mit der Rescue-App oder dem Applet über eine Peer-to-Peer-Netzwerkverbindung (P2P) (siehe Abbildung 1 in Abschnitt 3.1). Beim Start des Applets wird der P2P-Prozess initiiert und eine Verbindung zu einem Rescue-Gateway hergestellt, über das die Sitzung mit der Technikerkonsole aufgebaut wird.

Das GoTo-eigene Weiterleitungsprotokoll für den Schlüsselaustausch schützt die GoTo-Infrastruktur vor dem Abfangen oder Abhören von Daten. Insbesondere ermöglicht das Gateway die Verbindung zwischen dem Endbenutzer und dem Host, damit sichergestellt ist, dass sich der Endbenutzer unabhängig von der Netzwerkkonfiguration mit dem Host verbinden kann.

Der Host stellt eine TLS-Verbindung zum Gateway her, das den TLS-Schlüsselaustausch des Endbenutzers über eine proprietäre Anforderung zur Neuaushandlung des Schlüssels an den Host weiterleitet. So tauschen der Endbenutzer und der Host TLS-Schlüssel aus, ohne dass das Gateway den Schlüssel erfährt.

## 3.1 Schlüsselvereinbarung

Zum Beginn einer Supportsitzung, wenn die Verbindung zwischen dem Endbenutzer und dem Techniker hergestellt wird, müssen sich ihre Computer auf einen Verschlüsselungsalgorithmus aus den verfügbaren unterstützten Optionen und den dazugehörigen Schlüssel einigen, der für die gesamte Dauer der Sitzung verwendet wird.

Die Computer verwenden Zertifikate, um ihre Identitäten zu bestätigen. Da weder der Techniker noch der Endbenutzer auf ihrem Computer eine Software, die in der Lage ist, die Verbindung zu vermitteln und die installierten Sicherheitszertifikate zu überprüfen, und SSL-Zertifikat installiert haben, wenden sich beide an einen der Rescue-Server, um die erste Phase der Schlüsselvereinbarung abzuwickeln. Das Zertifikat wird sowohl von der Technikerkonsole als auch von der App oder dem Applet des Endbenutzers überprüft, um sicherzustellen, dass der Vermittler garantiert ein Rescue-Server ist.

## 3.2 Überblick über den Übergabeprozess des Rescue-Gateways

Wenn die digital signierte Rescue-App oder das Applet auf einem Rechner gestartet wird, enthält sie eine GUID (Globally Unique Identifier) für die Authentifizierung der Sitzung. Die GUID wird von der Website beim Herunterladen als Ressource in eine ausführbare Anwendung oder ein Applet (z. B. eine EXE-Datei) eingebettet. Daraufhin lädt die App oder das Applet eine Liste der verfügbaren Gateways von secure.logmeinrescue.com oder secure.logmeinrescue.eu herunter, wählt ein Gateway aus der Liste aus und verbindet sich mit diesem über TLS. Das Gateway wird dann vom Applet anhand seines SSL-Zertifikats authentifiziert. Das Gateway authentisiert das Applet in der Datenbank mit der GUID und verzeichnet, dass der Endbenutzer auf einen Techniker wartet.

Wenn ein Techniker eine Sitzung in der Rescue-Technikerkonsole aufruft, wird eine Anfrage mit der Sitzungsauthentifizierungs-GUID an das Gateway gesendet, um die Verbindungen zwischen der Technikerkonsole und der Endbenutzer-App oder dem Applet weiterzuleiten. Das Gateway ist der Vermittler, der die Verbindung authentifiziert und mit der Datenübertragung auf der Transportebene beginnt (Relay-Daten werden nicht entschlüsselt).

Nach dem Aufbau einer Relay-Verbindung versuchen die Teilnehmer, eine P2P-Verbindung herzustellen: Der Vorgang läuft folgendermaßen ab:

- Das Applet wartet nun auf eine TCP-Verbindung (Transmission Control Protocol) über einen von Windows, macOS oder Linux zugewiesenen Port.
- Wenn innerhalb von zehn Sekunden keine TCP-Verbindung aufgebaut werden kann, versucht das System, mit Hilfe des Gateways eine UDP-Verbindung (User Datagram Protocol) herzustellen.
- Sobald eine TCP- oder UDP-Verbindung besteht, wird der P2P-Kanal (mit Hilfe des Sitzungsauthentifizierungs-GUIDs) von den Teilnehmern authentifiziert und der Datenverkehr von der Relay-Verbindung auf diesen Kanal übertragen.
- Im Falle einer UDP-Verbindung wird TCP mit Hilfe von XTCP, einem GoTo-eigenen Protokoll, das auf dem TCP-Stack von BSD (Berkeley Software Distribution) basiert, über den UDP-Datagrammen emuliert.
- Alle Verbindungen werden durch das TLS-Protokoll gesichert (mittels AES-256-Bit-Verschlüsselung mit SHA256-MACs [Media Access Controls]). Beim GUID zur Sitzungsauthentifizierung handelt es sich um einen 128 Bit langen, kryptographisch zufälligen ganzzahligen Wert.

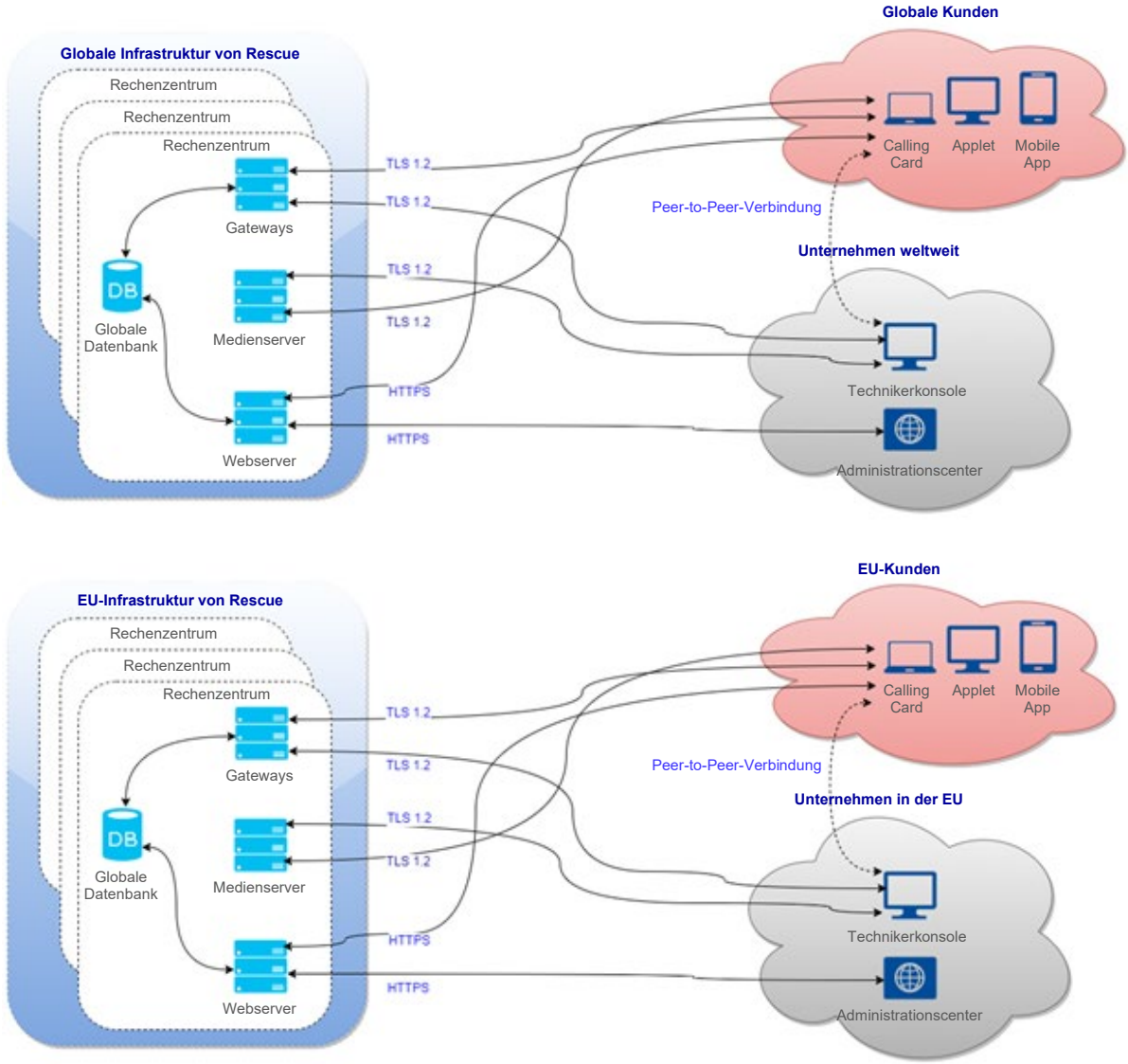


Abbildung 1: Rescue-Architektur

## 3.3 Die Medienarchitektur von Rescue

Beim Mediendienst von Rescue handelt es sich um einen eigenständigen Dienst, der auf WebRTC (Web Real-Time Communication) aufgebaut ist und das Videostreaming mit Rescue Lens möglich macht. Es verwaltet Konferenzen für Rescue-Sitzungen, bei denen die Lens-Funktion zum Einsatz kommt. Die Konferenzteilnehmer (Peers) treten den Konferenzen bei und verlassen sie, und die Endbenutzer senden Video- und Audiostreams, die dann von den anderen Teilnehmern empfangen werden. Lens überträgt die Videoinhalte in eine Richtung von der Lens-App an die Technikerkonsole.

Der Mediendienst besteht aus drei Hauptkomponenten: dem Media SDK (Media Software Development Kit), dem Sitzungsmanager und dem Streamingserver. Diese Komponenten sind für das Erstellen/Löschen und das Beitreten/Verlassen von Konferenzen zuständig. Sie kommunizieren über die bestehenden sicheren Kommunikationskanäle zwischen der Technikerkonsole und der Rescue-Website sowie der Lens-App und der Website.

### 3.3.1 Media SDK

Der Mediendienst ist auf WebRTC aufgebaut, und zwar in Form eines dünnen Wrappers über der WebRTC-Codebasis. Die Technikerkonsole und die mobile Lens-App verwenden Media SDK.

### 3.3.2 Sitzungsmanager

Der Sitzungsmanager ist eine einfache Website mit Lastenausgleich, die eine REST-API (Representational State Transfer) zur Verwaltung der Konferenzen (Erstellen/Löschen/Beitreten/Verlassen) bereitstellt. Der Sitzungsmanager nimmt nur Anforderungen von der Rescue-Website an.

### 3.3.3 Streamingserver

Der Mediendienst nutzt eine benutzerdefinierte Streamingserver-Lösung, um die Streams zwischen den Peers (der Technikerkonsole und der Lens-App) zu übertragen. Sowohl die Technikerkonsole als auch die Lens-App sind mit dem Streamingserver verbunden. Eine Lens-Sitzung besteht aus zwei Streams (einer wird gesendet, der andere empfangen): Die Lens-App streamt ihre Videoinhalte an den Streamingserver, während die Technikerkonsole die Videoinhalte vom Server streamt. Der Streamingserver fungiert wie ein Relayserver zwischen den Peers.

# 4 Technische Sicherheitskontrollen

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

## 4.1 Vertraulichkeit der Daten

Das sichere Online-System von Rescue wird durch SSL (Secure Sockets Layer) und TLS (Transport Layer Security) unterstützt und erfüllt die folgenden Ziele:

- Authentifizierung der kommunizierenden Parteien
- Sichere Aushandlung der verwendeten Schlüssel ohne Abhören
- Vertraulicher Nachrichtenaustausch
- Möglichkeit zur Erkennung von Nachrichten, die während der Übertragung modifiziert wurden

Rescue verwendet OpenSSL und zum Zeitpunkt der Veröffentlichung ist die von Rescue verwendete Version 1.1.1n.

## 4.2 Verschlüsselung

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

### 4.2.1 Verschlüsselung während der Übertragung

Der gesamte Netzwerkverkehr, der in die und aus den Rescue-Rechenzentren ein- und ausgeht, wird während der Übertragung mit TLS 1.2 und HTTPS verschlüsselt. Dies schließt auch alle Kundeninhalte ein. Darüber hinaus sind die Rescue-Sitzungen mit einer 256-Bit-AES-Verschlüsselung und einem MD5-Hash geschützt, um die Rückverfolgbarkeit von Dateiübertragungen zu verbessern.

Da alle drei Komponenten des Rescue-Kommunikationssystems der Kontrolle von GoTo unterliegen, wird immer dieselbe Verschlüsselungssammlung verwendet: AES256-SHA im CBC-Modus (Cipher Block Chaining) mit RSA-Schlüsselvereinbarung. Das bedeutet:

- Der Verschlüsselungs- bzw. Entschlüsselungsalgorithmus ist AES
- Der Verschlüsselungsschlüssel hat eine Länge von 256 Bit.
- Die Verschlüsselungsschlüssel werden wie im vorigen Abschnitt beschrieben über aus privaten und öffentlichen RSA-Schlüsseln bestehende Schlüsselpaare ausgetauscht.
- MAC basiert auf SHA-2. Ein MAC ist ein kurzer Datensatz, der zur Authentifizierung einer Nachricht dient. Der MAC-Wert schützt sowohl die Integrität einer Nachricht als auch ihre Authentizität, da die kommunizierenden Teilnehmer anhand dieses Codes erkennen können, ob die Nachricht auf irgendeine Weise modifiziert wurde.
- Der CBC-Modus sorgt dafür, dass jeder Chiffretextblock von allen vorangegangenen Klartextblöcken abhängt, und dass ähnliche Nachrichten im Netzwerk nicht als solche erkennbar sind.

Die zwischen dem Endbenutzer, der Support erhält, und dem Techniker übertragenen Daten sind durchgängig verschlüsselt und nur die betreffenden Teilnehmer haben Zugriff auf die im Nachrichtenstrom enthaltenen Daten.

### 4.2.2 Verschlüsselung ruhender Daten

Rescue-Kundeninhalte werden im Ruhezustand sowohl auf Server- als auch auf Datenbankebene mit AES256 und TDE verschlüsselt. Zu den Kundeninhalten gehören beispielsweise Chat-Protokolle und benutzerdefinierte Felder, also Felder, die vom Masterkontoinhaber oder Master-Administrator erstellt wurden.

## 4.3 Zugriffskontrollen von Rescue

Rescue-Administratoren können die Zugriffskontrollen anpassen. So können Administratoren von Rescue beispielsweise eine Richtlinie für Passwörter konfigurieren, die eine Mindeststärke und ein Höchstalter für Passwörter vorschreibt, das Zurücksetzen von Passwörtern erzwingt, eine Zwei-Faktor-Authentifizierung für die Anmeldungen bei Rescue erforderlich macht, den Zugriff von Technikern auf Rescue von IP-Adressen aus einschränkt, die für bestimmte Aufgaben vorab genehmigt wurden, oder Technikern nur Zugriff auf vordefinierte Anwendungen gewährt, indem sie eine einzige SSO-ID zur Anmeldung bei diesen Anwendungen verwenden. Falls erforderlich, können Administratoren die SSO-ID eines Technikers deaktivieren.

Zusätzliche Zugriffskontrollen umfassen:

- Auf Berechtigungen basierender differenzierter Zugriff (bestimmte Techniker können z. B. den Bildschirm nur ansehen, das Remotegerät aber nicht steuern)
- Keine Speicherung von Daten von Remotegeräten auf GoTo-Servern Nur Sitzungsprotokolle, Endbenutzer-IP-Adressen und Chat-Protokolle werden gespeichert – Chat-Textprotokolle können aus den Sitzungsdetails entfernt werden
- Verhindern der Datenübertragung durch Techniker
- Anwesenheit des Endbenutzers am Remotegerät erforderlich, um den Fernzugriff zu genehmigen
- Der Endbenutzer behält stets die Kontrolle und kann die Sitzung jederzeit beenden
- Verhindern, dass Techniker bestimmte Funktionen nutzen können, solange der Endbenutzer ihnen nicht ausdrücklich die Erlaubnis dazu erteilt hat (z. B. Fernsteuerung, Desktop-Ansicht, Dateiübertragung, Systeminformationen, Neustart und Wiederherstellung der Verbindung)

- Automatisches Aufheben der Zugriffsrechte bei Beendigung der Sitzung
- Die Möglichkeit, die automatische Abmeldung nach einer bestimmten Zeit der Inaktivität zu erzwingen
- Sperren eines Kontos nach fünf erfolglosen Anmeldeversuchen

### 4.3.1 Berechtigungsbasierte Zugriffskontrolle

Rescue-Administratoren können zudem im Administrationscenter bestimmte Berechtigungen gewähren oder verweigern. Zu diesen Berechtigungen gehören:

- Synchronisierung der Zwischenablage zulassen
- Bildschirmübertragung für Benutzer und Endbenutzer zulassen
- Skripte ausführen
- Desktopansicht starten
- Dateimanager starten
- Fernsteuerung starten
- Neustart
- Sitzungen aufzeichnen
- Zugangsdaten anfordern
- Dateien senden und empfangen
- URLs senden
- Private Sitzungen starten
- Sitzungen übertragen
- Eine einzige Aufforderung für alle Berechtigungen verwenden
- Systeminformationen anzeigen

Weitere Informationen zu Gruppenberechtigungen finden Sie im Handbuch für Rescue-Administratoren. Rescue-Lens-Techniker werden über ihre E-Mail-Adresse identifiziert und mit einem Passwort authentifiziert.

### 4.3.2 Authentifizierung

Die Authentifizierungsmaßnahmen von Rescue dienen der Sicherheit des Produkts, indem sie Maßnahmen ergreifen, die nur Technikern oder Administratoren die Anmeldung am System erlauben. Dem Techniker wird von seinem Administrator eine Login-ID (z. B. seine E-Mail-Adresse) samt Passwort zugewiesen. Techniker geben diese Zugangsdaten mindestens einmal zu Beginn ihrer Schicht in das Anmeldeformular auf der Rescue-Website ein. Administratoren können die Kontrollen so konfigurieren, dass eine Authentifizierung in kürzeren Abständen erforderlich ist (z. B. nach fünf Minuten ohne Aktivität).

Das Rescue-System authentifiziert sich zunächst über sein Premium-SSL-Zertifikat mit 2048-Bit-RSA-Schlüssel gegenüber dem Webbrowser des Technikers, um sicherzustellen, dass der Techniker seinen Benutzernamen und sein Passwort auf der richtigen Website eingibt. Der Techniker meldet sich dann mit seinen Zugangsdaten am System an. Rescue speichert keine Passwörter, sondern generiert stattdessen mit Hilfe von scrypt Hashwerte aus den Passwörtern, die dann in der Rescue-Datenbank gespeichert werden. Die Hashwerte werden mit einem 24 Zeichen langen Salt versehen, welcher von einem kryptographisch sicheren Zufallszahlengenerator (CSPRNG) für jedes individuelle Passwort erstellt wird.

Das Rescue-System authentifiziert sich auch dem Endbenutzer gegenüber, für den Support geleistet wird. Die vom Endbenutzer heruntergeladene und ausgeführte App bzw. das Applet ist mit dem GoTo-Codesignaturzertifikat (welches auf einem 2048-Bit-RSA-Schlüssel basiert) signiert. Diese Information wird dem Endbenutzer üblicherweise in seinem Webbrowser angezeigt, bevor er die Software ausführt. Rescue authentifiziert den Endbenutzer nicht gegenüber dem Techniker.

Rescue ermöglicht es den Administratoren außerdem, eine SSO-Richtlinie für die Einmalanmeldung (Single Sign-On) umzusetzen. Dabei kommt die Security Assertion Markup Language (kurz SAML) zum Einsatz; ein XML-Framework (Extensible Markup Language) zum Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen zwei Sicherheitsdomänen (zwischen einem Identitätsanbieter und einem Dienstanbieter).

Administratoren können auch eine zweistufige Verifizierung für die Anmeldung bei Rescue verlangen. Bei der zweistufigen Verifizierung werden Rescue-Konten mit Hilfe von E-Mail, SMS oder einen beliebigen zeitbasierten Einmalpasswort-Authentifikator (TOTP) um eine zweite Schutzschicht erweitert. Die ausgewählten Mitglieder der Organisation müssen dabei eine zusätzliche Möglichkeit einrichten, ihre Identität zu bestätigen. Die Einrichtung der Authenticator-App wird in folgenden Fällen ausgelöst:

- Der ausgewählte Benutzer versucht, sich auf der sicheren Website bei seinem Rescue-Konto anzumelden.
- Der ausgewählte Benutzer versucht, sich bei der Desktop-Technikerkonsole anzumelden.
- Der ausgewählte Benutzer versucht, sein Rescue-Passwort zu ändern.

### 4.3.3 Ermächtigung

Die Autorisierung erfolgt mindestens einmal während jeder Remotesupport-Sitzung. Nachdem der Endbenutzer, für den Support geleistet werden soll, das Applet heruntergeladen und ausgeführt hat, nimmt ein Techniker Kontakt mit ihm auf. Der Techniker kann über das Applet mit dem Endbenutzer chatten, aber alle anderen Maßnahmen wie etwa das Senden einer Datei oder die Anzeige des Remotedesktops müssen vom Endbenutzer ausdrücklich genehmigt werden. Ein „Single Prompt“ kann auch für langwierige Remotesupport-Arbeiten eingesetzt werden, bei denen der Benutzer möglicherweise nicht während der gesamten Dauer der Sitzung anwesend ist. Wenn diese Option für eine Technikergruppe aktiviert ist, können die Mitglieder dieser Gruppe vom jeweiligen Benutzer eine „globale“ Berechtigung anfordern. Wird diese gewährt, so können sie beispielsweise die Systeminformationen anzeigen oder die Fernsteuerung starten, ohne dass eine weitere Genehmigung durch den Benutzer erforderlich ist. Administratoren können auch IP-Adressbeschränkungen festlegen, so dass Techniker, denen eine bestimmte Aufgabe zugewiesen wurde, nur von vorher genehmigten IP-Adressen auf Rescue zugreifen und diese Aufgabe ausführen können. Der Administrator einer Technikergruppe kann außerdem im Administrationscenter bestimmte Funktionen deaktivieren.

Zu den Berechtigungen, die ein Administrator gewähren oder verweigern kann, gehören:

- Fernsteuerung starten
- Neustart
- Desktop-Ansicht starten
- Aufzeichnen von Sitzungen
- Dateien senden und empfangen
- Private Sitzungen starten
- Dateimanager starten
- Anmeldeinformationen anfordern
- URLs senden
- Synchronisierung der Zwischenablage zulassen
- Systeminformationen anzeigen
- Skripte ausführen

- Verwenden einer einzigen Aufforderung für alle Berechtigungen
- Sitzungen übertragen
- Bildschirmübertragung für Benutzer und Endbenutzer zulassen

### 4.4 Überwachungsmechanismen

Die folgenden Auditkontrollen sind für Rescue-Benutzer und Endbenutzer verfügbar:

- Die Option zur zwingenden Sitzungsaufzeichnung mit der Möglichkeit, die Protokolldateien in einem sicheren freigegebenen Netzwerk zu speichern
- Protokollierung von Technikersitzungen und Remotesitzungsaktivitäten auf dem Host-Computer, um die Sicherheit zu gewährleisten und die Qualitätskontrolle aufrechtzuerhalten (erfolgreiche Anmeldungen, erfolglose Anmeldungen, Start der Fernsteuerung, Ende der Fernsteuerung, Neustart initiiert, Abmeldung)
- Authentifizierung von Personen bzw. Einheiten
- Authentifizierung von Technikern über ihre eindeutige E-Mail-Adresse oder über eine SSO-ID
- Möglichkeit, den Technikern die Anmeldung nur von bestimmten IP-Adressen aus zu gestatten
- Der im Admin Center verfügbare Audit-Bericht enthält Änderungen an Kontoeinstellungen und Angaben zu jeder Aktion, die Administratoren in einem bestimmten Zeitraum für das ausgewählte Element des Organisationsbaums ausgeführt haben.

## 5 Aktualisierungen des Sicherheitsprogramms

Mindestens einmal jährlich überprüft und aktualisiert GoTo sein Sicherheitsprogramm und beauftragt unabhängige Dritte mit der Bewertung seiner maßgeblichen Sicherheitskontrollen, um sicherzustellen, dass es sich an die aktuelle Bedrohungslage anpasst und mit den relevanten Rahmenwerken, Branchenstandards, Kundenverpflichtungen und ggf. Änderungen von Gesetzen und Vorschriften in Bezug auf die Sicherheit der GoTo-Daten konform ist.

## 6 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo 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.

Die Rescue-Datenbank wird alle fünf Minuten mit einem anderen Rechenzentrum synchronisiert. Außerdem wird jede Nacht ein differentielles Backup und jedes Wochenende ein vollständiges Backup durchgeführt. Die Backup-Datenbank wird mit derselben Verschlüsselung wie das Original gespeichert. Backups werden einen Monat lang vor Ort aufbewahrt und dann zu einem Cloud-Dienst verschoben, nicht mehr aktiv verarbeitet und gemäß unseren internen Richtlinien zur Aufbewahrung von Unterlagen aufbewahrt. Für den Fall eines vollständigen Ausfalls des Rechenzentrums, in dem die primäre Datenbank gehostet wird, ist die Rescue-Architektur so konzipiert, dass sie schnell wiederhergestellt werden kann.

# 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-passive Rechenzentren oder
b) Rechenzentren von Cloud-Hosting-Anbietern

Bei der Erstellung eines Kontos können Rescue-Kunden wählen, ob sie die Dateninfrastruktur von GoTo in der Europäischen Union oder weltweit nutzen möchten, um ihre Kundeninhalte zu speichern. Die Hosting- bzw. Speicherorte sind nachfolgend angegeben:[2]

- **Europäische Union:** Deutschland und Irland
- **Global:** USA, Deutschland, Australien und Vereinigtes 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,

[2] Die Hosting-Standorte können variieren (d. h. abhängig von der Wahl des Datenspeicherorts verschieden sein). Lesen Sie die entsprechende Offenlegung der Unterauftragsverarbeiter (Sub-Processor Disclosure) für Rescue, die Sie im Abschnitt „Product Resources“ (Produktressourcen) im GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center) finden.

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.
- Internationale Organisation für Normung – **ISO/IEC 27001:2013** ISMS-Zertifizierung (Managementsystem für Informationssicherheit).
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Typ II** Zertifizierungsbericht
- **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.

Rescue-Chatprotokolle werden in der Rescue-Datenbank gespeichert. Das Chatprotokoll wird von der Technikerkonsole in Echtzeit an die Rescue-Server übermittelt und enthält die Ereignisse sowie die Chatnachrichten einer bestimmten Supportsitzung. In den Protokolldateien werden folgende Aktionen der Techniker angezeigt: Start- und Endzeit einer Fernsteuerungssitzung, Fälle, in denen Techniker Dateien mit Endbenutzern gemeinsam nutzen, sowie Metadaten im Zusammenhang mit der Dateifreigabe (z. B. der Name und der MD5-Hash-Thumbprint einer übertragenen Datei). Die Datenbank mit den Chatprotokollen lässt sich über das Administrationscenter abfragen.

Bei aktiven Konten wird der Inhalt der Protokolle zwei Jahre lang nach Beendigung einer Remotesupport-Sitzung online zur Verfügung gestellt und danach zwei Jahre lang archiviert.

Um die Integration mit CRM-Systemen zu erleichtern, kann Rescue Sitzungsdaten an eine URL senden und Administratoren können den Chat-Text aus diesen Daten ausschließen. Der Chat-Text ist standardmäßig enthalten, aber Kunden können diese Einstellung im Administrationscenter ändern. Die aufgezeichneten Chatnachrichten zwischen Techniker und Endbenutzern können zudem auch automatisch aus den in einem Rescue-Datenzentrum gespeicherten

Sitzungsdaten weggelassen werden. Rescue ermöglicht es Technikern, während einer Desktopansicht oder einer Fernsteuerungssitzung aufgetretene Ereignisse in einer Videodatei aufzuzeichnen. Die Aufnahmen werden in einem vom Techniker gewählten Verzeichnis gespeichert.

# 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 von GoTo

Verfahren zur logischen Zugriffskontrolle sollen das Risiko eines unbefugten Anwendungszugriffs und des Datenverlusts in Unternehmens- und Produktionsumgebungen verringern. GoTo-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 nutzt eine logisch auf Datenbankebene getrennte Multi-Tenant-Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Die Parteien müssen sich authentifizieren, um Zugriff auf ein Konto zu erhalten. Weiterhin hat GoTo Kontrollen implementiert, um zu verhindern, dass Benutzer oder Endbenutzer die Daten anderer Benutzer oder Endbenutzer sehen können.

# 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, um das Risiko einer unbefugten Änderung zu verhindern oder zu verringern
- WAF (Web Application Firewall) und DDoS-Präventionsdienst auf Anwendungsebene, durch die der GoTo-Datenverkehr über einen Proxy geleitet wird, um bösartigen Serververkehr zu blockieren
- Eine lokale Anwendungs-Firewall, die als zusätzlicher Schutz vor den OWASP Top Ten 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 (SOC) ist für die Erkennung von und die Reaktion auf Sicherheitsereignisse zuständig. Das SOC 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 die Prozesse, Richtlinien und Standardbetriebsverfahren von GoTo für kritische Kommunikation abgestimmt. Er wurde entwickelt, um relevante mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten des Unternehmens (einschließlich Rescue) 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.logmeinrescue.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 innerhalb von 140 Tagen nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden automatisch gelöscht.

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, Benutzer und Endbenutzer 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

### 20.2.1 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.

### 20.2.2 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.

### 20.2.3 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.

## 20.3 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, Benutzer und Endbenutzer 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.

## 20.4 Abkommen zur Datenübertragung

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

### 20.4.1 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.

### 20.4.2 Zertifizierungen zu 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.

## 20.5 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.

## 20.6 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.

## 20.7 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.

## 20.8 Einschränkungen bei der Verarbeitung sensibler Daten

Die folgenden Arten von sensiblen Daten dürfen nicht in Rescue 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.

### 20.9 Compliance in regulierten Umgebungen

Es liegt in der Verantwortung der Kunden, angemessene Richtlinien, Verfahren und andere Schutzmaßnahmen in Bezug auf die Verwendung von Rescue zur Unterstützung von Geräten 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 auf der Grundlage der 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. Entsprechend werden ergänzende Sicherheitsmaßnahmen mit geeigneten Kontrollen und Systemanforderungen mit den betreffenden Anbietern vereinbart. Der GoTo-DVN für Lieferanten enthält Beschränkungen bzgl. des „Verkaufs“ von Daten gemäß der Definition des CCPA.

## 22 Kontaktaufnahme mit GoTo

Kunden können GoTo unter https://support.goto.com für allgemeine Anfragen 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.