Technische und organisatorische Maßnahmen

GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage

Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage dargelegt. GoTo unterhält 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) oder Datagram Transport Layer Security (DTLS).
  - *Im Ruhezustand* Transparent Data Encryption (TDE) und Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte, die im Ruhezustand verschlüsselt sind.
- **Rechenzentren:** GoTo nutzt Cloud-Hosting-Anbieter, die Maßnahmen ergreifen, um hohe logische und physische Sicherheit, Verfügbarkeit und Skalierbarkeit zu gewährleisten.
- **Compliance-Audits:** GoTo Meeting, GoTo Webinar und GoTo Training sind nach SOC 2 Typ II, 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 Speicherebene.
- **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 Meeting, GoTo Webinar, GoTo Training und GoTo Stage 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 für GoTo Meeting, GoTo Webinar und GoTo Training zwischen neunzig und einhundert (90–100) Tage nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht.

Version 4.0 | April 2024

Inhalt

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

1 Produkteinführung

Bei GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage (zusammen der „Dienst“) handelt es sich um Online-Kommunikationsdienste, die es Einzelpersonen und Unternehmen ermöglichen, über verschiedene Funktionen zu interagieren, die je nach Dienstangebot die Desktop-Bildschirmübertragung, Videokonferenzen, Chats und integrierte Audiofunktionen umfassen. GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage nutzen eine gemeinsame Infrastruktur und werden über ein CDN für Webbrowser oder installierbare Anwendungen bereitgestellt.

- GoTo Meeting, GoTo Webinar und GoTo Training ermöglichen es Organisatoren, Online-Sitzungen zu planen, einzuberufen und zu moderieren, einschließlich Audio-, Webcam-, Bildschirmübertragung und mehr mit den GoTo-Web-, Desktop- und mobilen Anwendungen.
- GoTo Training stellt spezielle Funktionen für webbasierte Schulungen bereit, wie z. B. Online-Zugang zu Tests und Schulungsunterlagen und ein gehostetes Kursverzeichnis.
- GoTo Webinar bietet spezielle Unterstützung, um über das Internet Events und Präsentationen für ein größeres lokales oder globales Publikum durchzuführen.
- GoTo Stage ist eine Erweiterung von GoTo Webinar. GoTo-Webinar-Organisatoren können darüber anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo-Stage-Homepage vorgestellt. Organisatoren können die Veröffentlichung ihrer Aufzeichnung jederzeit über GoTo Webinar rückgängig machen, wodurch das Video von ihrer Kanalseite und aus der GoTo-Stage-Umgebung gelöscht wird.

1.1 Konferenzverwaltung und Registrierung

Organisatoren können Sitzungen direkt im Dienst planen. Sie können verschiedene Einstellungen für anstehende Sitzungen vornehmen und deren Inhalt und Teilnehmer vorbereiten.

1.2 Audiofunktion

Integrierte Audiokonferenzen für GoTo Meeting, GoTo Webinar und GoTo Training stehen sowohl über Voice over Internet Protocol (VoIP) als auch über das öffentliche Telefonnetz (PSTN) zur Verfügung.

1.3 Video

Alle Produkte bieten hochwertige Webcam-Videos, die sich an die Bandbreite und Latenz des Benutzers anpassen.

1.4 Hochladen von Inhalten (nur Webinar und Schulungen)

Organisatoren können Dateien und Medien zur Verwendung während der Sitzungen entweder vor einer Sitzung oder nach Beginn der Sitzung hochladen.

1.5 Sitzungsaufzeichnung

Organisatoren können in ihrem Sitzungsverlauf Teilnahmestatistiken und andere Sitzungs-statistiken einsehen.

1.6 Aufzeichnung und Transkripte

Sitzungen können lokal und in der Cloud aufgezeichnet werden. Kontoadministratoren und Sitzungsorganisatoren können Cloud-Aufzeichnungen zusätzlich zu oder anstelle von lokalen Aufzeichnungen aktivieren. Lokale Aufzeichnungen werden auf dem System des Organisators gespeichert und unterliegen nicht den Aufbewahrungsbeschränkungen von GoTo, wie in Abschnitt 18 (Löschung und Rückgabe von Inhalten) unten beschrieben.

Cloud-Aufzeichnungen sind automatisch direkt im Sitzungsverlauf des Organisators verfügbar. Transkripte werden automatisch erstellt, wenn diese Funktion vom Administrator aktiviert wurde. Transkripte zu Sitzungsaufzeichnungen werden entweder mit dem KI-gestützten Spracherkennungstool von GoTo oder mit der Google Cloud Speech-to-Text-Technologie erstellt.

Für **GoTo Meeting** kann ein Kontoadministrator Aufzeichnungen aktivieren und entscheiden, ob diese lokal oder in der Cloud gespeichert werden. Wenn Cloud-Aufzeichnungen aktiviert sind, kann der Organisator eines Meetings festlegen, dass dieses aufgezeichnet und in der Cloud gespeichert werden soll. Für Cloud-Aufzeichnungen werden automatisch Transkripte erstellt.

Für **GoTo Webinar** können Organisatoren wählen, ob alle Cloud-Aufzeichnungen automatisch transkribiert werden sollen. Nur ein Organisator kann eine Aufzeichnung starten. Wenn seine Einstellung für die automatische Transkription aktiviert ist, wird ein Transkript erstellt.

Für **GoTo Training** können Kontoadministratoren steuern, ob Organisatoren Aufzeichnungen in der Cloud speichern können. Kontoadministratoren können nicht verhindern, dass Organisatoren Sitzungen lokal aufzeichnen. Schulungen können nicht transkribiert werden.

1.7 Business Messaging (nur Meeting)

Mit Business Messaging, einer Erweiterung von GoTo Meeting, können GoTo-Meeting-Benutzer den Anwesenheitsstatus anderer Benutzer in ihrem Konto einsehen, Sofortnachrichten austauschen und Dateien freigeben. Der Kontoadministrator legt den Umfang der Sichtbarkeit und Auffindbarkeit der verschiedenen Benutzer fest.

Benutzer von Business Messaging sehen den Anwesenheitsstatus anderer Benutzer im selben Konto, sobald sie diese in ihre Kontaktliste aufgenommen haben. Nachrichten können mit allen Mitgliedern eines Teams sowie mit externen Benutzern ausgetauscht werden, wenn diese explizit über eine E-Mail-Einladung aufgenommen wurden. Externe Benutzer sind Benutzer von Business Messaging, die nicht zum internen Team eines Kunden gehören (z. B. Kunden, Interessenten oder Partner). Nachrichten können direkt (zwischen zwei Teilnehmern), in einer privaten Gruppe oder in einer öffentlichen Gruppe ausgetauscht werden.

Benutzer können auch andere Inhalte innerhalb von Business Messaging teilen, indem sie Dateien hoch- und herunterladen. Die freigegebenen Dateien stehen allen Benutzern mit Zugriff auf die Nachrichten in einer bestimmten Unterhaltung oder Gruppe zum Download zur Verfügung.

1.8 Webcast (nur Webinar)

GoTo-Webinar-Webcasts nutzen Broadcast-Gateways, Streaming-Engines von Drittanbietern und Content Delivery Networks, die darauf ausgelegt sind, Teilnehmern, die sich über einen Webbrowser anmelden, zuverlässig Bildschirm-, Ton- und Videoübertragung zu ermöglichen. Die Gateways empfangen Mediendaten von den Medienservern und transkodieren sie in Standard-Codecs. Die Streaming-Engine unterstützt HTTP Live Streaming (HLS) mit mehreren Bitraten, um eine adaptive Übertragung für Benutzer mit suboptimalen Netzwerkverbindungen zu ermöglichen.

1.9 GoTo Stage (nur Webinar)

Auf GoTo Stage veröffentlichte Videos können auf der GoTo-Stage-Startseite und in den Suchmaschinenergebnissen gefunden werden, es sei denn, der Organisator schränkt die Auffindbarkeit über die administrativen Einstellungen auf seiner Kanalseite ein. Nicht auffindbare Aufzeichnungen können von jedem Benutzer, der bei GoTo Stage registriert ist, über eine direkte URL zum Kanal oder zur individuellen „Jetzt ansehen"-Seite des Videos aufgerufen werden. Besucher registrieren sich für GoTo Stage mit ihrem Namen und ihrer E-Mail-Adresse oder können sich über ausgewählte Konten in sozialen Medien wie LinkedIn, Facebook und Gmail anmelden. Die URLs, über die Besucher auf die Videos zugreifen können, sind nur für eine begrenzte Zeit aktiv, um die unerwünschte Freigabe einzuschränken.

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 GoTo Meeting, GoTo Webinar und GoTo Training anwendet.

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 DSGVO, CCPA/CPRA, LGPD sowie mit unserem eigenen Datenverarbeitungsnachtrag (DVN) und den geltenden Richtlinien und Bekanntgaben 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. Sicherheitsfunktionen, die im Dienst konfiguriert werden können, helfen Administratoren, Bedrohungen und Risiken für Kundeninhalte zu minimieren.

3 Produktarchitektur

GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage sind Software-as-a-Service(SaaS)-Lösungen, die für hohe Leistung, Zuverlässigkeit, Skalierbarkeit und Sicherheit entwickelt wurden. Diese Dienste werden durch leistungsstarke Server und Netzwerkgeräte unterstützt, die über angemessene Sicherheitskontrollen und eine redundante Infrastruktur verfügen, um einen „Single Point of Failure" auszuschließen. Geclusterte Server und Backup-Systeme sollen die Anwendungsprozesse im Falle einer hohen Auslastung oder eines Systemausfalls unterstützen.

Anwendungs-/Serversitzungen werden zum Lastausgleich über geografisch verteilte Cluster verteilt, um die Leistung und angemessene Latenzzeiten zu gewährleisten.

Die Dienstinfrastruktur und Daten werden von Cloud-Hosting-Anbietern gehostet.

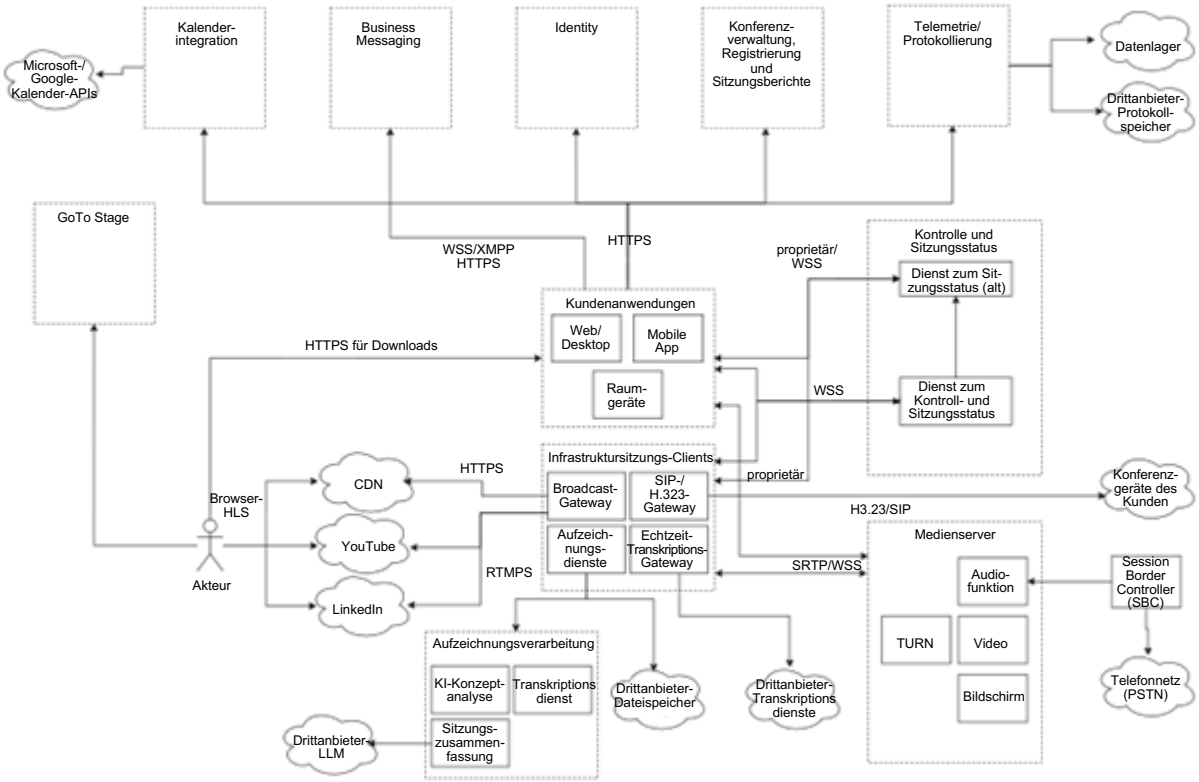

Abbildung 1: Central-Architektur

Kundenanwendungen (Web-, Desktop- und mobile Anwendungen oder „Clients“ von GoTo; ein Gerät namens GoTo Room (nur Meeting)): Die Kundenanwendungen bieten die oben in Abschnitt 1 (Produkteinführung) beschriebene Funktionsweise der Dienste.

Identitätsdienste: Verwaltet Benutzerkonten und ermöglicht die sichere und standardisierte Kontoautorisierung und Anmeldung.

Dienste für Konferenzverwaltung, Registrierung und Sitzungsberichte: Die Konferenzverwaltung liefert Informationen zu geplanten Sitzungen und ermöglicht die Planung neuer Sitzungen und die Anpassung bestehender Sitzungen. Registrierungsdienste ermöglichen die Registrierung für Sitzungen, bei denen dies erforderlich ist. Sitzungsberichte liefern Informationen zu vergangenen Sitzungen, einschließlich Aufzeichnungen, Transkriptionen, Teilnahme und mehr.

Business Messaging: Verwaltung von Kanälen sowie Versand, Empfang und Speicherung von Nachrichten und Anhängen; wird nur für Nachrichten außerhalb von Sitzungen verwendet.

Kalenderintegration: Ermöglicht es Benutzern, ihre Microsoft Outlook- oder Google-Kalender zu synchronisieren, um Benachrichtigungen zu GoTo-Sitzungen zu erhalten.

Telemetrie/Protokollierung: Versand von Telemetriesonden oder Protokollaussagen, um Nutzungsstatistiken zu erfassen und Probleme zu diagnostizieren.

Dienste zum Kontroll- und Sitzungsstatus: Bieten Funktionen, die von Client-Anwendungen verwendet werden, um nicht medienbezogene Änderungen des Sitzungsstatus zu initiieren und zu empfangen.

Medienserver: Verantwortlich für den Empfang, die Modifizierung und die Verbreitung von Audio-, Video- und Bildschirmübertragungen.

Telefonnetz (PSTN): Das öffentliche Telefonnetz ermöglicht es Benutzern, sich über physische oder IP-Telefone in Sitzungen einzuwählen.

Session Border Controller: Verbindet das Voice over Internet Protocol (VoIP) von GoTo mit kommerziellen Telefonieanbietern.

Aufzeichnungsdienste: Ermöglichen die Aufzeichnung von Audio- und Video-, Bildschirmübertragungen sowie Business Messaging-Inhalten in Sitzungen.

Broadcast-Gateway: Wird für GoTo-Webinar-Webcasts verwendet und unterstützt Layout, Transkodierung und Paketierung der Medienstreams in HLS-Streams, die über CDN an browserbasierte Clients verteilt oder an RTMP-fähige Streaming-Plattformen wie YouTube oder LinkedIn weitergeleitet werden.

H.323-/SIP-Gateway: Ermöglicht die Verbindung zum Sitzungsaudio über SIP- oder H.323-Konferenzgeräte.

Echtzeit-Transkriptions(RTT)-Gateway: Bietet eine Live-Transkription der Sprachinhalte der Sitzungsteilnehmer.

GoTo-Stage-Dienste: Verwaltung der GoTo-Webinar-Videoinhalte durch Organisatoren; bieten den Besuchern visuelle Inhalte.

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.

4.1.1 Verschlüsselung während der Übertragung

GoTo Meeting implementiert Sicherheitsmaßnahmen für Daten während der Übertragung, die zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten konzipiert sind. Sicherheitskontrollen für die Kommunikation werden für Bildschirm- und Videofreigabe, VoIP, Webcam-Video, Tastatur-/Maussteuerung, textbasierte Chat-Informationen und andere Sitzungsdaten implementiert.

Zum Schutz der TCP-Kommunikation zwischen Endpunkten verwendet GoTo TLS-Standardprotokolle der Internet Engineering Task Force (IETF).

HTTPS und WSS werden zum Schutz von Nicht-Mediendaten verwendet, während Mediendaten innerhalb von Sitzungen durch SRTP, WSS oder DTLS geschützt werden.

Intern verwendet GoTo auch die gegenseitige zertifikatsbasierte Authentifizierung (mTLS) auf Servern, die Mediendaten verarbeiten.

4.1.1.1 Audio- und Videosicherheit

Zum Schutz der Vertraulichkeit und Integrität von VoIP-Verbindungen zwischen den Endpunkten und Servern wird ein SRTP-basiertes Protokoll verwendet, das Standardverschlüsselungsmechanismen einsetzt, die mindestens AES128 nutzen.

4.1.1.2 Sicherheit für Websites, APIs und interne Webdienste

Alle Verbindungen zu den Websites, APIs und internen Webdiensten des Dienstes werden durch TLS geschützt. Dazu gehören das Hochladen von Inhalten, Sitzungsberichte, Aufzeichnungen, Transkripte und mehr.

4.1.1.3 Business Messaging

Anwesenheitsaktualisierungen, Nachrichten und Dateien werden über einen durch TLS geschützten Kanal an Chat-Dienste und weiter an die Benutzer übertragen. Dateiinhalte werden über kryptografisch signierte URLs zur Verfügung gestellt, die zum jeweiligen Inhalt führen.

4.1.1.4 Webcast-Sicherheit (nur Webinar)

Webcast-Streaming-Gateways leiten Datenverkehr innerhalb des sicheren internen Netzwerks von GoTo über SRTP an die Streaming-Engine weiter. CDNs rufen Daten aus der Streaming-Engine sicher über HTTPS ab. Die Clients rufen auch die Daten von CDNs über HTTPS sicher ab.

4.1.2 Verschlüsselung im Ruhezustand

4.1.2.1 Profildaten

Der Inhalt wird in einer relationalen Datenbank mit AES 256-Bit-Verschlüsselung gespeichert.

4.1.2.2 Konferenzverwaltung, Registrierung und Sitzungsberichte

Der Inhalt wird in einer relationalen Datenbank mit AES 256-Bit-Verschlüsselung gespeichert.

4.1.2.3 Hochladen von Inhalten

Hochgeladene Inhalte und zugehörige Metadaten werden in AWS S3, Amazon Aurora und Amazon Dynamo DB gespeichert, jeweils mit AES 256-Bit-Verschlüsselung. Außerdem werden die Metadaten in Apache Cassandra ohne Verschlüsselung im Ruhezustand gespeichert.

4.1.2.4 Aufzeichnungen und Transkripte

Cloud-Aufzeichnungen werden in AWS S3 gespeichert. Dateien werden im Ruhezustand durch serverseitige Verschlüsselung mit AES256 verschlüsselt.

Audiodateien für die Transkription werden mit AES256 verschlüsselt und sofort nach Abschluss der Speech-to-Text-Verarbeitung gelöscht.

4.1.2.5 Sicherheit von Business Messaging

Nachrichten werden in einer AWS Aurora-Datenbank und freigegebene Dateien in AWS S3 gespeichert, jeweils mit AES 256-Bit-Verschlüsselung im Ruhezustand.

4.1.2.6 GoTo Stage

Diese hochgeladenen Inhalte und die zugehörigen Metadaten werden in AWS S3 mit AES 256-Bit-Verschlüsselung gespeichert. Die Metadaten werden in Apache Cassandra und der Suchindex in Elasticsearch gespeichert, die beide im Ruhezustand nicht verschlüsselt sind.

4.2 Kompatibilität mit Firewalls und Proxyservern

Der Dienst verfügt über eine integrierte Proxy-Erkennungs- und Verbindungsverwaltungslogik, die bei der automatisierten Softwareinstallation hilft, keine komplexe (Neu-)Konfiguration des Netzwerks erfordert und die Benutzerproduktivität maximiert. Firewalls und Proxyserver, die bereits Teil Ihres Benutzernetzwerks sind, müssen nicht speziell konfiguriert werden, damit Sie den Dienst nutzen können.

Weitere Einzelheiten sowie die genauen Domänen, IPs und Ports, die verwendet werden, finden Sie auf den jeweiligen Supportseiten für Meeting, Webinar und Training.

4.3 Sicherheitsfunktionen für installierbare Clients

Die installierbaren Clients sind mit geeigneten Sicherheitsfunktionen ausgestattet und verwenden starke kryptografische Maßnahmen, einschließlich signierter Endpunkt-Software und „Client-only"-Verbindungen.

4.3.1 Signierte Endpunkt-Software

Die ausführbaren Dateien des Dienstes sind zum Schutz der Integrität und Authentizität digital signiert. Die Client-Anwendungssoftware von GoTo unterliegt während der Entwicklung und Bereitstellung Verfahren zur Qualitätskontrolle und Konfigurationsverwaltung sowie einem SDL-Modell (Security Development Lifecycle).

4.3.2 „Client-only"-Verbindungen

Um das Risiko zu verringern, dass sie von Remotesystemen mit Malware und Viren angegriffen werden, sind die installierbaren Clients nicht für den Empfang eingehender Verbindungen konfiguriert. Dadurch sind Sitzungsteilnehmer vor einer Infektion durch einen kompromittierten Host eines Teilnehmers geschützt.

4.3.3 Implementierung des Verschlüsselungssubsystems

Die Verschlüsselungsfunktionen und Sicherheitsprotokolle in den installierbaren Clients verwenden die kryptografischen Open-Source-Bibliotheken BoringSSL oder OpenSSL. Es gibt keine einsehbaren externen APIs, über die andere Software auf die im Client gebündelten kryptografischen Bibliotheken zugreifen könnte.

Die Webanwendung verwendet die kryptografischen Bibliotheken des Browsers. Es gibt keine vom Endbenutzer konfigurierbaren Verschlüsselungseinstellungen, sodass Benutzer die Sicherheit nicht durch eine unbeabsichtigte oder bewusste Fehlkonfiguration beeinträchtigen können.

4.4 Benutzerauthentifizierung

Damit eine rollenbasierte Autorisierung und angemessene Zugriffskontrollen möglich sind, muss jeder Benutzer identifiziert und authentifiziert werden können. Um sicherzustellen, dass Organisatoren und Teilnehmer über die richtigen Berechtigungen verfügen, sind in den Dienst Funktionen zur Authentifizierung von Konten und Sitzungen integriert.

4.4.1 Kontoanmeldung

Die Websites des Dienstes bieten die folgenden Anmeldemethoden:

- Direkte Anmeldung mit Benutzernamen und Passwort;
- Anmeldung über einen Social-Media- oder einen anderen Kontoanbieter wie LastPass, Google, Facebook, LinkedIn, Microsoft oder Apple (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in) und
- SAML-basiertes Single Sign-On.

Für die direkte Anmeldung gelten für alle Passwörter Mindestanforderungen an Zeichen und Komplexität. Es gibt Mechanismen zum Schutz vor Brute-Force-Angriffen und ungewöhnlichen Anmeldeaktivitäten.

GoTo speichert keine Kontopasswörter als Klartext. Stattdessen werden Passwörter mithilfe einer kryptografischen Salted-Hash-Funktion gespeichert, die gegen Wörterbuch-

und Brute-Force-Angriffe resistent ist. Passwörter werden über gesicherte Verbindungen (TLS) übertragen.

4.4.2 Authentifizierung der Sitzungsteilnehmer

Um Sitzungen für ein genau definiertes Zielpublikum zu ermöglichen, hat jede Sitzung eine eindeutige und zufällige ID. Organisatoren können außerdem festlegen, dass Teilnehmer ein Passwort benötigen, um an einer Sitzung teilzunehmen.

Um an einer Sitzung teilzunehmen, müssen Teilnehmer die eindeutige ID angeben. Dazu können sie entweder auf eine URL mit der ID klicken oder den Wert manuell in ein vom Dienst angezeigtes Formular eingeben. Bei der telefonischen Einwahl müssen die Teilnehmer die ID über die Telefontastatur eingeben. Wenn die ID gültig ist, erhält der Teilnehmer ein Rollen-Token, das bei seinem Beitritt an die Kommunikationsserver übermittelt wird.

4.4.3 Rollenbasierte Zugriffskontrolle

Anwendungsdefinierte Rollen können Dienstbenutzern zugewiesen werden und unterstützen Kunden bei der Durchsetzung von unternehmenseigenen Zugriffsrichtlinien in Bezug auf die Nutzung von Diensten und Funktionen. Benutzer können auf der Grundlage der ihnen zugewiesenen Rolle auf Kontrollen und Berechtigungen zugreifen:

Organisatoren (oder Schulungsleiter bei GoTo Training) sind berechtigt, Meetings, Webinare und/oder Schulungen zu planen. Der Organisator bereitet Sitzungen vor, lädt Teilnehmer ein, initiiert und beendet die Sitzungen und bestimmt, wer die Moderation übernimmt.

Teilnehmer sind Benutzer, die zu Sitzungen eingeladen werden. Teilnehmer können den geteilten Bildschirm des Moderators sehen, mit anderen Teilnehmern chatten und die Teilnehmerliste einsehen.

Moderatoren sind Teilnehmer, die ihren Bildschirm mit anderen Teilnehmern teilen können. Moderatoren können auch die Tastatur- und Maussteuerung für andere Teilnehmer freigeben.

Administratoren sind Personen, die zur Verwaltung von Mehrbenutzerkonten berechtigt sind. Administratoren können Kontofunktionen konfigurieren, Organisatoren Rechte erteilen und auf eine Vielzahl von Berichterstattungsfunktionen zugreifen.

Interne GoTo-Administratoren sind GoTo-Mitarbeiter, die berechtigt sind, GoTo-Meeting-, GoTo-Webinar- und GoTo-Training-Dienste und -Konten im Namen unserer Kunden zu verwalten.

4.5 Zugriffskontrolle für Aufzeichnungen

Durch eindeutige Direktlinks können Organisatoren die Aufzeichnungen nach der Sitzung mit Teilnehmern teilen, die die Aufzeichnung dann direkt im Webbrowser abspielen können.

Bei GoTo Webinar laufen die Freigabe-URLs nicht ab, solange die Aufzeichnung verfügbar ist. Um den Zugriff auf eine Aufzeichnung zu deaktivieren, können Organisatoren die Aufzeichnung jederzeit löschen.

Bei GoTo Meeting können Aufzeichnungen über URLs freigegeben werden, die ein zufälliges Token mit begrenzter Gültigkeit verwenden. Die Freigabe kann auf bestimmte Teile des Inhalts beschränkt werden und entweder für jeden mit der URL oder nur für Benutzer mit konfigurierbaren E-Mail-Adressen verfügbar sein. Diese Einschränkungen können auch nach der Freigabe der URL angepasst werden.

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.

7 Rechenzentren

Die GoTo-Infrastruktur setzt auf Rechenzentren von Cloud-Hosting-Anbietern, um die Zuverlässigkeit des Diensts zu erhöhen und das Risiko von Ausfallzeiten aufgrund eines Single Point of Failure zu verringern.

Einzelheiten zum Anbieter und Standort eines Rechenzentrums finden Sie im Dokument zur Offenlegung der Unterauftragsverarbeiter (Sub-Processor Disclosure) des Dienstes im GoTo Trust & Privacy Center.

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

7.1 Physische Sicherheit im Rechenzentrum

Cloud-Hosting-Anbieter bieten physische Sicherheits- und Umgebungskontrollen für Systeme und Server, die Kundeninhalte enthalten. 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

Cloud-Hosting-Anbieter beschränken den physischen Zugang zu den Produktionsrechenzentren auf autorisierte Personen. Um Zugang zu Serverräumen zu erhalten, muss ein Antrag über das entsprechende Ticketsystem gestellt werden, der vom zuständigen Manager genehmigt werden muss. Dieser wird dann geprüft und ggf. genehmigt. Der gesamte physische Zugang zu Rechenzentren und Serverräumen wird minimiert, protokolliert, und die Protokolle werden von den Anbietern 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, 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. Mehr zu unseren APEC-Zertifizierungen finden 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, Monitoring 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 und Betriebssysteme 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 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 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 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
- Cloud-Netzwerk-Firewalls, die eingehende und ausgehende Verbindungen filtern, darunter auch interne Verbindungen zwischen GoTo-Systemen und
- Interne Netzwerksegmentierung

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 Central und Pro) 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 automatisch innerhalb von neunzig (90) Tagen nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden zur Lösung gekennzeichnet und innerhalb von einhundert (100) Tagen gelöscht. Auf schriftliche Anfrage kann GoTo die Löschung von Inhalten schriftlich bestätigen/bescheinigen.

Die oben genannten Fristen gelten für alle Dienste. Zusätzliche dienstspezifische Löschfristen sind unten aufgeführt:

GoTo Meeting

Während der Laufzeit des Abonnements: Der Sitzungsverlauf und die Cloud-Aufzeichnungen von GoTo Meeting werden während der aktiven Abonnementlaufzeit des Kunden automatisch auf einer rollierenden Basis von einem (1) Jahr gelöscht, sowohl bei kostenpflichtigen als auch bei kostenlosen Konten.

Nach der Laufzeit des Abonnements: Nach Beendigung eines kostenpflichtigen GoTo-Meeting-Abonnements werden die Konten des Kunden, die eine kostenlose Lizenz enthalten, wieder in ein kostenloses Konto umgewandelt. Die Inhalte bleiben erhalten. Für Konten, die keine kostenlose Lizenz enthalten oder ausdrücklich gekündigt oder beendet werden, werden Kundeninhalte automatisch innerhalb von neunzig (90) Tagen nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden zur Lösung gekennzeichnet und innerhalb von einhundert (100) Tagen gelöscht. Darüber hinaus werden kostenlose GoTo-Meeting-Konten nach zwei (2) Jahren Inaktivität des Benutzers (z. B. keine Anmeldungen) automatisch gelöscht.

Entfernung eines Benutzers aus einem kostenpflichtigen Konto: Wenn ein Benutzer aus einem aktiven kostenpflichtigen Konto gelöscht oder anderweitig entfernt wird,

werden geplante Sitzungen automatisch nach neunzig (90) Tagen zur Löschung gekennzeichnet und innerhalb von einhundert (100) Tagen nach der Entfernung des Benutzers erfolgreich gelöscht.

GoTo Stage: GoTo-Stage-Benutzer mit einem aktiven GoTo-Webinar-Abonnement können veröffentlichte Webinare jederzeit eigenständig über die GoTo-Webinar-Dienstumgebung und/oder durch Einreichen einer Support-Anfrage an GoTo zurücknehmen/entfernen.

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 anderer Personen, die GoTo-Dienste nutzen („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 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 Data Privacy Framework

Das EU-U.S. und das Swiss-U.S. Data Privacy Framework (DPF) sowie die britische Erweiterung zum EU-U.S. DPF sind freiwillige Rahmenwerke, die jeweils Mechanismen für Unternehmen zur Übermittlung personenbezogener Daten aus der EU, der Schweiz und dem Vereinigten Königreich in die USA in Übereinstimmung mit den Datenschutzbestimmungen in diesen Ländern vorsehen. GoTo hält sich bei der Erfassung, Nutzung und Aufbewahrung personenbezogener Daten aus der EU, der Schweiz und dem Vereinigten Königreich an diese Rahmenwerke. Um mehr über die DPFs zu erfahren und die Zertifizierung von GoTo einzusehen, besuchen Sie die DPF-Website.

20.4.3 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.

20.4.4 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.

20.5 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.

20.6 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.

20.7 Einschränkungen bei der Verarbeitung sensibler Daten

Die folgenden Arten von sensiblen Daten dürfen nicht zu GoTo 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.

20.8 Compliance in regulierten Umgebungen

Es liegt in der Verantwortung der Kunden, angemessene Richtlinien, Verfahren und andere Schutzmaßnahmen in Bezug auf die Verwendung von GoTo Resolve 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. 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 Datenschutz oder -sicherheit besuchen Sie bitte unser IRM-Portal oder senden Sie eine E-Mail an privacy@goto.com.