Technische und organisatorische Maßnahmen
Miradore

Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für Miradore 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* Azure-Verschlüsselung auf dem Host, CMK (Customer Managed Key – vom Kunden verwalteter Schlüssel) RSA 4096 und Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte. Die Datenbanken werden mit AES256 verschlüsselt.
- **Rechenzentren:** Das Rechenzentrum in Deutschland sorgt für Redundanz und Stabilität.
- **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:** Miradore ist nach PCI DSS, ISO 27001 und 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:** Kundenbasierte Datenbankschemata unterstützen die Datentrennung und Sicherheitsberechtigungen werden angewendet, um Datenbankobjekte zu trennen und zu schützen.
- **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 Miradore 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 neunzig (90) Tage nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht, wenn der Kunde sein Konto kündigt oder auflöst.

Inhalt

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

1 Produkteinführung

Miradore ist die cloudbasierte Mobile Device Management(MDM)-Lösung von GoTo für Android- und iOS-Mobilgeräte sowie macOS- und Windows-Workstations (der „Dienst“). Mit den Funktionen von Miradore können Administratoren die Gerätesicherheit, Einstellungen und Einschränkungen, Datensicherheit, App-Einstellungen, Inhalte, Automatisierung und Berichterstattung verwalten – alles über ein einziges Portal.

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 Miradore anwendet.

2.1 Schutzmaßnahmen

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

I. Standardmäßige Integration von Sicherheit und Datenschutz in Produkte und Prozesse, einschließlich 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 des Dienstes 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

Miradore ist eine Geräteverwaltungslösung für mobile Geräte und Workstations mit einer mehrstufigen Architektur. Miradore nutzt Cloud-Ressourcen von Microsoft Azure, um eine skalierbare, hochverfügbare Lösung ohne Single Point of Failure bereitzustellen. Die Sicherheitsmaßnahmen bieten einen tiefgreifenden Schutz auf allen Ebenen, von der physischen Ebene bis zur Anwendungsebene.

Es gibt mehrere Miradore-Schnittstellen, darunter die primäre Benutzeroberfläche, die Webservice-API, Konnektoren zu Drittsystemen und verwaltete Geräte.

3.1 Die primäre Benutzeroberfläche

Die primäre Benutzeroberfläche von Miradore ist die Verwaltungskonsole. Sie ist browserbasiert und setzt das sichere HTTPS-Protokoll zwischen dem Dienst und dem verwalteten Gerät ein.

3.2 Webservice-API

Die Miradore-API ist ein Representational State Transfer(REST)-basierter Webservice, der Miradore die Integration mit externen Informationssystemen ermöglicht. Die API wird über HTTPS mit der GET-Methode aufgerufen, um Daten direkt aus der Datenbank von Miradore im XML- oder JSON-Format zu exportieren. Alle API-Anfragen werden mit Authentifizierungsschlüsseln authentifiziert, die in der Verwaltungskonsole jeder Miradore-Instanz verwaltet werden. Weitere Informationen finden Sie im API-Support-Artikel.

3.3 Miradore für verwaltete Geräte

Die Geräte kommunizieren mit dem Server des Dienstes entweder über den Miradore-Client, bei dem es sich um ein benutzerdefiniertes Programm handelt, das auf einer Workstation oder einem Gerät installiert ist, oder über das in die Plattform integrierte Framework zur Verwaltung mobiler Geräte, das von Apple (iOS), Google (Android) oder Microsoft (Windows) bereitgestellt wird.

Ein verwaltetes Gerät in Miradore muss zunächst einen Registrierungsprozess durchlaufen. Die Geräteregistrierung wird entweder von der Person, die das Gerät benutzt („Endbenutzer“) oder vom Administrator einer Miradore-Instanz („Benutzer“) initiiert und mit einmaligen Zugangsdaten, die für jede Registrierung erstellt werden, authentifiziert. Wenn der Benutzer den Registrierungsprozess initiiert, sind die Zugangsdaten in der Einladungsnachricht zur Registrierung enthalten, die dem Endbenutzer per E-Mail oder SMS zugesandt wird. Wenn der Endbenutzer den Registrierungsprozess initiiert (Self-Service), verwendet er einen unternehmensspezifischen Passcode, um das Gerät über das Registrierungsportal zu registrieren (https://login.online.miradore.com/enroll). Um auf die Self-Service-Registrierung zugreifen zu können, muss eine Person in der jeweiligen Miradore-Instanz als Endbenutzer des Geräts aufgeführt sein. Nach erfolgreicher Registrierung wird der Endbenutzer, der die Registrierung abgeschlossen hat, der zugewiesene Endbenutzer dieses Geräts in Miradore.

Daten werden zwischen einem verwalteten Gerät und dem Dienst übertragen, wenn der Miradore-Client den Dienst nach Befehlen abfragt, der Dienst die Befehle zurückgibt und der Miradore-Client die Ergebnisse der Aufgaben zurücksendet. Beispiele für Befehle sind die Durchsetzung von Konfigurationsrichtlinieneinstellungen, Software-Installationen und Ergebnisse geplanter Aufgaben (z. B. Hardware- und Software-Bestände). Wenn eine sofortige Synchronisierung erforderlich ist, kann der Dienst anfordern, dass ein verwaltetes Gerät den Dienst sofort über einen entsprechenden Push-Benachrichtigungsdienst abruft.

Die Push-Benachrichtigungsdienste der Anbieter (Apple Push-Benachrichtigungsdienste, Firebase Cloud Messaging, Azure SignalR und Windows-Push-Benachrichtigungsdienste) sind über HTTPS und anbieterspezifische Protokolle mit den verwalteten Geräten und dem Dienst verbunden. Außerdem ist der Miradore-Client für macOS, iOS, Windows und Android-Plattformen kryptografisch signiert, um Verbindungen mit dem Dienst zu authentifizieren.

Unabhängig vom Betriebssystem des Geräts können Endbenutzer immer sehen, ob ihr Gerät mit Miradore verwaltet wird. In der Regel gibt es eine Client-Anwendung oder ein MDM-Profil, das für die Endbenutzer sichtbar ist.

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 unsere 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

Miradore verwendet HTTPS TLS 1.2-Protokolle zur Sicherung des Netzwerkverkehrs. Die gesamte Kommunikation zwischen dem Endbenutzer und der Benutzeroberfläche wird verschlüsselt.

4.1.2 Verschlüsselung ruhender Daten

Alle Server sind verschlüsselt. Ruhende Serverdaten der virtuellen Maschinen werden mit Azure-Verschlüsselung auf dem Host und CMK Rivest-Shamir-Adleman (RSA) 4096 gespeichert. Die Datenbanken werden mit einer vom Dienst verwalteten transparenten Datenverschlüsselung mit AES 256-bit verschlüsselt.

4.2 Benutzerauthentifizierung

Benutzer werden mit einem Benutzernamen und einem Passwort, das mindestens acht Zeichen lang sein muss, authentifiziert. Benutzerpasswörter werden mit Salts versehen und in der Datenbank als Secure Hash Algorithm(SHA)-512-Hashes gespeichert und kryptografisch signiert. Alle Benutzerverbindungen zum Dienst und alle Aktionen innerhalb des Dienstes werden protokolliert und im Aktionsprotokoll angezeigt, um einen Audit-Trail bereitzustellen. Wenn ein Benutzer sein Passwort vergisst, kann er es über ein Microsoft-Schul- oder Geschäftskonto oder über den in den Dienst integrierten und über den Anmeldebildschirm verfügbaren Workflow zur Wiederherstellung des Passworts zurücksetzen. Im Passwort-Wiederherstellungs-Workflow wird dem Benutzer eine E-Mail mit einem Hyperlink zum Zurücksetzen des Benutzerpassworts gesendet. Die Zwei-Faktor-Authentifizierung ist im Dienst verfügbar und kann von einem Benutzer für seine eigene Anmeldung oder durch einen Administrator als Anforderung für ein gesamtes Miradore-Konto konfiguriert werden.

5 Aktualisierungen des Sicherheitsprogramms

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

6 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo 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 sind die verbleibenden

Standorte so konzipiert, dass sie die Anwendungslast ausgleichen. Die Notfallwiederherstellung für diese Systeme wird regelmäßig getestet.

Kundeninhalte werden im selben Rechenzentrum in 24-Stunden- und 7-Tage-Intervallen gesichert. Zusätzlich wird alle 7 Tage ein entsprechendes Backup in einem geografisch entfernten Rechenzentrum erstellt und 4 Wochen lang aufbewahrt.

Die Datenbank- und Front-End-Webserver, die den Service hosten, werden täglich gesichert. Für die Datenbanken sind für bis zu 14 Tage Zeitpunkt-Backups und wöchentliche langfristige Datenbank-Backups für ein Jahr verfügbar. Bei Webservern ist eine sofortige Wiederherstellung für zwei Tage möglich.

Firewalls werden bei Netzwerkverbindungen zwischen dem Internet und dem Netzwerk des Rechenzentrums eingesetzt, um ausschließlich Verbindungen über HTTPS (Port 443) zu bestimmten Webservern zuzulassen. Es wird ein Load Balancer verwendet, um die Anfragen gleichmäßig auf die Webserver zu verteilen.

Die Server-Hardware, die Betriebssysteme und der Miradore-Dienst werden kontinuierlich überwacht und die für die Server verantwortlichen Personen werden bei Abweichungen in der Funktionsfähigkeit des Dienstes benachrichtigt.

7 Rechenzentren

Die GoTo-Infrastruktur setzt auf die folgenden Komponenten, um die Zuverlässigkeit des Diensts zu erhöhen und das Risiko von Ausfallzeiten zu verringern. Der Dienst wird in Microsoft Azure in Deutschland gehostet. Dabei werden die Umgebungsbedingungen überwacht und Daten rund um die Uhr durch die nachfolgend erläuterten physischen Sicherheitsvorkehrungen geschützt[1].

7.1 Physische Sicherheit im Rechenzentrum

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungskontrollen für Serverräume zu gewährleisten, in denen Produktionsserver untergebracht sind. Zu diesen Kontrollen gehören die folgenden:

- Videoüberwachung und -aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- 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

[1] Hinweis: Die Miradore Premium+ Daten werden in Deutschland, Irland und den Niederlanden gehostet. Weitere Informationen finden Sie im Dokument „Miradore Sub-Processor Disclosure“, das Sie im Abschnitt „Product Resources“ (Produktressourcen) im GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center) finden.

Protokolle werden vom GoTo-Management mindestens vierteljährlich überprüft. Darüber hinaus wird die Autorisierung für den physischen Zugang zum Rechenzentrum bei einem Rollenwechsel (wenn ein solcher Zugang nicht mehr erforderlich ist) oder bei Kündigung oder Austritt eines zuvor autorisierten Mitarbeiters umgehend aufgehoben. Für hochsensible Bereiche, zu denen auch Rechenzentren gehören, ist eine Multifaktor-Authentifizierung (z. B. Biometrie, Ausweis und Tastatur) erforderlich, um Zugang zu erhalten.

8 Einhaltung von Standards

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

- **TRUSTe Enterprise Privacy- und Data Governance Practices-Zertifizierung** für betriebliche Datenschutz- und Datensicherheitskontrollen, die mit den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzrahmenwerken übereinstimmen. Um mehr zu erfahren, besuchen Sie unseren Blogbeitrag.
- **TRUSTe APEC CBPR- und PRP-Zertifizierungen** für die Übertragung von Kundeninhalten zwischen APEC-Mitgliedsländern, erworben und unabhängig validiert von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für Datenschutz-Compliance. Um mehr über unsere APEC-Zertifizierungen zu erfahren, klicken Sie hier.
- Internationale Organisation für Normung – **ISO/IEC 27001:2013** ISMS-Zertifizierung (Managementsystem für Informationssicherheit).
- **Payment Card Industry Data Security Standard (PCI DSS)**-Compliance für die E-Commerce- und Zahlungsumgebungen von GoTo.

9 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von Miradore folgt den Grundsätzen der sicheren Systemtechnik, um den Produktcode während des Entwicklungszyklus zu schützen. Der Kern des Programms ist ein Ansatz, bei dem Sicherheit an erster Stelle steht: einfaches Design, umfassender Schutz, Zugriff mit geringsten Rechten, Eingabevalidierung, Passwortverwaltung, Fehlerbehandlung und -protokollierung, manuelle Codeprüfungen und Bedrohungsmodellierung. Miradore setzt außerdem Qualitätssicherungsmethoden wie Peer-Codeprüfungen, Sicherheitstests, Penetrationstests und Sicherheitsaudits ein, um die Qualität und Sicherheit des entwickelten Informationssystems zu gewährleisten.

10 Protokollierung, Überwachung und Warnmeldungen

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

11 Endpoint Detection and Response (EDR)

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

12 Bedrohungsmanagement

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

13 Sicherheits- und Schwachstellenscans sowie Patch-Management

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

14 Logische Zugriffskontrolle

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

15 Datentrennung

GoTo hat Kontrollen implementiert, um zu verhindern, dass Benutzer die Daten anderer Benutzer sehen können. Miradore nutzt kundenbasierte Datenbankschemata und wendet Sicherheitsberechtigungen für die Trennung und den Schutz von Datenbankobjekten auf der Grundlage des GoTo-Kontos eines Benutzers oder Kunden an. Die Parteien müssen sich authentifizieren, um Zugriff auf ein Konto zu erhalten.

16 Perimeterabwehr und Erkennung von Eindringversuchen

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

- Systeme zur Erkennung von Eindringversuchen, die Systeme, Dienste, Netzwerke und Anwendungen auf unbefugten Zugriff überwachen
- Überwachung kritischer System- und Konfigurationsdateien, um das Risiko einer unbefugten Änderung zu verhindern oder zu verringern
- DDoS-Präventionsdienst auf Anwendungsebene, durch den der GoTo-Datenverkehr über einen Proxy geleitet wird, um bösartigen Serververkehr zu blockieren
- Host-basierte Firewalls auf GoTo-Webservern, die eingehende und ausgehende Verbindungen filtern, darunter auch interne Verbindungen zwischen GoTo-Systemen

17 Sicherheitsmaßnamen und Incident-Management

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

Der GoTo-Notfallplan ist auf 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 GoTo Resolve) 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 Rückgabe und Löschung von Kundeninhalten

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 neunzig (90) Tage nach Kündigung oder Stornierung und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden automatisch gelöscht. Wenn das Abonnement des Kunden abläuft, wird das Konto in ein kostenloses Konto umgewandelt und kann nur dann gelöscht werden, wenn das Konto über keine aktiven Benutzer und verwalteten Geräte verfügt. 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 verfügt über ein robustes globales Datenschutzprogramm, das die geltenden Gesetze berücksichtigt und rechtmäßige internationale Datenübertragungen unter den folgenden Rahmenbedingungen unterstützt:

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 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.

20.9 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 personenbezogene Daten oder Datenschutz besuchen Sie bitte unser IRM-Portal oder senden Sie eine E-Mail an privacy@goto.com.