TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR RESCUE UND RESCUE LENS

OPERATIVE SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

Dieses Dokument beschreibt die Sicherheits- und Datenschutzkontrollen für Rescue und Rescue Lens. Rescue ist eine webbasierte Lösung für Fernsupport und Kundenservice, mit der Helpdesk-Mitarbeiter ohne vorinstallierte Software über das Internet Fernunterstützung leisten können. Mit der Berechtigung des Endbenutzers kann Rescue es einem Helpdesk-Mitarbeiter ermöglichen, auf einen Benutzercomputer zuzugreifen, ihn anzuzeigen und/oder die Kontrolle zu übernehmen. Durch Kommunikation über ein Chat-Fenster kann der Techniker Computerprobleme untersuchen, diagnostizieren und beheben und einen Benutzer anderweitig bei Problemen mit dem Betriebssystem und der Softwareanwendung unterstützen.

Rescue Lens ermöglicht Kunden das Streamen ihrer Mobilgerät-Kameras zu einem Fern-Techniker, sodass dieser problematische Hardware wie einen falsch konfigurierten Router oder eine beschädigte Fahrzeugkomponente anzeigen kann. Rescue Lens ist ein optionales Feature in Rescue und kann im Rescue Admin Center aktiviert werden. Weitere Details zu Rescue Lens finden Sie im Rescue Lens-Benutzerhandbuch.

2 Produktarchitektur

Rescue ist eine SaaS-basierte Fernsupport-Lösung (Software-as-a-Service) aus drei Hauptkomponenten: einer Technikerkonsole, einem Kunden-Applet und einem Administration Center.

Die Technikerkonsole ist die Schnittstelle, die von Support-Technikern zum Durchführen von Fernsupport-Sitzungen verwendet wird. Techniker können neue Sitzungen initiieren oder auf Online-Kundenanfragen reagieren, die in einer freigegebenen Warteschleife warten. Mit der Berechtigung des Kunden wird das Rescue-Applet – die Schnittstelle, über die Techniker mit Kunden kommunizieren und Fernsupport durchführen – auf den Fern-PC des Benutzers heruntergeladen. Das Applet entfernt sich selbst vom Remote-PC, wenn die Sitzung abgeschlossen ist. Administratoren verwenden das webbasierte Administration Center, um Berechtigungen für andere Administratoren, Techniker und Technikergruppen zu erstellen und zuzuweisen.

Die Rescue-Technikerkonsole interagiert mit dem Rescue-Applet unter Verwendung einer Peer-to-Peer-Netzwerkverbindung (siehe Abbildung 1). Der Peer-to-Peer-Prozess wird beim Starten des Applet initiiert. Er stellt eine Verbindung zu einem Rescue-Gateway her, wo die Sitzung mit der Technikerkonsole verhandelt wird.

Das proprietäre Weiterleitungsprotokoll für den Schlüsselaustausch von GoTo ist so konzipiert, dass es gegen Abfangen oder Abhören unserer Infrastruktur abgesichert ist. Insbesondere die Verbindung zwischen dem Client und dem Host wird durch das Gateway

unterstützt, um sicherzustellen, dass der Client unabhängig vom Netzwerkaufbau eine Verbindung zum Host herstellen kann.

Da der Host bereits eine TLS-Verbindung zum Gateway aufgebaut hat, leitet das Gateway den TLS-Schlüsselaustausch des Clients über eine proprietäre Anforderung zur Neuaushandlung des Schlüssels an den Host weiter. Dies führt dazu, dass der Client und der Host TLS-Schlüssel austauschen, ohne dass das Gateway über den Schlüssel informiert ist.

Details zur Funktionsweise der Verbindung und den genutzten Sicherheitsmaßnahmen finden Sie im Abschnitt „Überblick über Rescue Gateway-Übergabeprozess“ im Whitepaper zur Rescue-Architektur und -Sicherheit.

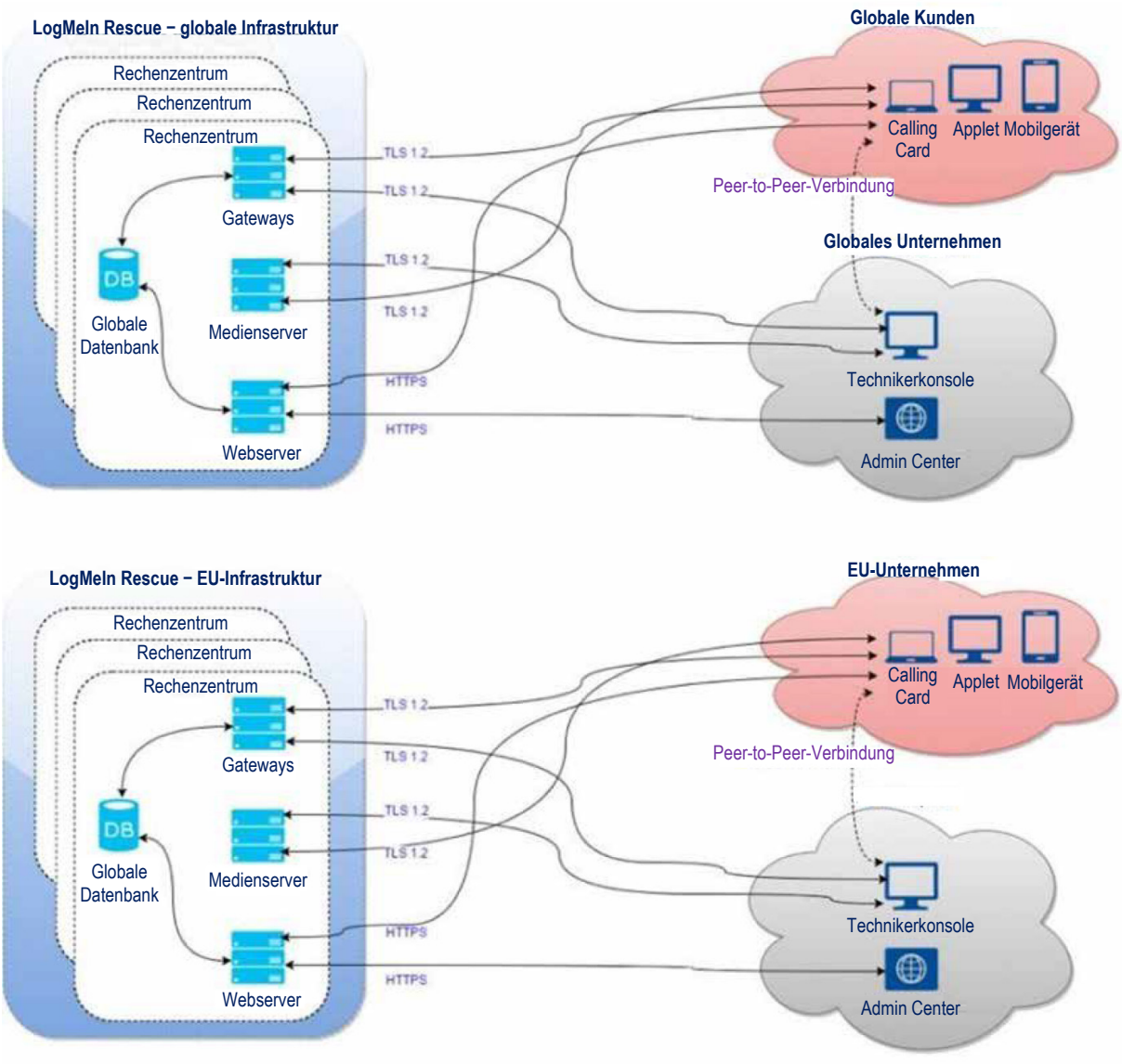

Abbildung 1 – Rescue – globale Infrastruktur

3 Rescue – technische Kontrollen

GoTo nutzt technische Sicherheitskontrollen nach Branchenstandard gemäß der Art und Weise und des Umfangs der Services (gemäß Definition des Begriffs in den Nutzungsbedingungen). Diese Kontrollen wurden zum Schutz der Service-Infrastruktur und der darin enthaltenen Daten entwickelt. Sie finden die Nutzungsbedingungen unter https://www.goto.com/company/legal/terms-and-conditions.

3.1 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen sowie Datenverlust in Unternehmens- und Produktionsumgebungen zu verhindern oder zu minimieren. Mitarbeiter erhalten bei Bedarf minimalen Zugriff (oder „Least Privilege"-Zugriff) auf angegebene GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte. Zudem sind Benutzerrechte basierend auf der funktionalen Rolle und Umgebung voneinander getrennt.

Rescue erlaubt Single Sign-On (SSO) unter Verwendung von Security Assertion Markup Language (SAML). Kunden können die Zugriffskontrolle anpassen. Beispielsweise können Rescue-Administratoren Passwortrichtlinien konfigurieren, Passwortzurücksetzungen erzwingen, Zwei-Faktor-Autorisierung für Rescue-Anmeldungen durchsetzen, Techniker-zugriff deaktivieren oder Technikerzugriff auf Rescue von IP-Adressen einschränken, die für bestimmte Aufgaben vorab genehmigt wurden.

Rescue-Administratoren können auch spezifische Berechtigungen im Administration Center gewähren oder ablehnen. Diese Gruppenberechtigungen umfassen:

- Synchronisation der Zwischenablage zulassen
- Bildschirmübertragung für Kunden zulassen
- Skripts bereitstellen
- Desktop-Anzeige starten
- Datei-Manager starten
- Fernsteuerung starten
- Neustarten
- Sitzungen aufzeichnen
- Windows-Anmeldedaten anfordern
- Dateien senden und empfangen
- URLs senden
- Private Sitzungen starten
- Sitzungen übertragen
- Einzelne Aufforderung für alle Berechtigungen verwenden
- Systeminformationen anzeigen

Weitere Details zu Gruppenberechtigungen finden Sie im Rescue-Handbuch für Administratoren. Anbieter von Rescue Lens-Support werden durch ihre E-Mail-Adresse identifiziert und unter Verwendung eines starken Passworts authentifiziert.

3.2 Perimeterverteidigung und Erkennung von Eindringversuchen

Die lokale GoTo-Netzwerkarchitektur ist in öffentliche, private und iLO-Netzwerkzonen (Integrated Lights-Out) für die Verwaltung segmentiert. Die öffentliche Zone enthält Server in Richtung Internet. Der gesamte Datenverkehr, der in dieses Netzwerk gelangt, muss eine Firewall durchqueren. Nur erforderlicher Netzwerk-Datenverkehr ist zulässig. Anderer Netzwerk-Datenverkehr wird abgelehnt. Es ist kein Netzwerkzugriff von der öffentlichen Zone auf die privaten oder iLO-Netzwerkzonen für die Verwaltung zulässig.

Die private Netzwerkzone hostet administrative und überwachende Systeme auf Anwendungsebene. Die iLO-Netzwerkzone für Verwaltung dient der Administration und Überwachung von Hardware und Netzwerk. Der Zugriff auf diese Netzwerke ist auf autorisierte Mitarbeiter über Zwei-Faktor-Authentifizierung eingeschränkt.

Darüber hinaus setzt GoTo Perimeterschutz-Maßnahmen ein, darunter einen Cloud-basierten DDoS-Schutzservice (Distributed Denial of Service) eines Drittanbieters, um nicht autorisierten Netzwerk-Datenverkehr beim Zugriff auf unsere Produktinfrastruktur zu vermeiden.

3.3 Datentrennung

GoTo nutzt eine Architektur mit mehreren Mandanten, die basierend auf dem GoTo-Konto eines Benutzers oder einer Organisation logisch auf Datenbankebene getrennt ist. Nur authentifizierten Parteien wird Zugriff auf die relevanten Konten gewährt.

3.4 Physische Sicherheit

Physische Rechenzentrumssicherheit

GoTo arbeitet mit Rechenzentren zusammen, um physische Sicherheits- und Umgebungskontrollen für Serverräume mit Produktionsservern zu bieten. Zu diesen Kontrollen gehören:

- Videoüberwachung und Aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- Temperaturregelung von Heizung, Lüftung und Klimaanlage
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (USV)
- Zwischenböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen Naturkatastrophen und vom Menschen verursachten Katastrophen entsprechend der Geografie und des Standorts des jeweiligen Rechenzentrums
- Geplante Wartung und Validierung aller wichtigen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu Produktionsrechenzentren nur auf autorisierte Einzelpersonen. Für den Zugang zu einer Hosting-Einrichtung in einem Serverraum vor Ort oder eines Drittanbieters ist die Einreichung eines Antrags über das entsprechende Ticketing-System und die Genehmigung des jeweiligen Managers sowie eine Überprüfung und Genehmigung der Technikabteilung erforderlich. Die GoTo-Verwaltung überprüft die Protokolle für den physischen Zugang zu Rechenzentren und Serverräumen mindestens auf

vierteljährlicher Basis. Darüber hinaus wird der physische Zugang zu Rechenzentren nach Beendigung der Tätigkeit des zuvor autorisierten Personals aufgehoben.

3.5 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Rescue bietet nahezu umgehendes Failover für die meisten Ausfallszenarios. Die Produktionsrechenzentren nutzen redundante ultra-schnelle Netzwerkverbindungen. Es sind Pools von Web- und Gateway-Servern in geografisch entfernten Rechenzentren vorhanden. Durch Lastenausgleich wird der Netzwerk-Datenverkehr verteilt und die Verfügbarkeit dieser Server bei Server- oder Rechenzentrumsausfällen aufrecht erhalten.

Die Rescue-Datenbank wird alle fünf Minuten in ein anderes Rechenzentrum synchronisiert. Zudem wird nachts ein differenzielles Backup und am Wochenende ein vollständige Backup durchgeführt. Die Backup-Datenbank wird mit derselben Verschlüsselung wie das Original gespeichert. Backups werden lokal einen Monat aufbewahrt und dann zu einem Cloud-Service rotiert, nicht mehr aktiv verarbeitet und gemäß unseren internen Richtlinien zur Aufzeichnungsaufbewahrung gespeichert. Bei einem kompletten Ausfall des Rechenzentrums, das die primäre Datenbank hostet, wird die Rescue-Architektur innerhalb von fünf Minuten wiederhergestellt.

3.6 Malware-Schutz

Malware-Schutzsoftware mit Überwachungsprotokollen wird auf allen Rescue-Servern eingesetzt. Warnmeldungen, die auf mögliche böswillige Aktivitäten hinweisen, werden an ein entsprechendes Reaktionsteam gesendet.

3.7 Verschlüsselung

GoTo verfügt über einen kryptografischen Standard, der sich nach Empfehlungen von Branchengruppen, staatlichen Veröffentlichungen und anderen seriösen Gruppen für Standards richtet. Der kryptografische Standard wird regelmäßig überprüft und ausgewählte Technologien und Cipher werden in Einklang mit dem bewerteten Risiko und der Marktakzeptanz neuer Standards aktualisiert.

3.7.1 Verschlüsselung während der Übertragung

Der gesamte Netzwerkverkehr, der in die und aus den GoTo-Rechenzentren fließt, einschließlich des gesamten Kundeninhalts, wird während der Übertragung verschlüsselt. Daneben werden Rescue-Support-Sitzungen durch AES-Verschlüsselung (256 Bit) geschützt.

3.7.2 Verschlüsselung im Ruhezustand

Chat-Protokolle und benutzerdefinierte Felder in Rescue, also vom Kunden erstellte Felder, werden im Ruhezustand mit AES-Verschlüsselung (256 Bit) verschlüsselt.

3.8 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden monatlich auf Schwachstellen überprüft. Es werden auch regelmäßig Schwachstellenprüfungen dynamischer und statischer Anwendungen vorgenommen und Penetrationstestaktivitäten für bestimmte Umgebungen ausgeführt. Für die Ergebnisse dieser Überprüfungen und Tests werden in

Netzwerküberwachungstools Berichte erstellt und wo dies basierend auf der Wichtigkeit der identifizierten Schwachstellen erforderlich ist, werden Abhilfemaßnahmen ergriffen.

GoTo kommuniziert und verwaltet Schwachstellen durch die Bereitstellung monatlicher Berichte für Entwicklungsteams und Management.

3.9 Protokollierung und Warnmeldungen

GoTo erfasst identifizierten anomalen oder verdächtigen Datenverkehr in entsprechenden Sicherheitsprotokollen in den jeweiligen Produktionssystemen.

4 Organisatorische Kontrollen

GoTo bietet einen umfassenden Satz an organisatorischen und administrativen Kontrollen zum Schutz des Sicherheits- und Datenschutzstatus von Rescue.

4.1 Sicherheitsrichtlinien und -verfahren

GoTo pflegt umfangreiche Sicherheitsrichtlinien und -verfahren, die an Geschäftszielen, Compliance-Programmen und der allgemeinen Unternehmensführung ausgerichtet sind. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um die Einhaltung von Vorschriften stets sicherzustellen.

4.2 Einhaltung der Standards

GoTo hält geltende rechtliche, finanzielle, datenschutzrechtliche und regulatorische Anforderungen ein und erfüllt die folgenden Zertifizierungen und externen Audit-Berichte:

- TRUSTe Enterprise Privacy & Data Governance Practices Zertifizierung, um operative Datenschutz- und Data Protection-Kontrollen zu adressieren, die sich an den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzabkommen orientieren. Weitere Informationen finden Sie in unserem Blog-Beitrag.
- Service Organization Control (SOC) 2 Type 2-Bericht des American Institute of Certified Public Accountants (AICPA)
- Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) bei den E-Commerce- und Zahlungsumgebungen von GoTo
- Interne Kontrollenbewertung wie im Rahmen der Jahresrechnungsprüfung durch das Public Company Accounting Oversight Board (PCAOB)

4.3 Sicherheitsvorgänge und Incident-Management

Das Security Operations Center (SOC) von GoTo ist mit dem Security Operations-Team besetzt und für das Erkennen von und Reagieren auf Sicherheitsereignisse verantwortlich. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um mögliche Probleme zu identifizieren und hat einen Vorfallsreaktionsplan entwickelt, der die entsprechenden Reaktionen vorgibt.

Der Vorfallsreaktionsplan ist auf die wichtigen GoTo-Kommunikationsprozesse, die Incident-Management-Richtlinie für Informationssicherheit sowie standardmäßige Betriebsvorgänge ausgerichtet. Diese Richtlinien und Verfahren wurden entwickelt, um vermutete oder

identifizierte Sicherheitsereignisse in den Systemen und Services von GoTo, einschließlich Rescue, zu verwalten, zu identifizieren und zu beheben. Laut Vorfallsreaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicherheit von Informationen identifizieren und alle vermuteten oder bestätigten Ereignisse gegebenenfalls an das Management eskalieren. Mitarbeiter können Sicherheitsvorfälle gemäß des auf der Intranet-Seite von GoTo dokumentierten Prozesses per E-Mail, Telefon und/oder Ticket melden. Alle identifizierten oder vermuteten Ereignisse werden über standardisierte Ereignistickets dokumentiert, eskaliert und je nach Wichtigkeit selektiert.

4.4 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL) für einen sicheren Produktcode. Zu den Hauptelementen dieses Programms gehören manuelle Codeüberprüfungen, Bedrohungsmodellierung, statische Codeanalysen, dynamische Analysen und Systemhärtung.

4.5 Personalsicherheit

Überprüfungen der Mitarbeiter – soweit dies nach geltendem Recht zulässig und für die Position angemessen ist – werden weltweit bei neuen Mitarbeitern vor dem Datum ihrer Einstellung vorgenommen. Die Ergebnisse werden im Personalstammblatt des Mitarbeiters hinterlegt. Die Kriterien der Mitarbeiterüberprüfung variieren in Abhängigkeit der Gesetze, der Arbeitsverantwortung und dem Führungsniveau des potenziellen Mitarbeiters und unterliegen den üblichen und zulässigen Praktiken des jeweiligen Lands.

4.6 Sicherheitsbewusstsein und Schulungsprogramme

Neu eingestellte Mitarbeiter werden zur Orientierung über die Sicherheitsrichtlinien und den Verhaltenskodex und Geschäftsethik von GoTo informiert. Diese obligatorische jährliche Schulung zu Sicherheit und Datenschutz wird für die entsprechenden Mitarbeiter durch das Talentförderungsteam und mit Unterstützung des Sicherheitsteams durchgeführt.

Die Mitarbeiter und Zeitarbeiter von GoTo werden regelmäßig über die Anweisungen, Verfahren, Richtlinien und Standards zu Sicherheit und Datenschutz informiert. Dazu werden verschiedene Medien wie Einarbeitungsunterlagen für Neueingestellte, Aufklärungskampagnen, Webinare mit dem CISO, ein Sicherheits-Champion-Programm und der Aushang von Plakaten oder anderes Begleitmaterial genutzt, die mindestens halbjährlich ausgetauscht werden und Methoden zum Schutz von Daten, Geräten und Anlagen veranschaulichen.

5 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten seiner Kunden, Abonnenten der GoTo-Services und Endbenutzer sehr ernst und verpflichtet sich, entsprechende Praktiken zur Verarbeitung und Verwaltung von Daten offen und transparent preiszugeben.

5.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die sich mit dem Schutz der Daten und der Privatsphäre von Einzelpersonen in der

Europäischen Union befasst. Sie zielt primär darauf ab, ihren Bürgern und Bewohnern Kontrolle über ihre personenbezogenen Daten zu geben und die regulative Umgebung in der EU zu vereinfachen. Rescue erfüllt die anwendbaren DSGVO-Bestimmungen. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2 CCPA

GoTo sichert hiermit zu, dass es mit dem California Consumer Privacy Act (CCPA) konform ist. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3 Data Protection- und Datenschutzerklärung

GoTo freut sich, einen umfassenden, globalen Datenverarbeitungsnachtrag (DVN) in Englisch und Deutsch bereitzustellen, um die Anforderungen von DSGVO, CCPA und mehr zu erfüllen und die GoTo-Verarbeitung personenbezogener Daten zu regeln.

Der DVN schließt folgende Datenschutz-Anforderungen in Bezug auf die DSGVO ein: (a) Details zur Datenverarbeitung, Offenlegung bzgl. Auftragsverarbeiter-Partnerunternehmen etc. gemäß Artikel 28 (b) EU-Standardvertragsklauseln (auch als EU-Modellklauseln bekannt) und (c) die technischen und organisatorischen Maßnahmen von GoTo. Im Zusammenhang mit dem Inkrafttreten des CCPA haben wir zusätzlich in unserem globalen DVN Folgendes aktualisiert: (a) Definitionen im Zusammenhang mit dem CCPA (b) Zugriffs- und Löschrechte und (c) Garantien, dass GoTo keine persönlichen Daten von Benutzern verkaufen wird.

Für Besucher unserer Webseiten veröffentlicht GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Services bereitzustellen, aufrechtzuerhalten, zu verbessern und zu sichern, in seiner Datenschutzerklärung auf der öffentlichen Website. Das Unternehmen kann seine Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen an seinen Informationspraktiken und/oder Änderungen geltender Gesetze zu berücksichtigen, weist aber auf seiner Website auf jegliche Materialänderungen hin, bevor diese wirksam werden.

5.4 Abkommen zur Datenübertragung

GoTo hat ein robustes globales Data Protection-Programm, das das geltende Recht berücksichtigt und rechtmäßige internationale Datenübertragungen im Rahmen der folgenden Abkommen unterstützt:

5.4.1 Standardvertragsklauseln

Die Standardvertragsklauseln („SCC“) sind standardisierte Vertragsbestandteile, die von der Europäischen Kommission anerkannt und übernommen wurden und vorrangig dem Zweck dienen, eine EU-datenschutzkonforme Übermittlung personenbezogener Daten in Regionen außerhalb des Europäischen Wirtschaftsraums („EWR“) sicherzustellen. GoTo hat ein ausgefeiltes Datenschutzprogramm eingerichtet, das die Ausführungsbestimmungen der SCC für die Übermittlung personenbezogener Daten einhält. GoTo bietet Kunden SCC (andere Bezeichnung: EU-Modellklauseln) an. Diese leisten als Bestandteil des globalen DVN von spezifische Garantien betreffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Services im Rahmen des globalen DVN. Der

Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Neben den in dieser SPOC angegebenen Maßnahmen hat GoTo die folgenden FAQ erstellt, um seine ergänzenden Maßnahmen zur Unterstützung rechtmäßiger Datenübertragungen gemäß Kapitel 5 der DSGVO zu skizzieren und alle Analysen zu adressieren und anzuleiten, die vom Europäischen Gerichtshof zusammen mit den SCCs empfohlen werden.

5.4.2 Zertifizierungen zu APEC, CBPR und PRP

GoTo hat zudem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschafts-gemeinschaft), CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC-, CBPR- und PRP-Rahmenregelungen sind die ersten Datenregelungen, die für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt wurden. Sie wurden von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für die Einhaltung von Datenschutzbestimmungen, eingeholt und unabhängig validiert.

5.5 Rückgabe und Löschung von Kundeninhalt

Kunden können die Rückgabe oder Löschung ihres Inhalts jederzeit über standardisierte Schnittstellen anfordern. Wenn diese Schnittstellen nicht verfügbar sind oder GoTo anderweitig nicht in der Lage ist, der Anfrage gerecht zu werden, ergreift GoTo wirtschaftlich zumutbare Maßnahmen, um den Kunden im Rahmen der technischen Möglichkeiten beim Abrufen oder Löschen seines Inhalts zu unterstützen. Der Kundeninhalt wird innerhalb von dreißig (30) Tagen nach der Anfrage des Kunden gelöscht.

Rescue-Inhalt von Kunden wird automatisch innerhalb von neunzig (90) Tagen nach Ablauf oder Beendigung des finalen Abonnementzeitraums gelöscht. Bei einer schriftlichen Anfrage bestätigt GoTo eine derartige Inhaltslöschung.

5.6 Sensible Daten

Es ist das Ziel von GoTo, den gesamten Kundeninhalt zu schützen. Regulatorische und vertragliche Beschränkungen verlangen jedoch, dass die Verwendung von Rescue für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in Rescue hochgeladen oder dort generiert werden:

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, die im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) und damit verbundenen Gesetzen und Vorschriften festgelegt sind.
- Informationen über Finanzkonten und Zahlungsinstrumente, einschließlich − aber nicht beschränkt auf − Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung betrifft ausdrücklich gekennzeichnete Zahlungsformulare und Seiten, die von GoTo verwendet werden, um Zahlungen für Rescue zu erheben.

- Alle Informationen, die besonders durch geltende Gesetze und Vorschriften geschützt sind, insbesondere Informationen über die Rasse, die ethnische Zugehörigkeit, religiöse oder politische Überzeugungen, organisatorische Mitgliedschaften der Person usw.

5.7 Nachverfolgung und Analysen

GoTo verbessert kontinuierlich seine Websites und Produkte mit Hilfe von Webanalysetools von Drittanbietern, um Folgendes besser zu verstehen: Nutzung der Websites, Desktop-Tools und mobilen Anwendungen durch Besucher, Benutzerpräferenzen und Probleme. Weitere Einzelheiten finden Sie in der Datenschutzrichtlinie.

6 Drittanbieter

6.1 Nutzung von Drittanbietern

Im Rahmen der internen Bewertung und der Prozesse im Zusammenhang mit Anbietern und Dritten können Anbieterbewertungen je nach Relevanz und Anwendbarkeit von mehreren Teams vorgenommen werden. Das Sicherheitsteam bewertet Anbieter von Services, die auf Informationssicherheit basieren, und nimmt auch die Bewertung der Hosting-Einrichtungen von Drittanbietern vor. Die Teams für Recht und Beschaffung können bei Bedarf nach internen Prozessen Verträge, Leistungsbeschreibungen und Servicevereinbarungen bewerten.

Angemessene Konformitätsdokumente oder -berichte können mindestens einmal jährlich eingeholt und bewertet werden, sofern dies für angemessen erachtet wird, um sicherzustellen, dass die Kontrollumgebung ordnungsgemäß funktioniert und alle erforderlichen benutzerbezogenen Kontrollen durchgeführt werden. Zudem müssen Drittanbieter, die sensible oder vertrauliche Daten hosten oder von GoTo Zugriff darauf erhalten haben, einen schriftlichen Vertrag zu unterzeichnen, in dem die relevanten Anforderungen für den Zugriff auf die Informationen sowie deren Speicherung oder Verarbeitung (sofern zutreffend) festgelegt sind.

6.2 Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Geschäftsprozessen und Datenverarbeitung durch Drittanbieter getroffen werden, überprüft GoTo die jeweiligen Nutzungsbedingungen von Drittanbietern und nutzt entweder von GoTo genehmigte Beschaffungsvorlagen oder verhandelt die Bedingungen dieser Drittanbieter, wenn dies als notwendig erachtet wird.

7 GoTo kontaktieren

Kunden können sich bei allgemeinen Anfragen an https://support.goto.com oder bei Fragen zum Datenschutz an privacy@goto.com wenden.