

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR RESCUE LIVE GUIDE

Operative Sicherheits- und Datenschutzkontrollen

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

In diesem Dokument werden die technischen und organisatorischen Maßnahmen (TOMs) für Rescue Live Guide beschrieben.

Rescue Live Guide ist ein webbasiertes Support-Tool, mit dem Kundenservice-Mitarbeiter remote und visuell Anleitung im Browser geben, ohne dass ein Skript zur unterstützten Website hinzugefügt oder Software heruntergeladen werden muss. Mit der Berechtigung des Endbenutzers ermöglicht Rescue Live Guide einem Kundenservice-Mitarbeiter das Co-Browsing auf Websites mit dem Endbenutzer auf sichere Weise und bietet ihm Anleitungstools.

2 Produktarchitektur

GoTo Rescue Live Guide ist eine SaaS-basierte visuelle Engagement-Lösung (Software-as-a-Service), die Endbenutzer und Serviceberater in einem Cloud-basierten sicheren Browser verbindet.

Sowohl die Anwendung des Serviceberaters als auch die des Endbenutzers sind Webanwendungen, die im unterstützten Browser der Wahl der Benutzer ausgeführt werden. Die Back-Ends für diese Anwendungen werden in der AWS-Cloud (Amazon Web Services) von GoTo gehostet. Sie stellen den Peers Mittel zum gegenseitigen Verbinden in einer Co-Browsing-Sitzung bereit.

Die Sitzung wird erstellt, wenn ein Endbenutzer eine freigegebene Browsing-Sitzung initiiert. Eine PIN für die Sitzung wird generiert und dem Endbenutzer zu Beginn der Sitzung angezeigt. Der Endbenutzer kann dem Serviceberater das Beitreten zur Sitzung erlauben, indem er die PIN für die Sitzung teilt. Wenn eine Co-Browsing-Sitzung zwischen Endbenutzer und Serviceberater aufgebaut wird, wird die unterstützte Website in einem isolierten Headless Browser in der GoTo-Cloud geladen.

Das tatsächliche Web-Browsing und die gesamte Kommunikation mit der unterstützten Website findet im Cloud-Browser statt. Das Image wird an die Webanwendungen beider Benutzer gestreamt und die Benutzeraktionen werden zurückgesendet, um im Cloud-Browser durchgeführt zu werden.

Die Instanzen des Cloud-Browsers sind komplett isoliert und abgesehen von den Berichterstattungsdaten, der Aufzeichnung (wenn aktiviert) und den Sitzungsinformationen werden Daten nach jeder Co-Browsing-Sitzung gelöscht.

Im nächsten Kapitel dieses Dokuments (Technische Sicherheitskontrollen) erfahren Sie mehr über die Sicherheitsmaßnahmen der Lösung.

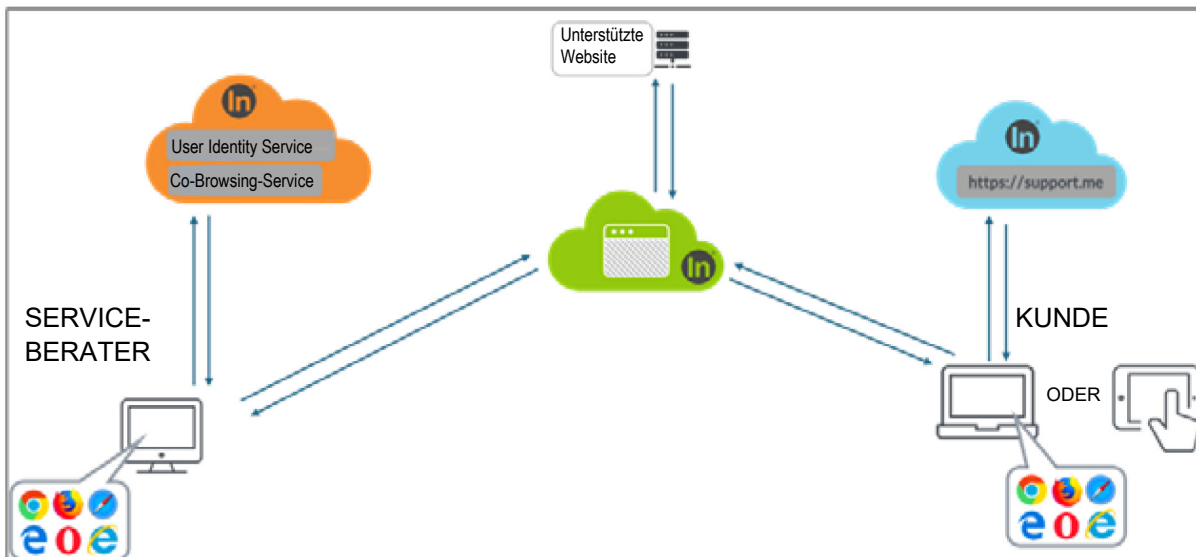


Abbildung 1 – Rescue Live Guide-Infrastruktur

3 Technische Sicherheitskontrollen

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 Zugriffskontrollen eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehende Bedrohung und einen 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.

Serviceberater in Rescue Live Guide sind an Unternehmenskonten gebunden und müssen sich mit Benutzername und starkem Passwort authentifizieren. Als optionale zusätzliche Sicherheitsmaßnahme kann der Kontoadministrator die verpflichtende Zwei-Faktor-Authentifizierung für alle Serviceberater des Kontos einrichten. Die Serviceberater-Konsole ist nur nach erfolgreicher Authentifizierung zugänglich.

Die Verfügbarkeit zusätzlicher Services (wie Berichterstattung, Aufzeichnungen, Konto-administration) für authentifizierte Serviceberater/Admins kann mit zugewiesenen Rollen kontrolliert und begrenzt werden.

3.2 Endbenutzer-Schutz

Der Datenschutz der Endbenutzer von Rescue Live Guide wurde bei der Erstellung dieses Service berücksichtigt: Die PIN für die Sitzung ist Eigentum des Endbenutzers und ein Support-Serviceberater kann einer Sitzung nur beitreten, wenn der Endbenutzer seine PIN

für die Sitzung mit ihm geteilt hat. Zudem ist die PIN für die Sitzung unternehmensspezifisch: Nur Serviceberater, die Teil des zur angegebenen unterstützten Website zugewiesenen Kontos sind, können einer auf einer bestimmten Website initiierten Sitzung beitreten.

GoTo speichert keinen Endbenutzerinhalt, der während der Support-Sitzung generiert wird. Wie bereits erwähnt, sind die Instanzen des Cloud-Browsers komplett isoliert und abgesehen von den Berichterstattungsdaten, der Aufzeichnung (wenn aktiviert) und den Sitzungsinformationen werden Daten nach jeder Co-Browsing-Sitzung gelöscht.

Die Schaltfläche *Stoppen* ist ebenfalls für den Endbenutzer während der gesamten Support-Sitzung verfügbar. Er kann die Support-Sitzung jederzeit durch Klicken auf diese Schaltfläche beenden.

3.3 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.

3.4 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.

3.5 Physische Sicherheit

Physische Rechenzentrumssicherheit

GoTo arbeitet mit Rechenzentren zusammen, um physische Sicherheits- und Umgebungs-kontrollen 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. Außerdem wird der physische Zugang zu Rechenzentren bei Kündigung von bereits autorisiertem Personal entfernt.

3.6 Daten-Backup, Notfallwiederherstellung, Verfügbarkeit

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 Architektur von GoTo wurde im Allgemeinen so konzipiert, dass die Replikation zu geografisch verteilten Standorten nahezu in Echtzeit erfolgt. Datenbanken werden mit Hilfe einer rollierende inkrementelle Backup-Strategie gesichert. Im Falle eines Notfalls oder eines Totalausfalls eines der vielen aktiven Standorte können die übrigen Standorte die Anwendungslast ausgleichen.

3.7 Malware-Schutz

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

3.8 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.

3.8.1 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. Um Schutz vor Abhörung, Modifizierung oder Replay-Angriffen zu bieten, werden Transport Layer Security-Protokolle nach IETF-Standard zum Schutz der gesamten Kommunikation zwischen Endpunkten und unseren Services verwendet. Unsere Services unterstützen mindestens folgende Verschlüsselungsprotokolle (falls zutreffend): TLS 1.2, RSA (2048 Bit), starke AES-256-Cipher mit SHA-2-Algorithmus (384 Bit).

3.8.2 Verschlüsselung im Ruhezustand

Rescue Live Guide-Konfigurationen, -Sitzungsdaten und -Aufzeichnungsdateien werden im Ruhezustand mit AES-Verschlüsselung (256 Bit) verschlüsselt.

3.9 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.

Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.10 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 Live Guide.

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) für Rescue Service
- 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. Er wurde entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services, einschließlich Rescue Live Guide, 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 Live Guide 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.

Die Datenspeicherort-Option von Rescue Live Guide ermöglicht Ihnen die Auswahl des Speicherorts der Endbenutzerdaten: entweder in der Europäischen Union (Frankfurt, Dublin) oder in den USA. GoTo garantiert, dass bei Auswahl des Datenspeicherorts in der EU nur die Rechenzentren in der EU genutzt werden und Kundendaten ausschließlich in der gewählten Region bleiben.

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 diesen TOMs 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 Wirtschaftsgemeinschaft), 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 Kundeneinhalt

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 Kundeneinhalt wird innerhalb von dreißig (30) Tagen nach der Anfrage des Kunden gelöscht.

Rescue Live Guide-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 Live Guide für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in Rescue Live Guide hochgeladen oder dort generiert werden (von Kunden oder Endbenutzern):

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, die im Health Insurance Portability and Accountability Act (HIPAA) von 1996 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 Live Guide 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. Das Team für Recht und Beschaffung kann 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.