TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN VON RESCUE LIVE GUIDE

Dokumentation zu organisatorischen Sicherheits- und Datenschutzkontrollen

Datum der Veröffentlichung: Februar 2022

1 Produkte und Dienste

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs) von Rescue Live Guide.

Rescue Live Guide ist ein webbasiertes Support-Tool, das vom globalen Kundensupport verwendet wird, um visuelle Anleitungen aus der Ferne im Browser bereitzustellen, ohne dass ein Skript zur unterstützten Website hinzugefügt oder eine Software heruntergeladen werden muss. Mit Genehmigung des Endbenutzers ermöglicht Rescue Live Guide einem Kundenbetreuer, gemeinsam mit dem Endbenutzer auf sichere Weise auf Websites zu surfen und stellt dem Techniker Tools zur Verfügung.

2 Produktarchitektur

GoTo Rescue Live Guide ist eine Software-as-a-Service (SaaS)-basierte Lösung für visuelles Co-Browsing, die den Endbenutzer und den Techniker über einen sicheren, cloudbasierten Browser miteinander verbindet.

Sowohl die Techniker- als auch die Endbenutzeranwendungen sind Webanwendungen, die in dem vom Benutzer unterstützten Browser seiner Wahl laufen. Die Backends, die diese Anwendungen bedienen, werden in der AWS-Cloud (Amazon Web Services) von GoTo gehostet, sodass die Peers die Möglichkeit haben, sich in einer Co-Browsing-Sitzung miteinander zu verbinden.

Die Sitzung wird aufgebaut, wenn ein Endbenutzer eine gemeinsame Browsersitzung initiiert. Eine Sitzungs-PIN wird generiert und dem Endbenutzer zu Beginn der Sitzung angezeigt. Der Endbenutzer kann den Techniker an der Sitzung teilnehmen lassen, indem er ihm die Sitzungs-PIN mitteilt. Sobald eine Co-Browsing-Sitzung zwischen Endbenutzer und Techniker hergestellt ist, wird die unterstützte Website in einem isolierten Headless-Browser in der GoTo-Cloud geladen.

Das eigentliche Surfen im Internet und die gesamte Kommunikation mit der unterstützten Website findet im Cloud-Browser statt. Das Bild wird an die Webanwendungen der beiden Benutzer gestreamt und die Benutzeraktionen werden zur Ausführung an den Cloud-Browser gesendet.

Die Cloud-Browser-Instanzen sind vollständig isoliert und abgesehen von den Berichtsdaten, der Aufzeichnung (falls aktiviert) und den Sitzungsinformationen werden die Daten nach Beendigung einer Co-Browsing-Sitzung gelöscht.

Weitere Informationen über die Sicherheitsmaßnahmen der Lösung finden Sie im nächsten Kapitel (Technische Sicherheitskontrollen) dieses Dokuments.

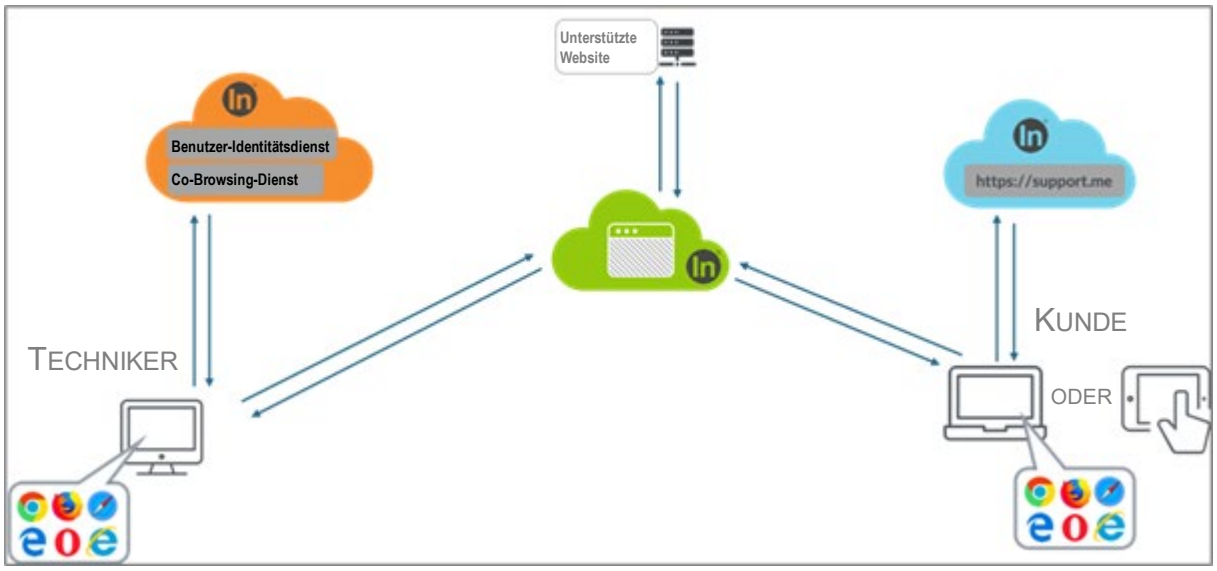

Abbildung 1: Infrastruktur von Rescue Live Guide

3 Technische Sicherheitskontrollen

GoTo setzt branchenübliche technische Sicherheitskontrollen ein, die der Art und dem Umfang der Dienste (wie in den Nutzungsbedingungen definiert) angemessen sind, um die Infrastruktur der Dienste und die darin enthaltenen Daten zu schützen. Die Nutzungsbedingungen finden Sie unter https://www.goto.com/company/legal/terms-and-conditions.

3.1. Logische Zugriffskontrolle

Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollen soll die Bedrohung des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden. Mitarbeitern wird nach Bedarf minimaler Zugriff (oder „geringste Rechte“) auf bestimmte GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte gewährt. Außerdem werden die Berechtigungen der Benutzer je nach funktionaler Rolle und Umgebung getrennt.

Techniker für Rescue Live Guide sind an Unternehmenskonten gebunden und müssen sich mit ihrem Benutzernamen und einem sicheren Passwort authentifizieren. Als optionale zusätzliche Sicherheitsmaßnahme kann der Administrator des Kontos die obligatorische Zwei-Faktor-Authentifizierung für alle Techniker unter seinem Konto einrichten. Auf die Technikerkonsole kann nur nach erfolgreicher Authentifizierung zugegriffen werden.

Die Verfügbarkeit zusätzlicher Dienste (z. B. Berichte, Aufzeichnungen, Verwaltung von Konten) für authentifizierte Techniker/Administratoren kann mit zugewiesenen Rollen kontrolliert und eingeschränkt werden.

3.2. Schutz für Endbenutzer

Bei der Entwicklung dieses Dienstes wurde die Privatsphäre der Endbenutzer von Rescue Live Guide berücksichtigt: Die Sitzungs-PIN ist Eigentum des Endbenutzers, und ein Techniker kann einer Sitzung erst dann beitreten, wenn der Endbenutzer ihm seine Sitzungs-PIN mitgeteilt hat. Darüber hinaus ist die Sitzungs-PIN unternehmensspezifisch: Einer

Sitzung, die auf einer bestimmten Website initiiert wird, können nur Techniker beitreten, die Teil des Kontos sind, das der jeweiligen unterstützten Website zugeordnet ist.

GoTo speichert die während der Support-Sitzung generierten Inhalte des Endbenutzers nicht. Wie bereits erwähnt, sind die Cloud-Browser-Instanzen vollständig isoliert und abgesehen von den Berichtsdaten, der Aufzeichnung (falls aktiviert) und den Sitzungsinformationen werden die Daten nach Abschluss einer Co-Browsing-Sitzung gelöscht.

Während der gesamten Support-Sitzung steht dem Endbenutzer auch die Schaltfläche *Stop* zur Verfügung. Der Endbenutzer kann die Support-Sitzung jederzeit beenden, indem er auf diese Schaltfläche klickt.

3.3. Perimeterabwehr und Erkennung von Eindringversuchen

Die On-Premise-Netzwerkarchitektur von GoTo ist in drei Netzwerkzonen unterteilt: öffentlich, privat und Integrated Lights-Out (iLO)-Management. Die öffentliche Zone enthält Server mit Internetzugriff, und der gesamte eingehende Datenverkehr dieses Netzwerks muss eine Firewall passieren. Nur der erforderliche Netzwerkverkehr wird zugelassen, jeglicher andere Netzwerkverkehr wird abgelehnt. Von der öffentlichen Zone aus ist kein Netzwerkzugriff auf die private oder die iLO-Management-Netzwerkzone zulässig.

In der privaten Netzwerkzone werden Administrations- und Überwachungssysteme auf Anwendungsebene gehostet, während die iLO-Management-Netzwerkzone für die Administration und Überwachung von Hardware und Netzwerk zuständig ist. Der Zugriff auf diese Netzwerke wird durch Zwei-Faktor-Authentifizierung auf autorisierte Mitarbeiter beschränkt.

Darüber hinaus setzt GoTo Maßnahmen zum Perimeterschutz ein, einschließlich eines Cloud-basierten DDoS-Präventionsdienstes (Distributed Denial of Service) eines Drittanbieters, der verhindern soll, dass nicht autorisierter Netzwerkverkehr in unsere Produktinfrastruktur gelangt.

3.4. Datentrennung

GoTo nutzt eine logisch auf Datenbankebene getrennte Multi-Tenant-Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Nur authentifizierte Parteien erhalten Zugriff auf die entsprechenden Konten.

3.5. Physische Sicherheit

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 (UPS)
- 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 überprüft und genehmigt werden muss. Das GoTo-Management überprüft mindestens vierteljährlich die Protokolle des physischen Zugangs zu den Rechenzentren und Serverräumen. Außerdem wird der physische Zugang zu den Rechenzentren widerrufen, wenn ein zuvor autorisierter Mitarbeiter entlassen wird.

3.6. Daten-Backup, Notfallwiederherstellung, Verfügbarkeit

Die Produktionsrechenzentren nutzen redundante Hochgeschwindigkeits-Netzwerkverbindungen. Es gibt Web- und Gateway-Serverpools über geografisch weit entfernte Rechenzentren hinweg. Load Balancer verteilen den Netzwerkverkehr und erhalten die Verfügbarkeit dieser Server bei Ausfällen von Servern oder Rechenzentren aufrecht.

Die Architektur von GoTo ist im Allgemeinen 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.

3.7. Schutz vor Malware

Auf allen Servern von Rescue Live Guide ist eine Malware-Schutzsoftware mit Audit-Protokollierung installiert. Alarme, die auf potenzielle bösartige Aktivitäten hinweisen, werden an das entsprechende Reaktionsteam weitergeleitet.

3.8. Verschlüsselung

GoTo nutzt einen kryptografischen Standard, der den Empfehlungen von Branchenverbänden, behördlichen Veröffentlichungen und anderen angesehenen Standardverbänden entspricht. Der kryptografische Standard wird regelmäßig überprüft, und die ausgewählten Technologien und Verschlüsselungsverfahren können je nach Risikobewertung und Marktakzeptanz neuer Standards aktualisiert werden.

3.8.1. Verschlüsselung während der Übertragung

Der gesamte Netzwerk-Datenverkehr, der in GoTo-Rechenzentren ein- und ausgeht, wird während der Übertragung verschlüsselt. Dies schließt auch alle Kundeninhalte ein. Zum Schutz vor Abhör-, Änderungs- oder Wiederholungsangriffen werden TLS-Protokolle (Transport Layer Security) nach IETF-Standard verwendet, um die gesamte Kommunikation zwischen Endpunkten und unseren Diensten zu schützen. Unsere Dienste unterstützen die folgenden oder höheren Verschlüsselungsprotokolle (falls zutreffend): TLS 1.2, 2048-Bit-RSA, sichere AES-256-Verschlüsselungs-Chiffren mit 384-Bit-SHA-2 Algorithmus.

3.8.2. Verschlüsselung ruhender Daten

Konfigurationen von Rescue Live Guide, Sitzungsdaten und Aufzeichnungsdateien werden im Ruhezustand mittels 256-Bit-AES verschlüsselt.

3.9. Schwachstellenmanagement

Interne und externe System- und Netzwerk-Schwachstellen-Scans werden einmal im Monat durchgeführt. Dynamische und statische Schwachstellenprüfungen von Anwendungen sowie Penetrationstests für bestimmte Umgebungen werden ebenfalls regelmäßig durchgeführt. Die Ergebnisse dieser Scans und Tests werden an die Netzwerküberwachungs-Tools übergeben, und je nach Schweregrad der identifizierten Schwachstellen werden gegebenenfalls Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch durch monatliche und vierteljährliche Berichte an die Entwicklungs- und Verwaltungsteams kommuniziert und verwaltet.

3.10. Protokollierung und Warnmeldungen

GoTo sammelt identifizierten anomalen oder verdächtigen Datenverkehr in den entsprechenden Sicherheitsprotokollen der jeweiligen Produktionssysteme.

4 Organisatorische Kontrollen

GoTo setzt eine umfassende Reihe von organisatorischen und administrativen Kontrollen ein, um die Sicherheit und den Datenschutz von Rescue Live Guide zu gewährleisten.

4.1. Sicherheitsrichtlinien und -verfahren

GoTo setzt eine umfassende Reihe von Sicherheitsrichtlinien und -verfahren ein, die den Geschäftszielen, Compliance-Programmen und den Interessen der allgemeinen Unternehmensführung entsprechen. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um ihre Einhaltung zu gewährleisten.

4.2. Einhaltung von Standards

GoTo erfüllt die geltenden rechtlichen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen und hält sich an die folgenden Zertifikate und externen Prüfberichte:

- 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.
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Typ 2 Zertifizierungsbericht für den Rescue-Dienst
- 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

4.3. Sicherheitsmaßnamen und Incident-Management

Das Security-Operations-Team des GoTo Security Operations Centers (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 einen Plan zur Reaktion auf Vorfälle entwickelt, der angemessene Reaktionen vorschreibt.

Der Plan zur Reaktion auf Vorfälle ist auf die kritischen Kommunikationsprozesse von GoTo, die Richtlinie für das Management von Vorfällen im Bereich der Informationssicherheit sowie die zugehörigen Standardbetriebsverfahren abgestimmt. Er wurde entwickelt, um mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten des Unternehmens zu verwalten, zu identifizieren und zu beheben, einschließlich Rescue Live Guide. Gemäß dem Plan für die Antwort auf Vorfälle gibt es technische Mitarbeiter, die potenzielle Ereignisse und Schwachstellen im Zusammenhang mit der Informationssicherheit identifiziert und vermutete oder bestätigte Ereignisse gegebenenfalls an die Verwaltung weiterleitet. Mitarbeiter können Sicherheitsvorfälle per E-Mail, Telefon und/oder Ticket melden, entsprechend dem auf der GoTo-Intranetseite dokumentierten Verfahren. Alle identifizierten oder vermuteten Ereignisse werden dokumentiert und über standardisierte Ereignistickets eskaliert und nach ihrer Kritikalität eingestuft.

4.4. Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL), um den Produktcode zu abzusichern. Die Kernelemente dieses Programms sind manuelle Codeprüfungen, Bedrohungsmodellierung, statische Codeanalyse, dynamische Analyse und Systemhärtung.

4.5. Mitarbeitersicherheit

Hintergrundüberprüfungen werden, soweit gesetzlich zulässig und für die jeweilige Position angemessen, bei neuen Mitarbeitern vor dem Einstellungsdatum global durchgeführt. Die Ergebnisse werden in der Personalakte des Mitarbeiters hinterlegt. Die Kriterien für die Hintergrundüberprüfung hängen von den Gesetzen, der beruflichen Verantwortung und der Führungsebene des potenziellen Mitarbeiters ab und unterliegen den üblichen und angemessenen Praktiken des jeweiligen Landes.

4.6. Programme für Sicherheitssensibilisierung und -schulung

Neu eingestellte Mitarbeiter werden bei der Einarbeitung über die Sicherheitsrichtlinien und den betrieblichen Verhaltenskodex und die ethischen Grundsätze von GoTo informiert. Diese obligatorische jährliche Sicherheits- und Datenschutzschulung wird den betreffenden Mitarbeitern bereitgestellt und vom Talent-Development-Team mit Unterstützung des Sicherheitsteams verwaltet.

GoTo-Mitarbeiter und Zeitarbeitskräfte werden regelmäßig über Sicherheits- und Datenschutzleitfäden, -verfahren, -richtlinien und -standards informiert, u. a. durch Onboarding-Kits für neue Mitarbeiter, Sensibilisierungskampagnen, Webinare mit dem CISO, ein Security-Champion-Programm und mindestens halbjährlich wechselnde Poster und andere Ressourcen, die Methoden zur Sicherung von Daten, Geräten und Einrichtungen erläutern.

5 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten seiner Kunden, der Abonnenten der GoTo-Dienste und der Endbenutzer sehr ernst und verpflichtet sich, relevante Praktiken zur Datenverarbeitung und -verwaltung offen und transparent darzulegen.

5.1. DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) über den Schutz der Daten und der Privatsphäre aller Personen in der EU. Hauptziel der DSGVO ist es, den Bürgern und Einwohnern mehr Kontrolle über ihre personenbezogenen Daten zu geben und das regulatorische Umfeld innerhalb der EU zu vereinfachen. Rescue Live Guide hält die geltenden Bestimmungen der DSGVO ein. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo versichert und garantiert hiermit, dass es den California Consumer Privacy Act (CCPA) einhält. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3. Datenschutzrichtlinien

GoTo bietet einen umfassenden globalen Datenverarbeitungsnachtrag (DVN), der in Englisch und Deutsch verfügbar ist und die Anforderungen der DSGVO, CCPA erfüllt bzw. sie übertrifft und die Verarbeitung personenbezogener Daten durch GoTo regelt.

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) zur Regelung der gesetzeskonformen Übermittlung gemäß der DSGVO mittels Anwendung der EU-Standardvertragsklauseln (auch als EU-Modellklauseln bekannt); und (c) die technischen und organisatorischen Maßnahmen von GoTo. Im Zusammenhang mit dem 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 legt GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Dienste bereitzustellen, zu pflegen, zu verbessern und zu sichern, in seiner Datenschutzrichtlinie auf der öffentlichen Website offen. Das Unternehmen kann die Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen seiner Informationspraktiken und/oder Änderungen des anwendbaren Rechts zu reflektieren, wird jedoch auf seiner Website über alle wesentlichen Änderungen informieren, bevor diese in Kraft treten.

Die Option zur Wahl des Datenspeicherorts von Rescue Live Guide ermöglicht es Ihnen, den Speicherort der Endbenutzerdaten festzulegen: entweder innerhalb der Europäischen Union (Frankfurt, Dublin) oder in den USA. GoTo garantiert allen Nutzern, die die EU als Datenspeicherort wählen, dass sie ausschließlich mit Rechenzentren innerhalb der EU verbunden werden und dass die Kundendaten die gewählte Region nie verlassen.

5.4. Abkommen zur Datenübertragung

GoTo verfügt über ein robustes globales Datenschutzprogramm, das die geltenden Gesetze berücksichtigt und rechtmäßige internationale Datenübertragungen unter den folgenden Rahmenbedingungen unterstützt:

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 DNV von GoTo spezifische Garantien betreffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Dienste. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Zusätzlich zu den in diesen TOMs genannten Maßnahmen hat GoTo die folgenden FAQs erstellt, die die zusätzlichen Maßnahmen zur Unterstützung rechtmäßiger Übertragungen gemäß Kapitel 5 der DSGVO darlegt und alle vom Europäischen Gerichtshof in Verbindung mit der SCCs empfohlenen Einzelfallanalysen behandelt und leitet.

5.4.2. Zertifizierung nach APEC CBPR und PRP

GoTo hat außerdem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft) CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC CBPR und PRP wurden als erste ihrer Art für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt und durch den APEC-konformen Datenschutzmanagement-Anbieter TrustArc erworben und unabhängig validiert.

5.5. Rückgabe und Löschung von Kundeninhalten

Kunden können jederzeit die Rückgabe oder Löschung ihrer Inhalte über standardisierte Benutzeroberflächen beantragen. Wenn diese Oberflächen nicht zur Verfügung stehen oder GoTo aus anderen Gründen nicht in der Lage ist, die Anfrage zu bearbeiten, wird GoTo im Rahmen der technischen Möglichkeiten alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um den Kunden bei der Abfrage oder Löschung seiner Inhalte zu unterstützen. Die Kundeninhalte werden innerhalb von dreißig (30) Tagen nach Aufforderung durch den Kunden gelöscht.

Die Kundeninhalte von Rescue Live Guide werden automatisch innerhalb von neunzig (90) Tagen nach Ablauf oder Beendigung der letzten Abonnementlaufzeit gelöscht. Auf schriftliche Anfrage wird GoTo die Löschung dieser Inhalte bestätigen.

5.6. Vertrauliche Daten

Obwohl GoTo bestrebt ist, alle Kundeninhalte zu schützen, sind wir aufgrund regulatorischer und vertraglicher Bestimmungen dazu gezwungen, die Verwendung von Rescue Live Guide für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in Rescue Live Guide (durch den Kunden oder seine Endbenutzer) hochgeladen oder generiert werden:

- 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) von 1996 und verwandte Gesetze 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 Rescue Live Guide 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.

5.7. Tracking und Analyse

GoTo verbessert seine Websites und Produkte kontinuierlich mithilfe von Webanalyse-Tools von Drittanbietern, die GoTo dabei helfen, zu verstehen, wie Besucher seine Websites, Desktop-Tools und mobilen Anwendungen nutzen und welche Benutzereinstellungen und Probleme sie haben. Weitere Informationen entnehmen Sie bitte der Datenschutzrichtlinie.

6 Drittanbieter

6.1. Einsatz von Drittanbietern

Im Rahmen der internen Beurteilung und der Prozesse in Bezug auf Anbieter bzw. Drittanbieter können Anbieterbeurteilungen je nach Relevanz und Anwendbarkeit von mehreren Teams durchgeführt werden. Das Sicherheitsteam evaluiert Anbieter, die auf Informationssicherheitsdienste anbieten, dazu gehört auch die Beurteilung von Hosting-Einrichtungen Dritter. Die Rechtsabteilung und die Beschaffungsabteilung können Verträge, Leistungsbeschreibungen (Statements of Work, SOW) und Dienstleistungsvereinbarungen nach Bedarf im Rahmen interner Prozesse beurteilen. Angemessene Unterlagen oder Berichte über die Einhaltung der Vorschriften können mindestens einmal jährlich eingeholt und ausgewertet werden, um sicherzustellen, dass das Kontrollumfeld angemessen funktioniert und alle notwendigen Kontrollen zwecks Berücksichtigung der Benutzer durchgeführt werden. Darüber hinaus müssen Dritte, die sensible oder vertrauliche Daten von GoTo hosten oder von GoTo Zugang zu diesen gewährt wird, einen schriftlichen Vertrag unterzeichnen, in dem die entsprechenden Anforderungen für den Zugang zu, die Speicherung oder den Umgang mit den Informationen (je nach Fall) dargelegt sind.

6.2. Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität der Geschäftsprozesse und der Datenverarbeitung Dritter getroffen werden, prüft GoTo die Geschäftsbedingungen der betreffenden Dritten und verwendet entweder von GoTo genehmigte Beschaffungsvorlagen oder handelt die Bedingungen dieser Drittanbieter aus, sofern dies für erforderlich gehalten wird.

7 Kontaktaufnahme mit GoTo

Kunden können GoTo unter https://support.goto.com für allgemeine Anfragen oder privacy@goto.com für Fragen zum Datenschutz kontaktieren.