TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR RESCUE LIVE LENS

Operative Sicherheits- und Datenschutzkontrollen

Datum der Veröffentlichung: Februar 2022

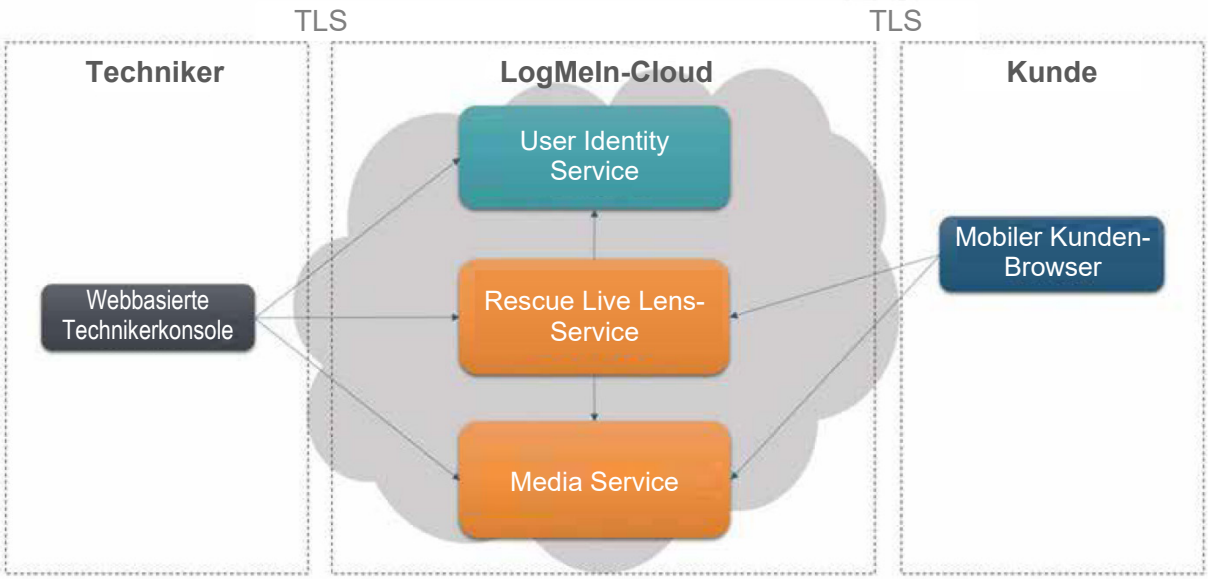
1 Produkte und Services

Dieses Dokument ist auf die technischen und organisatorischen Maßnahmen (TOMs) der Infrastruktur und Kommunikationskanäle von Rescue Live Lens fokussiert. Rescue Live Lens ermöglicht es IT und Support-Mitarbeitern, audiovisuellen Fernsupport für Mobilgeräte mit Kameraübertragung über eine webbasierte Technikerkonsole bereitzustellen.

Rescue Live Lens führt robuste Datensicherheitsmaßnahmen durch, um vor passiven und aktiven Angriffen zu verteidigen.

2 Produktarchitektur

Rescue Live Lens verwendet ein ASP-Modell (Application Service Provider), um für sichere Vorgänge bei der Integration mit einer vorhandenen Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens zu sorgen. Die Architektur ist auf optimale Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt. Redundante Switches und Router sind Teil der Architektur und sollen sicherstellen, dass es keinen „Single Point of Failure“ gibt. Geclusterte Server und Backup-Systeme mit hoher Kapazität stellen selbst bei hoher Last oder einem Systemausfall sicher, dass die Anwendungsprozesse weiterhin funktionieren. Service Broker verteilen die Last der Client/Server-Sitzungen auf geografisch verteilte Kommunikationsserver. Die Kommunikationsarchitektur für Rescue Live Lens wird in Abschnitt 2.1 unten gezeigt.



2.1 Kommunikationsarchitektur

Bei der Techniker-Authentifizierung kommt der User Identity Service von GoTo zum Einsatz. Die Kommunikation zwischen Teilnehmern in einer Rescue Live Lens-Sitzung erfolgt über einen Overlay Networking Stack, der logisch auf dem konventionellen UDP und TCP/IP aufsetzt. Dieses Netzwerk wird von Rescue Live Lens und dem Media Service bereitgestellt (gehostet in Amazon AWS).

Teilnehmer an Rescue Live Lens-Sitzungen (webbasierte Technikerkonsole und mobiler Kunden-Browser) kommunizieren mit Rescue Live Lens und dem Media Service unter Verwendung ausgehender TCP-Verbindungen auf Port 443 oder UDP-Port 15000, abhängig von der Verfügbarkeit. Da Rescue Live Lens ein webbasierter Service ist, können Teilnehmer sich nahezu überall befinden, wo es Internet gibt − im Remote Office, zu Hause, in einem Business Center oder verbunden mit dem Netzwerk eines anderen Unternehmens.

3 Rescue Live Lens − 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 Authentifizierung

Rescue Live Lens-Techniker und -Kontoadministratoren werden durch ihre E-Mail-Adresse identifiziert und unter Verwendung eines Passworts authentifiziert. Bei der autorisierten Authentifizierung wird das Passwort nicht in unverschlüsseltem Zustand von GoTo übertragen.

Authentifizierungsverfahren sind durch folgende Richtlinien geregelt:

Starke Passwörter: Ein starkes Passwort muss mindestens acht (8) Zeichen lang sein und die entsprechenden Komplexitätsanforderungen erfüllen (d. h. Buchstaben und Zahlen aufweisen). Passwörter werden beim Erstellen oder Ändern auf ihre Stärke überprüft.

Zwei-Faktor-Authentifizierung: Als zusätzliche Sicherheitsmaßnahme ist optional Zwei-Faktor-Authentifizierung für jedes Rescue Live Lens-Technikergruppenkonto verfügbar. Bei Aktivierung erfordert die Zwei-Faktor-Authentifizierung, dass sich jeder Benutzer beim Zugriff über zwei separate Methoden autorisiert.

Kontosperre: Nach fünf aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen wird das Benutzerkonto in einen obligatorischen Soft Lockout-Zustand versetzt. Das bedeutet, dass der Inhaber des Benutzerkontos sich fünf Minuten nicht anmelden kann. Nach Ablauf des Sperrzeitraums kann der Inhaber des Benutzerkontos versuchen, sich erneut anzumelden.

3.2 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen 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.

Benutzer, die zum Zugriff auf Rescue Live Lens-Produktkomponenten autorisiert sind, können autorisierte technische Mitarbeiter von GoTo (z. B. Technikabteilung und Engineering DevOps), Kundenadministratoren oder Endbenutzer des Produkts sein. Lokale Produktionsserver sind nur von Jumphosts oder über das Virtual Private Network (VPN) von Operations verfügbar. Cloud-basierte Produktionskomponenten sind über SSU-Authentifizierung (Self Service Unix) verfügbar.

3.3 Berechtigungsbasierte Zugriffskontrolle

3.3.1 Sitzung mit Kameraübertragung

Ein wichtiger Bestandteil der Rescue Live Lens-Sicherheit ist das berechtigungs-basierte Zugriffskontrollmodell zum Schutz des Zugriffs auf Kamera und Mikrofon des Kunden. Bei Live Lens-Supportsitzungen wird der Kunde vor der Initiierung des Zugriffs auf Kamera oder Mikrofon nach seiner Zustimmung gefragt.

3.4 Rollenbasierte Zugriffskontrolle

Rescue Live Lens bietet Zugriff auf eine Vielzahl von Ressourcen und Services unter Verwendung eines rollenbasierten Zugriffskontrollsystems, das durch seine unter-schiedlichen Komponenten zur Servicebereitstellung erzwungen wird. Die folgenden Rollen sind definiert:

Kontoadministrator: Rescue Live Lens-Benutzer mit vollständigen Administrator-privilegien zur Durchführung administrativer Funktionen von Technikern. Konto-administratoren können Techniker-Konten erstellen, modifizieren und löschen sowie Abonnementdaten ändern.

Techniker: Rescue Live Lens-Benutzer. Der Techniker kann Live Lens-Sitzungen initiieren, um Kunden per Kameraübertragung zu unterstützen.

Kunde: nicht authentifizierte Person, die Support vom Techniker anfordert. Der Kunde kann Sitzungen schließen und muss dem Techniker den Zugriff auf sein Gerät gewähren.

3.5 Perimeterverteidigung und Erkennung von Eindringversuchen

GoTo setzt Standard-Tools, -Techniken und -Services für den Perimeterschutz ein, die verhindern sollen, dass nicht autorisierter Netzwerkdatenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk enthält nach außen gerichtete Firewalls und eine interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch Host-basierte Firewalls.

3.6 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.

3.7 Physische Sicherheit

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. Außerdem wird der physische Zugang zu Rechenzentren bei Kündigung von bereits autorisiertem Personal entfernt.

3.8 Daten-Backup, Notfallwiederherstellung, Verfügbarkeit

Die Architektur von GoTo wurde 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. Die Notfallwiederherstellung dieser Systeme wird regelmäßig getestet.

3.9 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.

Zentrale Punkte hinsichtlich der Verschlüsselung in Rescue Live Lens sind u. a.:

- Rescue Live Lens-Sitzungsdaten sind während der Übertragung maximal durch AES-Verschlüsselung (256 Bit) mit Transport Layer Security (TLS) 1.2 (falls unterstützt) geschützt.
- Sitzungsschlüssel werden serverseitig durch den Agent generiert und bleiben dort, um eine Verbindung zwischen Kunde und Agent zu ermöglichen. Der Service soll sicherstellen, dass diese Schlüssel nie der Öffentlichkeit preisgegeben werden oder für diese sichtbar sind.
- Verschlüsselte Kommunikation zwischen Kunde und Techniker in Rescue Live Lens erfolgt über den Media Service.
- Endpunkte in der Rescue Live Lens-Infrastruktur verwenden TLS-Verbindungen.

3.9.1 Verschlüsselung während der Übertragung

Um Kundeninhalt zusätzlich zu sichern, verwendet GoTo aktuelle TLS-Protokolle und verknüpfte Cipher Suites.

Kunden-Endpunkt und Back-End-Kommunikation sind über OpenSSL verschlüsselt. Sicherheitskontrollen für die Kommunikation basierend auf starker Kryptografie werden auf der TCP-Schicht über TLS-Standardlösungen implementiert.

Starke Authentifizierungsmaßnahmen sollen die Wahrscheinlichkeit potenzieller Angreifer reduzieren, sich als Infrastrukturserver auszugeben oder sich in die Kommunikation der Supportsitzung einzuschalten.

Um Schutz vor Abhörung, Modifizierung oder Replay-Angriffen zu bieten, werden TLS-Protokolle nach IETF-Standard zum Schutz der gesamten Kommunikation zwischen Endpunkten und unseren Services verwendet. Alle sitzungsbezogenen Daten werden während der Übertragung mit bis zu TLS 1.2 verschlüsselt, falls unterstützt (RSA mit 2048 Bit, starke AES256-Cipher mit SHA-2-Algorithmus mit 384 Bit).

GoTo empfiehlt auch, dass Techniker ihre Browser standardmäßig für die Verwendung starker Kryptografie konfigurieren (wenn möglich), um technische Schutzmaßnahmen auf dem Techniker-Rechner zu erhöhen, und immer die aktuellen Sicherheitspatches für Betriebssystem und Browser zu installieren.

Beim Herstellen von Verbindungen zur Rescue Live Lens-Website und zwischen den Rescue Live Lens-Komponenten authentifizieren sich die GoTo-Server mit Hilfe von Public-Key-Zertifikaten von GlobalSign bei den Clients. APIs zwischen Servern sind nur im privaten Netzwerk von GoTo hinter robusten Firewalls zugänglich.

3.9.2 Verschlüsselung im Ruhezustand

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

3.9.3 Sicherheit der TCP-Schicht

Die Kommunikation zwischen Endpunkten wird durch TLS-Protokolle nach IETF-Standard (Internet Engineering Task Force) geschützt.

GoTo empfiehlt allen Benutzern zu ihrer eigenen Sicherheit, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden, und sicherzustellen, dass die Sicherheitspatches für Betriebssystem und Browser aktuell sind.

3.10 Schwachstellen-Management

Sicherheit und Schutz des Inhalts der GoTo-Kunden und -Systeme haben oberste Priorität. GoTo implementiert verschiedene Sicherheitsmaßnahmen während des Lebenszyklus aller Produkte. Sicherheitsaspekte werden bei der Entwicklung und beim Betrieb von Rescue Live Lens berücksichtigt.

Dynamische und statische Tests von Anwendungsschwachstellen sowie Sicherheits-bewertungstests für anvisierte Umgebungen werden ebenfalls regelmäßig durchgeführt. Relevante Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.10.1 Sicherheitsteam

Das Sicherheitsteam von GoTo überwacht fortlaufend Produktentwicklung und -betrieb in enger Zusammenarbeit mit den Product Engineers, damit Rescue Live Lens sicher bleibt und um mögliche Risiken zu vermeiden oder zu reduzieren.

3.10.2 Interne und externe Audits

Der interne Auditprozess von GoTo beinhaltet regelmäßige Sicherheitsbewertungen auf Infrastruktur- und Software-Ebene. Interne Audits werden anhand verschiedener unabhängiger externer Bewertungen durchgeführt, um die Einhaltung der Branchen-standards durch GoTo sicherzustellen.

3.11 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 Lense.

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 Compliance-Zertifizierungen und externen Audit-Berichte:

- Service Organization Control des American Institute of Certified Public Accountants (AICPA)
- (SOC) 2 Type II-Bericht inkl. BSI Cloud Computing Catalogue (C5)
- 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)
- 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.

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 Lens, 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 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 und des Datenschutz-teams 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, Aufklärungs-kampagnen, 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 Lens 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 Lens 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 Kundeninhalt

Rescue Live Lens-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 für Rescue Live Lens wird innerhalb von dreißig (30) Tagen nach der Anfrage des Kunden gelöscht. Rescue Live Lens-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 Lens für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in Rescue Live Lens 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, geschützte 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 Lens 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 relevante Anbieter von Services, die auf Informationssicherheit basieren, und nimmt auch die Bewertung der Hosting-Einrichtungen von Drittanbietern vor. Die Teams für Recht und Beschaffung von GoTo 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 in Zusammenarbeit mit Teams für Sicherheit, Recht, Beschaffung und Finanzen (wie angemessen) 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.

8 Anhang – Terminologie

Techniker: Rescue Live Lens-Benutzer, der Rescue Live Lens-Sitzungen erstellt, um Kunden per Kameraübertragung audiovisuell zu unterstützen.

Webbasierte Technikerkonsole: webbasierte Anwendung, die auf dem PC, Mac, Tablet oder Chromebook in einem beliebigen der unterstützten Browser (Chrome, Firefox, Safari) ausgeführt wird und eine Verbindung zum Rescue Live Lens Service herstellt. Sie ermöglicht dem Techniker das Erstellen und Durchführen von Live Lens-Supportsitzungen per Kamera-übertragung sowie verschiedene Funktionen für Kontoverwaltung, Serviceverwaltung und Berichterstattung.

Supportsitzung: Für Rescue Live Lens bedeutet eine Supportsitzung, dass Techniker und Kunde über den Rescue Live Lens Service per Kameraübertragung verbunden sind, sodass der Techniker den Kunden unterstützen kann.

Kunde: Person, die Support vom Techniker über eine Rescue Live Lens-Supportsitzung erhält.

Mobiler Kunden-Browser: webbasierte Anwendung, die in jedem beliebigen unterstützten Browser auf dem Computer/Mobilgerät des Kunden ausgeführt wird und mit einer Rescue Live Lens-Sitzung über den Rescue Live Lens-Service verbunden ist. Sie kann Kamera-übertragungs-Funktionen mit Anmerkungen und VOIP bereitstellen.

Media Service: mehrere global verteilte Server mit Lastenausgleich, die eine Vielzahl von hoch verfügbaren Unicast- und Multicast-Kommunikationsservices basierend auf WebRTC-Protokollen bieten.

Rescue Live Lens-Service: mehrere global verteilte Server mit Lastenausgleich, die sicheren Zugriff für die webbasierte Technikerkonsole und den mobilen Kunden-Browser über verschlüsselte Web Socket-Verbindungen und API-Aufrufe bieten.