TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR GOTO CONNECT

OPERATIVE SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Januar 2022

1 Produkte und Services

GoTo Connect ist eine UCaaS-Komplettlösung (Unified Communications as a Service), die speziell für die Geschäftswelt entwickelt wurde. Es vereint die Leistungsstärke und Zuverlässigkeit unserer Cloud-VoIP-Telefonsysteme mit den Web-, Audio- und Videokonferenzen von GoTo Meeting* in einer einfachen, verlässlichen und flexiblen Collaboration-Lösung für große und kleine Unternehmen.

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs) für GoTo Connect, einen Cloud-basierten Telefonservice, um herkömmliche lokale Telefonanlagen zu ersetzen. Es bietet eine robuste Suite an Kommunikationsfeatures und einfache Kontoverwaltung über einen Webbrowser oder eine mobile Anwendung (der Service).

Die folgenden Features und Angebote sind im Service enthalten:

- GoTo Connect Business Continuity (JBC) ist ein optionaler Premium-Service (Hardware), der am Kundenstandort installiert wird. Er bietet einen lokalen Telefonservice bei einem Netzwerkausfall über einen unabhängigen Drittanbieter, dessen Services separat vom Kunden erworben werden.

- Contact Center wurde entwickelt, damit Benutzer Anruf-Warteschleifen und eingehende Kundenanrufe über interaktive Sprachantworten, automatische Anrufverteilung und Customer Relationship Management-Integrationen verwalten können.

- Im PBX-Administrationsportal können Benutzer mit Administratorrechten von jedem internetfähigen Gerät aus die Systemeinstellungen anzeigen und globale Änderungen vornehmen.

- Der visuelle Wählplan-Editor ist ein Tool zum Bearbeiten des Anruf-Flusses, um Wartezeiten zu konfigurieren oder Anrufe zu bestimmten Voicemailboxen, automatischen Telefonzentralen und Rufgruppen zu leiten.

- PSTN-Ersatzservices sind Services, die über Partnerschaften mit einigen der weltweit führenden Telekommunikationsanbieter bereitgestellt werden.

*Weitere Informationen über den GoTo Meeting Service und seine technischen und organisatorischen Maßnahmen finden Sie in der Dokumentation zu UCC-Lösungen von GoTo unter https://www.goto.com/company/trust/resource-center.

2 Produktarchitektur

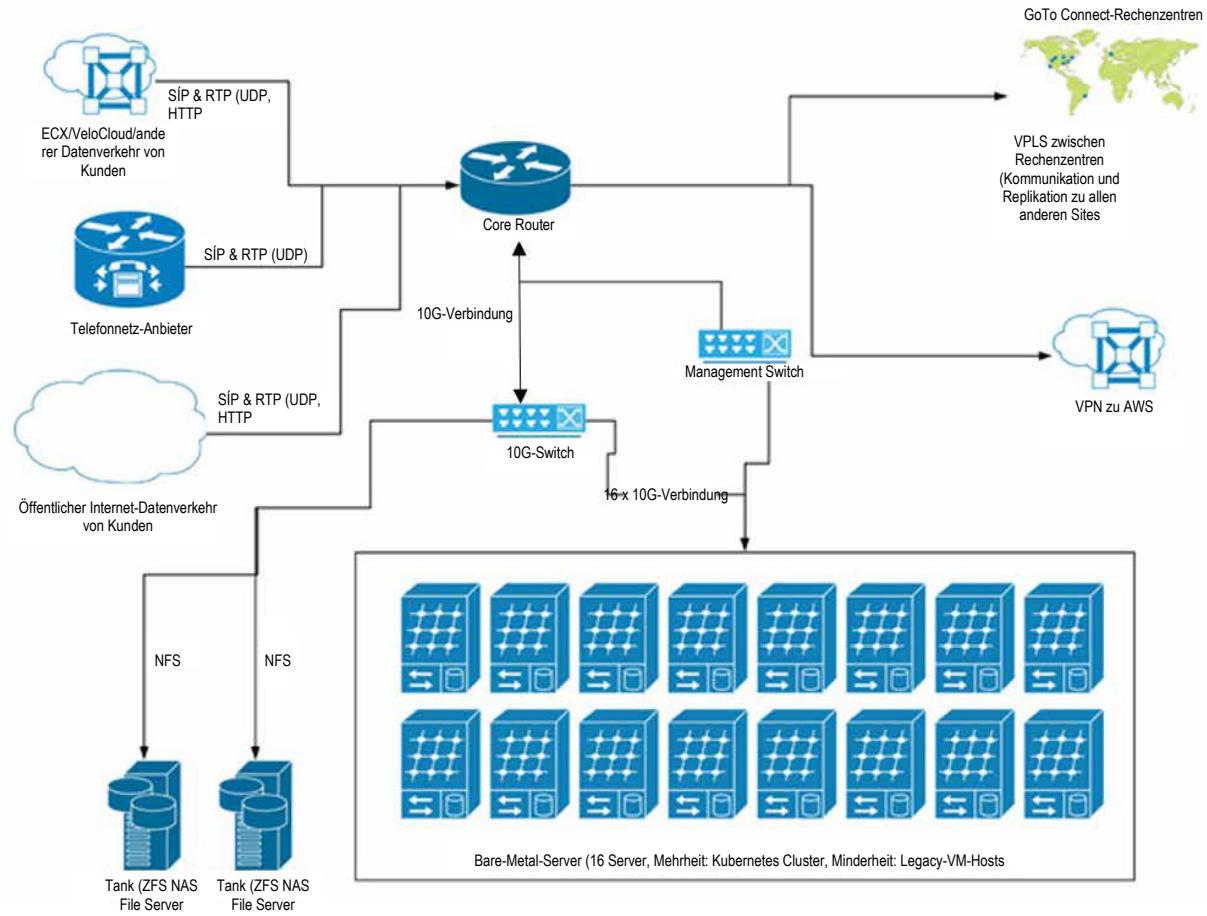

Abbildung 1 – GoTo Connect-Infrastruktur

3 GoTo Connect – 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 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.

Das integrierte Service-Angebot von GoTo Connect nutzt die proprietäre Identitätsverwaltungsplattform von GoTo für die Kundenbereitstellung, bietet Single Sign-On (SSO) unter Verwendung der Security Assertion Markup Language (SAML) und ist über eine API direkt

mit der Plattform von GoTo integriert. Dies bietet zuverlässige administrative Kontrollen, einschließlich die Möglichkeit für Administratoren von Kundenkonten, Passwortrichtlinien zu konfigurieren, Passwortzurücksetzungen zu erzwingen und die Verwendung von SAML für die Anmeldung zu verlangen.

Service-Administratoren für Telefonanlagen (Superadministratoren) können bestimmte Berechtigungen im PBX-Administrationsportal gewähren oder ablehnen. Diese Gruppenberechtigungen ermöglichen die Konfiguration der Telefonanlage, die Bearbeitung von Notrufadressen/-standorten, die Anzeige und Bezahlung von Rechnungen sowie die Erstellung, Aktualisierung und Löschung von Einstellungen und Konten für:

- Benutzer
- Benutzergruppen
- Durchwahlen
- Geräte
- Hardware
- Sites und
- Telefonnummern (Löschen und Erstellen, verwaltet über Nummernreihenfolge).

Berechtigungen auf Benutzerebene werden nicht direkt konfiguriert, da sie von den Benutzer-, Gerät- und Leitungsbeziehungen abgeleitet werden.

Für weitere Details zu Gruppenberechtigungen referenzieren Sie bitte das GoTo Connect-Handbuch für Administratoren von Telefonanlagen.

3.2 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. Wichtige Systemdateien werden vor böswilliger oder unbeabsichtigter Infizierung oder Zerstörung geschützt.

3.3 Datentrennung

Der Service nutzt eine Architektur mit mehreren Mandanten (und Telefonanlagen), die basierend auf dem Servicekonto 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. Außerdem wird der physische Zugang zu Rechenzentren bei Kündigung von bereits autorisiertem Personal entfernt.

3.5 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Um Redundanz, Anruf-Failover, Skalierbarkeit und hohe Verfügbarkeit bereitzustellen, verwendet der Service einen vermaschten containerisierten Microservice, der eine schnelle Bereitstellung und Skalierung von Services zur Erfüllung der Anforderungen von GoTo-Kunden ermöglicht. Dieses komplett vermaschte Design erlaubt die Selbsterkennung und -wiederherstellung durch Microservices bei einem Ausfall in einem spezifischen Rechenzentrum oder einem im öffentlichen Internet geografisch lokalisierten Problem. Services sind für ein automatisches Failover zwischen Rechenzentren ausgelegt.

Die Infrastruktur zwischen Rechenzentren ist über Cluster mit Interkonnektivität eines Virtual Private LAN Service (VPLS)/vermaschten Netzwerks verbunden. Für VPLS-Verbindungen kann ein Failover zu einem Dynamic Multipoint Virtual Private Network (DMVPN) stattfinden, wenn primäre Verbindungen offline gehen. Jede Site hat mehrere Peering-Verbindungen mit dem öffentlichen Internet. Alle Produktionsrechenzentren sind so verbunden, dass interne Anwendungen die Services von jedem Standort aus erreichen können. Jedes Rechenzentrum wird in privater Hardware (Rack Blades) gehostet.

Die Verbindung zum Telefonnetz erfolgt von jedem Rechenzentrumsstandort zu mehreren Telefonnetz-Partnern/-Anbietern per SIP-Trunks (Session Initiation Protocol) über das öffentliche Internet.

Für hohe Verfügbarkeit betreibt GoTo ein Netzwerk aus Rechenzentren mit vollständiger Vermaschung. Diese Rechenzentren werden mit einer Kapazität von N+1 Rechenzentren betrieben. Das heißt, dass der Service dem Ausfall des Äquivalents eines Rechenzentrums im Wert der Kapazität standhalten und dennoch den Betrieb aufrechterhalten kann, indem er den Datenverkehr automatisch an zusätzliche Rechenzentrumssites weiterleitet.

3.6 Malware-Schutz

Warnmeldungen bei anomaler Aktivität werden aktiv im Service bereitgestellt und überwacht. Warnmeldungen, einschließlich möglicher böswilliger Aktivität, werden an entsprechende Reaktionsteams zur Lösung oder Schadensminderung 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.

Verschlüsselung während der Übertragung

Der Service bietet durchgängige Maßnahmen für Datensicherheit. Er wurde entworfen, um sicherzustellen, dass Kommunikationsdaten nicht in unverschlüsselter Form für Kommunikationsserver oder während der Übertragung zwischen öffentlichen oder privaten Netzwerken offengelegt werden.

Transport Layer Security-Protokolle (TLS) nach Internet Engineering Task Force-Standard (IETF) werden zum Schutz der Kommunikation zwischen Endpunkten verwendet. Der gesamte Netzwerkverkehr, der in die und aus den GoTo-Rechenzentren fließt, einschließlich des gesamten Kundeninhalts, wird während der Übertragung verschlüsselt. In den Nutzungsbedingungen finden Sie weitere Informationen.

GoTo empfiehlt Kunden zu ihrer eigenen Sicherheit, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Kryptografie verwenden und sicherstellen, dass die Sicherheitspatches für ihr Betriebssystem und ihre Browser aktuell sind.

Beim Herstellen einer TLS-Verbindung authentifizieren sich GoTo-Server mit Hilfe von Public-Key-Zertifikaten bei den Clients. TLS wird auch zur Signalübertragung zwischen physischen Telefonen und der Service-Infrastruktur verwendet, um Datenverkehr und Kommunikation zu sichern, wenn dies von den Geräten des Kunden unterstützt wird. Medien werden unter Verwendung des Secure Real-time Transport Protocol (sRTP) übertragen, das freigegebene Schlüssel nutzt, die zum Sichern des Audiodatenverkehrs über Session Initiation Protocol Secure (SIPS) übertragen werden. Provisioning-Informationen mit den Anmeldedaten für physische Telefone von der Service-Infrastruktur zu den Telefonen sind auch mit TLS gesichert.

Verschlüsselung im Ruhezustand

Voicemail-Aufzeichnungen, Voicemail-Ansagen und Anruf-Aufzeichnungen werden im Ruhezustand im Cloud-Speicher von GoTo mit AES-Verschlüsselung (256 Bit) verschlüsselt.

3.8 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden mindestens 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 zur Verfügung gestellt werden.

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 des Service.

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 wahrt Compliance mit den folgenden Zertifizierungen und externen Audit-Berichten:

- TRUSTe Enterprise Privacy & Data Governance Practices Certification, 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). BSI Cloud Computing Catalogue (C5).
- Service Organization Control (SOC) 3 Type II-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 Security Operations und Incident-Management

Das Security Operations Center (SOC) von GoTo ist mit dem Security Operations-Team besetzt und ist 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. Es wurde entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services zu verwalten, zu identifizieren und zu beheben. Laut Vorfalls-reaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicher-heit 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, 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. GoTo Connect ist mit den anwendbaren DSGVO-Bestimmungen kompatibel. 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 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 anwendbare Gesetze 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

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. Bei Ablauf oder Kündigung eines Kundenkontos wird Kundeninhalt automatisch dreißig (30) Tage nach dem tatsächlichen Datum des Ablaufs oder der Kündigung des Kontos 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 und zu sichern. Regulatorische und vertragliche Beschränkungen verlangen jedoch, dass die Verwendung von GoTo Connect für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoTo Connect 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, wie im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) sowie anderen relevanten anwendbaren Gesetzen und Vorschriften festgelegt.
- 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 den Service 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 Anbieter- und Drittanbieter-Verwaltung von GoTo 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.