TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN FÜR DAS DIGITALE ENGAGEMENT VON GOTO

DOKUMENTATION ZU ORGANISATORISCHEN SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Version 2.0 | Dezember 2023

Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für GoTo Contact dargelegt. Insbesondere unterhält GoTo robuste globale Datenschutz- und Sicherheitsprogramme sowie organisatorische, administrative und technische Schutzmaßnahmen, um: (i) die Vertraulichkeit, Integrität und Verfügbarkeit von Kundeninhalten sicherzustellen; (ii) vor Bedrohungen und Gefahren für die Sicherheit von Kundeninhalten zu schützen; (iii) vor Verlust, Missbrauch, unbefugtem Zugriff, Offenlegung, Veränderung und Zerstörung von Kundeninhalten zu schützen; und (iv) die Einhaltung geltender Gesetze und Vorschriften, einschließlich Datenschutzgesetzen, zu gewährleisten. Solche Maßnahmen umfassen:

- **Verschlüsselung:**
  - *Während der Übertragung* Transport Layer Security (TLS) Version 1.2.
  - *Im Ruhezustand* Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte.
- **Rechenzentren:** Standorte in den USA, Brasilien, Deutschland, Australien, Singapur und im Vereinigten Königreich, um Redundanz und Stabilität zu gewährleisten.
- **Physische Sicherheit:** Geeignete physische Sicherheits- und Umgebungskontrollen sind vorhanden und darauf ausgelegt, den physischen Zugang zu Systemen und Servern mit Kundeninhalten zu schützen, zu kontrollieren und einzuschränken, um die Verpflichtungen hinsichtlich Betriebszeit, Leistung und Skalierbarkeit einhalten zu können.
- **Compliance-Audits:** GoTo Contact ist nach SOC 2 Typ II, SOC 3 Typ 2, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy sowie APEC CBPR und PRP zertifiziert.
- **Einhaltung gesetzlicher/behördlicher Vorschriften:** GoTo unterhält ein umfassendes Datenschutzprogramm mit Prozessen und Richtlinien, die sicherstellen sollen, dass Kundeninhalte in Übereinstimmung mit den geltenden Datenschutzgesetzen, einschließlich DSGVO, CCPA/CPRA und LGPD, behandelt werden.
- **Sicherheitsprüfungen**: GoTo führt nicht nur interne Tests durch, sondern beauftragt zusätzlich externe Firmen mit der regelmäßigen Durchführung von Sicherheitsprüfungen und/oder Penetrationstests.
- **Logische Zugriffskontrollen:** Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollen soll die Bedrohung des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden.
- **Datentrennung**: GoTo verwendet eine Multi-Tenant-Architektur und trennt Kundenkonten logisch auf der Datenbankebene.
- **Perimeterabwehr und Erkennung von Eindringversuchen**: Tools, Techniken und Dienste zum Schutz des Perimeters sollen verhindern, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung.
- **Datenaufbewahrung:**
  - Kunden von GoTo Contact können jederzeit einen Antrag auf Rückgabe oder Löschung von Kundeninhalten stellen, der innerhalb von dreißig (30) Tagen nach Antragstellung des Kunden bearbeitet wird.
  - Kundeninhalte werden dreißig (30) Tage nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht. Während der Laufzeit des Abonnements werden Anrufaufzeichnungen und Anrufberichte ab dem Datum ihrer Erstellung dreizehn (13) Monate lang aufbewahrt.

1 Produkte und Dienste

GoTo Contact ist eine Contact-Center-as-a-Service(CCaaS)-Lösung, die auf der GoTo-Connect-Plattform aufbaut und es Unternehmen ermöglicht, bessere Ergebnisse bei der Kommunikation mit Kunden und Leads über verschiedene Kommunikationskanäle wie Sprachtelefonie, SMS, Webchat und soziale Medien zu erzielen. Diese Lösung eignet sich für Organisationen jeder Größe, ist aber besonders nützlich für kleine und mittlere Unternehmen.

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs) von GoTo Contact und teilweise von GoTo Connect, welches die Grundlage für GoTo Contact ist.

Im Folgenden sind Funktionen und Angebote aufgeführt, die Teil des GoTo Contact-Dienstes (der Dienst) sind:

- GoTo Contact wurde entwickelt, um Benutzern bei der Verwaltung von Warteschleifen und eingehenden Kundenanrufen durch interaktive Sprachantworten, automatische Anrufverteilung und Integrationen für das Customer Relationship Management (CRM) zu unterstützen.

- Mit Chatwarteschlangen können Benutzer eine Nachricht an eine Warteschlange senden, die dann an einen Unternehmensvertreter weitergeleitet wird, als wäre die externe Nummer die Direktnummer des Vertreters. Nachrichten in der Chatwarteschlange können über verschiedene Kommunikationskanäle gesendet werden: SMS, Webchat, Facebook und andere soziale Medienkanäle.

- Andere Kanäle können bei der Kundenkommunikation unterstützen, z. B. Sprachtelefonie zu Video und Chat zu Video.

- GoTo Contact Analytics bietet Echtzeit- und Verlaufsberichte, die es Supervisoren und Managern ermöglichen, Kundeninteraktionen zu verbessern, das Kundenerlebnis zu optimieren, die aufgewendete Zeit der Mitarbeiter für die Kundenbetreuung zu verringern und die Mitarbeiter in ihren Kommunikationsfähigkeiten zu schulen.

2 Produktarchitektur

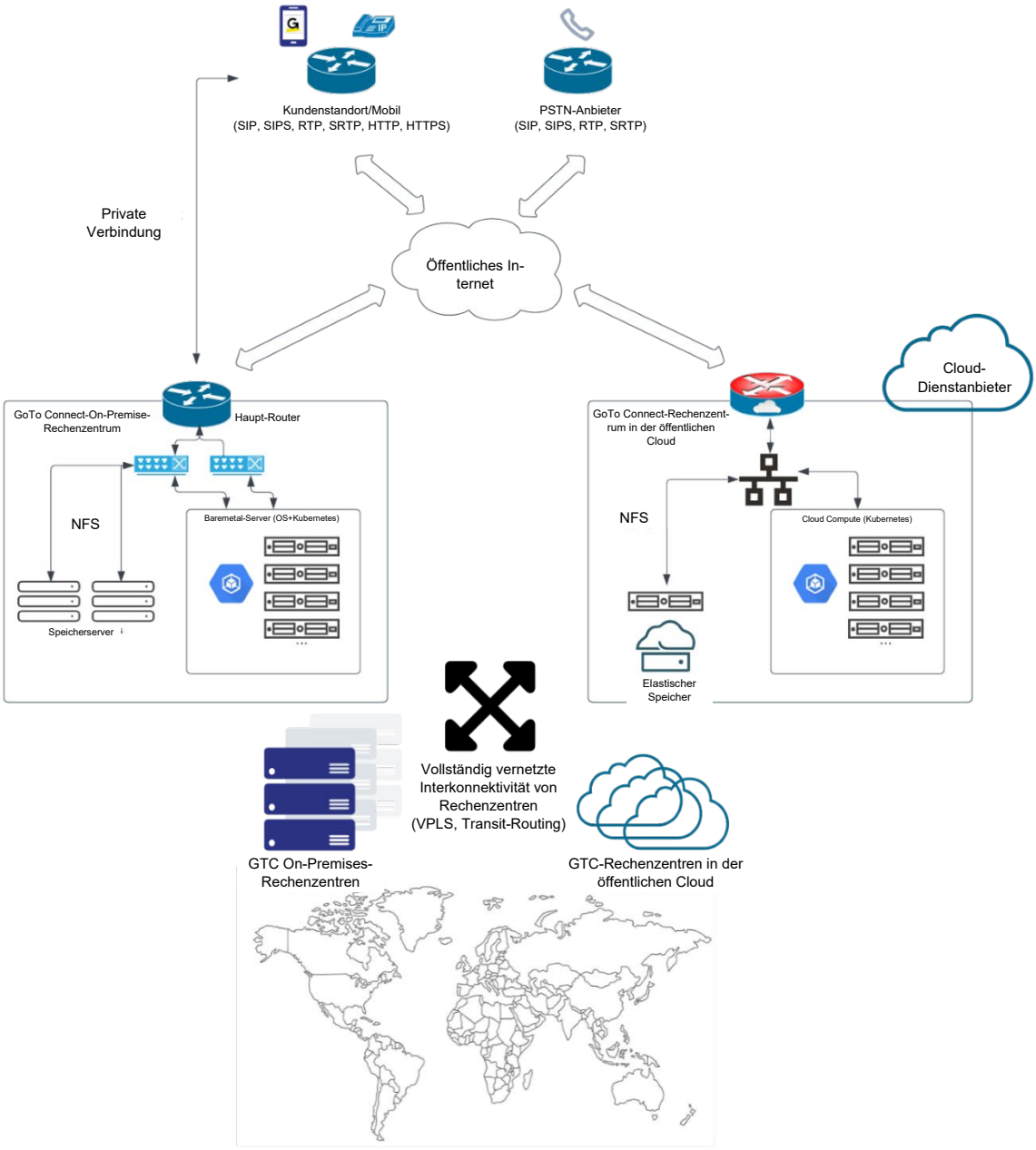

Abbildung 1 – Infrastruktur von GoTo Contact

3 Technische Kontrollen von GoTo Contact

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.

Das integrierte Dienstangebot von GoTo Contact nutzt die GoTo-eigene Identitätsverwaltungsplattform von GoTo für die Kundenbereitstellung, bietet Single Sign-On (SSO) mit Security Assertion Markup Language (SAML) und ist über eine API direkt mit der Plattform integriert. Dies ermöglicht robuste Administrationskontrollen, einschließlich der Möglichkeit für Administratoren von Kundenkonten, Passwort-Richtlinien zu konfigurieren, das Zurücksetzen von Passwörtern zu erzwingen und die Verwendung von SAML für die Anmeldung zu erfordern.

PBX-Superadministratoren für GoTo Contact können Berechtigungen für andere Benutzer festlegen. Dazu gehört unter anderem die Ernennung von Administratoren. Diese Gruppenberechtigungen umfassen die Möglichkeit, die PBX-Anlage zu konfigurieren, Notrufadressen/-standorte zu bearbeiten, Berichte anzuzeigen, Rechnungen anzuzeigen und zu bezahlen sowie Einstellungen und Konten für folgende Elemente zu erstellen, zu aktualisieren und zu löschen:

- Benutzer
- Benutzergruppen
- Durchwahlen
- Geräte
- Hardware
- Standorte
- Telefonnummern (Löschen und Erstellen wird über die Bestellung von Telefonnummern verwaltet)

Berechtigungen auf Benutzerebene werden nicht direkt konfiguriert, da sie aus den Beziehungen zwischen Benutzer, Gerät und Leitung abgeleitet werden.

Weitere Einzelheiten zu den Gruppenberechtigungen finden Sie im PBX-Leitfaden für GoTo-Connect-Administratoren.

3.2 Perimeterabwehr und Erkennung von Eindringversuchen

GoTo setzt branchenübliche Perimeterabwehr-Tools, Techniken und Dienste zum Schutz des Perimeters ein, die verhindern sollen, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung. Kritische Systemdateien werden vor böswilliger und unbeabsichtigter Infektion oder Zerstörung geschützt.

3.3 Datentrennung

Der Dienst nutzt zum Beispiel eine logisch auf Datenbankebene getrennte Multi-Tenant- (und Multi-PBX-)Architektur, die auf dem Dienstkonto eines Benutzers oder einer Organisation basiert. Nur authentifizierte Parteien erhalten Zugriff auf die entsprechenden Konten.

3.4 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.

3.5 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Um Redundanz, Anruf-Failover, Skalierbarkeit und hohe Verfügbarkeit zu gewährleisten, verwendet der Dienst ein containerisiertes Microservice-Netzwerk, das eine schnelle Bereitstellung und Skalierung von Diensten ermöglicht, um die Anforderungen der GoTo-Kunden zu erfüllen. Dank dieses vollständig vernetzten Designs können sich Microservices bei einem Ausfall in einem bestimmten Rechenzentrum oder im Fall eines geografisch begrenzten Problems im öffentlichen Internet selbst erkennen und wiederherstellen. Die Dienste sind für ein automatisches Failover zwischen den Rechenzentren ausgelegt.

Die Infrastruktur ist zwischen Rechenzentren in Form von „Clustern“ verbunden, mit der Interkonnektivität eines Virtual Private LAN Service(VPLS)-Netzwerks. Falls die primären Verbindungen getrennt werden, können VPLS-Verbindungen auf ein Dynamic Multipoint Virtual Private Network (DMVPN) ausweichen. Jeder Standort verfügt über mehrere Peering-Verbindungen mit dem öffentlichen Internet. Alle Produktionsrechenzentren sind so verbunden, dass interne Anwendungen die Dienste von jedem Standort aus erreichen können. Jedes Rechenzentrum wird mit privater Hardware (Rack Blades) gehostet.

Die Verbindung zum öffentlichen Telefonnetz (Public Switch Telephone Network, PSTN) erfolgt von jedem Rechenzentrum aus über Session Initiation Protocol(SIP)-Trunks über das öffentliche Internet mit mehreren PSTN-Partnern/Anbietern.

Um eine hohe Verfügbarkeit zu gewährleisten, betreibt GoTo ein Netzwerk von Rechenzentren, die vollständig miteinander vernetzt sind. Diese Rechenzentren arbeiten mit einer Kapazität von N+1-Rechenzentren, d. h., der Dienst ist so konzipiert, dass er den Kapazitätsverlust bei Ausfall des Äquivalents eines Rechenzentrums verkraften und den Betrieb aufrechterhalten kann, indem der Datenverkehr automatisch an andere Rechenzentrumsstandorte weitergeleitet wird.

3.6 Schutz vor Malware

Der Dienst setzt aktiv Funktionen zur Meldung anormaler Aktivitäten ein und überwacht diese. Alarme, die auf potenzielle bösartige Aktivitäten hinweisen, werden zur Lösung oder Abwehr an die entsprechenden Teams weitergeleitet.

3.7 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.

Verschlüsselung während der Übertragung

Der Dienst stellt Ende-zu-Ende-Maßnahmen für die Datensicherheit bereit. Der Dienst ist so ausgelegt, dass sichergestellt wird, dass Kommunikationsdaten während der Übertragung über öffentliche oder private Netzwerke oder zu Kommunikationsservern nicht unverschlüsselt offenliegen.

Zum Schutz der Kommunikation zwischen Endpunkten werden Transport Layer Security(TLS)-Standardprotokolle der Internet Engineering Task Force (IETF) verwendet. Der gesamte Netzwerk-Datenverkehr, der in GoTo-Rechenzentren ein- und ausgeht, wird während der Übertragung verschlüsselt. Dies schließt auch alle Kundeninhalte ein. Weitere Informationen finden Sie in den Nutzungsbedingungen.

Zu ihrer eigenen Sicherheit empfiehlt GoTo seinen Kunden, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden, und stets die aktuellsten Sicherheitspatches für ihr Betriebssystem und ihre Browser zu installieren.

Beim Aufbau von TLS-Verbindungen nutzen GoTo-Server Zertifikate mit öffentlichem Schlüssel, um sich bei Clients zu authentifizieren. TLS wird auch für Signale zwischen physischen Telefonen und der Dienstinfrastruktur unterstützt, um den Datenverkehr und die Kommunikation zu sichern, sofern dies von Kundengeräten unterstützt wird. Medien werden mit dem Secure Real-time Transport Protocol (SRTP) übertragen, während Audiodatenverkehr mit vorinstallierten Schlüsseln abgesichert wird, die über Session Initiation Protocol Secure (SIPS) übertragen werden. Die Bereitstellung von Informationen, die die Zugangsdaten für die physischen Telefone der Dienstinfrastruktur enthalten, an die Telefone, wird ebenfalls über TLS gesichert.

Verschlüsselung ruhender Daten

Kunden-Voicemail-Aufzeichnungen, Voicemail-Begrüßungen und Anrufaufzeichnungen werden im Ruhezustand mit 256-Bit-AES-Verschlüsselung verschlüsselt, wenn sie im Cloud-Speicher von GoTo gespeichert sind.

3.8 Schwachstellenmanagement

Interne und externe System- und Netzwerk-Schwachstellen-Scans werden mindestens 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 Entwicklungsteams kommuniziert und verwaltet.

3.9 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 des Dienstes 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 inkl. BSI Cloud Computing Katalog (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Typ II Zertifizierungsbericht
- 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. 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. GoTo Contact 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.

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. Bei Ablauf oder Kündigung des Kundenkontos werden die Inhalte des Kunden dreißig (30) Tage nach dem Datum des Ablaufs oder der Kündigung des Kontos automatisch gelöscht. Auf schriftliche Anfrage wird GoTo die Löschung dieser Inhalte bestätigen.

5.6 Vertrauliche Daten

Obwohl GoTo bestrebt ist, alle Kundeninhalte zu schützen und zu sichern, sind wir aufgrund regulatorischer und vertraglicher Bestimmungen dazu gezwungen, die Verwendung von GoTo Contact für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoTo Contact 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) sowie anderen einschlägigen geltenden Gesetzen 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 den Dienst 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 von GoTo in Bezug auf die Verwaltung von Anbietern bzw. Drittanbietern 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.