TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN VON GOTOASSIST CORPORATE

DOKUMENTATION ZU ORGANISATORISCHEN SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Februar 2022

1 Produkte und Dienste

Dieses Dokument enthält die technischen und organisatorischen Maßnahmen (TOMs) von GoToAssist Corporate, einem gehosteten Dienst, der es Supportteams mit mehreren Technikern ermöglicht, technischen Remotesupport für Benutzer von Windows- und Mac-Computern in Unternehmen zu leisten. GoToAssist Corporate lässt sich an die individuelle Umgebung eines Unternehmens anpassen und verfügt über fortschrittliche Funktionen für Administration, Zusammenarbeit und Kundenwarteschleifen, einschließlich Teamzusammenarbeit, Sitzungsübertragung, Kundenumfragen und Sitzungsaufzeichnung.

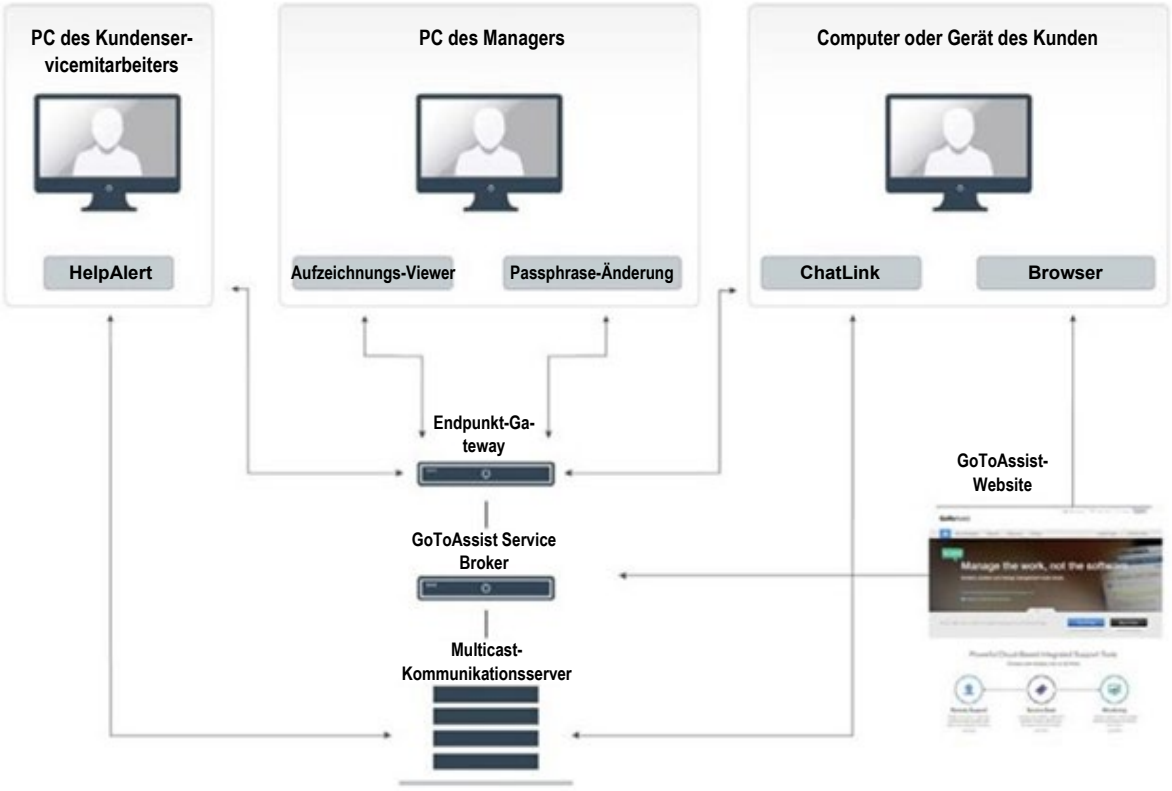
2 Produktarchitektur

GoToAssist Corporate verwendet ein ASP-Modell (Application Service Provider), das für einen sicheren Betrieb sorgt und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt. Die Architektur ist auf Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt. Redundante Switches und Router sind Teil der Architektur, damit es keinen „Single Point of Failure“ geben kann. Kapazitätsstarke, geclusterte Server und Backup-Systeme sollen die Anwendungsprozesse im Falle einer hohen Auslastung oder eines Systemausfalls sicherstellen. Service Broker verteilen für eine optimale Leistung die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver.

Unsere Web-, Anwendungs-, Kommunikations- und Datenbankserver sind in sicheren Colocation-Rechenzentren untergebracht, die über redundante Stromversorgungen und Einrichtungen zur Kontrolle der Umgebungsbedingungen verfügen. Der physische Zugang zu den Servern ist stark beschränkt und wird kontinuierlich überwacht. Unsere privaten Netzwerke und Backend-Server sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und unabhängige, externe Prüfer führen regelmäßige Tests auf Schwachstellen durch.

3 Technische Sicherheitskontrollen von GoToAssist Corporate

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.



GoToAssist-Website – Webanwendung, die den Zugriff auf die GoToAssist-Website und auf interne und externe webbasierte Administrationsportale ermöglicht. Die Websites werden in Tier-1-Colocation-Rechenzentren gehostet.

GoToAssist Service Broker – Webanwendung, die die Konto- und Serviceverwaltung, persistente Speicherung und Berichterstattungsfunktionen von GoToAssist Corporate bereitstellen. Die Broker werden in Tier-1-Colocation-Rechenzentren gehostet.

Endpunkt-Gateway (EGW) – Ein spezielles Gateway, das von verschiedenen Endpunktanwendungen für den sicheren Zugriff auf den GoToAssist Service Broker zu verschiedenen Zwecken über Remote Procedure Calls verwendet wird. EGW werden von Amazon Web Services gehostet.

Multicast-Kommunikationsserver (MCS) – Eine Gruppe weltweit verteilter Server, die eine Vielzahl von hochverfügbaren Unicast- und Multicast-Kommunikationsdiensten bereitstellen MCS wird in Tier-1-Colocation-Rechenzentren gehostet.

3.1. Logische Zugriffskontrolle

Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollverfahren sollen die Bedrohungen 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.

Zu den Benutzern, die zum Zugriff auf die Produktkomponenten von GoToAssist Corporate berechtigt sind, gehören möglicherweise die technischen Mitarbeiter von GoTo (z. B. Technical Operations und Engineering DevOps), Kundenadministratoren oder Endbenutzer des Produkts. On-Premise-Produktionsserver sind nur über Jump-Hosts oder das VPN des Betriebs verfügbar und beide sind durch Multifaktor-Authentifizierung (MFA) geschützt. Cloudbasierte Produktionskomponenten sind über die SSU(Self Service Unix)-Authentifizierung verfügbar.

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 unsere Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch hostbasierte Firewalls. Darüber hinaus wird ein cloudbasierter DDoS-Präventionsdienst eines Drittanbieters zum Schutz vor volumetrischen DDoS-Angriffen eingesetzt, der mindestens einmal pro Jahr getestet wird. Kritische Systemdateien werden vor böswilliger und unbeabsichtigter Infektion oder Zerstörung geschützt.

3.3. Datentrennung

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

3.4. Physische Sicherheit

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

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. Die Notfallwiederherstellung dieses Systems wird regelmäßig getestet.

3.6. Schutz vor Malware

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

Die wichtigsten Punkte bei der Verschlüsselung in GoToAssist Corporate sind:

- Die Authentifizierung über das SRP(Secure Remote Passwort)-Protokoll auf Grundlage öffentlicher Schlüssel ermöglicht die Authentifizierung und die Einrichtung von Schlüsseln zwischen Endpunkten.
- 128-Bit-AES-Verschlüsselung wird zum Schutz der Sitzungsdaten verwendet.
- Die Sitzungsschlüssel werden von den Endpunkten generiert und sind GoTo oder seinen Systemen nicht bekannt.
- Kommunikationsserver leiten nur verschlüsselte Pakete weiter und verfügen nicht über den Verschlüsselungsschlüssel der Sitzung.

3.7.1. Verschlüsselung während der Übertragung

Um Kundeninhalte während der Übertragung zusätzlich zu schützen, verwendet GoTo aktuelle Transport Layer Security(TLS)-Protokolle und zugehörige Verschlüsselungssammlungen zum Schutz von vielen Internetprotokollen. Darüber hinaus verwendet GoTo die neueste Version von Secure Shell (SSH) für bestimmte administrative Funktionen. Die Verbindung zu internen Netzwerken wird durch geeignete Virtual Private Network(VPN)-Technologien geschützt, um die Vertraulichkeit und Integrität des internen GoTo-Datenverkehrs zu gewährleisten.

Funktionen für die Kommunikationssicherheit

Die Kommunikation zwischen den Teilnehmern einer GoToAssist-Corporate-Sitzung erfolgt über einen Overlay-Multicast-Netzwerkstapel, der logisch über dem konventionellen TCP/IP-Stapel auf den Computern der einzelnen Benutzer angeordnet ist. Dieses Netzwerk besteht aus einer Reihe von Multicast-Kommunikationsservern (MCS).

Vertraulichkeit und Integrität der Kommunikation

GoToAssist Corporate bietet zusätzliche Sicherheitsmaßnahmen zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Die Daten, die bei der Bildschirmfreigabe, der Tastatur- und Maussteuerung und in Chats anfallen, liegen niemals in unverschlüsselter Form vor, während sie temporär auf Kommunikationsservern lagern oder über öffentliche oder private Netzwerke übertragen werden.

Wenn die Aufzeichnung deaktiviert ist, wird der GoToAssist-Corporate-Sitzungsschlüssel in keiner Form an die Server gesendet. So würde zum Beispiel die Kompromittierung eines Servers nicht den Schlüssel für einen verschlüsselten Stream preisgeben, den ein böswilliger Akteur in diesem Szenario möglicherweise erbeutet hätte. Wenn die Aufzeichnung aktiviert ist, werden die Daten von Chats, Bildschirmübertragungen und Bildschirmanzeigen verschlüsselt gespeichert. Der Sitzungsschlüssel wird ebenfalls gespeichert, ist aber mit einer 1024-Bit RSA-Verschlüsselung mit öffentlichem/privatem Schlüssel geschützt. Es werden portalspezifische öffentliche Schlüssel und eine anpassbare Passphrase verwendet, um den Sitzungsschlüssel vor der Speicherung zu verschlüsseln. Um Sitzungsdaten zu schützen, erfordert die Wiedergabe von Sitzungsaufzeichnungen Folgendes: Zugriff auf die Sitzungsaufzeichnung, den verschlüsselten Sitzungsschlüssel und den privaten Schlüssel des Portals sowie die Passphrase. In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: der „TCP-Schicht“ und dem „Multicast Packet Security Layer“ (MPSL).

Sicherheit der TCP-Schicht

Zum Schutz der Kommunikation zwischen Endpunkten werden TLS-Standardprotokolle der Internet Engineering Task Force (IETF) verwendet.

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 zur Website und zwischen GoToAssist Corporate-Komponenten nutzen GoTo-Server Zertifikate mit öffentlichem Schlüssel, um sich bei Clients zu authentifizieren. Als zusätzlicher Schutz vor Infrastrukturattacken erfolgt eine gegenseitige zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z. B. MCS-zu MCS, MCS zu Broker).

Multicast Packet Security Layer

Weitere Funktionen, die von den TLS-Funktionen unabhängig sind, verschlüsseln die während der Tastatur-/Maussteuerung und des Chats übermittelten Daten zusätzlich. Insbesondere werden alle Sitzungsdaten durch Verschlüsselungs- und Integritätsmechanismen geschützt, die verhindern, dass Personen mit Zugriff auf unsere Kommunikationsserver (ob mit guten oder bösen Absichten) bei einer Sitzung „mithören“ oder unerkannt Daten manipulieren können.

Die Schlüsselvereinbarung erfolgt mittels eines zufällig generierten 128-Bit-Startwerts („Seed“), der vom GoToAssist Corporate Service Broker ausgewählt und über TLS an

alle Endpunkte verteilt wird. Er dient als Eingabe für eine vom NIST genehmigte Schlüsselableitungsfunktion. Am Ende der Sitzung wird der Seed-Wert aus dem Speicher des GoToAssist Corporate Service Brokers gelöscht.

Des Weiteren werden die Sitzungsdaten mittels 128-Bit-AES-Verschlüsselung im Counter-Modus vor Abhörversuchen geschützt. Zur Optimierung der Bandbreite werden Klartextdaten in der Regel vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert. Der Schutz der Datenintegrität wird durch eine ICV-Prüfsumme gewährleistet, die derzeit mit dem HMAC-SHA-1-Algorithmus generiert wird. Durch den konsequenten Einsatz starker Verschlüsselungsverfahren können unsere Kunden darauf vertrauen, dass ihre Sitzungsdaten vor unbefugter Offenlegung und unbemerkten Änderungen geschützt sind.

Darüber hinaus ziehen diese wichtigen Maßnahmen für die Kommunikationssicherheit keine Zusatzkosten oder Leistungseinbußen nach sich und erschweren nicht die Benutzerfreundlichkeit. Eine leistungsfähige und auf Standards basierende Datensicherheit ist eine integrale Funktion jeder Sitzung.

3.8. 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.

3.9. 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 von GoToAssist Corporate 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
- 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, einschließlich der Dienste von GoToAssist, 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. GoToAssist Corporate 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 die Verarbeitung personenbezogener Daten durch GoTo regelt, in Englisch sowie Deutsch verfügbar ist und die Anforderungen der DSGVO, CCPA erfüllt bzw. sie übertrifft.

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

GoToAssist-Corporate-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 Inhalte von GoToAssist-Corporate-Kunden 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 GoToAssist Corporate für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoToAssist Corporate 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) 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 GoToAssist Corporate 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.