

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN VON GOTOASSIST REMOTE SUPPORT V4 (EINSCHL. SERVICE DESK UND SEEIT)

**DOKUMENTATION ZU ORGANISATORISCHEN SICHERHEITS-
UND DATENSCHUTZKONTROLLEN**

Datum der Veröffentlichung: Februar 2022

1 Produkte und Dienste

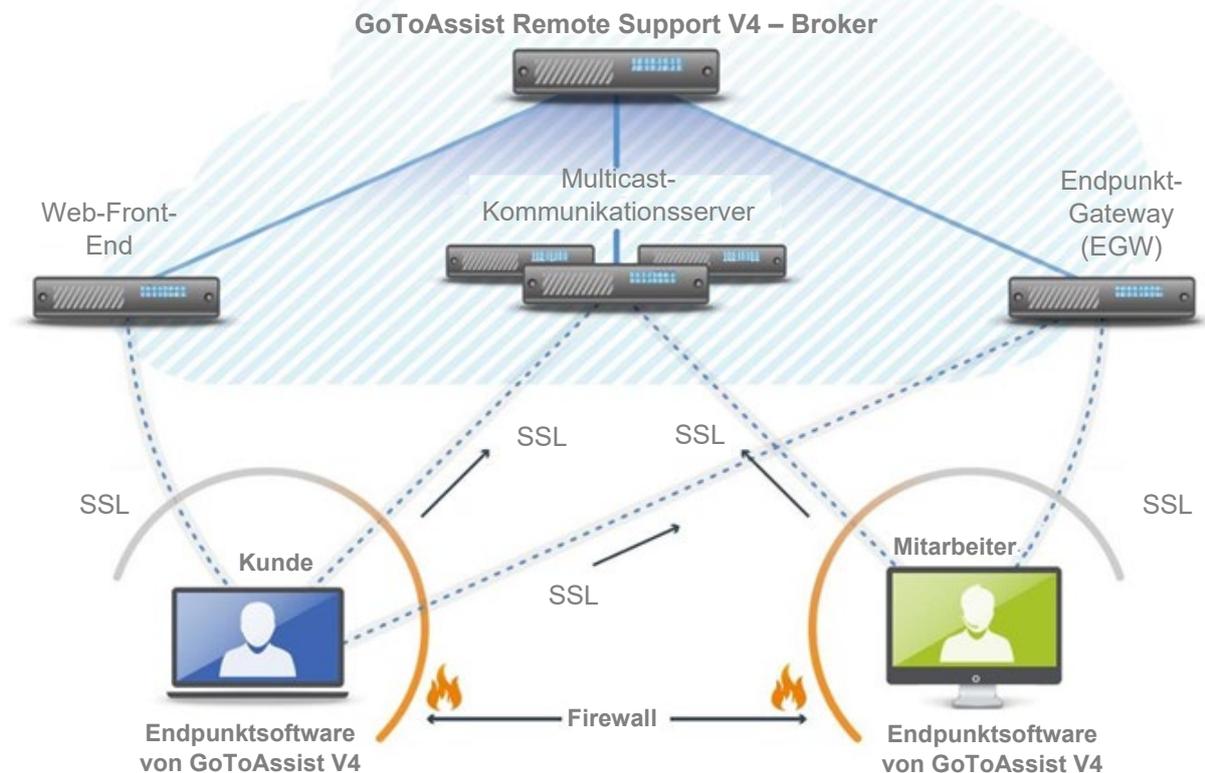
Dieses Dokument behandelt die technischen und organisatorischen Maßnahmen (TOMs) für GoToAssist Remote Support V4, GoToAssist Service Desk und GoToAssist Seeit (gemeinsam als GoToAssist Remote Support V4 bezeichnet).

- **GoToAssist Remote Support V4** ist ein cloudbasierter Dienst, mit dem Supportspezialisten Fehler auf Kundensystemen mit Hilfe von Bildschirmübertragung, der Steuerung von Tastatur und Maus und anderen Funktionen beheben können. Techniker können einzeln oder im Team Ad-hoc-Support leisten und dafür auch auf unbeaufsichtigte Desktops und Server zugreifen.
- **GoToAssist Service Desk** ist eine cloudbasierte IT-Dienstanwendung für Incident-, Problem-, Änderungs-, Release- und Konfigurationsmanagement. Service Desk ist über Service-Desk-Tickets mit GoToAssist Remote Support V4 integriert.
- Mit **GoToAssist Seeit** können Kunden das Videobild ihrer Mobilgerätkamera an einen Remote-Techniker übertragen, damit dieser sich die fehlerhafte Hardware wie etwa einen falsch konfigurierten Router oder eine beschädigte Fahrzeugkomponente ansehen kann.

2 Produktarchitektur

GoToAssist Remote Support V4 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 für optimale Leistung, Zuverlässigkeit und Skalierbarkeit konzipiert. Redundante Switches und Router sind Teil der Architektur, damit es keinen „Single Point of Failure“ geben kann. Kapazitätsstarke, geclusterte Server und Backup-Systeme stellen sicher, dass Anwendungsprozesse im Falle einer hohen Auslastung oder eines Systemausfalls weiter ausgeführt werden. Service Broker verteilen die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver. Die Kommunikationsarchitektur für GoToAssist Remote Support V4 ist unten dargestellt:

GoToAssist Remote Support V4 – Technologiearchitektur



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. Die privaten Netzwerke und Backend-Server von GoTo sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und unabhängige, qualifizierte Prüfer führen regelmäßige Tests auf Schwachstellen durch.

Das GoTo-eigene Weiterleitungsprotokoll für den Schlüsselaustausch schützt unsere eigene Infrastruktur vor dem Abfangen oder Abhören von Daten. Insbesondere ermöglicht das Gateway die Verbindung zwischen dem Client und dem Host, damit sichergestellt ist, dass sich der Client unabhängig von der Netzwerkkonfiguration mit dem Host verbinden kann.

Wenn der Host bereits eine TLS-Verbindung zum Gateway aufgebaut hat, leitet das Gateway den TLS-Schlüsselaustausch des Clients über eine proprietäre Anforderung zur Neuaushandlung des Schlüssels an den Host weiter. So tauschen der Client und der Host TLS-Schlüssel aus, ohne dass das Gateway den Schlüssel erfährt.

3 Technische Sicherheitskontrollen von GoToAssist Corporate

GoTo setzt branchenübliche technische Kontrollen 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 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 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 virtuelle private Netzwerk (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 die 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. Diese Kontrollen sollen wichtige Systemdateien vor böswilliger und unbeabsichtigter Infektion oder Zerstörung schützen.

3.3. Datentrennung

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

3.4. Physische Sicherheit

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungs-kontrollen 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 Umgebungs-kontrollen

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 für diese Systeme wird regelmäßig getestet.

3.6. Schutz vor Malware

Auf allen Servern von GoToAssist Remote Support V4 ist eine Malware-Schutzsoftware mit Audit-Protokollierung installiert. Relevante 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 der GoToAssist-Produktseite sind:

GoToAssist Remote Support V4

- Die SRP-Authentifizierung auf Grundlage öffentlicher Schlüssel ermöglicht die Authentifizierung und die Einrichtung von Schlüsseln zwischen Endpunkten.
- Die Sitzungsdaten von GoToAssist Remote Support V4 sind mittels 128-Bit-AES-Verschlüsselung geschützt.
- Die Sitzungsschlüssel werden serverseitig vom Techniker generiert und verbleiben dort, um den Kunden mit dem Techniker verbinden zu können. Diese Schlüssel werden weder offengelegt noch sind sie öffentlich einsehbar.

- Kommunikationsserver leiten nur verschlüsselte Pakete weiter und verfügen nicht über den Verschlüsselungsschlüssel der Sitzung.

GoToAssist Seeit

- Die Endpunkte innerhalb der Seeit-Infrastruktur nutzen SSL-Verbindungen.
- Seeit-Sitzungen werden auf Datenbankebene mit AES-256 verschlüsselt.
- Die verschlüsselte Kommunikation zwischen Benutzer und Techniker in Seeit erfolgt über den OpenTok-WebRTC-Stapel.

GoToAssist Service Desk

- Der Dienst setzt bei der Kommunikation mit dem Browser auf Transport Layer Security (TLS) und 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard).

3.7.1. Verschlüsselung während der Übertragung

Um Kundeninhalte während der Übertragung zusätzlich zu schützen (wie in den Nutzungsbedingungen definiert), verwendet GoTo aktuelle 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.

GoToAssist Remote Support V4 bietet Datensicherheitsmaßnahmen zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Alle Rotesupport-Verbindungen sind verschlüsselt und nur für autorisierte Supportsitzungsteilnehmer zugänglich. Daten in Bildschirmübertragungen, Tastatur-/Maussteuerungsdaten, übertragene Dateien, Daten von Remotediagnosen und Informationen aus Text-Chats werden verschlüsselt, während sie temporär auf GoTo-Kommunikationsservern lagern und über öffentliche oder private Netzwerke übertragen werden.

In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: der Transmission Control Protocol(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 Komponenten der GoToAssist-Produktsuite 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.

Multicast Packet Security Layer (MPSL)

Es wurden zusätzliche Funktionen implementiert, um vollständige Sicherheit für Multicast-Paketdaten zu bieten, unabhängig von den durch TLS bereitgestellten Funktionen. Insbesondere werden alle Multicast-Sitzungsdaten durch Verschlüsselungs- und Integritätsmechanismen geschützt, die verhindern sollen, dass Personen mit Zugriff auf die Kommunikationsserver von GoTo (ob mit guten oder bösen Absichten) bei einer Remotesupport-Sitzung „mithören“ oder unerkannt Daten manipulieren können. Die MPSL bietet eine zusätzliche Ebene der Vertraulichkeit und Integrität der Kommunikation, die es nur bei GoTo-Produkten gibt.

Die Erstellung des MPSL-Schlüssels erfolgt mit einer auf öffentlichen Schlüsseln basierenden, authentifizierten SRP6-Schlüsselvereinbarung (Secure Remote Password), die einen 1024-Bit-Modulus einsetzt, um einen Wrapping Key zu erstellen.

Dieser Wrapping Key wird anschließend für die Verteilung von symmetrischen Gruppenschlüsseln mit dem AES Key Wrap Algorithm (IETF RFC 3394) verwendet. Sämtliche Schlüssel werden mit einem Generator für Pseudozufallszahlen erzeugt, der auf den einschlägigen FIPS-Standards sowie Seeding von Entropie basiert, die zur Laufzeit aus mehreren Quellen auf dem Hostcomputer erfasst wird. Diese robusten, dynamischen Methoden zur Schlüsselgenerierung und zum Schlüsselaustausch bieten einen starken Schutz gegen das Erraten und Knacken von Schlüsseln. Des Weiteren schützt die MPSL Multicast-Paketdaten vor Abhörversuchen mit Hilfe einer 128-Bit-AES-Verschlüsselung im Counter-Mode. Zur Optimierung der Bandbreite werden Klartextdaten vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert. Der Schutz der Datenintegrität wird durch Einschluss eines Integritätskontrollwerts erreicht, der mit dem HMAC-SHA-1-Algorithmus generiert wird. Die GoToAssist-Produktsuite verwendet starke, auf Branchenstandards basierende Verschlüsselungsverfahren, um die Daten von Multicast-Sitzungen vor unbefugter Offenlegung oder unbemerkten Änderungen zu schützen.

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.

GoTo kommuniziert und verwaltet Schwachstellen, indem es den Entwicklungsteams und der Verwaltung monatliche Berichte zur Verfügung stellt.

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 der GoToAssist-Produktsuite 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 Compliance-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 II 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. Sicherheitsmaßnahmen 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. Diese Richtlinien und Verfahren wurden entwickelt, um mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten von GoTo, einschließlich der GoToAssist-Produktsuite, 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 absichern. 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 Datenschutzbildung 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, d. h. der Abonnenten der GoTo-Dienste im Sinne dieses Abschnitts 5, 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 Remote Support V4 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 unseres globalen DNV 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 Remote Support V4- oder Service-Desk-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 für GoToAssist Remote Support V4 oder Service Desk werden innerhalb von dreißig (30) Tagen nach Aufforderung durch den Kunden gelöscht. Die Inhalte von GoToAssist Remote Support V4- oder Service-Desk-Kunden werden automatisch innerhalb von neunzig (90) Tagen nach Ablauf oder Beendigung der letzten Abonnementlaufzeit gelöscht. Die Inhalte von GoToAssist-Seeit-Kunden werden innerhalb von 72 Stunden nach Ende einer Sitzung 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 relevante Anbieter, die auf Informationssicherheitsdienste anbieten, dazu gehört auch die Beurteilung von Hosting-Einrichtungen Dritter. Die Rechts- und Beschaffungsabteilungsteams von GoTo 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.

8 Anhang – Begriffserklärungen

Interaktive Sitzung: Eine Supportsitzung, bei der der Kunde während der Sitzung anwesend ist und daran teilnehmen kann.

Kunde: Person, die vom Experten über eine GoToAssist Remote Support V4-Sitzung technische Unterstützung erhält.

Kunden-Desktop-App: Eine Desktop-Anwendung, die auf dem Computer des Kunden (Windows oder Mac) ausgeführt wird und über den GoToAssist Remote Support V4-Dienst eine Verbindung zu einer GoToAssist Remote Support V4-Sitzung herstellt. Sie bietet eine Remotesteuerungsfunktion sowie andere erweiterte Funktionen und die Möglichkeit, die Fernzugangs-App auf dem Computer des Kunden zu installieren.

Kundenendpunkt: Sammelbegriff, der sich auf einen beliebigen Kundenendpunkt bezieht: Kunden-Web-App, Kunden-Desktop-App, Mobile Kunden-App, Fernzugangs-Kunden-App.

Mobile Kunden-App: Eine mobile Anwendung (nur Android), die auf dem Mobilgerät/Tablet des Kunden ausgeführt wird und über den GoToAssist Remote Support V4-Dienst eine Verbindung zu einer GoToAssist Remote Support V4-Sitzung herstellt. Sie bietet Funktionen zur Bildschirmanzeige und Remotesteuerung.

Experte: Ein Benutzer von GoToAssist Remote Support V4, der GoToAssist Remote Support V4-Sitzungen initiieren kann, um Kunden per Bildschirmanzeige, Remotesteuerung oder Kameraübertragung technische Unterstützung zu leisten.

Expert Desktop App: Eine Desktop-Anwendung, die auf MacOS- und Windows-Computern ausgeführt wird und eine Verbindung zum GoToAssist Remote Support V4-Dienst herstellt.

Expert Mobile App: Eine mobile Anwendung (Android und iOS), die von einem Experten verwendet wird und eine Verbindung zum GoToAssist Remote Support V4-Dienst herstellt.

GoToAssist Remote Support V4-Sitzungen: Interaktive Sitzung mit Chat, Bildschirmanzeige, Remotesteuerung oder Kameraübertragung und Remotesteuerung per Fernzugang.

GoToAssist Remote Support V4-Dienst: Eine Gruppe von global verteilten Servern mit Lastausgleich, die über eine verschlüsselte WebSocket-Verbindung und API-Aufrufe einen sicheren Zugriff für die GoToAssist Expert Desktop-Anwendung und die Kunden-Endgeräte bieten.

Fernzugangs-Kunden-App: Eine installierbare Desktop-Anwendung (Windows und Mac), die im Hintergrund auf dem Computer des Kunden ausgeführt wird. Mit dieser App kann eine Kunden-Desktop-App heruntergeladen und ausgeführt werden, um eine Verbindung zu einer autorisierten Fernzugangssitzung herzustellen.

Fernzugangssitzung: Eine Supportssitzung, bei der der Kunde nicht anwesend ist. Die Sitzung wird vom Experten ohne Beteiligung des Kunden über eine autorisierte Fernzugangs-Kunden-App initiiert und aufgebaut.