TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN VON GOTOMYPC

DOKUMENTATION ZU ORGANISATORISCHEN SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Februar 2022

1.1. Produkte und Dienste

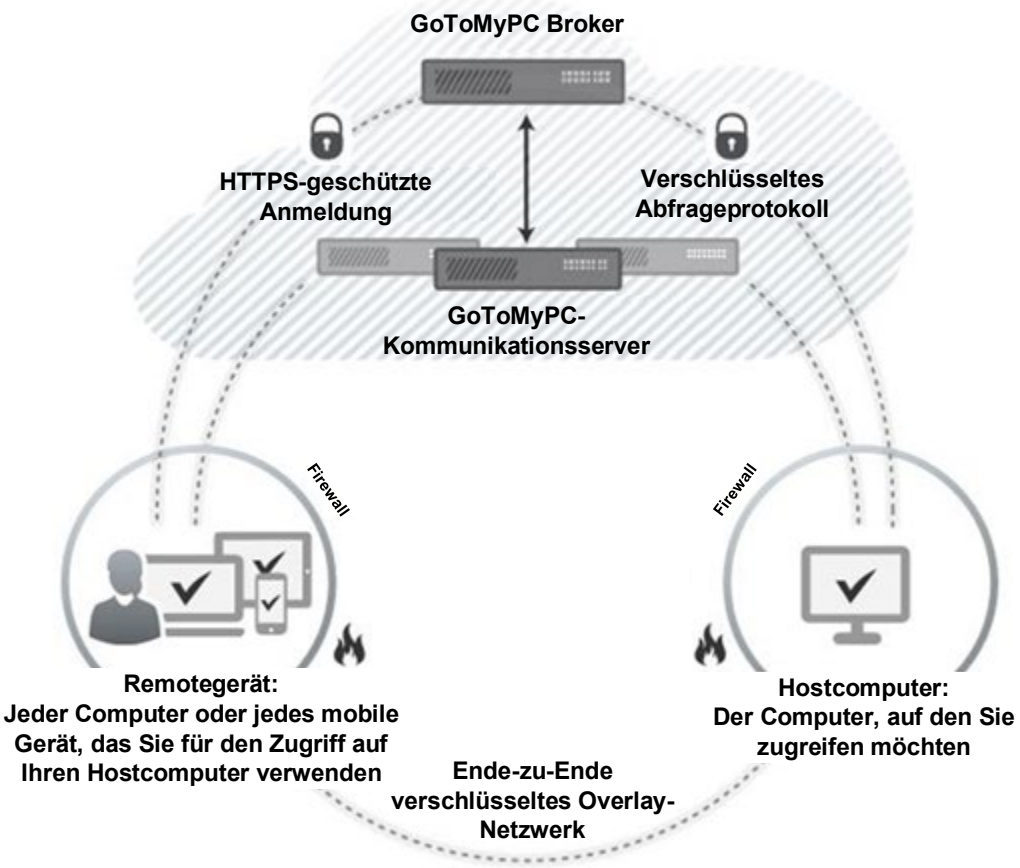
Dieses Dokument umfasst die technischen und organisatorischen Maßnahmen (TOMs) von GoToMyPC, einem gehosteten Dienst, der einen sicheren Remotezugriff von einem mit dem Internet verbundenen Windows- oder Mac-Hostcomputer über einen beliebigen Remote-Computer, iPad, iPhone oder Android-Gerät ermöglicht. Zu den Funktionen gehören ein Viewer für die Bildschirmübertragung die Dateiübertragung per Drag-and-Drop, das Drucken per Fernzugriff, das Einladen von Gästen, die Verwendung mit mehreren Monitoren, mobile Apps und ein Chat. GoToMyPC ist in drei Versionen erhältlich, um die Anforderungen von Einzelpersonen, Teams und kleinen und mittleren Unternehmen (KMU) zu erfüllen.

2 Produktarchitektur

GoToMyPC ist ein gehosteter Dienst, der aus fünf Komponenten besteht:

- *Hostcomputer:* In der Regel ein Heim- oder Bürocomputer mit permanentem Internetzugang, auf dem ein Server mit geringem Platzbedarf installiert ist. Dieser Server registriert und authentifiziert sich beim GoToMyPC Broker.
- *Browser:* Der Benutzer startet auf dem Remote-Computer (dem sogenannten Client) einen Webbrowser, besucht die sichere GoToMyPC-Website, gibt seinen Benutzernamen und sein Passwort ein und klickt auf „Verbinden“, um dem Broker eine authentifizierte, verschlüsselte Anfrage für den Zugriff auf den gewünschten Hostcomputer zu senden. Alternativ kann der Benutzer die GoToMyPC-App auf einem unterstützten Tablet oder Smartphone installieren, seine Kontodaten eingeben und auf „Verbinden“ klicken, um die Anfrage zu senden.
- *Broker:* Der Broker ist ein Vermittler, der auf Verbindungsanfragen wartet und diese registrierten Computern zuordnet. Wenn eine Übereinstimmung vorliegt, weist der Broker die Sitzung einem Kommunikationsserver zu. Als nächstes wird der Client-Viewer – ein sitzungsspezifisches ausführbares Applet – automatisch von unserem automatischen Startprogramm geladen.
- *Kommunikationsserver:* Der Kommunikationsserver ist ein Zwischensystem, das während jeder GoToMyPC-Sitzung einen nicht einsehbaren und stark komprimierten verschlüsselten Stream zwischen dem Client und dem Hostcomputer überträgt.
- *Direkte Verbindungen:* Sobald der Benutzer authentifiziert und verbunden ist, versucht GoToMyPC eine direkte Verbindung zwischen dem Client und dem Host herzustellen. Dabei wird der GoToMyPC-Kommunikationsserver nach Möglichkeit umgangen, um die Verbindungsgeschwindigkeit zu erhöhen und die Sitzungsleistung zu verbessern. Die Funktion für direkte Verbindungen weist sowohl den Client als auch den Host an, eine bestimmte Zeit lang auf eingehende Verbindungen zu warten und zu versuchen, ausgehende Verbindungen zueinander herzustellen. Je nachdem, welches Signal zuerst ankommt, wird die Verbindung hergestellt. Der Client und der Host führen dann eine auf dem SRP-Protokoll (Secure Remote Passwort) basierende authentifizierte Schlüsselvereinbarung aus und stellen eine sichere Verbindung her, die so ausgelegt ist, dass sie das Risiko für „Man-in-the-Middle“-Angriffe verringert oder beseitigt. Sollte die direkte Verbindung blockiert oder unterbrochen werden, bleibt die zuvor über den Kommunikationsserver hergestellte Verbindung für den Remotezugriff-Dienst erhalten. Die Funktion für direkte Verbindungen ist für

GoToMyPC und GoToMyPC-Pro-Konten immer aktiviert und ist für GoToMyPC Corporate optional.



Die Infrastruktur ist so konzipiert, dass sie sowohl robust als auch sicher ist. Redundante Router, Switches, Server-Cluster und Backup-Systeme werden entwickelt und eingesetzt, um eine hohe Verfügbarkeit zu gewährleisten. Um Skalierbarkeit und Zuverlässigkeit zu gewährleisten, verteilen Switches eingehende Anfragen transparent auf Webserver. Um eine optimale Leistung zu sicherzustellen, verteilt der GoToMyPC Broker die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver.

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 Kontrollen von GoToMyPC

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 Zugriffskontrollverfahren sollen die Bedrohungen des unbefugten Anwendungszugriff und des Datenverlusts sowohl in Unternehmens- als auch in 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.

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.

Die mehrschichtige Perimetersicherheit wird durch zwei Firewalls gewährleistet: eine zwischen dem Internet und den Webservern und eine weitere zwischen dem GoToMyPC Broker und den Backend-Datenbanken. Cloud-Ressourcen nutzen auch hostbasierte Firewalls. Darüber hinaus setzt GoTo Maßnahmen zum Perimeterschutz ein, einschließlich eines cloudbasierten DDoS-Präventionsdienstes eines Drittanbieters zum Schutz vor volumetrischen DDoS-Angriffen, der mindestens einmal pro Jahr getestet wird. Kritische Systemdateien sind so konzipiert, dass sie vor böswilliger und unbeabsichtigter Infektion oder Zerstörung geschützt werden.

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

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. Die Verwaltung von GoTo 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

GoToMyPC führt eine Datenbankreplikation nahezu in Echtzeit zu einem sekundären Standort durch, der sich an einem anderen geografischen Ort befindet. 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 GoToMyPC 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 einschlägigen Standardverbänden entspricht. Der kryptografische Standard wird regelmäßig überprüft, und die ausgewählten Technologien und Verschlüsselungsverfahren können je nach Risikobewertung und Marktakzeptanz neuer Standards aktualisiert werden.

3.7.1. Verschlüsselung während der Übertragung

GoToMyPC Corporate verfügt über eine integrierte 256-Bit Advanced Encryption Standard(AES)-Verschlüsselung. Der gesamte Datenverkehr zwischen dem GoToMyPC-Browser-Client und dem Hostcomputer ist stark komprimiert und verschlüsselt. GoToMyPC generiert eindeutige, geheime Verschlüsselungsschlüssel für jede Verbindung unter Verwendung einer vollständig beitragenden und gegenseitig authentifizierten Schlüsselvereinbarung.

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 es 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 von GoToMyPC 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
- 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 potenzielle Sicherheitsereignisse in den Systemen und Diensten, einschließlich GoToMyPC, 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 an die Verwaltung weiterleitet. Mitarbeiter können Sicherheitsvorfälle per E-Mail, Telefon und 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. GoToMyPC 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

GoToMyPC-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 GoToMyPC-Kunden werden außerdem 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 GoToMyPC für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo erhalten hat, dürfen die folgenden Daten nicht in GoToMyPC hochgeladen, generiert oder eingegeben 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 GoToMyPC einzuziehen oder zu empfangen.
- 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 Rechts- und Beschaffungsabteilungsteams 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.