TECHNICAL AND ORGANIZATIONAL MEASURES FOR GOTO DIGITAL ENGAGEMENT

SECURITY AND PRIVACY OPERATIONAL CONTROLS

Version 2.0 | December 2023

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for GoTo Contact. Specifically, GoTo maintains robust global privacy and security programs and organizational, administrative and technical safeguards designed to: (i) ensure the confidentiality, integrity and availability of Customer Content; (ii) protect against threats and hazards to the security of Customer Content; (iii) protect against any loss, misuse, unauthorized access, disclosure, alteration and destruction of Customer Content; and (iv) maintain compliance with applicable law and regulations, including data protection and privacy laws. Such measures include:

- **Encryption:**
  - *In-Transit* Transport Layer Security (TLS) v1.2.
  - *At Rest* Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Data Centers:** Located in the United States, Brazil, Germany, Australia, Singapore and the United Kingdom to support redundancy and stability.
- **Physical Security:** Suitable physical security and environmental controls are in place and designed to protect, control and restrict physical access for systems and servers that maintain Customer Content to support uptime, performance and scalability commitments.
- **Compliance Audits:** GoTo Contact holds SOC 2 Type II, SOC 3 Type 2, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy and APEC CBPR and PRP certifications.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA/CPRA and LGPD.
- **Security Assessments**: In addition to in-house testing, GoTo contracts with external firms to conduct regular security assessments and/or penetration testing.
- **Logical Access Controls:** Logical access controls are implemented and designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: GoTo employs a multi-tenant architecture and logically separates Customer accounts at the database level.
- **Perimeter Defense and Intrusion Detection**: Perimeter protection tools, techniques and services are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation.
- **Retention**:
  - GoTo Contact Customers may request the return or deletion of Customer Content at any time, which will be fulfilled within thirty (30) days of Customer's request.
  - Customer Content will automatically be deleted thirty (30) days after expiration of a Customer's then-final subscription term. During the subscription term, call recordings and call reports are retained for thirteen (13) months from the date they are created.

1 Products and Services

GoTo Contact is a Contact Center as a Service (CCaaS) solution built on top of the GoTo Connect platform that enables organizations to improve the outcomes of their customer and prospect communications over multiple communication channels, such as voice, text, web chat, and social media. This solution is good for organizations of all sizes but is particularly useful in small to medium sized businesses.

This document describes the Technical and Organizational Measures (TOMs) of GoTo Contact and some of GoTo Connect, on which GoTo Contact is built.

The following are features and offerings within the GoTo Contact service (the Service):

- GoTo Contact is designed to help users manage call queues and incoming customer calls through interactive voice responses, automatic call distribution and customer relationship management integrations.

- Chat Queues allow people to send a message to a queue and have that message delivered to a company representative (rep) as if the external number were the rep’s direct number. Chat queue messages can be sent through different communication channels: Text, Web Chat, Facebook, and other social media channels.

- Other channels can aid customer communication, such as voice to video and chat to video.

- GoTo Contact analytics provides real-time and historical reporting enabling supervisors and managers to improve customer interactions, optimize customer experience, optimize rep time to service customers and to coach representatives on their communication skills.

2 Product Architecture

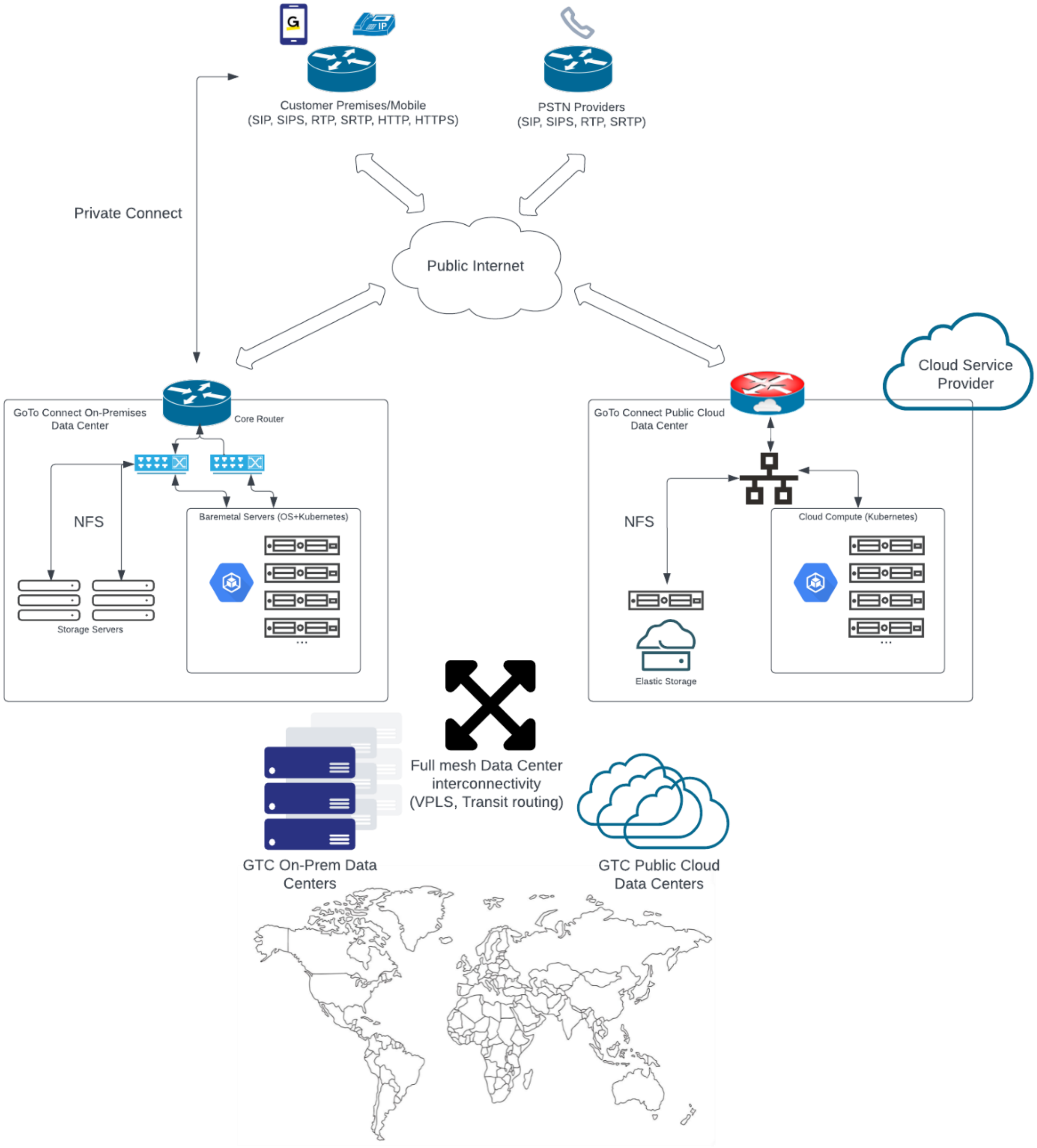
G
IP
Customer Premises/Mobile
(SIP, SIPS, RTP, SRTP, HTTP, HTTPS)
PSTN Providers
(SIP, SIPS, RTP, SRTP)
Private Connect
Public Internet
Cloud Service Provider
GoTo Connect On-Premises Data Center
Core Router
NFS
Baremetal Servers (OS+Kubernetes)
Storage Servers
GoTo Connect Public Cloud Data Center
NFS
Cloud Compute (Kubernetes)
Elastic Storage
Full mesh Data Center interconnectivity (VPLS, Transit routing)
GTC On-Prem Data Centers
GTC Public Cloud Data Centers

Figure 1- GoTo Contact Infrastructure

3 GoTo Contact Technical Controls

GoTo employs industry standard technical security controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service) designed to safeguard the

Service infrastructure and data residing therein. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

3.1 Logical Access Control

Logical access controls are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or “least privilege”) access to specified GoTo systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

The GoTo Contact integrated Service offering utilizes GoTo’s proprietary identity management platform for customer provisioning, offers Single sign-on (SSO) using Security Assertion Markup Language (SAML), and integrates directly with the platform via API. This permits robust administrative controls, including allowing Customer account administrators to configure password policies, force password resets, and require utilization of SAML for login.

Service PBX administrators (Super Administrators) can grant or deny specific permissions in the PBX Administration Portal and grant GoTo Contact Admin role permissions to users of the GoTo. These group permissions include the ability to configure the PBX, edit E911 addresses/locations, view reports, view and pay invoices, as well as create, update, and delete settings and accounts for:

- Users;
- User Groups;
- Extensions;
- Devices;
- Hardware;
- Sites; and
- Phone Numbers (delete and create managed through number ordering).

User level permissions are not directly configured as they are derived from the user, device, and line relationships.

For more details on group permissions, please reference the GoTo Connect Administrator PBX Guide.

3.2 Perimeter Defense and Intrusion Detection

GoTo employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

The Service leverages a multi-tenant (and multi-PBX) architecture, logically separated at the database level, based on a user’s or organization’s Service account. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Datacenter Physical Security

GoTo contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant datacenter
- Scheduled maintenance and validation of all critical security and environmental controls

GoTo limits physical access to production datacenters to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. GoTo management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.5 Data Backup, Disaster Recovery and Availability

In order to provide redundancy, call failover, scalability, and high availability, the Service uses a containerized microservice mesh which allows for rapid deployment and scaling of services to satisfy the needs of GoTo's customers. This full-mesh design allows for microservices to self-discover and self-recover in the event of an outage at any specific datacenter or in the event of an issue localized geographically on the public Internet. Services are designed to fail-over between datacenters automatically.

The infrastructure is connected between datacenters in the form of "clusters" with interconnectivity of a Virtual Private LAN Service (VPLS)/mesh network. VPLS connections can fail-over to a Dynamic Multipoint Virtual Private Network (DMVPN) in case primary links go offline. Each site has multiple peering connections with the public Internet. All production datacenters are connected in such a manner that internal applications can reach services from any location. Each datacenter is hosted in private hardware (rack blades).

Connectivity to the Public Switch Telephone Network (PSTN) is made from each datacenter location to multiple PSTN Partners/providers via Session Initiation Protocol (SIP) trunks through the public Internet.

In order to provide high availability, GoTo operates a network of datacenters in a fully interconnected mesh. These datacenters operate with a capacity of N+1 datacenters, meaning that the Service has been designed to sustain the failure of the equivalent of one datacenter worth of capacity, and still have the ability to maintain uptime by automatically forwarding traffic to additional datacenter sites.

3.6 Malware Protection

Anomalous activity alerting capabilities are actively deployed and monitored on the Service. Alerts indicating potential malicious activity are sent to appropriate response teams for resolution or mitigation.

3.7 Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption

The Service provides end-to-end data security measures. The Service is designed to ensure that communication data is not exposed in unencrypted form with communication servers or during transmission across public or private networks.

Internet Engineering Task Force (IETF) standard Transport Layer Security (TLS) protocols are used to protect communication between endpoints. All network traffic flowing in and out of GoTo datacenters, including all Customer Content, is encrypted in transit. See the Terms of Service for more information.

For their own protection, GoTo recommends that customers configure their browsers to use strong cryptography by default whenever possible and to ensure that operating system and browser security patches are kept up to date.

When TLS connections are established GoTo servers authenticate themselves to clients using public key certificates. TLS is also supported for signaling between physical phones and the Service infrastructure to secure the traffic and communication when supported by Customer equipment. Media is transmitted using Secure Real-time Transport Protocol (sRTP) utilizing shared keys transmitted over Session Initiation Protocol Secure (SIPS) to secure audio traffic. Provisioning information containing the physical phones credentials from the Service’s infrastructure to the phones are also secured using TLS.

At-Rest Encryption

Customer voicemail recordings, voicemail greetings, and call recordings are encrypted at-rest using 256-bit AES encryption when stored with GoTo’s cloud storage

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted on no less than a monthly basis. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams.

3.9 Logging and Alerting

GoTo collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

GoTo maintains a comprehensive set of organizational and administrative controls designed to protect the security and privacy posture of the service.

4.1 Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

GoTo complies with applicable legal, financial, data privacy, and regulatory requirements, and maintains compliance with the following certifications and external audit reports:

- TRUSTe Enterprise Privacy & Data Governance Practices Certification to address operational privacy and data protection controls that are aligned with key privacy laws and recognized privacy frameworks. To learn more, please visit our blog post.
- American Institute of Certified Public Accountants' (AICPA) Service Organization Control (SOC) 2 Type 2 attestation report. BSI Cloud Computing Catalogue (C5).
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Payment Card Industry Data Security Standard (PCI DSS) compliance for GoTo's eCommerce and payment environments
- Internal controls assessment as required under a Public Company Accounting Oversight Board (PCAOB) annual financial statements audit

4.3 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with GoTo's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the GoTo intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

GoTo’s application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the GoTo Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

GoTo employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire onboarding kits, awareness campaigns, webinars with the CISO, a security champion program and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

GoTo takes the privacy of its Customers, the subscribers to the GoTo Services, and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. GoTo Contact is compliant with the applicable provisions of GDPR. For more information, please visit https://www.goto.com/company/trust/privacy.

5.2 CCPA

GoTo hereby represents and warrants that it is in compliance with the California Consumer Privacy Act (CCPA). For more information, please visit https://www.goto.com/company/trust/privacy.

5.3 Data Protection and Privacy Policy

GoTo is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs GoTo's processing of Personal Data.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of GoTo's technical and organizational measures. Additionally, to account for CCPA, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that GoTo will not sell our users' 'personal information.'

For visitors to our webpages, GoTo discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on the public website. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.4 Transfer Frameworks

GoTo has a robust global data protection program which takes into account applicable laws and supports lawful international transfers under the following frameworks:

5.4.1. Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the European Economic Area ("EEA") will be transferred in compliance with EU data-protection law. GoTo has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. GoTo offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope GoTo services as part of its global DPA. Execution of the SCCs helps ensure that GoTo customers can freely move data from the EEA to the rest of the world.

Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created the following FAQ designed to outline its supplemental measures utilized to support lawful transfers under Chapter 5 of the GDPR and address and guide any "case-by-case" analyses recommended by the European Court of Justice in conjunction with the SCCs.

5.4.2. APEC CBPR and PRP Certifications

GoTo has additionally obtained Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP") certifications. The APEC CBPR and PRP frameworks are the first data regulation frameworks approved for the transfer of personal data across APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance.

5.5 Return and Deletion of Customer Content

Customers may request the return or deletion of their Content through standardized interfaces at any time. If these interfaces are not available or GoTo is otherwise unable to complete the request, GoTo will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request. Upon expiration or termination of a Customer's account, Customer's Content shall automatically be deleted thirty (30) days after the effective date of the account expiration or termination. Upon written request, GoTo will certify to such Content deletion.

5.6 Sensitive Data

While GoTo aims to protect and safeguard all Customer Content, regulatory and contractual limitations require us to restrict the use of GoTo Contact for certain types of information. Unless Customer has written permission from GoTo, the following data must not be uploaded or generated to GoTo Contact:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) as identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as other relevant applicable laws and regulations.
- Information related to financial accounts and payment instruments, including – but not limited to – credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by GoTo to collect payment for the Service.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics

GoTo is continuously improving its websites and products using third-party web analytics tools which help GoTo understand how visitors use its websites, desktop tools, and mobile applications, as well as user preferences and problems. For further details please reference the Privacy Policy.

6 Third Parties

6.1 Use of Third Parties

As part of GoTo’s internal assessment and processes related to vendor and third-party management, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by GoTo are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, GoTo reviews relevant third party’s terms and conditions and either utilizes GoTo-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting GoTo

Customers can contact GoTo at https://support.goto.com for general inquiries or privacy@goto.com for privacy-related questions.