Technical and Organizational Measures
GoTo Connect

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for GoTo Connect. 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).
  - *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 Connect holds SOC 2 Type II, 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 Connect 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.

Table of Contents

Click the page numbers below to go to the relevant TOMs section

1 Product Introduction

GoTo Connect is an all-in-one Unified Communications as a Service (UCaaS) solution for enterprises and businesses. It combines cloud-based Voice-over-Internet Protocol (VoIP) phone systems with the web, audio and video conferencing services of GoTo Meeting* in one simple, reliable and flexible collaboration solution (the "Service").

The Service includes the following features and offerings:

- GoTo Connect's cloud-based phone service is designed to replace traditional, on-premise Private Branch Exchange (PBX) phone equipment. The PBX administration portal allows Users with administrator permissions to view and make universal changes to system settings from any device with an internet connection.
- Public Switched Telephone Network (PSTN) replacement services (including phone numbers and minutes) are provided through partnerships with some of the world's leading telecommunications providers.
- Visual dial plan editor is a call flow editing tool that can direct calls to specific voicemail boxes, auto attendants or ring groups or set up wait times.
- GoTo Connect business continuity (formerly known as 'JBC') is an optional, premium service and hardware offering installed on the premises of an individual using the Service ("User") that provides local phone service via an independent third-party whose services are separately procured by a User in the event of a network outage.

*For more information about the GoTo Meeting Service and its technical and organizational measures, consult the GoTo Meeting TOMs available at https://www.goto.com/company/trust/resource-center.

Capitalized terms in this document that are not defined within the text are defined in the Terms of Service.

2 Technical Measures

GoTo's products are designed to provide solutions that are secure, reliable and private. The technical measures defined below describe how GoTo implements that design and applies it in practice.

2.1 Safeguards

GoTo's implementation of safeguards, features and practices involves:

I. Building products that take security and privacy by design and default into account, and including additional layers of security in order to protect Customer Content;

II. Maintaining organizational controls that operationalize internal policies and procedures related to standards compliance, incident management, application security, personnel security and regular training programs; and

III. Ensuring privacy practices are in place to govern data handling and management in accordance with applicable law, including the GDPR, CCPA/CPRA, LGPD, as well as with our own Data Processing Addendum (DPA), and applicable GoTo policies and commitments.

By building security safeguards into the product, we strive to protect GoTo Customer Content from threats and ensure security controls are appropriate to the nature and scope of the Services. GoTo's configurable security features can help administrators minimize threats and risks to systems and networks posed by individuals who use GoTo services.

3 Product Architecture

The diagram below (Figure 1) shows the GoTo Connect network architecture.

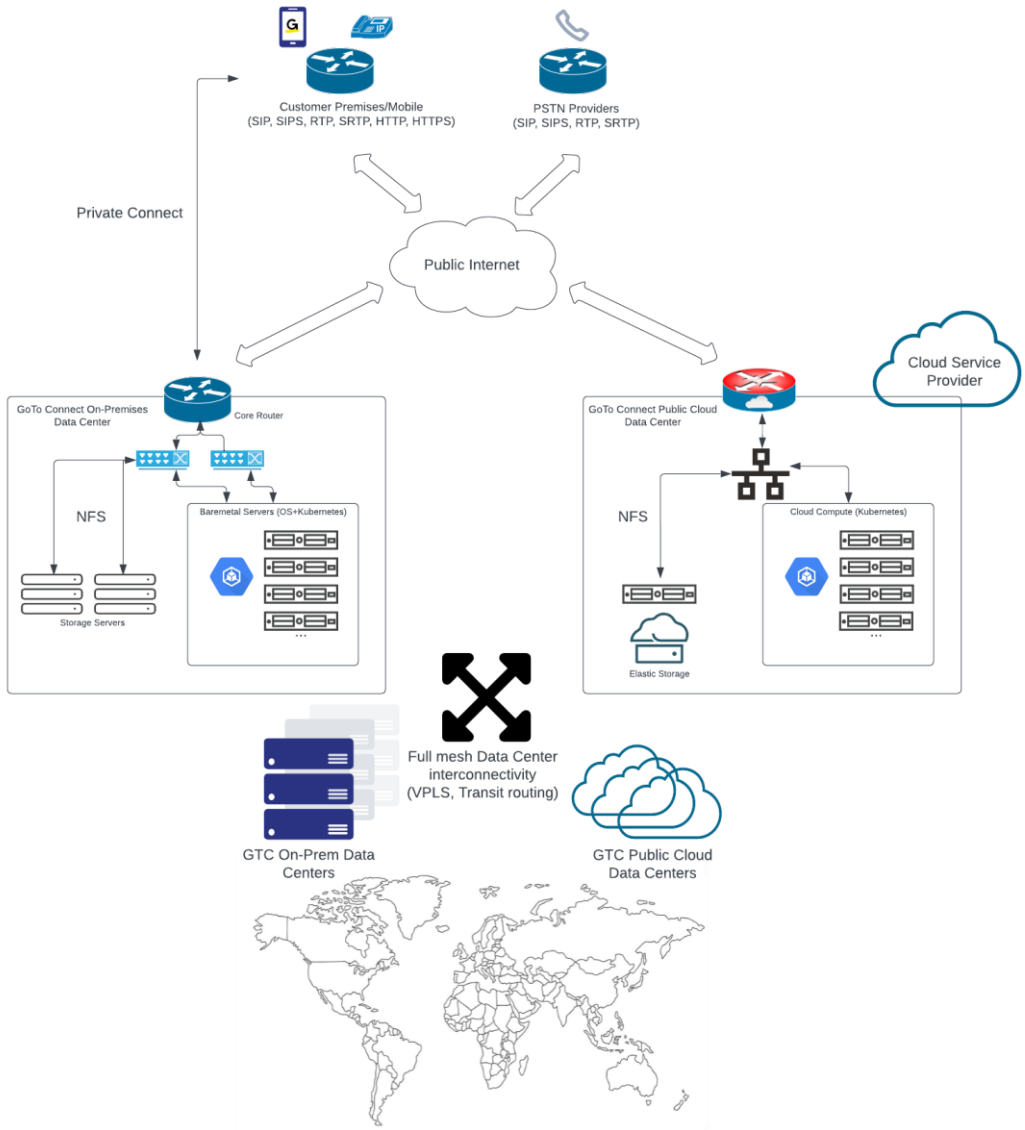

Figure 1: GoTo Connect Architecture

4 Technical Security Controls

GoTo employs technical security controls that are designed to safeguard the Service infrastructure and data residing therein.

4.1 Encryption

GoTo regularly reviews its encryption standards and may update the ciphers and/or technologies used in accordance with the assessed risk and market acceptance of new standards.

4.2 Encryption In Transit

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

Internet Engineering Task Force (IETF) standard TLS protocols are used to protect communication between endpoints. All network traffic flowing in and out of data centers that hold GoTo data, including all Customer Content, is encrypted in transit.

When TLS connections are established, GoTo servers authenticate themselves to clients (i.e., workstations or devices), using public key certificates. When supported by User equipment, TLS is used to secure the traffic between User equipment and the Service's infrastructure. TLS also secures the transfer of provisioning information, which includes the physical phone's credentials, from the Service's infrastructure to the phones. Media is transmitted using Secure Real-time Transport Protocol (SRTP) while audio traffic is secured using shared keys transmitted over Session Initiation Protocol Secure (SIPS).

4.3 Encryption At Rest

Voicemail recordings, voicemail greetings, and call recordings are encrypted at rest using 256-bit AES encryption when stored in GoTo's cloud storage.

4.4 User Authentication

GoTo Connect provisions User access using GoTo's proprietary identity management platform, uses Security Assertion Markup Language (SAML) to offer single sign-on (SSO), and integrates directly with the GoTo platform via API. The identity management platform supports administrative controls related to User authentication including configuring password policies, forcing password resets and requiring utilization of SAML for login.

Service PBX administrators (super administrators) can grant or deny specific permissions in the PBX administration portal. These permissions include the ability to configure the PBX, edit E911 addresses/locations, view reports, view and pay invoices and update and delete settings and accounts for:

- Users;
- User Groups;
- Extensions;
- Devices;
- Hardware;

- Sites; and
- Phone Numbers (deletion and creation of phone numbers is managed through the phone number ordering process).

For more details on group permissions in PBX administration, visit the Getting Started Guide for Admins.

5 Security Program Updates

GoTo reviews and updates our security program and engages independent third parties to assess our relevant security controls at least annually to ensure we evolve against the current threat landscape and to ensure compliance with relevant frameworks, industry standards, Customer commitments and, as applicable, changes in laws and regulations pertaining to the security of GoTo data.

6 Data Backup, Disaster Recovery and Availability

GoTo Connect's architecture is designed to perform replication in near real time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. In the event of a disaster or total site failure in any one of the multiple active locations, the remaining locations are designed to balance the application load. Disaster recovery related to these systems is tested periodically.

To provide high availability, GoTo operates a network of data centers in a fully interconnected mesh. These data centers operate with a capacity of N+1 data centers, meaning that the Service has been designed to sustain the failure of one data center worth of capacity and still maintain uptime by automatically forwarding traffic to additional data center sites.

Specifically, the Service uses a containerized microservice platform that allows for rapid deployment and scaling of services and provides redundancy, call failover, scalability, and high availability to Users. This full mesh design allows for microservices to self-discover and self-recover in the event of an outage at any specific data center or in the event of an issue localized geographically on the public internet. The Service is designed to automatically fail over between data centers.

The infrastructure is connected between data centers in the form of "clusters" with interconnectivity of a meshed Virtual Private LAN Service (VPLS) network and transit routing. VPLS connections can fail over to an encrypted Dynamic Multipoint Virtual Private Network (DMVPN) over internet links in case primary links go offline. Cloud data centers are connected to regional cloud provider locations by encrypted tunnels that protect data by keeping it off the public internet until necessary. All production data centers are connected to each other to allow internal applications to reach services from any location. GoTo Connect data is hosted on premise in private hardware (rack blades) or in cloud-hosting provider data centers following a similar but adapted architecture. Each data center location connects to multiple PSTN partners/providers via Session Initiation Protocol (SIP) trunks through the public internet.

7 Data Centers

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using:

a) redundant, active-active data centers; or
b) cloud hosting provider data centers.

Hosting data centers are located in the United States, Brazil, Germany, Australia, Singapore and the United Kingdom.

All data centers include monitoring of environmental conditions and have around-the-clock physical security measures addressed below.

7.1 Data Center Physical Security

GoTo contracts with data centers to provide physical security and environmental controls for systems and servers that contain Customer Content. These controls include the following:

- Video surveillance and recording;
- Heating, ventilation and air conditioning temperature control;
- Fire suppression and smoke detectors;
- Uninterruptible power supply;
- 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 data center; and
- Scheduled maintenance and validation of all critical security and environmental controls.

GoTo limits physical access to production data centers 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 GoTo's technical operations team. All physical access to data centers and server rooms is logged and GoTo management reviews logs on at least a quarterly basis. Additionally, data center physical access authorization is removed promptly upon role change (where such access is no longer required) or upon termination of any previously authorized personnel. Multi-factor access (e.g., biometrics, badge and keypad) is required for highly sensitive areas, which include data centers.

8 Standards Compliance

GoTo regularly assesses its compliance with applicable legal, security, financial, data privacy and regulatory requirements. GoTo's privacy and security programs have met rigorous and internationally recognized standards, been assessed in accordance with comprehensive external audit standards and achieved key certifications, including:

- **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, visit our blog post.

- **TRUSTe APEC CBPR and PRP Certifications** for the transfer of Customer Content between APEC-member countries obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance. To learn more about our APEC certifications, click here.
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Type II** attestation report incl. **BSI Cloud Computing Catalogue (C5)**.
- **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.

9 Application Security

GoTo's application security program follows the Microsoft Security Development Lifecycle (SDL) to secure product code. The Microsoft SDL program includes manual code reviews, threat modeling, static code analysis, dynamic analysis and system hardening. GoTo teams also periodically perform dynamic and static application vulnerability testing and penetration testing activities for targeted environments.

10 Logging, Monitoring and Alerting

GoTo maintains policies and procedures around logging, monitoring and alerting, which set out the principles and controls that are implemented to bolster our ability to detect suspicious activity and respond to them on a timely basis. GoTo collects identified anomalous or suspicious traffic in relevant security logs in applicable production systems.

11 Endpoint Detection and Response

Endpoint Detection and Response software with audit logging is deployed on all GoTo servers to minimize disruption or impact on the performance of the Service. Security investigations will be initiated in accordance with our incident response procedures if suspicious activity is detected, as appropriate and necessary. See section 17 for more information on GoTo's Security Operations Center and incident response procedures.

12 Threat Management

GoTo's Cyber Security Incident Response Team ("CSIRT") is comprised of multiple teams and is responsible for cyber threat protection. Specifically, the Cyber Threat Intelligence team within the CSIRT collects, vets and disseminates information as it pertains to current and emerging threats. GoTo stays current with threat intelligence and mitigation through review of open and closed sources and participation in sharing groups and industry memberships (IT-ISAC, FIRST.org, etc.).

13 Security and Vulnerability Scanning and Patch Management

GoTo maintains a formal patch management program and, on at least a quarterly basis, performs patch management activities on all relevant systems, devices, firmware, operating systems, applications and other software that process Customer Content. GoTo assesses and scans for system-level, internal and external host/network ("Systems") vulnerabilities, on no less than a monthly basis, as well as after any material change to such Systems and remediates relevant discovered vulnerabilities in accordance with documented policies that prioritize remediation based on risk.

14 Logical Access Control

Logical access control procedures are in place to reduce the risk of unauthorized application access and data loss in corporate and production environments. Employees are granted access to specified GoTo systems, applications, networks and devices based on the principle of least privilege. User privileges are segregated based on functional role (role-based access control) and environment using segregation of duties controls, processes and/or procedures.

15 Data Segregation

GoTo has implemented controls to prevent Users from seeing the data of other Users. For instance, GoTo leverages a multi-tenant (and multi-PBX) architecture, logically separated at the database level, based on a User's or organization's GoTo account. Parties must be authenticated to gain access to an account.

16 Perimeter Defense and Intrusion Detection

GoTo uses perimeter protection tools, techniques and services to protect against unauthorized network traffic entering GoTo's product infrastructure. These include, but are not limited to:

- Intrusion detection systems that monitor systems, services, networks and applications for unauthorized access;
- Critical system and configuration file monitoring;
- Web application firewall (WAF) and application-layer DDoS prevention services that proxy GoTo traffic;
- A local application firewall that provides an additional layer of protection against OWASP top ten and other web application vulnerabilities and malicious traffic; and
- Host-based firewalls on GoTo web servers that filter inbound and outbound connections, including internal connections between GoTo systems.

17 Security Operations and Incident Management

GoTo's Security Operations Center is responsible for detecting and responding to security events. The Security Operations Center uses security sensors and analysis systems to identify potential

issues and has developed incident response procedures, including a documented Incident Response Plan.

GoTo's Incident Response Plan is aligned with our critical communication processes, policies and standard operating procedures. It is designed to manage, identify and resolve relevant suspected or identified security events across its systems and services, including GoTo Connect. The Incident Response Plan sets out mechanisms for employees to report suspected security events and escalation paths to follow when appropriate. Suspected events are documented and escalated as appropriate via standardized event tickets and triaged based upon criticality.

18 Deletion and Return of Content

Deletion and/or Return: Customers may request return and/or deletion of their Customer Content by submitting a request using GoTo's Individual Rights Management Portal ("IRM"), via support.goto.com, or by e-mailing privacy@goto.com. Requests shall be processed within thirty (30) days of receipt by GoTo, however, in the unlikely event we need more time, we will provide notice as soon as possible of any anticipated delayed and revised completion deadline.

Customer Content Retention Schedule: Unless otherwise required by applicable law Customer Content shall automatically be deleted thirty (30) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription. During the Customer's subscription term, call recordings and call reports are deleted on a rolling basis and retained for thirteen (13) months from the date they are created. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

19 Organizational Controls

19.1 Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures that are periodically reviewed and updated as necessary to support GoTo's security objectives, changes in applicable law, industry standards and compliance efforts.

19.2 Change Management

GoTo maintains a suitable change management process and changes to GoTo Systems are assessed, tested and approved before implementation to reduce the risk of disruption to GoTo services.

19.3 Security Awareness and Training Programs

GoTo's privacy and security awareness program involves training employees about the importance of handling Personal Data and confidential information ethically, responsibly, in compliance with applicable law, and with due care. Newly hired employees, contractors and interns are informed of security policies and the GoTo Code of Conduct and Business Ethics during onboarding. GoTo Employees complete privacy and security awareness training at least annually. Awareness activities take place throughout the year and can include campaigns for Data Privacy Day, Cybersecurity Awareness Month, webinars with the Chief Information Security Officer and a security champions program.

Where appropriate, employees may also be required to complete role-specific trainings. Additionally, all GoTo employees, contractors and subsidiaries must review and adhere to GoTo's policies related to security and data protection.

20 Privacy Practices

GoTo takes the privacy of our Customers and Users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

20.1 Privacy Program

GoTo maintains a comprehensive privacy program that involves coordination from multiple functions within the company, including Privacy, Security, Governance, Risk and Compliance (GRC), Legal, Product, Engineering and Marketing. This privacy program is centered around compliance efforts and involves the implementation and maintenance of internal and external policies, standards and addenda to govern the company's practices.

20.2 Regulatory Compliance

20.2.1 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law regarding data protection and privacy for individuals within the EU. GoTo maintains a comprehensive GDPR compliance program and to the extent GoTo engages in processing of Personal Data subject to the GDPR on behalf of the Customer, we will do so in accordance with the applicable requirements of the GDPR. For more information, visit https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively referred to as "CCPA") grants Californians additional rights and protections regarding how businesses may use their personal information. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the CCPA on behalf of the Customer, we will do so in accordance with the applicable requirements of the CCPA. For more information about our compliance with the CCPA, see GoTo's Privacy Policy and Supplemental California Consumer Privacy Act Disclosures.

20.2.3 LGPD

The Brazilian Data Protection Law (LGPD) regulates the processing of Personal Data in Brazil and/or of individuals located in Brazil at the time of collection. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the LGPD on behalf of the Customer, we will do so in accordance with the applicable requirements of the LGPD. For more information, visit https://www.goto.com/company/trust/privacy.

20.3 Data Processing Addendum

GoTo offers a global Data Processing Addendum (DPA), available in English and German. This DPA meets the requirements for GDPR, CCPA, LGPD and other applicable regulations and governs GoTo's processing of Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including:

(a) data processing details and sub-processor disclosures as required under Article 28;
(b) revised (2021) Standard Contractual Clauses (a.k.a. the EU Model Clauses); and
(c) GoTo's product-specific technical and organizational measures.

Additionally, to account for CCPA requirements, our global DPA includes:

(a) revised definitions mapped to the CCPA;
(b) access and deletion rights; and
(c) warranties that GoTo will not sell our Customer's or Users' personal information.

Our global DPA also includes provisions to:

(a) address GoTo's compliance with the LGPD;
(b) support lawful transfers of Personal Data to/from Brazil; and
(c) ensure that our Users enjoy the same privacy benefits as our other global Users.

20.4 Transfer Frameworks

GoTo supports lawful international data transfers under the following frameworks:

20.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), sometimes referred to as EU Model Clauses, are standardized contractual terms, recognized and adopted by the European Commission, to ensure that any Personal Data leaving the European Economic Area (EEA) will be transferred in compliance with EU data protection law. The SCCs, revised and issued in 2021, are incorporated in GoTo's global DPA to enable GoTo Customers to transfer data out of the EEA in compliance with the GDPR.

20.4.2 Data Privacy Framework

The EU-U.S. and Swiss-U.S. Data Privacy Frameworks (DPF) and the UK Extension to the EU-U.S. DPF are voluntary frameworks that, respectively, provide mechanisms for companies to transfer personal data from the EU, Switzerland and the UK to the U.S. in compliance with the data protection regulations in these jurisdictions. GoTo complies with each of these frameworks regarding the collection, use, and retention of personal data from the EU, Switzerland, and the UK, respectively. To learn more about the DPF, and to view GoTo's certification, please visit the DPF website.

20.4.3 APEC CBPR and PRP Certifications

GoTo has 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 between APEC-member countries and were obtained and

independently validated through TrustArc, an APEC-approved third-party data protection compliance vendor.

20.4.4 Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created an FAQ designed to outline the supplemental measures implemented 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 use of the SCCs.

20.5 Data Requests

GoTo maintains comprehensive processes to facilitate receiving data protection and security-related requests, including the IRM portal, Privacy email address (privacy@goto.com) and Customer support at https://support.goto.com.

20.6 Sub-Processor and Data Center Disclosures

GoTo publishes Sub-Processor Disclosures on its Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). These disclosures show the names, locations and processing purposes of data hosting providers and other third parties that process Customer Content as a part of providing the Service to GoTo Customers.

20.7 Sensitive Data Processing Restrictions

Unless expressly requested by GoTo or Customer has otherwise received written permission from GoTo, the following types of sensitive data must not be uploaded to GoTo Connect or otherwise provided to GoTo:

- 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.

20.8 Compliance in Regulated Environments

Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of GoTo Connect in regulated environments.

21 Security and Privacy Third-Party Controls

Prior to engaging third-party vendors that process Customer Content or confidential, sensitive, or employee data, GoTo reviews and analyzes the vendor's security and privacy practices using the appropriate Procurement channels. As appropriate, GoTo may obtain and evaluate compliance

documentation or reports from vendors periodically to ensure their control environment and standards continue to be sufficient.

GoTo enters into written agreements with all third-party vendors and either utilizes GoTo-approved procurement templates or negotiates such third parties' standard terms and conditions to meet GoTo-accepted privacy and security standards, where deemed necessary. The Finance, Legal, Privacy and Security teams are involved in the vendor review process and verify that vendors meet specific mandatory data handling and contractual requirements, as necessary and/or appropriate. GoTo's third party risk policies govern privacy and security requirements of vendors in light of the type and duration of data processing and level of access. Where appropriate (e.g., where Customer Content is processed or stored), agreements with vendors include "compliance with applicable law" requirements, a DPA or similar document that addresses topics such as GDPR, CCPA, LGPD and use and sale restrictions, as appropriate. For instance, GoTo's Supplier DPA has restrictions around data "selling" as defined under the CCPA. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors.

22 Contacting GoTo

Customers can contact GoTo at support.goto.com for general inquiries. For questions or requests related to Personal Data or privacy, please visit our IRM portal or send an email to privacy@goto.com.