Technical and Organizational Measures
GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage. 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) or Datagram Transport Layer Security (DTLS)
  - *At Rest* Transparent Data Encryption (TDE) and Advanced Encryption Standard (AES) 256-bit for Customer Content that is encrypted at rest.
- **Data Centers:** GoTo makes use of cloud hosting providers employing measures to provide high logical and physical security, availability, and scalability.
- **Compliance Audits:** GoTo Meeting, GoTo Webinar and GoTo Training hold SOC 2 Type II, 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 storage layer.
- **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.
- **Data Retention**:
  - GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage 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.
  - For GoTo Meeting, GoTo Webinar and GoTo Training, Customer Content will automatically be deleted between ninety and one hundred (90-100) days after expiration of a Customer's then-final subscription term.

Table of Contents

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

1 Product Introduction

GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage (together, the "Service") are online communication solutions that enable individuals and organizations to interact using various features, depending upon service offering, including desktop screen sharing, video conferencing, chat, and integrated audio. GoTo Meeting, GoTo Webinar, GoTo Training, and GoTo Stage share infrastructure and are delivered via a CDN to web browsers or installable applications.

- GoTo Meeting, GoTo Webinar and GoTo Training enable organizers to schedule, convene, and moderate online sessions including audio, webcam, screen sharing and more using the GoTo web, desktop and mobile applications.
- GoTo Training provides specific features applicable to web-based training, such as online access to tests and materials and a hosted course catalog.
- GoTo Webinar provides special support to conduct one-to-many information presentation events reaching local and global attendees over the internet.
- GoTo Stage is an extension of GoTo Webinar where GoTo Webinar organizers can create customizable channels and publish their webinar recordings. Published recordings are showcased on the GoTo Stage homepage, organized by business categories. At any point, organizers can unpublish their recording through GoTo Webinar, which removes the video from their channel page and the GoTo Stage ecosystem.

1.1 Conference Management and Registration

Organizers can schedule sessions directly within the Service. They can adjust various settings of upcoming sessions and prepare their content and attendees.

1.2 Audio

Integrated audio conferencing for GoTo Meeting, GoTo Webinar and GoTo Training sessions is available through Voice over Internet Protocol (VoIP) and the public switched telephone network (PSTN).

1.3 Video

All products offer high quality webcam video that adjusts to a user's bandwidth and latency.

1.4 Content Uploading (Webinar and Training only)

Organizers can upload files and media for use during sessions, either ahead of a session or once the session has started.

1.5 Session Reporting

Organizers can see participation statistics and other session statistics in their session history.

1.6 Recording and Transcripts

Sessions can be recorded locally and to the cloud. Account administrators and session organizers can choose to enable cloud recordings in addition to or instead of local recordings. Local

recordings are stored on the organizer's system and are not subject to GoTo's retention limits, set out in section 18 (Deletion and Return of Content) below.

When this feature is enabled by the administrator and the organizer, cloud recordings are automatically available directly in the organizer's session history and transcripts are automatically created. Session recording transcripts are created using either the GoTo hosted models or Google Cloud Speech-to-Text technology.

For **GoTo Meeting**, an account administrator can choose to enable recordings and decide whether those are stored locally or in the cloud. If cloud recordings are enabled, the meeting organizer can choose to record a given meeting and store it in the cloud. Transcripts are automatically created for cloud recordings.

For **GoTo Webinar**, organizers can choose to auto-transcribe all cloud recordings. Only an organizer can start a recording and if their auto-transcribe setting is enabled, a transcript will be created.

For **GoTo Training**, account administrators can control whether organizers are able to save recordings to the cloud. Account administrators are not able to prevent organizers from recording sessions locally. Trainings cannot be transcribed.

1.7 Business Messaging (Meeting only)

An extension of GoTo Meeting, business messaging allows GoTo Meeting users to see the presence status of other users within their account, exchange instant messages and share files. The account administrator defines the scope for visibility and discoverability of various users.

Business messaging users can see the presence status of any other user within their account once they are included in their contact list. Messages can be exchanged with all members of a team and with external users if they have been explicitly included via an invite by email. External users are business messaging users who are not members of a Customer's internal team (e.g., customer, prospect, or partner). Messages can be direct (between two participants), in a private group or in a public group.

Users can also share other content within business messaging by uploading and downloading files. The shared files are available for download by all users with access to the messages in a given conversation or group.

1.8 Webcast (Webinar only)

GoTo Webinar webcasts use broadcast gateways, third-party streaming engines and content delivery networks designed to reliably deliver screen sharing, audio, and video media to attendees joining from a web browser. The gateways receive media data from the media servers and transcode them into standard codecs. The streaming engine produces HTTP Live Streaming (HLS) at multiple bitrates to enable adaptive delivery for users with sub-optimal network connections.

1.9 GoTo Stage (Webinar only)

Videos published to GoTo Stage are available for discovery on the GoTo Stage homepage and in search engine results, unless the organizer restricts discoverability using the administrative

settings on their channel page. Undiscoverable recordings can be accessed by anyone registered to GoTo Stage using a direct URL to the channel or to the video's unique "Watch Now" page. Visitors register for GoTo Stage using their name and email address or may connect via select social media accounts such as LinkedIn, Facebook, and Gmail. The URLs for visitors to access videos are live for a limited amount of time to limit unwanted sharing.

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 for GoTo Meeting, GoTo Webinar, GoTo Training.

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

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 the GDPR, CCPA/CPRA, LGPD and our own Data Processing Addendum (DPA), as well as applicable GoTo policies and public disclosures.

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. Security features that can be configured in the service help administrators to minimize threats and risks to Customer Content.

3 Product Architecture

GoTo Meeting, GoTo Webinar, GoTo Training, and GoTo Stage are Software as a Service (SaaS) solutions designed for high performance, reliability, scalability, and security. These Services are supported by high-capacity servers and network equipment with appropriate security controls in place and redundant infrastructure designed to preclude single points of failure. Clustered servers and backup systems are in place to support application processes in the event of a heavy load or system failure.

Application/server sessions are load balanced across geographically distributed clusters designed to ensure performance and adequate latency.

The Service infrastructure and data are hosted by cloud hosting providers.

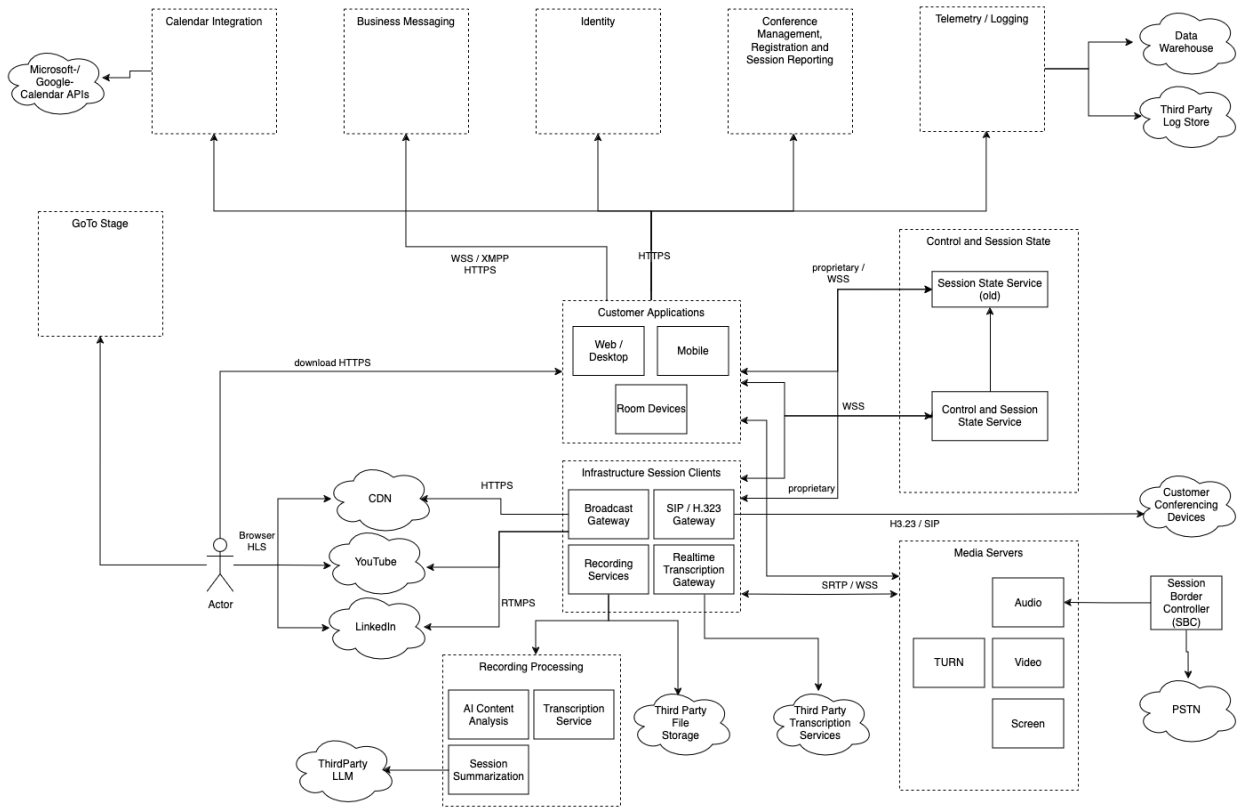

Figure 1: Central Architecture

Customer Applications (GoTo web, desktop and mobile applications or "clients"; a device called GoTo Room (Meeting only)): The Customer Applications provide the Service functionality as described above in Section 1 (Product Introduction).

Identity Services: Manages user accounts and enables secure and standardized account authorization and login.

Conference Management, Registration and Session Reporting Services: Conference Management provides information about scheduled sessions and enables scheduling new sessions and adjusting existing sessions. Registration Services enable registration for sessions where this is required. Session Reporting provides information on past sessions including recordings, transcriptions, attendance and more.

Business Messaging: Management of channels as well as sending, receiving and storage of messages and attachments; used for out of session messaging only.

Calendar Integration: Allows users to synchronize their Microsoft Outlook or Google calendars to get notifications about GoTo sessions.

Telemetry/Logging: Sending of telemetry probes or log statements to help gather usage statics and diagnose issues.

Control and Session State Services: Provide functionality used by client applications to initiate and receive non-media related changes to the session state.

Media Servers: Responsible for receiving, modifying, and distributing audio, video, and screen sharing content.

PSTN: Public switched telephone network allows users to dial into sessions via physical or IP telephones.

Session Border Controller: Connects GoTo's Voice over Internet Protocol (VoIP) with commercial telephony providers.

Recording Services: Enables recording of session audio, video, screen sharing and business messaging content.

Broadcast Gateway: Used for GoTo Webinar Webcasts and supports layout, transcoding, and packetizing the media streams into HLS streams, which are distributed via CDN to browser-based clients or pushed to RTMP-enabled streaming platforms like YouTube or LinkedIn.

H.323-/SIP-Gateway: Enables connection to session audio via SIP or H.323 conferencing devices.

Realtime Transcription (RTT) Gateway: Provides live transcription of session participants' speech.

GoTo Stage Services: Management of GoTo Webinar video content by organizers; provides viewing experience to visitors.

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.

4.1.1 Encryption In Transit

GoTo implements security measures for data in transit that are designed to protect against passive and active attacks on confidentiality, integrity, and availability. Communications security controls are implemented for screen and video sharing, VoIP, webcam video, keyboard/mouse control, text-based chat information and other session data.

GoTo uses Internet Engineering Task Force (IETF)-standard TLS protocols to protect TCP communication between endpoints.

HTTPS and WSS are used to protect non-media data, while in-session media data is protected by SRTP, WSS, or DTLS.

Internally, GoTo also uses mutual certificate-based authentication (mTLS) on servers that handle media data.

4.1.1.1 Audio and Video Security

An SRTP-based protocol using standard encryption mechanisms that leverage AES128 at a minimum is used to protect the confidentiality and integrity of VoIP connections between the endpoints and servers.

4.1.1.2 Website, API, and Internal Web Service Security

All connections to the Service websites, APIs and internal web services are protected using TLS. This includes Content Uploading, Session Reporting, Recordings and Transcripts, and others.

4.1.1.3 Business Messaging

Presence updates, messages, and files are transferred via a TLS-secured channel to chat services and onward to users. File content is made available through cryptographically signed URLs that link to the content.

4.1.1.4 Webcast Security (Webinar only)

Webcast streaming gateways forward traffic to the streaming engine over SRTP, all within GoTo's secure internal network. CDNs pull data from the streaming engine securely over HTTPS. The clients also pull data securely from CDNs over HTTPS.

4.1.2 Encryption at Rest

4.1.2.1 Profile Data

The content is stored in a relational database with AES 256-bit encryption.

4.1.2.2 Conference Management, Registration and Session Reporting

The content is stored in a relational database with AES 256-bit encryption.

4.1.2.3 Content Uploading

Uploaded content and related metadata are stored in AWS S3, Amazon Aurora and Amazon Dynamo DB, all with AES 256-bit encryption. Additionally, metadata is stored in Apache Cassandra without encryption at rest.

4.1.2.4 Recordings and Transcripts

Cloud recordings are stored in AWS S3. Files are encrypted at rest using server-side encryption with AES256.

Audio files for transcription are encrypted using AES256 and deleted immediately after speech-to-text processing is complete.

4.1.2.5 Business Messaging Security

Messages are stored in an AWS Aurora database and shared files are stored in AWS S3, both with AES 256-bit encryption at rest.

4.1.2.6 GoTo Stage

This uploaded content and related meta data is stored in AWS S3 with AES 256-bit encryption. The metadata is stored in Apache Cassandra and the search index in Elasticsearch, both not encrypted at rest.

4.2 Firewall and Proxy Compatibility

The installable clients include built-in proxy detection and connection management logic to help automate software installation, avoid the need for complex network (re)configuration and maximize user productivity. Firewalls and proxies already present in a user's network generally do not need any special configuration to enable use of the Service.

For more details, and the exact domains, IPs and ports used, please visit the respective support pages for Meeting, Webinar and Training.

4.3 Installable Client Security Features

The installable clients are designed with appropriate security features and employ strong cryptographic measures, including signed endpoint software and "client-only" connections.

4.3.1 Signed Endpoint Software

The Service's executables are digitally signed for integrity protection and authenticity. GoTo's client application software follows appropriate quality control procedures, configuration management procedures, and a Security Development Lifecycle (SDL) model during development and deployment.

4.3.2 "Client-only" Connections

To reduce the risk that remote systems can target them with malware and viruses, the installable clients are not configured to receive inbound connections. This helps protect users participating in a session from being infected by a compromised host used by another attendee.

4.3.3 Cryptographic Subsystem Implementation

Cryptographic functions and security protocols implemented in the installable clients use the open source BoringSSL or OpenSSL cryptographic libraries. No external APIs are exposed that would allow other software to access the cryptographic libraries bundled in the client.

The web application uses the browser's cryptographic libraries. There are no end-user-configurable cryptographic settings that allow for accidental or intentional misconfiguration.

4.4 User Authentication

Role-based authorization and appropriate access controls depend upon the ability to identify and authenticate users. To ensure that organizers and attendees have the right privileges, account and session authentication features are incorporated into the Service.

4.4.1 Account Login

The Service websites offer the following login methods:

- Direct sign-in with username and password;

- Sign-in through a social or other account provider using LastPass, Google, Facebook, LinkedIn, Microsoft, or Apple. (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in); and
- SAML-based single sign-on.

For direct sign-in, all passwords have minimum character and complexity requirements. Mechanisms are in place to protect against brute-force login attacks and unusual login activity.

GoTo does not store account passwords in plaintext. Rather, passwords are stored using a salted cryptographic hash function designed to be resilient to dictionary and brute force attacks. Passwords are transmitted over secured connections (TLS).

4.4.2 Authentication of Session Attendees

To enable sessions with restricted attendance, each session has a unique and random ID. Organizers can also choose to require a password for participants to join a session.

To join a session, attendees must provide the unique ID by either clicking a URL that contains the ID or by manually entering the value into a form presented by the Service. When dialing in using a telephone, attendees must enter the ID on their keypad. If the ID is valid, each attendee is provided a role token that is then presented to the communication servers during the join process.

4.4.3 Role-Based Access Control

Application-defined roles can be assigned to Service users and support Customers in enforcing company access policies related to Service and feature use. Users can access controls and privileges based on their assigned role:

Organizers (or trainers for GoTo Training) are authorized to schedule meetings, webinars, and/or training sessions. An organizer sets up each session, invites attendees, initiates and ends the session and designates the current presenter.

Attendees are people invited to participate in sessions. Attendees can view the presenter's shared screen, chat with other attendees and view the attendee list.

Presenters are attendees that can share their screen with other attendees. Presenters can also grant other attendees shared control of their keyboard and mouse.

Administrators are individuals authorized to manage a multi-user account. Administrators can configure account features, authorize organizers, and access a variety of reporting tools.

GoTo internal administrators are GoTo staff members authorized to manage GoTo Meeting, GoTo Webinar, and GoTo Training services and accounts on behalf of our Customers.

4.5 Recordings Access Control

Organizers can easily share recordings with attendees after a session through unique, direct links, and attendees can view the recording playback from within their web browser.

For GoTo Webinar, the sharing URLs do not expire as long as the recording is available. To disable access to a recording, organizers can delete the recording at any time.

For GoTo Meeting, recordings can be shared via URLs that use a random token with limited validity. Sharing can be restricted to defined parts of the content, and either be available to everyone with the URL or only to users with configurable email addresses. These restrictions can be adjusted even after the URL is shared.

5 Security Program Updates

GoTo reviews and updates its security program and engages independent third parties to assess its relevant security controls at least annually to ensure it evolves 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'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.

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 cloud hosting provider data centers.

For data center provider and location details please see the Service's Sub-Processor Disclosure document in GoTo's Trust Center.

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

7.1 Data Center Physical Security

Cloud hosting providers 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
- Scheduled maintenance and validation of all critical security and environmental controls

Cloud hosting providers limit physical access to production data centers to authorized individuals only. Access to server rooms requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval. All physical access to data centers and server rooms is minimized, logged and reviewed by the providers 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, 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, please 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, please 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 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 (EDR) 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 and operating systems that process Customer Content. GoTo assesses and scans for system-level, 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 leverages a multi-tenant 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. GoTo has also implemented controls to prevent Users or End Users from seeing the data of other Users.

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;
- Cloud Network firewalls filtering inbound and outbound connections, including internal connections between GoTo systems; and
- Internal network segmentation.

17 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is responsible for detecting and responding to security events. The SOC 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 GoTo's 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 Central and Pro. 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 tagged for deletion within ninety (90) days and successfully deleted within one hundred (100) days of the termination, cancellation, or expiration

and, in each case, deprovisioning of Customer's then-final subscription. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

The above timelines are applicable for all Services, and additional Service-specific deletion timelines are set out below:

GoTo Meeting

During subscription term: GoTo Meeting session history and cloud recordings shall be deleted automatically on a rolling one (1) year basis during a Customer's active subscription term, for both paid and free accounts.

After subscription term: Upon the conclusion of a paid subscription to GoTo Meeting, Customer's accounts that contain a free license will revert to a free account and Content will be retained. For accounts that do not contain a free license or are explicitly cancelled or terminated, Content shall automatically be tagged for deletion within ninety (90) days and successfully deleted within one hundred (100) days of the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription. Further, free GoTo Meeting accounts shall automatically be deleted after two (2) years of user inactivity (e.g., no logins).

Removal of user from paid account: If a user is deleted or otherwise removed from an active paid account, scheduled sessions are automatically tagged for deletion after ninety (90) days and successfully deleted within one hundred (100 days) of user removal.

GoTo Stage: GoTo Stage users with an active GoTo Webinar subscription may unpublish/remove any published webinars at any time via self-service through the GoTo Webinar services environment and/or by submitting a support request to GoTo.

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, Users and other individuals who use GoTo services ("End 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 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, Users' and End 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 specify 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 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 Resolve to support devices 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 on the basis of 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 data protection or security, please visit our IRM portal or send an email to privacy@goto.com.