TECHNICAL AND ORGANIZATIONAL MEASURES FOR GOTO MEETING, GOTO WEBINAR, GOTO TRAINING, AND GOTO STAGE

Security and Privacy Operational Controls

Publication date: February 2022

1 Products and Services

This document covers the Technical and Organizational Measures (TOMs) for GoTo Meeting, GoTo Webinar, GoTo Training, and GoTo Stage (collectively referred to as “GoTo UCC Solutions”).

The GoTo UCC Solutions Products are online communication services that enable individuals and organizations to interact using various features, depending upon service offering, that may include desktop screen sharing, video conferencing, and integrated audio. The GoTo UCC Solutions services are delivered via web browser or client executable, through a globally distributed network of proprietary hardware and software.

- GoTo Meeting enables users to schedule, convene and moderate meetings using the GoTo Meeting web site and/or executable customer software.
- GoTo Webinar enables organizations to conduct one-to-many information presentation events reaching local and global attendees over the Internet. Webinars are scheduled, convened and moderated using the GoTo Webinar web site and/or executable customer software.
- GoTo Training enables users to schedule, convene and moderate training sessions using the GoTo Training web site and/or executable customer software. It provides specific features applicable to web-based training, such as online access to tests and materials and a hosted course catalog.
- GoTo Stage is an online portal 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.

2 Product Architecture

Screen-sharing between participants in GoTo UCC Solutions sessions occurs via an overlay networking stack that logically sits on top of the conventional TCP/IP stack within each user’s PC (see Figure 1).

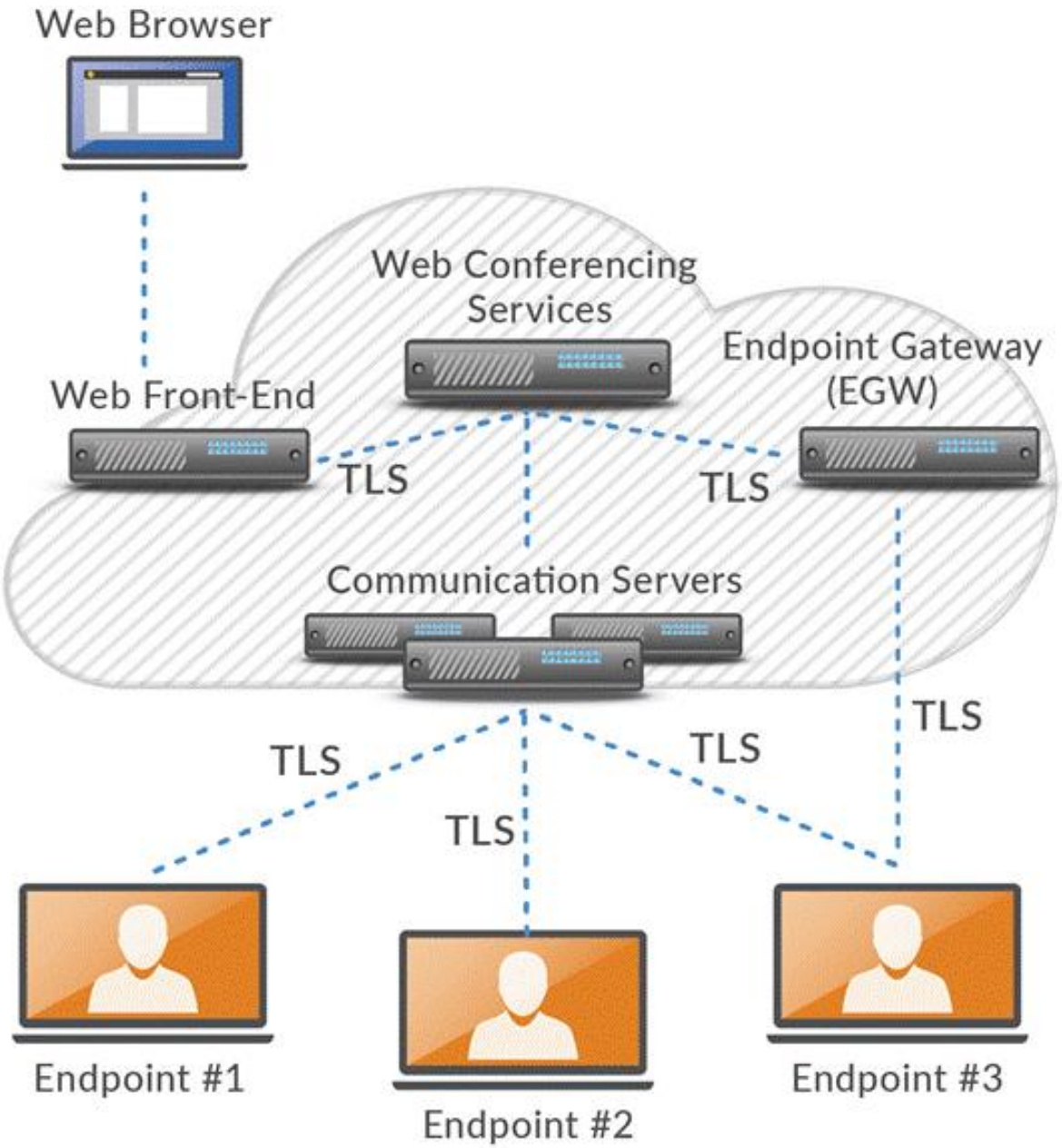

Figure 1 - GoTo Meeting, GoTo Webinar, GoTo Training, & GoTo Stage architecture.

***Web Front-End** – Portal Web Page of GoTo suite; Hosted in Tier 1 co-location data centers and on AWS*

***WCS** – Session Scheduling; Meeting History; GTM Organizer Settings; Hosted in Tier 1 co-location data centers*

***Communication Server** – incl. Screen Sharing Server, Audio Bridges & Voice gateways (acts as proxy), H.323 gateways – hosted on Amazon Web Services / **Multicast Communication Server** and Video Cluster Server are hosted in Tier 1 co-location data centers*

***Endpoint Gateway (EGW)** – handles Organizer and Participant Endpoint connections and encryption mechanism – EGW is hosted on Amazon Web Services*

Participants (session endpoints) communicate with infrastructure communication servers and gateways using outbound TCP/IP connections on port 443, where the participants can be located anywhere on the Internet. Clients generally communicate to GoTo UCC Solutions via

the endpoint gateway. However, new clients communicate directly using Representational State Transfer (REST) calls to the backend services via load balancers. The service infrastructure also allows public switched telephone network (PSTN) users to dial into a meeting.

GoTo UCC Solutions products use an application service provider (ASP) model designed to ensure secure operations while integrating with a company's existing network and security infrastructure.

The architecture has been designed for high performance, reliability and scalability, and is driven by high-capacity servers and network equipment with appropriate security patches in place. Redundant switches and routers are designed to preclude single points of failure. Clustered servers and backup systems are in place to ensure application processes in the event of a heavy load or system failure. Web Conferencing Services load balance the client/server sessions across geographically distributed communication servers intended to ensure performance and adequate latency.

The service infrastructure is primarily hosted in Tier 1 co-location data centers, with some component services hosted on cloud hosting providers. The audio bridge services are hosted completely on cloud providers, while some of the product Web Conferencing Services are hosted on cloud providers. The data associated with any service hosted on a cloud provider is also stored on that provider.

Physical access to co-location hosted servers is restricted and continuously monitored. All facilities have redundant power and appropriate environmental controls. Firewall, router and VPN-based access controls are employed to secure GoTo private-service networks and backend servers. Infrastructure security is continuously monitored, and vulnerability testing is conducted regularly by internal staff and external third-party auditors.

For more information, please see the UCC Security White Paper.

3 GoTo UCC Solutions Technical Security Controls

GoTo employs industry standard technical 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 control procedures are in place, designed to prevent or mitigate the threats 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.

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 our product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls. In addition, a third party, cloud-based distributed

denial of service (DDoS) prevention service is used to protect against volumetric DDoS attacks; this service is tested at least once per year. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

GoTo leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's GoTo 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 a 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

GoTo's architecture is generally 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 the system is tested periodically.

3.6 Malware Protection

Malware protection software with audit logging is deployed on all GoTo UCC Solutions servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.7 Data Confidentiality and Authenticity

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant 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.

3.7.1 Data in Transit

GoTo Meeting, GoTo Webinar and GoTo Training provide security measures for data in transit that are designed to protect against passive and active attacks against confidentiality, integrity and availability. Screen and video-sharing, VoIP, webcam video, keyboard/mouse control and text-based chat information (each, “Session Data”) have industry standard communications security controls.

Session Data is never exposed in clear text during transmission between endpoints and GoTo’s Communication Servers.

Communications security controls based on strong cryptography are implemented at two layers: (i) on top of the transmission control protocol (TCP) and user datagram protocol (UDP); and (ii) in the multicast packet security layer (MPSL).

TCP and UDP Security

Internet Engineering Task Force (IETF)-standard transport layer security (TLS) protocols are used in order to protect TCP communication between endpoints.

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 to the website and between GoTo Meeting, GoTo Webinar or GoTo Training components, GoTo servers authenticate themselves to clients using public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., Communication Servers to Web Conferencing Services).

For data sent with UDP, an existing TLS connection is leveraged to securely exchange cryptographic keys that are used to encrypt and authenticate UDP data.

Multicast Packet Layer Security

Multicast Data such as keyboard/mouse control, chat and in-session state information are protected by encryption in transit and integrity mechanisms, designed to prevent anyone with access to the communications servers (whether friendly or hostile) from eavesdropping on a session or manipulating data without detection. Unique to GoTo products, the MPSL provides an added level of communication confidentiality and integrity This additional security layer uses a 128-bit AES encryption in counter mode for further protection against eavesdropping and manipulation.

Plaintext data is typically compressed before encryption using proprietary, high-performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value currently generated with the HMAC-SHA-1 algorithm.

Key establishment is accomplished by using a randomly generated 128-bit seed value selected by the GoTo service, that is distributed to all endpoints over TLS and used as the input to a NIST-approved key-derivation function. The seed value is erased from the service memory when the session ends.

Audio Security

Integrated audio conferencing for GoTo Meeting, GoTo Webinar and GoTo Training sessions is provided through the PSTN as well as Voice over Internet Protocol (VoIP). The PSTN is, by design, intended to provide for the confidentiality and integrity of voice communications. To protect the confidentiality and integrity of VoIP connections from the endpoints to the voice servers, an SRTP-based protocol using AES-128-HMAC-SHA1 is used over UDP and TCP. Keys are exchanged by the client and server over an established TLS connection.

Video Security

To protect the confidentiality and integrity of video connections from the endpoints to the video servers, GoTo leverages a SRTP-based protocol with AES-128-HMAC-SHA1. Keys are exchanged by the client and server over an established TLS connection.

Webcast Security

GoTo Webinar webcasts use communications servers, broadcast gateways, third-party streaming engines and content delivery networks which are designed to reliably deliver screen sharing, audio, and video to attendees joining from a browser. The gateways receive media data from the communication servers, transcode them into standard codecs and forward them to the streaming engine over RTP - all within our secure internal network. The streaming engine produces HTTP Live Streaming (HLS) at multiple bitrates to enable adaptive delivery for clients with sub-optimal network connections. CDNs have been set up to pull data from the streaming engine securely over https. The clients also pull data securely from CDNs over https.

GoTo Stage

GoTo Stage is an online portal where GoTo Webinar organizers can create customizable channels on which to publish their webinar recordings. Published recordings are showcased on the GoTo Stage homepage, organized by business categories. A video published to GoTo Stage is available for discovery on the GoTo Stage homepage and in search engine results, unless the organizer restricts discoverability using the administrative settings on his or her channel page. Otherwise, anyone registered to GoTo Stage can view the recording with a direct link 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. Once registered, a signed S3 URL with a set TTL is used to playback the webinar recording. At any point, organizers can unpublish their recording through GoTo Webinar, which removes the video from their channel page and the GoTo Stage ecosystem. GoTo Stage administrative functions are password secured, and all connections in the GoTo Stage portal are protected using TLS.

3.7.2 Data at Rest

GoTo Meeting, GoTo Webinar and GoTo Training allow organizers to record their live sessions, including audio, video and screen content. When an organizer starts recording, every attendee is notified that the recording has begun, and a visual indicator appears on the control panel to reflect that recording is in progress. Customers can elect to store session recordings on their local machine or in the cloud.

Cloud Recordings

Cloud recordings are stored on AWS S3. Files are encrypted at rest using server-side encryption using 256-bit AES

Transcripts

If enabled by the organizer, Google Cloud Speech-to-Text technology is used to transcribe session recordings. Audio files are transferred using TLS for transcription, where the file is encrypted using 256-bit AES and deleted immediately after speech-to-text processing is complete. Transcripts will be maintained by GoTo using its AWS S3 instance and made available to the organizer under Cloud Recordings.

Content uploading

Some of GoTo's services provide capabilities for organizers to upload videos for use in live sessions. This uploaded content is also stored in AWS S3 with 256-bit AES encryption enabled at rest, as well as in transit.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. 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, as well as management.

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 GoTo UCC Solutions.

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
- 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. These policies and procedures are designed to manage, identify and resolve suspected or identified security events across GoTo systems and Services, including GoTo UCC Solutions. 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 deemed 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 GoTo UCC Solutions, 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 UCC Solutions 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), which governs GoTo's processing of Personal Data and is available in English and German, to meet the requirements of the GDPR, CCPA, and beyond.

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 coming into force, 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 law 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

At any time, GoTo UCC Solutions Customers may request the return or deletion of their Content, and such requests will be fulfilled within thirty (30) days of request (or sooner where required by applicable law). Additionally, GoTo Meeting meeting history and cloud recordings shall be deleted automatically on a rolling one (1) year basis during a Customer's active subscription term.

Upon the conclusion of a paid subscription to GoTo Meeting, Customer's accounts shall revert to a free account. If an account is explicitly cancelled or terminated, Content shall be deleted within 90 days of cancellation or termination. Free GoTo Meeting accounts shall be subject to the same one year rolling deletion schedule described above. Further, free GoTo Meeting accounts shall automatically be deleted after two (2) years of user inactivity (e.g., no logins).

To account for a seasonal user base, GoTo Webinar and GoTo Training accounts shall be deleted two (2) years after expiration or termination of the then-final term. GoTo Stage users may unpublish/remove any published webinars at any time, during an active GoTo Webinar subscription, via self-service through the GoTo Webinar services environment and/or by submitting a support request to GoTo. Upon written request, GoTo will certify to relevant account and Content deletion.

5.6 Sensitive Data

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

- 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) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related 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 GoTo Meeting, GoTo Training, GoTo Webinar, and GoTo Stage.
- 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 the internal assessment and processes related to vendors and third parties, 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. The legal and procurement teams 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 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

In order 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 parties' 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.