Technical and Organizational Measures
Rescue and Rescue Lens

Executive Summary

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

- **Encryption**:
  - *In-Transit* Transport Layer Security (TLS) v1.2.
  - *At Rest* Transparent Data Encryption (TDE) using Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Data Centers[1]:** United States, Germany and Ireland data center locations 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:** Rescue holds ISO/IEC 27001:2013, SOC 2 Type II, 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**:
  - Rescue 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 within (140) days of the expiration of a Customer's then-final subscription term.

[1] Hosting locations may vary (i.e., depending on data residency election). Consult the Rescue Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https:/www.goto.com/company/trust/resource-center) for details.

Contents

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

1 Product Introduction

Rescue is an online remote support service used by technicians to provide remote assistance via the internet, without the need for pre-installed software. With the permission of the User or other individual using Rescue/receiving support from a technician (End User), Rescue allows a technician to access and view and/or assume control of an End User's computer. Communicating through a chat window, the technician can vet, diagnose and repair computer problems and otherwise assist an End User with operating system and software application issues.

Rescue Lens allows End Users to stream their mobile device cameras (through the Lens mobile app) to a remote technician, allowing the remote technician to view problematic hardware such as a misconfigured router or a damaged automotive component. Rescue Lens is an optional feature within Rescue and can be activated in the Rescue Admin Center. For more details on Rescue Lens, please see the Rescue Lens User Guide.

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 for Rescue and Rescue Lens.

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 and 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

Rescue is a Software-as-a-Service (SaaS)-based remote support solution comprised of three main components: a technician console, an End User mobile app or desktop applet, and an administration center.

The technician console is the interface used by technicians to conduct remote support sessions. Technicians can initiate new sessions or respond to online End User requests waiting in a shared queue. Technicians communicate with and provide support to End Users through Rescue's mobile app (Android oriOS) or desktop applet (Windows, MacOS or Linux). The applet is downloaded to the End User's remote PC and is designed to remove itself when the session concludes.

The Rescue technician console interacts with the Rescue app or applet using a peer-to-peer (P2P) network connection (see Figure 1 in section 3.1). When the applet is started, the P2P process is initiated and connects to a Rescue gateway where the session with the technician console is negotiated.

GoTo's proprietary key exchange forwarding protocol is designed to provide security against interception or eavesdropping on GoTo's infrastructure. Specifically, the connection between the End User and the host is facilitated by the gateway to ensure that the End User can connect to the host independently of the network setup.

The host establishes a TLS connection to the gateway, which forwards the End User's TLS key exchange to the host via a proprietary key renegotiation request. Thus, the End User and the host exchange TLS keys without the gateway learning the key.

3.1 Key Agreement

When a support session starts and a connection is established between the supported End User and the technician, their computers must agree on an encryption algorithm from available supported options and a corresponding key to be used for the duration of the session.

The computers use certificates to validate their identities. Since neither the technician nor the End User have software capable of brokering the connection and validating installed security certificates and an SSL certificate installed on their computers, they both turn to one of the Rescue servers and perform the initial phase of the key agreement. Verification of the certificate by both the technician console and the End User app or applet ensures that only a Rescue server can mediate the process.

3.2 Overview of the Rescue Gateway Hand-off process

When the digitally signed Rescue app or applet is started on a machine, it contains a session authentication Globally Unique Identifier (GUID). The GUID is embedded in an executable app or applet (e.g., a .exe file) as a resource by the site when downloaded. The app or applet then downloads a list of available gateways from secure.logmeinrescue.com or secure.logmeinrescue.eu, picks a gateway from the list and connects to it using TLS. The gateway is then authenticated by the applet using its SSL certificate. The gateway authenticates the applet in the database with the GUID and registers that the End User is waiting for a technician.

When a technician picks up a session in the Rescue technician console, a request is sent to the gateway with the session authentication GUID to pass connections between the technician console and the End User app or applet. The gateway is the intermediary that authenticates the connection and starts relaying data at the transport level (it does not decrypt relayed data).

When a connection relay is started, the parties try to establish a P2P connection. The process is as follows:

- The applet starts listening for a Transmission Control Protocol (TCP) connection on a port assigned by Windows, Mac OS or Linux.
- If the TCP connection cannot be established within 10 seconds, an attempt is made to establish a User Diagram Protocol (UDP) connection with the help of the gateway.
- If either a TCP or a UDP connection is established, the parties authenticate the P2P channel (using the session authentication GUID), and it takes over traffic from the relayed connection.
- If a UDP connection has been set up, TCP is emulated on top of the UDP datagrams using XTCP, a GoTo-proprietary protocol based on the Berkeley Software Distribution ("BSD") TCP stack.
- Every connection is secured with the TLS protocol (using AES256 encryption with SHA256 Media Access Controls [MAC]). The session authentication GUID is a 128-bit, cryptographically random integer value.

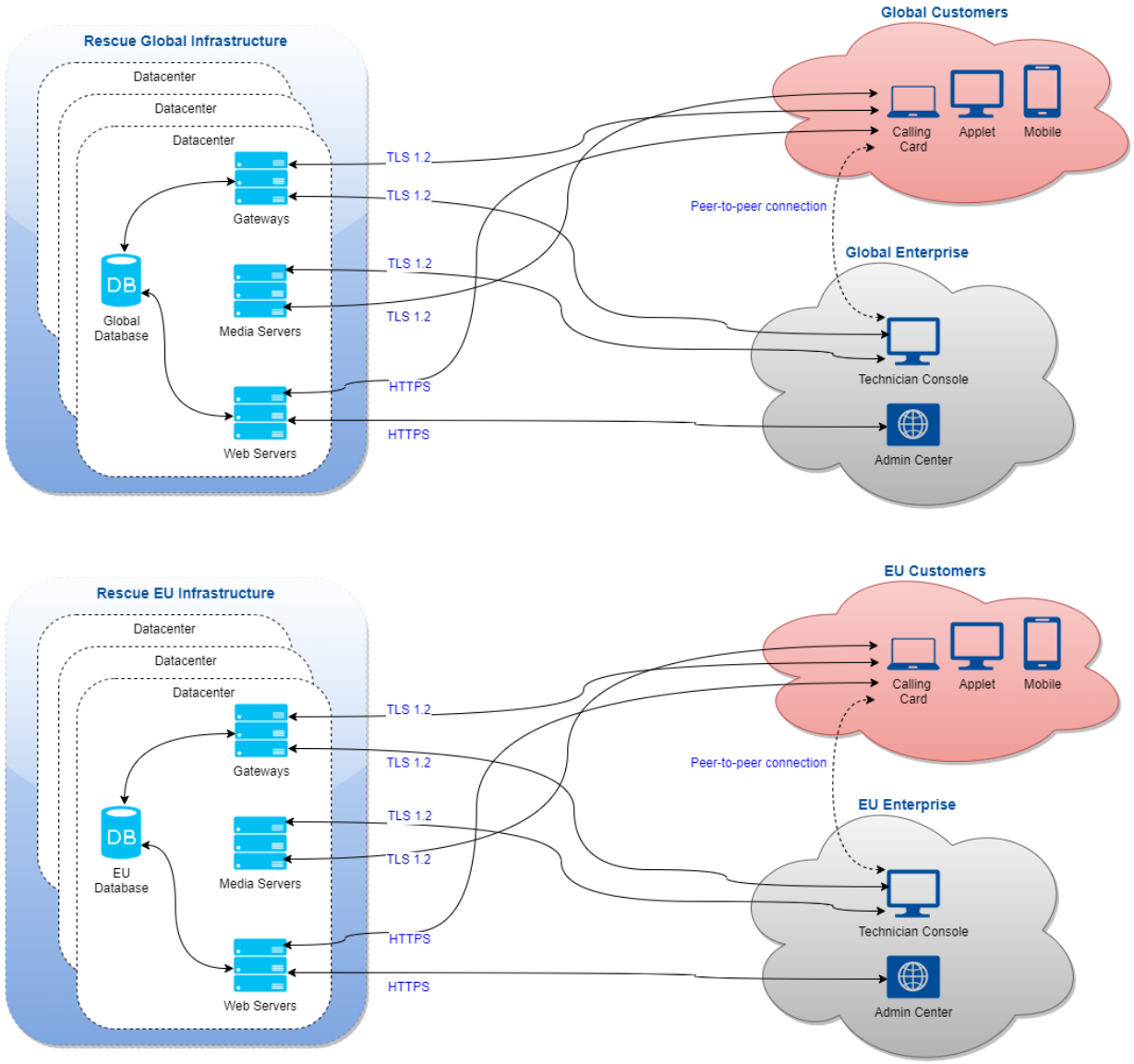

Figure 1: Rescue Architecture

3.3 Rescue Media Architecture

The Rescue media service is a web real-time communication (WebRTC)-based standalone service that powers Rescue Lens video streaming. It manages conferences for Rescue sessions that use the Lens feature. Conference participants (peers) join and leave conferences and End Users send video and audio streams for other participants to receive. Lens sends video content in a unidirectional stream from the Lens app to the technician console.

There are three main components of the media service: the Media Software Development Kit (MediaSDK), the session manager and the streaming server. These components manage the process of creating/destroying and joining/leaving conferences. These components communicate via the existing secure connections between the technician console and the website and between the Lens app and the website.

3.3.1 MediaSDK

The media service was built on top of WebRTC with a thin wrapper around the WebRTC code base. The technician console and the mobile Lens app use MediaSDK.

3.3.2 Session Manager

The session manager is a load balanced website providing a Representational State Transfer (REST) API to manage (create/destroy/join) the conferences. The session manager only accepts requests from the website.

3.3.3 Streaming Server

The media service uses a custom streaming server solution to handle streams between peers (the technician console and the Lens app). Both the technician console and the Lens app are connected to the streaming server. A Lens session has two streams (one is sent, the other is received): the Lens app streams its video content up to the streaming server, while the technician console streams video content down from the server. The streaming server behaves like a relay server between peers.

4 Technical Security Controls

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

4.1 Data Confidentiality

Rescue's secure online system is supported by Secure Sockets Layer and Transport Layer Security (SSL/TLS) and meets the following objectives:

- Authentication of the communicating parties
- Negotiation of encryption keys without interception
- Confidential exchange of messages
- Ability to detect if a message has been modified in transit

Rescue uses OpenSSL and at the time of publication, the version used by Rescue is 1.1.1n.

4.2 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.

4.2.1 Encryption In Transit

All network traffic flowing in and out of the Rescue data centers, including all Customer Content, is encrypted in transit with TLS 1.2 and HTTPS. In addition, Rescue support sessions are protected with 256-bit AES encryption and MD5 Hash for enhanced traceability of file transfers.

Since all three components of the Rescue communications system are under GoTo's control, the cipher suite used by these components is always the same: AES256-SHA in cipher-block chaining mode with RSA key agreement. This means the following:

- The encryption/decryption algorithm is AES

- The encryption key is 256 bits long
- The encryption keys are exchanged using RSA private/public key pairs, as described in the previous section
- The basis of MAC is SHA-2. A MAC is a short piece of information used to authenticate a message. The MAC value protects both a message's integrity, as well as its authenticity, by allowing the communicating parties to detect any changes to the message.
- Cipher-block chaining (CBC) mode ensures that each ciphertext block is dependent on the plaintext blocks up to that point and that similar messages cannot be distinguished on the network.

Data traveling between the supported End User and the technician are encrypted end-to-end and only the respective parties have access to the information contained within the message stream.

4.2.2 Encryption At Rest

Rescue Customer Content is encrypted at rest at both the server and database levels with AES256 and TDE. As an example, Customer Content includes chat logs and custom fields, which are fields created by the master account holder or master administrator.

4.3 Rescue Access Controls

Rescue administrators can customize access controls. For example, Rescue administrators can configure a password policy including, a minimum required password strength and a maximum password age, force password resets, enforce two-factor authorization for Rescue logins, restrict technician access to Rescue from IP addresses preapproved for specific tasks, or grant technicians access to only pre-defined applications using a single SSO ID to log in to those applications. If needed, administrators can disable a technician's SSO ID.

Additional access controls include:

- Permission-based access on a granular level (such as permitting some technicians to use remote view, but not remote control)
- Not storing data from remote devices on GoTo servers. Only session logs, End User IP addresses and chat logs are stored — chat text logs can be removed from session details
- Preventing technicians from transferring files
- Requiring that the End User be present at the remote device to permit remote access
- Requiring that the End User maintain control and can terminate the session at any time
- Preventing technicians from using certain features until the End User has explicitly granted them permission (e.g., remote control, desktop view, file transfer, system information, reboot and reconnect)
- Automatic access rights revocation when the session is terminated
- The ability to force automatic logoff on the basis of a predetermined time of inactivity
- Locking an account after five unsuccessful login attempts

4.3.1 Permission-Based Access Control

Rescue administrators can also grant or deny specific permissions in the administration center. These group permissions include:

- Allowing clipboard synchronization
- Allowing screen sharing with Users and End-Users
- Deploying scripts
- Launching desktop viewing
- Launching file manager
- Launching remote control
- Rebooting
- Recording sessions
- Requesting credentials
- Sending and receiving files
- Sending URLs
- Starting private sessions
- Transferring sessions
- Using a single prompt for all permissions
- Viewing system information

For more details on group permissions, please reference the Rescue Administrators Guide. Rescue Lens technicians are identified by their email address and authenticated using a password.

4.3.2 Authentication

Rescue's authentication measures are designed to secure the product by employing measures to only permit technicians or administrators to login to the system. Technicians are assigned login IDs (e.g., matching their email addresses) and corresponding passwords by their administrators. Technicians enter these credentials into the login form on the Rescue website upon the beginning of their shift at a minimum. Administrators can configure controls to require authentication on a more frequent basis (e.g., after five minutes idle).

The Rescue system is first authenticated to the technician's web browser with its 2048-bit premium RSA SSL certificate ensuring that the technician will be entering their username and password into the correct website. The technician then logs in to the system with their credentials. Rescue does not store any passwords but instead uses SCrypt to create hashes from passwords that are then stored in the Rescue database. The hashes are salted with a 24-character string generated by CSPRNG for each unique password.

The Rescue system is also authenticated to the supported End User. The app or applet, downloaded and run by the End User, is signed with GoTo's code-signing certificate (based on a 2048-bit RSA key) and this information is typically displayed to the End User by their web browser when they are about to run the software. Rescue does not authenticate the End User to the technician.

Rescue also allows Administrators to implement a Single Sign-On (SSO) policy. Security Assertion Markup Language (SAML) is employed, which is an Extensible Markup Language (XML) standard for exchanging authentication and authorization data between security domains (between an identity provider and a service provider).

Administrators can also require two-step verification for logging in to Rescue. The two-step verification feature can use email, SMS or any Time-based One-time Password (TOTP) authenticator to provide a second layer of protection to a Rescue account by requiring selected members of the organization to set up an additional way of verifying their identity. Setting up the authenticator app is triggered in any of the following cases:

- The selected member tries to log in to their Rescue account on the secure website
- The selected member tries to log in to desktop technician console
- The selected member tries to change their Rescue password

4.3.3 Authorization

Authorization happens at least once during every remote support session. After downloading and running the applet, the supported End User will be contacted by a technician. The technician can chat with the End User via the applet but any further action, such as sending a file or viewing the End User's desktop, requires the End User's express permission. A "single prompt" can also be implemented for lengthy remote support work where the End User might not be present for the entire duration of the session. If this setting is enabled for a technician group, the technicians in that group can request a "global" permission from the End User and, if granted, can perform actions such as viewing system information or entering a remote control session without being further authorized by the End User. Administrators can also impose IP address restrictions so that technicians assigned to a particular task can only access Rescue and perform that task from pre-approved IP addresses. The administrator of a technician group can also disable certain features in the administration center.

The permissions an administrator can grant or deny include:

- Launch remote control
- Reboot
- Launch Desktop Viewing
- Record sessions
- Send and receive files
- Start private sessions
- Launch File Manager
- Request credentials
- Send URLs
- Allow clipboard synchronization
- View system information
- Deploy scripts
- Use single prompts for all permissions
- Transfer sessions
- Allow screen sharing with Users and End Users

4.4 Audit Controls

The following audit controls are available to Rescue Users and End Users:

- The option to force session recording, with the ability to store audit files on a secure shared network
- Technician sessions and remote session activity logging on the host computer to ensure security and maintain quality control (successful logins, unsuccessful logins, remote control started, remote control ended, reboot initiated, logout)
- Person or entity authentication
- Technician authentication using their unique email address, or via an SSO ID
- Allowing technicians to log in only from approved IP addresses
- Audit report available in Admin Center includes changes to account settings and data for each action taken by Administrators on the selected item of the Organization Tree during a particular period

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.

The Rescue database is synchronized every five minutes to another datacenter. In addition, a differential back-up is completed nightly and full backups are conducted every weekend. The backup database is stored with the same encryption as the original. Backups are retained on premise for one month and then rotated to a cloud service, no longer actively processed and retained pursuant to our internal record retention policies. In the event of a complete failure of the datacenter hosting the primary database, Rescue architecture is designed to be rapidly restored.

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-passive data centers; or
b) cloud hosting provider data centers.

Upon account creation, Rescue Customers may elect to utilize either GoTo's European Union or Global data infrastructure to store their Customer Content. Hosting/storage locations are specified below[2]:

- **European Union:** Germany and Ireland
- **Global:** the United States, Germany, Australia 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
- 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

[2] Hosting locations may vary (i.e., depending on data residency election), consult the applicable Rescue Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

through TrustArc, an APEC-approved third-party leader in data protection compliance. To learn more about our APEC certifications, click here.

- International Organization for Standardization – **ISO/IEC 27001:2013** Information Security Management System (ISMS) Certification.
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 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.

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 it on a timely basis. GoTo collects identified anomalous or suspicious traffic in relevant security logs in applicable production systems.

Rescue chat logs are saved in the Rescue database. The chat log is transmitted to the Rescue servers by the technician console in real time and contains events as well as chat messages that pertain to a particular support session. Log files will display the following actions by technicians: start and end time of a remote control session, instances of technicians sharing files with End Users and metadata relating to file sharing (e.g., the name and MD5 Hash thumbprint of a transmitted file). The chat log database can be queried from the administration center.

For active accounts, the contents of the logs will be made available online for two years after the end of a remote support session and archived for two years after that.

To facilitate integration with CRM systems, Rescue can post session details to a URL and administrators can choose to exclude chat text from these details. Chat text is included by default, but Customers can change that setting in the administration center. Additionally, all records of chat texts between technicians and End Users can automatically be omitted from the session details stored at a Rescue data center. Rescue allows technicians to record the events that transpire during a desktop viewing or remote control session into a video file. The recording files are stored in a directory specified by the technician.

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 GoTo 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. GoTo 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 or End 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 to prevent or reduce the likelihood of unauthorized modification

- Web application firewall (WAF) and application-layer DDoS prevention service through which GoTo traffic is proxied to block malicious server traffic
- A local application firewall that provides an additional layer of protection against OWASP top ten and other web application vulnerabilities and malicious traffic
- 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 (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 Rescue. 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.logmeinrescue.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 within (140) 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.

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 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, 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, 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 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.

20.5 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.

20.6 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.

20.7 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.

20.8 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 Rescue 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.

20.9 Compliance in Regulated Environments

Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of Rescue 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. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors. GoTo's Supplier DPA has restrictions around data "selling" as defined under the CCPA.

22 Contacting GoTo

Customers can contact GoTo at https://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.