Technical and Organizational Measures
Business Operations

Contents

1 Introduction

This document outlines the Technical and Organizational Measures (TOMs) implemented by GoTo to ensure the security, reliability, and privacy of our corporate processes. These measures are designed to protect customer content and maintain compliance with applicable laws and regulations. GoTo's TOMs include a comprehensive set of safeguards, features, and practices that are embedded into our products and services to minimize threats and risks.

For detailed information on product-specific measures, please refer to the respective product-specific TOMs documents.

2 Security Policy Governance

GoTo maintains a comprehensive set of security policies and procedures that align with business goals, compliance and privacy programs, and overall corporate governance. These policies and procedures are reviewed and updated at least annually to support GoTo's security and business objectives, adapt to changes in applicable laws, and meet industry standards.

3 Security Awareness and Training Programs

GoTo's privacy and security awareness program educates employees on the importance of handling Personal Data and confidential information ethically, responsibly, and in compliance with applicable laws. Newly hired employees, contractors, and interns are introduced to security policies and the GoTo Code of Conduct and Business Ethics during onboarding. GoTo employees complete privacy and security awareness training quarterly, covering topics based on current trends and threats. Awareness activities occur throughout the year, including campaigns for Data Privacy Day, Cybersecurity Awareness Month, webinars with the Chief Information Security Officer, and a security champions program. To further strengthen our security posture, GoTo conducts monthly phishing simulation campaigns to ensure employees remain vigilant against phishing attacks. Where appropriate, employees may also be required to complete role-specific training.

4 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees. 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.

5 Risk Management

GoTo's Risk Management is structured to identify, assess, and manage risks systematically. We begin by identifying potential risks through various assessments, including threat modeling, risk and control assessments, and compliance audits. Once risks are identified, we determine appropriate mitigating controls and remediation efforts to reduce these risks. This involves implementing strong access controls, data encryption, and regular security audits. Our process also includes prioritizing security objectives based on the identified risks, ensuring that our security measures align with our strategic goals. By embedding risk management into our culture and processes, we ensure that risk-based decisions are consistent and disciplined, protecting the GoTo brand and enhancing our overall security posture.

6 Independent Audits and Certifications

GoTo continuously reviews and enhances our security and privacy program by partnering with independent third parties to conduct annual audits of our controls and maintain key certifications. This proactive approach ensures that our measures evolve with the ever-changing threat landscape, keeping us compliant with industry standards, customer commitments, and applicable laws and regulations. More information is available at the GoTo Trust and Privacy Center at https://www.goto.com/company/trust.

- TRUSTe Enterprise Privacy & Data Governance Practices Certification to address operational privacy and data protection controls aligned with key privacy laws and recognized frameworks.
- TRUSTe APEC CBPR and PRP Certifications is for the transfer of Customer Content between APEC-member countries, independently validated by TrustArc.
- ISO/IEC 27001:2022 Information Security Management System (ISMS) Certification[1]
- AICPA SOC 2 Type II and SOC 3 Type II to provide assurance to our customers that we have implemented effective controls to protect Customer Content and ensure the reliability of our services.[2]
- BSI C5 (Cloud Computing Compliance Criteria Catalogue) that ensures secure cloud computing.[2]
- PCI DSS compliance for GoTo's eCommerce and payment environments.
- Internal controls assessment as required under a PCAOB annual financial statements audit.

7 Penetration Testing

GoTo partners with reputable independent third-party vendors to conduct annual penetration testing, ensuring the identification and remediation of potential vulnerabilities. This proactive approach helps GoTo stay ahead of emerging threats and maintain the highest security standards. By leveraging the expertise of these third-party vendors, GoTo continuously enhances its security posture and protects its systems and data.

[1] Applicable to LogMeIn Resolve, LogMeIn Rescue, LogMeIn Miradore, GTARSv5

[2] Applicable to LogMeIn Resolve, LogMeIn Rescue, Rescue Live Guide, Rescue Live Lens, LogMeIn Miradore, GoToAssist v4 & v5, GoToAssist Corporate, LogMeIn Central/Pro, GoToMyPC, GoToMeeting, GoToWebinar, GoToTraining, GoToConnect, Customer Engagement, Contact Center

8 Change Management

GoTo's Change Management is designed to ensure the highest level of performance and availability of our products. This process begins with recording and tracking all proposed changes, ensuring that every modification is documented and monitored. Each change undergoes a thorough review and approval process, involving key stakeholders to assess potential impacts and benefits. Once approved, changes are rigorously tested in a controlled environment to validate their effectiveness and identify any issues. Proper rollback plans are established to ensure that, in the event of unforeseen problems, changes can be safely reverted without disrupting service. This comprehensive approach ensures that our products remain reliable and available, providing our customers with the best possible experience.

9 Endpoint Detection and Response

GoTo deploys Endpoint Detection and Response software with audit logging across all servers to ensure minimal disruption on service performance. Should any suspicious activity be detected, security investigations are promptly initiated in accordance with our incident response procedures.

10 Data Backup, Disaster Recovery and Availability

GoTo’s architecture ensures robust data backup and disaster recovery measures to guarantee the availability of our services. We perform near real-time replication to geographically diverse locations, and our databases are backed up using snapshots and point-in-time recovery. In the event of a disaster or total site failure at any of our multiple active locations, the remaining locations are designed to seamlessly balance the application load. To ensure the effectiveness of these systems, we conduct disaster recovery tests at least annually.

11 Application Security

GoTo’s application security program is crafted around the principles of the Microsoft Security Development Lifecycle (SDL) to ensure the utmost security of our product code. At the heart of this program are comprehensive manual code reviews, sophisticated threat modeling, rigorous static and dynamic code analysis, and robust system hardening measures.

12 Logging, Monitoring and Alerting

GoTo prioritizes the security of our systems through comprehensive logging, monitoring, and alerting. These measures are designed to enhance our ability to detect and respond to suspicious activities promptly. We continuously collect and analyze security logs from our environments to identify any anomalous or suspicious traffic. Our Security Operations Team monitors these logs in real-time, utilizing advanced detection mechanisms to flag potential threats. This proactive approach ensures that any identified vulnerabilities are swiftly addressed, maintaining the integrity and security of our environment.

13 Threat Management

GoTo’s Cyber Security Incident Response Team (CSIRT) is a robust and multi-faceted unit dedicated to comprehensive cyber threat protection. Our CSIRT is comprised of multiple specialized teams, each playing a critical role in safeguarding our digital environment. At the core of this effort is the Cyber Threat Intelligence team, which diligently collects, vets, and disseminates information on current and emerging threats. This proactive approach ensures that we stay ahead of potential risks. This proactive approach ensures that we stay ahead of potential risks.

GoTo remains at the forefront of threat intelligence and mitigation by continuously reviewing information from both open and closed sources. We actively participate in sharing groups and industry memberships, such as IT-ISAC and FIRST.org, to stay informed about the latest developments in cybersecurity. This collaborative effort allows us to implement cutting-edge security measures and respond swiftly and effectively to any threats, ensuring the highest level of protection for our customers and their data.

14 Vulnerability Management

GoTo employs a comprehensive vulnerability management approach to safeguard the security and integrity of our systems and data. Our process involves systematically identifying, assessing, prioritizing, and remediating vulnerabilities to maintain a robust security posture. We utilize a variety of security tools, platforms, and external sources to detect vulnerabilities, followed by thorough reviews and rigorous testing to address any identified issues. By consolidating, correlating and interpreting findings from diverse sources, we implement effective security measures that ensure our products remain secure and reliable for our customers.

GoTo’s Security Automation Framework Engine (SAFE) is vital for remediation, accurately classifying and assigning vulnerabilities to ensure a sustainable reduction over time. We continuously scan our cloud environments for vulnerabilities, sort them based on priority, and report them to engineering and management via SAFE, enabling prompt resolution.

15 Patch Management

GoTo's patch management strategy is designed to minimize the technical and business impact of known vulnerabilities through a series of well-defined steps that leverages Microsoft Azure Update Manager. Patches are deployed in phases, starting with a small test group and gradually expanding to encompass all systems. This phased approach helps identify and resolve issues early, reducing risk and maintaining system availability. Zero-day patches are given higher priority and expedited timelines to address critical vulnerabilities promptly. Systems are rebooted as necessary to ensure patches take effect. The strategy includes monitoring patch levels, obtaining patches from trusted sources, assessing risks, testing patches, prioritizing deployment, reporting on deployment status, and managing failed deployments with rollback procedures.

16 Logical Access Control

GoTo implements robust logical access control procedures to mitigate the risk of unauthorized access and data loss. Access to GoTo systems, applications, networks, and devices is granted to employees based on the 'principle of least privilege,' ensuring that users only have the minimum level of access necessary for their roles. User privileges are segregated based on functional roles (role-based access control) and environments, utilizing segregation of duties controls, processes, and procedures. To maintain the highest level of security, these logical access controls are reviewed quarterly, ensuring they remain effective and up-to-date in preventing unauthorized access.

17 Data Segregation

GoTo's multi-tenant architecture guarantees that Customer data is logically separated at the database level according to each client's GoTo account. This ensures that customer data is securely segregated from other customers' data. Access to accounts is strictly controlled and requires authentication to gain entry.

18 Physical Security

GoTo contracts with world-class cloud hosting providers to maintain physical security and environmental controls for server rooms that house production servers. These controls typically 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.

Our hosting providers limit, control, and manage physical access to their infrastructure through robust practices aligned and audited yearly against the highest security standards.

19 Perimeter Defense and Intrusion Detection

GoTo employs a comprehensive suite of perimeter protection tools, techniques, and services to safeguard against unauthorized network traffic entering our infrastructure. Our robust security measures include:

- Intrusion detection systems that continuously monitor systems, services, networks, and applications for any unauthorized access.
- Critical system and configuration file monitoring to ensure the integrity and security of our infrastructure.
- Web application firewall (WAF) and application-layer DDoS prevention services that act as a proxy for GoTo traffic, providing an additional layer of defense.
- A local application firewall that offers enhanced protection against OWASP top ten vulnerabilities and other web application threats.
- Host-based firewalls that filter inbound and outbound connections, including internal connections between GoTo systems.

20 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is dedicated to detecting and responding to security events with precision and efficiency. Our SOC employs advanced security sensors and analysis systems to identify potential issues. To ensure a swift and effective response, we have developed comprehensive incident response procedures, including a documented Incident Response Plan that is tested annually.

This Incident Response Plan is meticulously aligned with GoTo's critical communication processes, policies, and standard operating procedures. It is designed to identify, manage, and resolve suspected or identified security events across our systems and services. The plan outlines clear mechanisms for employees to report suspected security events and provides detailed escalation paths to follow when necessary.

To enhance our threat detection capabilities, GoTo utilizes a Security Information and Event Management (SIEM) tool. This tool helps correlate security events, enabling us to identify suspicious activities more effectively. Suspected events are documented and escalated as appropriate via standardized event tickets and are triaged based on their criticality. This robust approach ensures that we maintain a secure environment and respond promptly to any potential threats.

21 Deletion and Return of Content

Account administrators may request the return and/or deletion of Customer Content by submitting a ticket via support.goto.com. Requests shall be processed within thirty (30) days of receipt by GoTo.

22 Privacy Practices

GoTo takes the privacy of our Customers, Users and 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.

19.1 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 GoTo’s practices.

19.2 Regulatory Compliance

a. 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 GDPR on behalf of the Customer, we will do so in accordance with the applicable requirements of GDPR.

b. 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 CCPA on behalf of the Customer, we will do so in accordance with the applicable requirements of CCPA.

c. 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 LGPD on behalf of the Customer, we will do so in accordance with the applicable requirements of LGPD.

19.3 Data Processing Addendum

GoTo’s global Data Processing Addendum (DPA) forms part of the Terms of Service or other written agreement between GoTo and the customer and applies to GoTo’s processing of Customer’s Personal Data in connection with the Services purchased under the Agreement.

Specifically, our DPA governs GoTo’s processing of Customer Content and incorporates data privacy protections designed to meet the requirements of applicable global data privacy requirements. These include:

a. GDPR and UK Data Protection Law: Our DPA includes data processing details; sub-processor disclosures as required under Article 28; the EU Standard Contractual Clauses (EU SCCs); the UK Addendum for lawful transfer of data; and incorporates GoTo's product-specific technical and organizational measures.

b. CCPA: Additionally, to account for CCPA requirements, the DPA includes definitions mapped to the CCPA; applicable access and deletion rights; and commitments that GoTo will not sell or share our customer's personal information.

c. LGPD: Our DPA includes provisions that address GoTo's compliance with LGPD; incorporates the Brazilian Standard Contractual Clauses to support lawful transfers of Personal Data to/from Brazil; and ensure users enjoy the same privacy benefits as our other global users.

d. HIPAA: For our customers who are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we offer a Business Associate Agreement as an addendum to our Data Processing Addendum to support the parties' compliance with their compliance obligations.

19.4 Transfer Frameworks

GoTo supports lawful international data transfers under the following frameworks:

a. Data Privacy Framework

On July 10, 2023, the European Commission adopted its adequacy decision on the EU-U.S. Data Privacy Framework ("DPF"), concluding that the U.S. ensures an adequate level of protection for personal data transferred from the EU/EEA to U.S. companies certified to the EU-U.S. DPF without having to put in place additional data protection safeguards. GoTo has certified our compliance with the EU-U.S. DPF, the UK Extension to the DPF, and the Swiss-U.S. DPF to the US Department of Commerce.

b. Standard Contractual Clauses

i. EU Standard Contractual Clauses

The EU Standard Contractual Clauses (EU 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. In addition to the DPF certification, GoTo's DPA incorporates the EU SCCs and the UK Addendum to the EU SCCs. These SCCs apply if the scope of our DPF certifications do not cover the transfer of EU, UK and Swiss personal data to GoTo and will automatically apply to all applicable data transfers if the DPF is invalidated.

GoTo also maintains a group data processing agreement that incorporates national data transfer requirements, including the EU SCCs, and documents each GoTo Group entity's obligation to comply with applicable data privacy law when processing personal data transferred to it by another GoTo Group entity.

ii. Brazilian Standard Contractual Clauses
GoTo's DPA incorporates the Brazilian Standard Contractual Clauses to meet requirements under LGPD for cross-border data transfers.

c. 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.

d. 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 EUSCCs.

19.5 Contacting GoTo and Support for Data Subject Requests
GoTo maintains mechanisms to address data privacy and information security requests. You may contact our privacy team at privacy@goto.com. Our Information Security team may be reached at security@goto.com. If you receive a request from a data subject seeking to exercise their data subject rights provided to them under applicable privacy law and you need assistance to fulfill the request, please contact our support team at https://support.goto.com.

19.6 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.

19.7 Compliance in Regulated Environments
Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of the product to support devices in regulated environments.

23 Third Party Risk Management

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 proper Procurement channels. As appropriate, GoTo may obtain and evaluate compliance documentation or reports from vendors periodically to ensure their technical and organizational measures are 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, GRC 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 Management Policy governs privacy and security requirements of vendors based on 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” and “sharing” as defined under CCPA. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors.