Technical and Organizational Measures

GoTo Business Operations - TOMS

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 maintains a comprehensive awareness program to ensure employees handle personal and confidential data responsibly and in compliance with applicable laws and industry standards. All new hires, contractors, and interns receive privacy and security training during onboarding. Employees complete quarterly awareness training that addresses current risks, including AI security considerations. We also provide secure coding training for developers to strengthen product security. Annual campaigns and role-specific training reinforce our commitment to meeting regulatory requirements such as HIPAA and PCI, supporting audit readiness and internal maturity goals.

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 follows a structured, control-based approach to manage risk. We identify threats through assessments like threat modeling and compliance reviews, then apply safeguards such as access controls, encryption, and continuous monitoring. Security priorities are set based on risk impact, ensuring consistent, risk-informed decisions that strengthen resilience and protect our brand.

6 Independent Audits and Certifications

GoTo partners with independent third parties for annual audits and maintains key certifications to keep our security and privacy program aligned with industry standards, customer commitments, and applicable laws. Learn more at https://www.goto.com/company/trust.

We follow trusted frameworks and maintain certifications across three areas:

Privacy & Data Protection

- TRUSTe Enterprise Privacy & Data Governance
- TRUSTe APEC CBPR and PRP for cross-border data transfers

Security & Compliance

- ISO/IEC 27001:2022 Information Security Management System
- AICPA SOC 2 Type II and SOC 3 Type II
- BSI C5 (Cloud Computing Compliance Criteria)
- PCI DSS for eCommerce and payment environments

Regulatory & Financial Controls

- Internal controls assessment under PCAOB annual audit
- HIPAA assessed for select products

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.

8 Change Management

GoTo’s Change Management process ensures product reliability and availability. All proposed changes are documented and tracked, then reviewed and approved by key stakeholders to assess impact and benefits. Approved changes are tested in a controlled environment, with rollback plans in place to safely revert if needed. This structured approach helps maintain high performance and a seamless experience for our customers.

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.

22.1 Privacy Program

GoTo maintains a comprehensive privacy program that involves coordination from multiple functions within the company, including Legal, Security, Governance, Risk and Compliance (GRC), 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. Our privacy officer reports into our Chief Legal Officer, and we have appointed data protection officers for several jurisdictions, including the EU, the UK, Brazil, Canada and Singapore.

22.2 Regulatory Compliance

As a global company, GoTo maintains a comprehensive privacy compliance program designed to address the privacy laws to which we are subject. Below are some key legal frameworks that guide our privacy program's design and operation.

a. GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law regarding data protection and privacy for Personal Data originating or processed in the EU.

b. UK Data Protection Law

The UK's data protection laws are similar to the EU GDPR and apply to Personal Data originating or processed in the UK.

c. CCPA
The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively referred to as "CCPA"), grants California residents additional rights and protections regarding how businesses and service providers may use their personal information.

d. LGPD
The Brazilian Data Protection Law (LGPD) regulates the processing of Personal Data originating or processed in Brazil.

22.3 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), our Business Associate Agreement (BAA) is incorporated into our standard Terms of Service through our DPA. This structure is designed to support customer HIPAA compliance obligations for applicable service offerings.

22.4 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. For more information, please see our Data Privacy Framework Notice.

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.

      Finally, for transfers within the GoTo group of companies, GoTo maintains a group data processing agreement that incorporates national data transfer requirements, including the EU and Brazilian SCCs and the UK addendum to 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
      Brazil's privacy law, the LGPD, contains similar restrictions on cross-border data transfers of personal data originating in Brazil. In 2024, Brazil published its own set of standard contractual clauses in resolution CD/ANPD No 19. GoTo's DPA incorporates these clauses to provide for the lawful transfer of personal data to locations outside of Brazil.

c. Global Cross Border Privacy Rules System and Privacy Recognition for Processors System
   GoTo has obtained the Global Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications. The Global CBPR and PRP certifications are voluntary accountability-based certifications that are designed to facilitate cross-border flows of personal data in a manner that respects data privacy. The Global CBPR and PRP extends and builds on the APEC CBPR and PRP.

22.5 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.

22.6 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. You can sign up to receive updates about changes to our Sub-Processors on that site.

22.7 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

GoTo follows a structured procurement process before engaging any third-party vendor that handles Customer Content or sensitive data. This process includes:

- Reviewing the vendor’s security and privacy practices
- Obtaining and evaluating compliance documentation when required by regulation or contractual obligations
- Ensuring written agreements meet GoTo’s privacy and security standards

Our Finance, Legal, Privacy, GRC, and Security teams collaborate to verify mandatory data handling and contractual requirements. Agreements include compliance with applicable laws and, where required, Data Processing Agreements (DPAs) covering regulations such as GDPR, CCPA, LGPD, and HIPAA. For HIPAA-related services, GoTo also executes Business Associate Agreements (BAAs) with relevant vendors. Security addenda with appropriate controls are applied to vendors as needed.

24 Revision History

Version	Month/Year	Description
Version 1.4	April 2025	Updated and published to include common verbiage across all GoTo Products.
Version 1.5	August 2025	Updated the Privacy verbiage to add section 22.4c – “Global Cross Border Privacy Rules System and Privacy Recognition for Processors System”
Version 1.6	December 2025	Updated Privacy and GRC related verbiage.