International Data Transfers:
Frequently Asked Questions

July 2024

INTRODUCTION

As a global company dedicated to making IT and business communications easy, GoTo offers products such as GoTo Resolve, LogMeIn Rescue, and GoTo Connect to help securely support and connect businesses to what's most important: their teams and customers. We maintain a global data privacy program designed to protect and permit the lawful transfer of data entrusted to us by our customers and their end-users.

This document is intended to address some frequently asked questions regarding GoTo's data transfer practices when transferring personal data outside of the European Union ("EU"), European Economic Area ("EEA"), and the United Kingdom ("UK"), including:

- Data transfer mechanisms (e.g., the Standard Contractual Clauses);
- Transparency information on locations and means of processing;
- Information designed to aid with any required transfer impact analysis;
- Information on GoTo's privacy and security practices; and
- Supplementary data protection measures.

FREQUENTLY ASKED QUESTIONS (FAQ)

What categories of personal data does GoTo collect and process for its customers?

GoTo strives to limit the types and categories of personal data that it collects and further processes from its customers to that which is necessary to achieve the purpose(s) of providing and operating GoTo's Services. Ultimately, the types of information provided to GoTo by its customers and processed by GoTo are dependent upon each customer's particular GoTo Service and use case.

Additionally, it is important to note that personal data processed by GoTo when providing our Services is done in accordance with user instructions, which, unless otherwise agreed in a separate writing, shall be in the form of GoTo's Terms of Service (including any Data Processing Addendum executed in connection therewith). Additional information regarding the categories and types of information GoTo may process can be found within GoTo's Legal Terms of Service and Data Processing Addendum located at www.goto.com/company/legal, as well as in the applicable Technical and Organizational Measures ("TOMs") documentation found at www.goto.com/company/trust.

Where are GoTo's data centers located?

To provide for Service availability and redundancy needed to deliver our global user base with the best possible experience, GoTo leverages a combination of physical co-location facilities and cloud hosting providers in Australia, Brazil, Germany, India, the United Kingdom, the United States, and Singapore. Similarly, GoTo has employees and/or operations in Australia, Brazil, Canada, Guatemala, Germany, Hungary, India, Mexico, the United Kingdom, and the United States. However, this does not mean that personal data will be hosted, processed, or accessible in all of these regions – Service-specific data centers are identified in the applicable Sub-processor Disclosure located in the Product Resources section of our Trust and Privacy Center at www.goto.com/company/trust.

Where can I find information about GoTo's sub-processors?

Service-specific disclosures about the data center and third-party sub-processor regions utilized to provide our Services are specified in the relevant Sub-processor Disclosures found in the Product Resources section of our Trust and Privacy Center (www.goto.com/company/trust). Similarly, GoTo publishes a disclosure of its wholly-owned affiliate entities, which may be found in its Affiliate Disclosure available at GoTo's Trust and Privacy Center.

EU Transfers of Personal Data

What is an international transfer of personal data?

An international or "cross-border" transfer of personal data occurs when personal data is provided by a party in one country (or subject to certain laws) to another party in a different country. Some privacy laws regulate these transfers of personal data. For example, the GDPR prohibits these transfers unless a legally recognized transfer mechanism is in place, including where: a) the recipient is located in a country whose data privacy laws have been formally determined by the European Commission as substantially similar to the GDPR or "adequate"; b) certain conditions apply, such as where the individual consents to the transfer; or c) appropriate safeguards exist, such as where the recipient is located in the United States and has certified to the Data Privacy Framework, or if the recipient is not located in a country with laws that have been "deemed adequate," where the parties have agreed to certain contractual commitments about how the data will be handled, such as the EU's Standard Contractual Clauses (EU SCCs).

Does GoTo transfer personal data outside the EU and the UK?

Yes. GoTo operates in many countries, providing Services that empower millions of people and businesses around the world. Depending on the specific Service, GoTo may host and/or process data outside the EU/EEA and the UK. For these transfers, GoTo has taken steps to ensure adequate measures are in place to protect personal data in accordance with applicable data privacy laws, including the GDPR.

Our Data Processing Addendum ("DPA"), together with our standard Terms of Service, explain how GoTo, in its capacity as a service provider and data processor, processes personal data when providing and operating our Services. For additional information on the location of GoTo's affiliates and sub-processors, please review GoTo's Affiliate Disclosure and the applicable Sub-processor Disclosures found at its Trust and Privacy Center.

What lawful methods does GoTo use under Chapter 5 of the GDPR to make these transfers?

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.

In addition to this 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.

Further, it is important to note that a customer purchasing GoTo Services from the EU/EEA* will be contracting with GoTo's Irish affiliate, GoTo Technologies Ireland Unlimited Company, and the Services agreement will be subject to Irish (Member State) law, including applicable data protection laws (such as the GDPR and Data Protection Act 2018), and any data processed would therefore be protected pursuant to the governing laws of Ireland.

*UK customers will contract with GoTo Technologies UK Limited, and the agreement shall be subject to English and Welsh law.

What steps do I need to take if my organization is transferring data to GoTo on the basis of SCCs?

GoTo has updated its DPA to include the latest SCCs and made pre-signed executable versions available online at www.goto.com/legal.

Are GoTo's sub-processors bound by the SCCs?

Yes. It is GoTo's practice to enter into Data Processing Addendums containing provisions required by applicable law and protections that are no less protective than

those in our DPA. Where required, our vendor data processing addendums incorporate the EU SCCs and UK addendum to support lawful transfers of personal data to third countries. Information about GoTo's sub-processors and their locations is available here.

What technical and organizational measures does GoTo have in place to protect personal data?

As part of GoTo's commitment to privacy and data security, we have implemented and maintain additional technical data security and privacy measures, including encryption, which go beyond the minimum requirements of the SCCs. Each of our product offerings have implemented their own product specific technical and organizational measures, including, but not limited to:

- **Encryption**: The utilization of Transport Layer Security ("TLS") v1.2 encryption to protect and reduce the risk of eavesdropping or interception of data in transit (e.g., communications during a "Computer Audio" or "VoIP" call).
- **Security and Data Protection Principles**: A company-wide secure development lifecycle ("SDL") program which takes security and data protection principles into account in relevant phases of the development process and supports developers in their creation of highly secure software, compliance with security requirements, and the reduction of development costs.
- **Privacy by Design ("PbD")**: We maintain PbD standards and requirements, as well overall Security and Technical Privacy standards to ensure our products take into account data protection and security guidelines in relevant aspects of business operations.
- **Third-Party Security and Privacy Assessments/Frameworks**: GoTo's data security and/or privacy programs, as applicable, are regularly assessed against recognized third-party tested and validated standards, including:
    - The American Institute for Certified Public Accountants ("AICPA") Service Organization Control Report #2 ("SOC2") Type II
    - AICPA Service Organization Control Report #3 ("SOC3") Type II
    - Bundesamt für Sicherheit in der Informationstechnik ("BSI") Cloud Computing Compliance Controls Catalogue ("C5")
    - ISO 27001 (for GoTo Resolve, LogMeIn Rescue, GoToAssist Remote Support v5, and Miradore)
    - TRUSTe Enterprise Privacy Certification
    - APEC Cross Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP")

  The security standards noted above include robust access controls and procedures, as well as those addressing encryption, access management, confidentiality, and security.
- **Robust Internal Privacy and Regulatory Compliance Programs:** These programs, overseen by subject matter experts and trained professionals across GoTo's Legal, Security, and Governance, Risk, and Compliance ("GRC") groups, help us maintain policies, procedures, and operations to ensure that GoTo stays apprised of, and in compliance with, applicable data protection rules and regulations.

GoTo's internal teams consistently assess and seek to improve our privacy programs and undertake actions including, but not limited to, conducting annual internal privacy audits (to validate compliance with GDPR, CCPA, and other applicable data protection laws) in furtherance of this goal.

Detailed and product-specific information about these additional technical data security and privacy measures can be found within GoTo's Technical and Organizational Measures ("TOMs") documentation available in the "Product Resources" Section of our Trust and Privacy Center (www.goto.com/company/trust).

Transfer Impact Assessments

What is a Transfer Impact Assessment (TIA)?

Following the European Court of Justice's C-311/18 decision, frequently known as the "Privacy Shield Invalidation" or "Schrems II," the European Commission released revised SCCs and the European Data Protection Board ("EDPB") published its final recommendations regarding supplementary measures to ensure compliance with data protection laws when transferring personal data outside the EU/EEA. As a result, it was recommended that "data exporters" (i.e., a GoTo customer) verify, on a case-by-case basis, whether the laws of the third country afford personal data a level of protection that is essentially equivalent to the EU/EEA's protections. If not, the data exporter will need to determine whether appropriate supplementary measures have been implemented by the "data importer" (i.e., GoTo) to help ensure the requisite level of protection.

GoTo has designed its data protection and security programs to ensure an appropriate level of data protection, consistent with applicable law, and we have outlined the supplemental measures and safeguards taken to provide these assurances in this FAQ (see "*What technical and organizational measures does GoTo have in place to protect personal data*?" above, as well as the policies, procedures, and documentation referenced directly below).

What other resources does GoTo provide its customers to conduct a TIA?

The following resources may assist GoTo customers in conducting a TIA in relation to our Services:

- Trust and Privacy Center
- EDPB Recommendations 01/2020 on Supplementary Measures
- Sub-processor Disclosures
- Product Resources
- Government Request Policy
- GDPR Whitepaper
- U.S. Dept. of Justice Whitepaper Re: Schrems II Decision
- GoTo's Data Processing Addendum
- Data Privacy Framework Program

Government Requests

Does GoTo fall under 50 U.S. Code § 1881a ("FISA 702") or is it otherwise subject to the requirements of Executive Order 12333?

GoTo is subject to the applicable laws and regulations of each country in which it operates. It is important to note that, while GoTo may be headquartered in the United States, EU-based customers are contracting with, and agreeing to data protection terms with, a Member State-based GoTo entity (e.g., GoTo Technologies Ireland Unlimited Company*). As such, all requests received from U.S. government or law enforcement agencies, whether part of the above provisions, the U.S. Cloud Act, or otherwise, would need to be validly recognized within and under the laws of the Republic of Ireland or the applicable Member State. Additional information on GoTo's approach to government requests for access to data can be found in our Government Request Policy.

*UK customers are contracting with GoTo Technologies UK Limited, and all requests would need to be validly recognized within and under the laws of England or Wales.

What is GoTo's approach to government requests for access to data?

GoTo has published a Government Request Policy which is designed to provide greater transparency regarding the guidelines used by GoTo to determine how and when we will process demands received from law enforcement, national security, and other regulatory bodies ("Government") for information about our customers, their employees, and/or their users. GoTo will review all international Government requests on a country-by-country and case-by-case basis to consider and balance our local legal obligations against our commitments to promote public safety and user privacy. It is GoTo's policy not to provide any customer data to any Government entity, unless the requesting party has appropriate authority to request such information under applicable law and has provided GoTo with a valid warrant, subpoena, court order or equivalent legal process.

Who should I contact if I have questions regarding GoTo's data protection practices?

Please reach out to privacy@goto.com for any additional questions regarding GoTo's data protection practices. Note that GoTo cannot provide legal advice to its customers and recommends that they consult their own legal counsel if they have questions regarding the legality of their own data protection compliance programs.