International Data Transfers:
Frequently Asked Questions

Published: 27 September 2021

INTRODUCTION

As the global "work from anywhere" company, LogMeIn provides products that are used to simplify how people connect with each other and the world around them to drive meaningful interactions, deepen relationships, and create better outcomes for professionals and businesses. With users in nearly every country around the world, we are committed to maintaining a global data privacy program designed to protect and permit the lawful transfer of data entrusted to us by our customers, users, and their end-users.

This document is intended to provide our valued customers, users, and end-users with answers to some frequently asked questions regarding LogMeIn'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 LogMeIn's privacy and security practices; and
- Supplementary data protection measures.

FREQUENTLY ASKED QUESTIONS (FAQ)

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

LogMeIn strives to limit the types and categories of personal data that it collects from, and processes on behalf of, its users to include only information which is necessary to achieve the purpose(s) of providing and operating LogMeIn's Services. Ultimately, the types of information collected and processed by LogMeIn are dependent upon each customer's particular LogMeIn Service and use case.

Additionally, it is important to note that personal data processed by LogMeIn 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 LogMeIn's Terms of Service (including any Data Processing Addendum executed in connection therewith). Additional information regarding the categories and types of information LogMeIn may process can be found within LogMeIn's Legal Terms of Service and Data Processing Addendum located at www.logmein.com/legal, as well as in the applicable Security and Privacy Operational Controls documentation found at www.logmein.com/trust.

Where are LogMeIn's data centers located?

To ensure sufficient Service availability, uptime, and redundancy needed to provide our global user base with the best possible experience, LogMeIn leverages a combination of physical co-location facilities and cloud hosting providers in Australia, Brazil, Germany, India, Ireland, The United Kingdom, The United States, and Singapore. Similarly, LogMeIn has employees and/or operations in Australia, Brazil, Canada, Guatemala, Germany, Hungary, India, Ireland, 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.logmein.com/trust.

Where can I find information about LogMeIn'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.logmeininc.com/trust). Similarly, LogMeIn publishes a disclosure of its wholly-owned affiliate entities, which may be found in its Affiliate Disclosure available at LogMeIn's Trust and Privacy Center.

EU Transfers of Personal Data

What is an international transfer of personal data?

An international transfer of data occurs when personal data is transferred out of the EU/EEA. Currently, EU/EEA data protection laws specify that international transfers may only take place to a "third country," for example, under one of the conditions identified under Chapter 5 of the GDPR, which include where: a) a formal adequacy decision by the European Commission has been provided regarding a "third-country" whose laws are determined to be substantially similar or "adequate"; b) consent is provided; or c) appropriate safeguards are agreed upon, such as those within the Standard Contractual Clauses ("SCCs").

Does LogMeIn transfer personal data outside the EU?

LogMeIn has a global reach, with operations in over 15 different countries providing Services which empower millions of people and businesses around the world to do their best work simply and securely — on any device, from any location and at any time. Depending on the specific Service, LogMeIn may host and/or process data outside the EU. For these transfers, LogMeIn has taken steps to ensure adequate measures are in place to protect personal data in accordance with the GDPR and applicable data protection laws and regulations.

Our Data Processing Addendum ("DPA"), together with our standard Terms of Service, explain how LogMeIn, 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 LogMeIn's affiliates and sub-processors, please review LogMeIn's Affiliate and the applicable Sub-processor Disclosures found at its Trust and Privacy Center.

What is the legal basis (under Chapter 5 of the GDPR) for these transfers?

On June 4, 2021, the European Commission published an updated version of the SCCs designed to be utilized for international transfers of personal data. These SCCs were drafted specifically to reflect the additional requirements imposed under GDPR for international transfers of personal data. While LogMeIn has generally relied on a mixture of transfer mechanisms to support lawful data transfers from and to the EU/EEA in compliance with Chapter 5 of the GDPR, we will continue to rely on the SCCs as the primary legal basis for EU/EEA data transfers. The most current version of the SCCs are incorporated into LogMeIn's DPA – available pre-signed and online for execution.

Further, it is important to note that a customer purchasing LogMeIn Services from the EU/EEA* will be contracting with LogMeIn's Irish affiliate, LogMeIn 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.

*Note that LastPass users located in the EU/EEA shall be contracting with LastPass Ireland Limited. Additionally, UK users shall be contracting with LogMeIn Technologies UK Limited, and the agreement shall be subject to English law, including the Data Protection Act.

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

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

Additionally, it is important to note that while the European Commission has affirmed that any existing SCCs executed prior to September 27, 2021 may continue to be utilized for the lawful transfer of personal data

until December 27, 2022, any customers who wish to execute LogMeIn's revised DPA with the most current SCCs sooner may do so by visiting www.logmein.com/legal.

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

Yes. Not only does LogMeIn conduct appropriate due diligence on all of its sub-processors, but we also take steps to ensure that they are bound by an Article 28-compliant Data Processing Addendum with protections that are no less protective than those in our DPA and which incorporate and utilize the SCCs for applicable lawful transfers of personal data. LogMeIn is actively working to ensure that the newest SCCs substitute the prior SCCs within the permitted transition period (ending on December 27, 2022) with respect to its applicable existing sub-processing agreements.

Does LogMeIn still rely on the Privacy Shield for transfers of personal data?

No. LogMeIn is no longer relying on the EU-U.S. or Swiss-U.S. Privacy Shield to facilitate transfers of personal data. In addition, the Company's DPA no longer includes Privacy Shield as a utilized framework, and instead relies on other lawful means of data transfer as permitted by Chapter 5 of the GDPR, including the SCCs. More information on LogMeIn's transfer mechanisms can be found in our Trust and Privacy Center.

Has Brexit impacted LogMeIn's international data transfers?

No. On June 28, 2021, the European Commission adopted two adequacy decisions for the UK which have the effect of permitting lawful transfers of EU personal data to and from the UK without the need for further action by LogMeIn or our customers. We continue to monitor developments in the UK in relation to potential new UK SCCs, which, if approved and deemed necessary, will be incorporated into a later revised version of our DPA in order to ensure our UK customers may continue to make lawful data transfers. In the interim, customers may continue to execute our current DPA, (found at www.logmein.com/legal), which is designed to permit lawful transfer to and from the UK.

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

As part of LogMeIn'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**: LogMeIn'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 LogMeIn Rescue and GoToAssist Remote Support v5)
    - 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 LogMeIn's Legal, Security, and Governance, Risk, and Compliance ("GRC") groups, help us maintain policies, procedures, and operations to ensure that LogMeIn stays apprised of, and in compliance with, applicable data protection rules and regulations. LogMeIn'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 LogMeIn's Security and Privacy Organizational Controls ("SPOC") documentation available in the "Product Resources" Section of our Trust and Privacy Center (www.logmeininc.com/trust). We have also highlighted a selection of technical and organizational measures for some of our most popular products in Appendix A below.

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 LogMeIn 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., LogMeIn) to help ensure the requisite level of protection.

LogMeIn 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 LogMeIn have in place to protect personal data*?" above, as well as the policies, procedures, and documentation referenced directly below).

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

The following resources may assist LogMeIn 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
- LogMeIn's Data Processing Addendum

Government Requests

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

LogMeIn is subject to the applicable laws and regulations of each country in which it operates. It is important to note that, while LogMeIn may be headquartered in the United States, EU-based customers are contracting with, and agreeing to data protection terms with, a Member State-based LogMeIn entity (LogMeIn 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 LogMeIn's approach to government requests for access to data can be found in our Government Request Policy.

*Note that LastPass users in the EU/EEA shall be contracting with LastPass Ireland Limited. Additionally, UK users shall be contracting with LogMeIn Technologies UK Limited, and the agreement shall be subject to English law, including the Data Protection Act.

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

LogMeIn has published a Government Request Policy which is designed to provide greater transparency regarding the guidelines used by LogMeIn 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. LogMeIn 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 LogMeIn'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 LogMeIn with a valid warrant, subpoena, court order or equivalent legal process.

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

Please reach out to privacy@logmein.com for any additional questions regarding LogMeIn's data protection practices. Note that LogMeIn 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.

Appendix A – Technical and Organizational Measures

A selection of "supplemental" technical and organizational measures employed by some of our most popular offerings are found below (please visit www.logmein.com/trust for more complete information about all LogMeIn Services):

All **GoToConnect** network traffic flowing in and out of LogMeIn datacenters, including all Customer Content, is encrypted in transit utilizing up to TLS v1.2 (if supported). Customer voicemail recordings, voicemail greetings, meeting recordings, meeting transcripts, meeting notes, and call recordings are encrypted at-rest using Advanced Encryption Standard ("AES") 256-bit encryption when stored within LogMeIn's cloud hosting environment. Where a customer requires more granular control of their information, they may elect to store meeting recordings locally at a location of their choosing and may similarly elect to utilize their own Amazon Web Service ("AWS") S3 cloud hosting instance (at a AWS location of their choosing) for call recordings. GoToConnect's integrated Service offering utilizes LogMeIn's proprietary identity management platform for customer provisioning, offers Single sign-on ("SSO") using Security Assertion Markup Language ("SAML"), and integrates directly with LogMeIn's GoToMeeting platform via Application Programming Interface ("API"). GoToConnect also offers robust administrative controls, such as allowing customer account administrators to configure password policies and requiring utilization of SAML for login.

GoToMeeting permits the use of screen sharing and chat-sessions over an end-to-end encrypted ("E2EE") channel by utilizing a meeting password – which results in screen sharing and chat information being unavailable to LogMeIn or anyone other than the customer and their attendees who have that customer supplied password. Further, GoToMeeting users can elect to store meeting recordings locally on their device (or another location of their choice), thereby permitting them to maintain the information both within the confines of the EU and in a manner inaccessible to LogMeIn (or to others by way of LogMeIn). To the extent GoToMeeting users elect to utilize LogMeIn's cloud hosting, their meeting recordings, transcripts, and notes shall be stored in a US-based instance of AWS and encrypted at rest utilizing AES-256-bit encryption. Additional options are also available to store chat logs local to a user, as well as disable chat collection or Business Messaging.

LastPass employs a zero-knowledge model for all tiers of its offerings, which means that decryption of a users' sensitive vault contents occurs entirely at the user and user-device level (called "local-only encryption"). In other words, LogMeIn does not have access to decrypted sensitive vault information of any kind – this is made possible not only because of user-level decryption and encryption, but because only the user maintains the Master Password, which serves as the encryption key – which LogMeIn never has access to in unencrypted form. LastPass' device-level encryption implements AES-256-bit encryption, PBKDF2 SHA256 bit, which is salted and hashed in order to ensure complete security in the cloud. Learn more about how LastPass secures vault data here. Additionally, upon new account creation, LastPass users can elect to have their encrypted vault hosted in either Australia, Europe, Singapore, or the United States.

Rescue employs AES-256-bit encryption for custom reporting and chat sessions and utilizes a proprietary peer-to-peer architecture, whereby remote sessions initiated between a LogMeIn customer and their end-user or data subject are not only encrypted in transit at TLS v1.2 (where supported), but also directly between the parties – Rescue establishes the connection via a gateway and then drops off once said connection is established. Specifically, Rescue's proprietary key exchange forwarding protocol is designed to provides security even against interception or eavesdroppers on LogMeIn's infrastructure. The connection between the client and the host is facilitated by the gateway in order to ensure that the client can connect to the host independently of the network setup. With the host already having established a TLS connection to the gateway, the gateway forwards the client's TLS key exchange to the host via a proprietary key re-negotiation request. This results in the client and the host exchanging TLS keys without the gateway learning the key. In addition, upon new account creation, LogMeIn Rescue also permits customers to request that their account be configured to store Customer Content (including any personal data therein), within the European Union or the United States. Not only does Rescue, by default, collect limited information during a remote session, but it also provides its users with additional data minimization capabilities such as the ability to disable the chat feature as well as ability to disable the collection for reporting purposes of any IP address of users or their data subjects.