Privacy Shield Invalidation:
Overview and Frequently Asked Questions

Published: 21 October 2020

INTRODUCTION

LogMeIn is aware of the European Court of Justice's C-311/18 decision, frequently known as the "Privacy Shield Invalidation" or "Schrems II," and is actively monitoring the situation. This document is intended to provide our valued European-based customers, users, and end-users (or those users otherwise subject to the territorial scope of the GDPR and applicable EU data protection laws) with answers to some frequently asked questions regarding LogMeIn's data transfer practices in light of the Schrems II decision.

OVERVIEW

Key Points: LogMeIn maintains a privacy program designed to meet the needs of our global user base and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were just two of several mechanisms which LogMeIn has relied upon to lawfully transfer personal data from and to the European Union ("EU") and European Economic Area ("EEA"). Additional data transfer mechanisms remain in place and if you previously executed LogMeIn's **Data Processing Addendum ("DPA"),** which has incorporated the **Standard Contractual Clauses ("SCCs")**, no further action is required and you can continue to enjoy our services in the same manner and fashion as before. If you still need to execute the DPA and SCCs, please click here.

Details: We will continue to monitor the recommendations and guidance issued by the European Data Protection Board and the Data Protection Authorities of the Member States, and evaluate whether any changes may need to be made to our privacy program in order to continue to support our global customers. In the meantime, it is important to note that, while the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks have been invalidated, other data transfer mechanisms already in use by LogMeIn, including, but not limited to, the SCCs (part of LogMeIn's global DPA) remain a valid means of transferring data from and to the EU and EEA. In addition, LogMeIn has taken steps to implement additional safeguards, mechanisms, and contractual terms, which afford users protections which go above and beyond the SCCs, including:

- A comprehensive global DPA that incorporates and supplements the SCCs, as well as the requirements under Article 28 of the GDPR, to ensure an adequate level of protection for LogMeIn's customers, users, and end-users;
- Participation in and submission to additional voluntary privacy frameworks, including the APEC CBPR and PRP, which demonstrate LogMeIn's commitment to guidelines such as those of the Organization for Economic Co-operation and Development ("OECD") and similar guidelines which underpin modern European privacy law;
- A global privacy program which strives to afford all of our users the same rights to privacy as those afforded to our European-based data subjects and customers; and
- A robust and transparent Trust and Privacy Center, which provides any visitor, including LogMeIn customers, users, and end-users, with detailed information about LogMeIn's data protection practices.

At LogMeIn, we take the privacy and security of our customers and their data very seriously. Should you have additional questions or require further diligence, we have also published responses to some frequently asked questions below.

FREQUENTLY ASKED QUESTIONS (FAQ)

Does LogMeIn transfer data outside the EU? If so, to which countries?

LogMeIn offers a broad range of category-defining products designed to unlock the potential of the modern workforce by making it possible for millions of people and businesses around the globe 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. Our Data Processing Addendum, together with our standard Terms of Service, explain how, in LogMeIn's capacity as a service provider and data processor, we process personal data in order to provide and operate our services. Specifically, LogMeIn's Terms of Service state: "You understand that your personal data may be processed in connection with your use of our Services, software, and websites which are provided via equipment and resources located in the United States and other locations throughout the world."

In order 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 co-location facilities and cloud hosting providers in Australia, Brazil, Germany, India, The United Kingdom, The United States, and Singapore. Similarly, LogMeIn has offices and employees in Australia, Brazil, Canada, Guatemala, Germany, Hungary, India, Israel, Mexico, The United Kingdom, and The United States. However, this does not mean that your personal data will be hosted, processed, or accessible in all of these regions. Service-specific disclosures about the data center and third-party subprocessor regions utilized to provide our products 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.

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

While LogMeIn has generally relied on a mixture of transfer mechanisms to support lawful data transfers from and to the EU and EEA in compliance with Chapter 5 of the GDPR, it primarily leveraged both the Standard Contractual Clauses (SCCs) and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Following the recent invalidation of the Privacy Shield, LogMeIn has continued to rely on the SCCs as the legal basis for EU data transfers. The SCCs are incorporated into LogMeIn's Data Processing Addendum – available in English and German online for execution.

Further, it is important to note that a Customer purchasing LogMeIn services from the EU* will be contracting with LogMeIn's Irish affiliate, LogMeIn Ireland Limited, 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. In addition, when relying on the SCCs, the governing law shall be that of the customer, who acts as the controller or data exporter, such that transfers are protected by and subject to the customer's local Member State law.

*Note that U.K. users shall be contracting with LogMeIn Technologies UK Limited, and the agreement shall be subject to English law, including the Data Protection Act.

Where can I find a copy of LogMeIn's Standard Contractual Clauses (SCCs)?

Please click here to review and execute LogMeIn's Data Processing Addendum and SCCs.

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

It is important to note that, while LogMeIn may be headquartered in the United States, EU-based customers are contracting and agreeing to data protection terms with a Member State-based LogMeIn entity (LogMeIn Ireland Limited). 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.

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

In certain instances, we may receive requests from courts, law enforcement, government or regulatory agencies to produce information about specific LogMeIn customers. It is LogMeIn's policy not to provide any customer data to any court, law enforcement, government or regulatory agency, unless the requesting party has appropriate authority under applicable law and has provided LogMeIn with a valid warrant, subpoena, court order or equivalent legal process. LogMeIn may seek to narrow requests that we believe are overly broad in scope, request additional context if the nature of the investigation is not clear, or push back on the request for other reasons.

If LogMeIn transfers personal data to the U.S., which technical measures does it take, support, and/or offer in order to prevent or reduce the risk of interception or eavesdropping?

As part of LogMeIn's commitment to maintain world-class privacy and data security programs, we have continued to build-upon and enhance our offerings with additional technical data security and privacy measures, including encryption, which go beyond the minimum requirements of the SCCs.

On a company and portfolio-wide basis, our products take into account industry standard or better privacy and security standards, including, but not limited to:

- 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).
- A company-wide secure development lifecycle (SDL) program which takes security and data protection principles into account in all 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. Similarly, we maintain Privacy-by-Design standards and requirements, as well overall Security and Technical Privacy standards to ensure our products take into account data protection and security guidelines in all aspects of business operations.
- LogMeIn's data security and/or privacy programs, as applicable, are regularly assessed against:
    - Recognized third-party tested and validated security standards, including the American Institute for Certified Public Accountants (AICPA) Service Organization Control Report #2 (SOC2) Type II, Service Organization Control Report #3 (SOC3), and Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls Catalogue (C5), which include robust access controls and procedures, as well as those addressing encryption, access management, confidentiality, and security. LogMeIn's Bold and Rescue offerings also maintain ISO 27001 certifications.
    - Applicable regulatory and legal requirements, including annual internal privacy audits (to validate compliance with GDPR, CCPA, and other applicable data protection laws) conducted by LogMeIn's internal Privacy Team, which includes subject matter experts from within its Legal, Security, and Governance, Risk, and Compliance (GRC) groups, as well as external validation by way of a TRUSTe

Verified Privacy certification and participation in the APEC CBPR and PRP frameworks. Click here to learn more about LogMeIn's privacy programs.

In addition to the controls noted above, each of our world-class offerings have implemented their own product-specific technical and organizational measures. Detailed information about these measures can be found in each products' Security and Privacy Organizational Controls (SPOC), available in the "Product Resources" Section of our Trust and Privacy Center (www.logmeininc.com/trust). For convenience, we have also highlighted a selection of technical and organizational measures employed by some of our most popular offerings below:

- **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 Amazon Web Services and encrypted at rest utilizing Advanced Encryption Standard (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 SHA-256 bit, which is salted and hashed 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 also 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. 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 Europe 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.

- **Bold360 and Bold** both encrypt data at rest at AES-256 bit. Additionally, upon new account creation, a customer can request that their account be configured to store Customer Content (including any personal data therein) within Europe or the United States. Bold360 also includes other robust features and controls to limit the categories of data which are retained, including the ability to configure custom or rolling data retention periods to help minimize any hosted or stored data on LogMeIn's systems or servers. Similarly, the Bold offerings include export API's so that a customer can elect to export and store a machine-readable copy of their information locally and then subsequently can request or initiate deletion to reduce or minimize data hosted by and/or accessible to LogMeIn.

We encourage you to visit our Trust and Privacy Center at www.logmeininc.com/trust, including the "Product Resources" Section to review more product-specific information for your own applicable offering. For best results, please choose the "Filter by" option at the top of the Product Resources section to choose your relevant products.

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. LogMeIn'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. Further, standard templates with third-party suppliers and vendors included the SCCs and are relied on for transfers within the territorial scope of the GDPR.

Additional information about LogMeIn's data privacy and security programs can be found in our Trust and Privacy Center Resources, our DPA, and our Privacy Policy. However, should you be unable to find the information you need, please don't hesitate to contact us at privacy@logmein.com.