DATA PROCESSING ADDENDUM

Based on European Commission Decision 2010/87/EU
Standard Contractual Clauses (processors)

This Data Processing Addendum ("DPA") supplements any current Terms of Service or other agreement ("Commercial Agreement") in place between LogMeIn, Inc., ("LMI") and the customer executing below ("Customer"), in reliance on the following facts and agreed terms. All capitalized terms not defined in this DPA or the exhibits attached hereto shall have the meaning set forth in the Commercial Agreement:

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Attachment 1 (including Appendices 1 and 2)
2. This DPA has been pre-signed on behalf of LMI. The Standard Contractual Clauses in Attachment 1 have been pre-signed by LMI.
3. To complete this DPA, Customer must:
   i. Complete the information in the signature box to this DPA, sign and date (**page 2**)
   ii. Complete the information regarding the data exporter on the first page of Attachment 1 (**page 3**)
   iii. Complete the information in the signature box and sign Attachment 1 (**page 9**), and Appendix 1 (**page 11**)
   iv. Submit the completed and signed DPA to LMI.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Commercial Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, LMI is party to this DPA. No other LMI entity is party to this DPA, notwithstanding the pre-filled signature below.

If the Customer entity signing this DPA has executed an order form or similar ordering document for SaaS services ("Order Form") with LMI or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and LMI is party to this DPA.

This DPA shall replace and supersede any prior agreement entered into between the parties relating to the processing of the types of Customer data identified below.

A. LMI provides the products, solutions and services set forth in the Commercial Agreement (together, "Solutions"). LMI and Customer desire to enter into this DPA to define the parties' obligations with respect to the processing of personal data ("EEA+ Data") relating to data subjects in the European Economic Area and Switzerland ("EEA+ Data Subjects").

B. In order to enable Customer to meet requirements under applicable data protection laws pursuant to Articles 25(1) and 26(1) of Directive 95/46/EC of 24 October 1995, the parties hereby agree on the attached Standard Contractual Clauses (processors) ("SCC 2010" which shall supersede any conflicting terms in the Commercial Agreement and Sections A through E of this DPA if and to the extent EEA+ Data Subjects assert rights as third party beneficiaries regarding their EEA+ Data. LMI assumes all rights and obligations as 'data importer' and may terminate the SCC 2010 only if and when the Commercial Agreement expires or is terminated or if LMI offers alternative means to Customer to meet requirements under applicable law. Customer assumes all rights and obligations as 'data exporter' and may terminate the SCC 2010 at Customer's discretion by written notice to LMI.

C. The Commercial Agreement and Sections A through E of this DPA shall apply only between the parties and shall not confer any rights to any third parties. With respect to the
rights and obligations of the parties vis-à-vis each other, and if and to the extent either party asserts rights or remedies against the other party, the Commercial Agreement and Sections A through E of this DPA shall supersede and take precedent over any conflicting terms in the SCC 2010.

D. Customer has instructed or authorized the use of subprocessors to assist LMI with respect to the performance of LMI's obligations under the Commercial Agreement on the condition that LMI has executed a written agreement with such subprocessors whereby the subprocessors assume all obligations of a subprocessor under the SCC 2010 or stricter or materially similar obligations, as permitted or required by applicable law.

E. With respect to requests for audits as required by applicable provisions of the SCC 2010, prior to commencement of any such audit, LMI and Customer shall mutually agree upon the scope, timing and duration of the audit, as well as the applicable fees for reimbursement of reasonable expenses associated with the audit. If the parties are unable to mutually agree on such payments, requests or instructions, Customer may terminate the Commercial Agreement, subject to payment of any outstanding fees owed for services provided and/or products purchased prior to termination of the Commercial Agreement.

Agreed by Customer:	Agreed by LogMeIn , Inc.:
By:	By:
Name:	Name: Anthony Bishop
Title:	Title: Vice President, Deputy General Counsel
Date	Date

[Remainder of page intentionally left blank]

ATTACHMENT 1
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: ..... ; .....fax:.....;

e-mail: .....

(the data **exporter**)

And

Name of the data importing organisation: LogMeIn, Inc.

Address: 333 Summer Street, Boston, MA 02210 USA

Tel.: +1-781-897 5580; fax: 1.781.437.1820; e-mail: DPA@logmein.com

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement

with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature…….

On behalf of the data importer:

Name (written out in full): Anthony Bishop

Position: Vice President, Deputy General Counsel

Address: 333 Summer Street, Boston, MA 02210 USA

Signature…….

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased the Solutions on the basis of one or more Order Form(s).

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
LMI, Inc. is a provider of solutions that enable its customers and their employees to work from any location from any device, and such solutions may processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Data exporter may submit Personal Data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Subscribers/users
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)

Categories of data
The personal data transferred concern the following categories of data (please specify):
In using the solutions, data exporter may submit Personal Data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to: first and last name; title; position; employer; communication data, inventory data, and traffic data (e.g. telephone, email); data uploaded to the solution; limited contact information; and possibly professional life information such as compensation information, geography, and some ID data such as employee number.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
The parties do not anticipate any special categories of information will be provided.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
The objective of Processing of Personal Data by data importer is in furtherance of servicing the customer and the performance of the Solutions pursuant to the Agreement.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER
Name: Anthony Bishop, Vice President, Deputy General Counsel

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of any Personal Data, as described in the Technical and Organizational Data Security Measures and as may be applicable, as updated from time to time, and accessible via https://secure.logmein.com/home/policies/technical-measures and set forth below.

TECHNICAL AND ORGANIZATIONAL DATA SECURITY MEASURES

Contents

Introduction 11
The Technical and Organizational Data Security Measures 11
Access Control of Processing Areas (Physical) 11
Access Control to Data Processing Systems (Logical) 11
Availability Control 12
Transmission Control 13
Input Control 13
Separation of Processing for Different Purposes 14
Documentation 14
Monitoring 14
Definitions 14
Document History 15

• Introduction

This Technical and Organizational Data Security Measures articulates the technical and organizational security measures implemented by LogMeIn, Inc. ("LMI") in support of its Security Program.

• The Technical and Organizational Data Security Measures

LMI has implemented and maintains a security program that leverages the ISO/IEC 27000-series of control standards as its baseline.

• Access Control of Processing Areas (Physical)

Web applications, communications infrastructure, and database servers of LMI are located in secure data centers. LMI has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where Personal Data are processed or used.

This is accomplished by:

- Establishing security areas;
- Protection and restriction of access paths;
- Securing the data processing equipment and personal computers;
- Establishing access authorizations for employees and third parties, including the respective documentation;
- Regulations/restrictions on card-keys;
- Restricting physical access to the servers by using electronically-locked doors and separate cages within co-location facilities;
- Access to the data center where Personal Data are hosted is logged, monitored, and tracked via electronic and CCTV video surveillance by security personnel; and
- Data centers, where Personal Data may be hosted, are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication procedures (e. g., hand geometry), and/or electronic proximity identity cards with users' photographs.

• Access Control to Data Processing Systems (Logical)

LMI has implemented suitable measures to prevent its data processing systems from being used by unauthorized persons.

This is accomplished by:

- Establishing the identification of the terminal and/or the terminal user to the LMI systems;
- Automatic time-out of user terminal if left idle, identification and password required to reopen;
- Automatic lock out of the user ID when several erroneous passwords are entered. Events are logged and logs are reviewed on a regular basis;
- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end-servers;
- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third party auditors;
- Issuing and safeguarding of identification codes; and

- Role-based access control implemented in a manner consistent with principle of least privilege.
- Remote access to LMI's services delivery network infrastructure is secured using two-factor authentication tokens.
- Access to host servers, applications, databases, routers, switches, etc., is logged.
- Access and account management requests must be submitted through internal approval systems.
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at minimum: the employee's manager and the role approver or "owner" for the particular system or internal application.
- Passwords must adhere to the LMI password policy, which includes minimum length requirements, enforcing complexity and set periodic resets.
- Password resets are handled via LMI ticketing system. New or reset passwords are sent to the employee using internal secure, encrypted email system or by leaving a voicemail for the employee.

LMI employs intrusion detection systems and also uses commercial and custom tools to collect and examine its application and system logs for anomalies.

• Access Control to Use Specific Areas of Data Processing Systems

Persons entitled to use the data processing system are only able to access Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied, modified or removed without authorization.

This is accomplished by:

- Employee policies and training in respect of each employee's access rights to the Personal Data;
- Users have unique log in credentials -- role based access control systems are used to restrict access to particular functions;
- Monitoring activities that add, delete or modify the Personal Data;
- Effective and measured disciplinary action against individuals who access Personal Data without authorization;
- Release of Personal Data to only authorized persons;
- Controlling access to account data and customer Personal Data via role-based access controls (RBAC) in compliance with the security principle of "least-privilege";
- Internal segmentation and logical isolation of LMI's employees to enforce least-privilege access policies;
- Requirements-driven definition of the authorization scheme and access rights as well as their monitoring and logging;
- Regular review of accounts and privileges (typically every 3-6 months depending on the particular system and sensitivity of data it provides access to);
- Control of files, controlled and documented destruction of data; and policies controlling the retention of back-up copies.

• Availability Control

LMI has implemented suitable measures to ensure that Personal Data is protected from accidental destruction or loss.

This is accomplished by:

- Global and redundant service infrastructure that is set up with full disaster recovery sites;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regards to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Rapid failover capability; and
- Maintaining full capacity disaster recovery (DR) sites and annually testing DR centers by shutting down primary sites for at least 24 hours unless the product is running in active/active configuration.
- Systems and processes in place to detect and defend against DDoS attacks.

• Transmission Control

LMI has implemented suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media.

This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Certain types of customer Sensitive Personal Data and other confidential customer data (e.g. payment card numbers) are encrypted at rest within the system;
- Protecting web-based access to account management interfaces by employees through encrypted TLS
- End-to-end encryption of screen sharing for remote access, support, or real time communication;
- Use of integrity checks to monitor the completeness and correctness of the transfer of data.

• Input Control

LMI has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed.

This is accomplished by:

- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;
- Physical security of data processing facilities;
- Session time outs.

• Separation of Processing for Different Purposes

LMI has implemented suitable measures to ensure that Personal Data collected for different purposes can be processed separately.

• Documentation

LMI keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. LMI takes reasonable steps to ensure that persons employed by it and other persons at the place of work, are aware of and comply with the technical and organizational measures set forth in this document. LMI, at its election, may make non-confidential portions of audit reports available to customers to verify compliance with the technical and organizational measures undertaken in this Program.

• Monitoring

LMI does not access Customer Personal Data, except to provide services to the Customer which LMI is obligated to perform, to monitor, analyze and improve the services, in support of the Customer experience, as required by law, or on request by Customer; LMI has implemented suitable measures to monitor access restrictions of LMI's system administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and responsibilities.

• Definitions

"LMI" means LogMeIn, Inc., and all of its direct and indirect subsidiaries.

"Customer" means any purchaser of any LMI offering.

"Personal Data" means any information directly or indirectly relating to any identified or identifiable natural person.

"Sensitive Personal Data" means Personal Data (1) consisting of an individual's first name and last name, or first initial and last name, in combination with some other data element that could lead to identify theft or financial fraud, such as a government issued identification number, financial account number, payment card number, date of birth, mother's maiden name, biometric data, electronic signature, health information, or (2) consisting of log-in credentials, such as a username and password or answer to security question, that would permit access to an online account or an information system; or (3) revealing the personal health information (PHI) of a natural person.

"Security Framework" refers to the collection of LMI's policies and procedures governing information security, including, but not limited to, policies, trainings, education, monitoring, investigation and enforcement of its data management and security efforts.

Document History

Version	Revision Date	Author	Notes
1.0	6/30/2015	Stacey Simson	
2.0	7 April 2016	Lisa Hall	
3.0	1 October 2016	Kari Zeni	
4.0	1 February 2017	Margaret Granger	