



## DATA PROCESSING ADDENDUM

Revised: December 26, 2019

This Data Processing Addendum (“DPA”) supplements and forms part of the Terms of Service or other written or electronic agreement between LogMeIn and Customer for the purchase of online services from LogMeIn (hereinafter defined as “Services”) (the “Agreement”). This DPA reflects the parties’ agreement with respect to LogMeIn’s Processing of Customer Content, including any Personal Data located therein, on behalf of Customer, during any relevant term and specifically applicable to Customer’s use of the LogMeIn Services. Going forward, any references to the Agreement will be construed as including this DPA. All capitalized terms not defined herein shall have the meaning given to them in the Agreement. This DPA consists of distinct parts: the main body of the DPA, and, as applicable, Schedules 1, 2, and 3 (including Appendices 1-2).

### HOW TO EXECUTE THIS DPA

To execute this DPA, Customer must:

1. Customer must complete the information in the signature box and sign on Page 5;
2. [If the Standard Contractual Clauses (defined below) are applicable] Complete the information as the data exporter on Page 8; and
3. Send the completed and signed DPA to LogMeIn by email to [DPA@logmein.com](mailto:DPA@logmein.com). Such DPA shall become legally binding upon receipt (provided that the terms of the DPA have not been supplemented, overwritten, or otherwise modified).

### HOW THIS DPA APPLIES

The LogMeIn and Customer entity that is party to the Agreement is party to this DPA. Customer’s Authorized Affiliates will also be covered by this DPA, provided that Customer shall remain the responsible for the acts and omissions of its Authorized Affiliates. For the avoidance of doubt, the Customer entity that is the contracting party to the Agreement shall, on behalf of itself and its Authorized Affiliates: (a) remain responsible for coordinating, making, and receiving all communication with LogMeIn under this DPA; and (b) exercise any rights herein in a combined manner with LogMeIn under this DPA.

### DATA PROCESSING TERMS

#### 1. DEFINITIONS

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Authorized Affiliate**” means any of Customer’s Affiliate(s) which (a) are subject to the Data Protection Laws and Regulations; and (b) are permitted to use the Services pursuant to the Agreement between Customer and LogMeIn but have not signed their own Order Form with LogMeIn and are not otherwise a “Customer” as defined under the Agreement.

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended, and its implementing regulations.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

“**Customer Content**” means any files, documents, recordings, chat logs, transcripts, and similar data that LogMeIn maintains on Customer and/or its end-users’ behalf, as well as any other information Customer or its users may upload to Customer’s Service account in connection with the Services.

“**Data Protection Laws and Regulations**” means all international, national, federal, and state laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

“**Data Subject**” means, as applicable: (i) the identified or identifiable person to whom Personal Data relates as defined by Data Protection Laws and Regulations; and/or (ii) a “Consumer” as the term is defined in the CCPA.

“**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“**LogMeIn Group**” means LogMeIn and its Affiliates engaged in the Processing of Personal Data.

“**Personal Data**” means any information relating to: (i) an identified or identifiable natural person (e.g., a Data Subject or Consumer); and/or (ii) an identified or identifiable legal entity (e.g., a household under CCPA), in each case, where such information is maintained on behalf of Controller by Processor within its Services environment and is protected similarly as personal data, personal information, or personally identifiable information under Data Protection Laws and Regulations.

“**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller, including, as applicable, any “Service Provider” as the term is defined by the CCPA.

“**Security and Privacy Operational Controls**” means the Security and Privacy Operational Controls (SPOC) applicable to the specific Services purchased or used by Customer, as updated from time-to-time and made accessible via LogMeIn’s [Privacy & Trust](#)

[Center](#) or via [www.logmeininc.com/trust](http://www.logmeininc.com/trust) under the "Product Resources" tab (provided that if no such SPOC is available, the [Technical and Organizational Data Security Measures](#) shall apply) or as otherwise made reasonably available by LogMeIn.

"**Standard Contractual Clauses**" means the agreement by and between Customer and LogMeIn and attached hereto as [Schedule 3](#) pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Sub-processor**" means any Processor engaged by LogMeIn or a member of the LogMeIn Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

## 2. PROCESSING OF PERSONAL DATA

**2.1 Roles of the Parties.** The parties agree that with regard to the Processing of Personal Data by LogMeIn on behalf of Customer, Customer is the Controller, LogMeIn is the Processor and that LogMeIn and/or members of the LogMeIn Group will engage Sub-processors as further detailed in Section 5 "Sub-processors" below.

**2.2 Customer's Responsibilities.** When using the Services, Customer shall Process Personal Data in accordance with Data Protection Laws and Regulations, including maintaining lawful basis (e.g., consent) and rights to use and provide Personal Data, as part of Customer Content. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations.

**2.3 LogMeIn's Responsibilities.** When Processing Customer Content, LogMeIn shall treat Customer's Personal Data in a confidential manner, consistent with Section 6 of this DPA, and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions, which is deemed given, for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Subject to Article 28(h) of the GDPR, LogMeIn shall immediately inform Customer if, in its opinion, it believes that any instructions of Customer conflict with or infringe the requirements of Applicable Data Protection Laws and Regulations.

**2.4 Processing Details.** The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects Processed under this DPA are specified in [Schedule 2](#) (Details of the Processing) to this DPA.

## 3. RIGHTS OF DATA SUBJECTS

To the extent legally permitted, if LogMeIn receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (e.g., a "right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (each a "**Data Subject Request**"), LogMeIn shall promptly notify Customer or shall otherwise direct such Data Subject to Customer. Taking into account the nature of the Processing, LogMeIn shall assist Customer by appropriate technical and organizational measures, as is technically feasible and commercially reasonable, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

## 4. LOGMEIN PERSONNEL

LogMeIn shall ensure that its personnel engaged in the Processing of Personal Data are: (a) informed of the confidential nature of the Personal Data and have executed written confidentiality agreements; (b) have received appropriate training on their responsibilities, specifically pertaining to security and privacy measures; and (c) only have access to Personal Data to the extent reasonably determined to be necessary in order to perform any obligations, responsibilities, or duties as further specified in this DPA and the Agreement. Further, to the extent permitted by applicable law, LogMeIn shall ensure that the confidentiality obligations specified in this Section 4 shall survive the termination of the personnel engagement.

## 5. SUB-PROCESSORS

**5.1 Appointment of Sub-processors.** Customer acknowledges and agrees that: (a) LogMeIn's Affiliates may be retained as Sub-processors; and (b) LogMeIn and its Affiliates may engage third-party Sub-processors in connection with the provision and operation of the Services. Prior to engaging any third-party Sub-processors, LogMeIn or a LogMeIn Affiliate shall carry out appropriate due diligence on each Sub-processor and enter into a written agreement with each Sub-processor containing data protection obligations substantially similar to those in this Agreement with respect to the protection of Customer Content to the extent applicable to the nature of the Services provided by such Sub-processor.

**5.2 Current Sub-processors and Notice of New Sub-processors.** LogMeIn's current list of Sub-processors utilized for the Services and their geographic location ("**Sub-processor Disclosure**") may be found at LogMeIn's [Privacy & Trust Center](#) (also accessible via [www.logmeininc.com/trust](http://www.logmeininc.com/trust) under the "Product Resources" tab), as well as a mechanism to subscribe to e-mail notifications of new Sub-processors for each applicable Service. If subscribed, LogMeIn shall provide e-mail notification of any new

Sub-processors no less than ten (10) business days before authorizing such Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

**5.3 Objection Rights.** Customer may in good faith reasonably object to LogMeIn's use of a new Sub-processor by notifying LogMeIn promptly in writing (e-mail acceptable) within ten (10) business days after LogMeIn's notice in accordance with the mechanism set out in Section 5.2. Such notice shall explain the Customer's good faith, reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, LogMeIn will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If the parties are unable to resolve such objection or LogMeIn is otherwise unwilling to resolve or make available such change within a reasonable period of time, Customer may terminate the applicable Order Form(s) with respect to those Services which cannot be provided by LogMeIn without the use of the objected-to new Sub-processor by providing written notice to LogMeIn. LogMeIn will refund Customer any prepaid, unused, fees covering the remainder of the term of such Order Form(s) following the effective date of termination solely with respect to such terminated Services, without imposing a penalty for such termination on Customer.

**5.4 Liability.** LogMeIn shall be liable for the acts and omissions of its Sub-processors to the same extent LogMeIn would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

## 6. SECURITY

**6.1 Protection of Customer Content.** As further specified in Article 32 of the GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, LogMeIn shall implement and maintain appropriate technical and organizational measures for protection of the security (including protection against a Security Incident, as defined below), confidentiality and integrity of Customer Content, as set forth in the applicable Security and Privacy Operational Controls. LogMeIn regularly monitors compliance with these measures and will not materially decrease the overall security of the Services during a subscription term.

**6.2 Third-Party Certifications and Audits.** Customer may request, no more than once annually: (a) any written technical documentation that LogMeIn makes available or generally provide to its customer base; and (b) information regarding LogMeIn's compliance with the obligations in this DPA, in the form of the relevant third-party certifications and audits (as may be specified in the Security and Privacy Operational Controls). If, after Customer's review of the written records described in (a) and (b) above, Customer reasonably believes, in good faith, that an on-site audit is necessary to validate LogMeIn's compliance with this DPA, Customer may contact LogMeIn to request an audit of the procedures relevant to the protection of Personal Data. Before the commencement of any audit, Customer and LogMeIn shall mutually agree upon the scope, timing, and duration of the audit in addition to the reasonable reimbursement rate for which Customer shall be responsible. Customer shall promptly provide LogMeIn with information regarding any non-compliance discovered during the course of an audit. When conducting any such audit, Customer shall use best efforts to minimize interference with LogMeIn's business operations.

## 7. NOTIFICATIONS REGARDING CUSTOMER CONTENT

LogMeIn maintains security incident management policies and procedures, as further specified in the Security and Privacy Operational Controls, and shall notify Customer, without undue delay, of any breach of its security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Content, including any Personal Data therein, transmitted, stored or otherwise Processed by LogMeIn or its Sub-processors of which LogMeIn becomes aware and which requires notification to be made to Customer, a Supervisory Authority and/or Data Subject under Data Protection Laws and Regulations (a "**Security Incident**"). "Security Incident(s)" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. Notification provided under this Section 7 shall not be interpreted or construed as an admission of fault or liability by LogMeIn. LogMeIn shall make reasonable efforts to identify the cause of such Security Incident and take those steps as LogMeIn deems necessary and reasonable in order to remediate the cause of such a Security Incident to the extent the remediation is within LogMeIn's reasonable control. Additionally, upon request, LogMeIn shall provide Customer with relevant information about the Security Incident, as reasonably required to assist the Customer in ensuring Customer's compliance with its own obligations under Data Protection Laws and Regulations to notify any Supervisory Authority or Data Subject in the event of a Security Incident. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users or any non-LogMeIn products or services.

## 8. DELETION AND RETURN OF CUSTOMER CONTENT

Upon written request, LogMeIn shall return Customer Content to Customer (or otherwise direct Customer to self-service export, if available and subject to technical feasibility) and/or, to the extent allowed by applicable law, delete and make irretrievable Customer Content. To the extent applicable, automatic data retention periods shall be in accordance with the procedures and timeframes specified in the Security and Privacy Operational Controls.

## 9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and LogMeIn, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference to the liability of a party means the total liability of that party and all of its Affiliates under the Agreement and all DPAs together.

## 10. EUROPEAN-SPECIFIC PROVISIONS

The following provisions shall apply solely to the extent that LogMeIn is required to Process Personal Data belonging to Data Subjects residing in Europe and subject to Data Protection Laws and Regulations in connection with delivering the Services to Customer:

**10.1 GDPR.** To the extent LogMeIn Processes Personal Data on behalf of Customer, it shall do so in accordance with the requirements of GDPR directly applicable to LogMeIn in the provision of its Services.

**10.2 Data Protection Impact Assessment.** If, pursuant to Data Protection Laws and Regulations, Customer are required to perform a data protection impact assessment (or prior consultation with a regulator having appropriate jurisdiction), upon Customer's request, LogMeIn shall provide such relevant written documentation as is made available by LogMeIn pursuant to this DPA and the Agreement. Any additional assistance, should the written documentation specified in this Section 10.2 be deemed insufficient, shall be subject to written agreement between the parties.

**10.3 Data Transfer Mechanisms.** Subject to the additional terms in Schedule 1, LogMeIn makes available the transfer mechanisms listed below, which shall apply, in the order of precedence (if both mechanisms are applicable) as set forth in this Section 10.3, to any transfers of Personal Data under this DPA from the European Union, the European Economic Area, and/or Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. LogMeIn's EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications apply to the Services (the "**EU-US and Swiss-US Privacy Shield Services**"), subject to the additional terms in Section 1 of Schedule 1;
2. The Standard Contractual Clauses set forth in Schedule 3 to this DPA apply to the Services (the "**SCC Services**"), subject to the additional terms in Section 2 of Schedule 1.

**10.4 Alternative Data Transfer Mechanism.** For the avoidance of doubt, should the specified or relevant transfer mechanism(s) specified in Section 10.3 be deemed invalid by a regulator or court with applicable authority and subject to the requirements in Principle 3 of the EU-U.S. and Swiss-U.S. Privacy Shield Framework, the parties shall endeavor in good faith to negotiate an alternative mechanism (if available) to permit the continued transfer of Personal Data.

## 11. CALIFORNIA CONSUMER PRIVACY ACT

LogMeIn shall not: (a) sell any Personal Data or; (b) receive any Personal Data as consideration for any services or other items provided or performed by LogMeIn as a Service Provider under this Agreement. LogMeIn shall not collect, retain, share or use any Personal Data except as necessary for a business purpose pursuant to a written contract (i.e., to provide and operate the LogMeIn services) and subject to the restrictions specified in Section 1798.140 (v) of the CCPA. LogMeIn agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Customer to qualify as "selling personal information" under the CCPA or any other similar applicable privacy laws.

*(remainder of page left intentionally blank)*

**12. LEGAL EFFECT AND CONFLICT**

This DPA shall become legally binding between Customer and LogMeIn upon execution of the Agreement. Once effective, this DPA shall be incorporated into and form part of the Agreement or applicable Order Form. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

**List of Schedules:**

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

**Customer:**

By: \_\_\_\_\_

Name:

Title:

Effective Date:

**LogMeIn:**

By: \_\_\_\_\_

Name:

Title:

SAMPLE

## SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

### 1. ADDITIONAL TERMS FOR EU-US AND SWISS-US PRIVACY SHIELD SERVICES

Subject to Section 10.4 of this DPA, LogMeIn, Inc. and its U.S. Affiliates self-certify to and comply with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce, and LogMeIn shall ensure that such entities maintain their self-certifications to and compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to the Processing of Personal Data that is transferred from the European Economic Area and/or Switzerland to the United States.

### 2. ADDITIONAL TERMS FOR SCC SERVICES

- 2.1. Customers Covered by the Standard Contractual Clauses.** The Standard Contractual Clauses and the additional terms specified in this Section 2 of this Schedule 1 apply to: (i) the Customer legal entity as a data exporter and its Authorized Affiliates; and (ii) all Affiliates of Customer established within the European Economic Area, and/or Switzerland, which have signed Order Forms for the SCC Services. For the purpose of the Standard Contractual Clauses and this Section 2, the entities referenced in this Section 2.1 shall be deemed "data exporters."
- 2.2. Instructions.** This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to LogMeIn for the Processing of Personal Data on Customer's behalf by LogMeIn. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by users in their use of the SCC Services and (c) Processing to comply with other reasonable documented instructions provided by Customer where such instructions are consistent with the terms of the Agreement.
- 2.3. Appointment of New Sub-processors and List of Current Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that: (a) LogMeIn's Affiliates may be retained as Sub-processors; and (b) LogMeIn and LogMeIn's Affiliates, respectively, may engage third-party Sub-processors in connection with the provision of the SCC Services. LogMeIn shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA
- 2.4. Notice and Objection Rights for New Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that LogMeIn may engage new Sub-processors as described in Sections 5.2, 5.3, and 5.4 of the DPA.
- 2.5. Copies of Sub-processor Agreements.** The parties agree that if copies of Sub-processor agreements must be provided pursuant to Clause 5(j) of the Standard Contractual Clauses, they may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed beforehand; and, that such copies will be provided in a manner determined by LogMeIn, in its sole discretion and only upon request by Customer. If permitted by applicable law, LogMeIn reserves the right to satisfy the obligations referenced in this section by providing proof of the Sub-processor agreements as opposed to copies thereof.
- 2.6. Audits and Certifications.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out pursuant to Section 6.2 of the DPA.
- 2.7. Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by LogMeIn to Customer only upon request.

## SCHEDULE 2 - DETAILS OF THE PROCESSING

### Subject-Matter of the Processing

LogMeIn provides a portfolio of cloud-based communication and collaboration, identity and access, and customer engagement and support solutions. The objective and subject of the Processing of Personal Data by LogMeIn, as a Processor, is servicing Customer and providing, supporting, and operating the provision of the Services.

### Duration of Processing

Subject to Section 6 of the DPA, LogMeIn will Process Personal Data, in its capacity as a Processor, for the duration of the Agreement (as further specified in the Security and Privacy Operational Controls), unless otherwise agreed upon in writing.

### Nature and Purpose of Processing

LogMeIn will Process Personal Data, in its capacity as a Processor, as necessary to perform and operate the Services pursuant to the Agreement, as further specified in the Security and Privacy Operational Controls and further instructed by Customer through its use of the Services.

### Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Device identification data and traffic data (e.g. MAC addresses, web logs, etc.)
- Professional life data
- Personal life data
- Localisation data

### Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer 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 Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

**SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES**

**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:

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation:

Country	LogMeIn Entity (as applicable)
<i>United States</i>	LogMeIn, Inc. LogMeIn USA, Inc. Jive Communications, Inc. Grasshopper Group, LLC
<i>United Kingdom</i>	LogMeIn Technologies UK Limited

Address: please see <https://www.logmeininc.com/legal/contracting-entities>

Tel.: 781-897-5580; e-mail: DPA@logmein.com

Other information needed to identify the organisation: Not applicable

(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 (c), 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 (c) 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 (c) 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 or 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. 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.

## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses and must be completed 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 Customer legal entity that is defined as a data exporter in the Standard Contractual Clauses; and (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased SCC Services on the basis of one or more Order Form(s), Agreements, or similar documents.

### **Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

LogMeIn provides a portfolio of cloud-based communication and collaboration, identity and access, and customer engagement and support solutions which process Personal Data upon the written instruction of the data exporter in accordance with the terms of the Agreement and this DPA.

### **Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the SCC Services, 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)
- 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)
- Any other users (who are natural persons) authorized by data exporter to use the SCC Services

### **Categories of data**

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the SCC Services, 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 the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (e.g., company, email, phone, IP address, physical business address)
- Device identification data and traffic data (e.g. MAC addresses, web logs, etc.)
- Professional life data
- Personal life data
- Localisation data

### **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, however, data exporter may submit special categories of data to the SCC Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

### **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, as well as the performance and operation of the SCC Services pursuant to the Agreement.

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

**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 uploaded to the SCC Services or otherwise maintained on behalf of data exporter (as Data Controller), as described in the Security and Privacy Operational Controls. Data importer reserves the right to update the Security and Privacy Operational Controls from time-to-time, provided that at no time shall data importer materially and to the adverse impact of data exporter, decrease the overall security of the SCC Services during a subscription term. Should a Security and Privacy Operational Controls document be unavailable for the applicable SCC Service, the Technical and Operational Data Security Measures accessible via <https://secure.logmein.com/home/policies/technical-measures> shall apply until such time as an applicable Security and Privacy Operational Controls document is made publicly available.

SAMPLE