Data Processing Amendment

This Data Processing Amendment (this "**DPA**") is entered into by and between ThingLink, Inc. ("**ThingLink**") and the customer that electronically accepts or otherwise agrees or opts-in to this DPA ("**Customer**").

Customer has entered into one or more agreements with ThingLink (each, as amended from time to time, an "**Agreement**") governing the provision of ThingLink's applications or software services (the "**Service**"). This DPA will amend the terms of the Agreement to reflect the parties' rights and responsibilities with respect to the processing and security of Customer's data under the Agreement. If you are accepting this DPA in your capacity as an employee, consultant or agent of Customer, you represent that you have the authority to bind Customer to this DPA.

This DPA becomes effective as of the date on which you electronically accept or otherwise agree or opt-in to this DPA and shall remain in effect until the date the Agreement terminates or expires.

1. DEFINITIONS

The following definitions apply to this DPA:

"**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

"**Authorized Users**" shall means individuals authorized by Customer to access Customer's ThingLink account

"Customer Account Data" shall mean personal data that relates to Customer's relationship with ThingLink, including the names and/or contact information of Authorized Users and billing information of individuals that Customer has associated with its ThingLink account;

"Customer Usage Data" shall mean personal data processed by ThingLink for the purposes of transmitting, distributing or exchanging End User Content; including data used to trace and identify the source and destination of a communication, such as individual data subjects' IP addresses, data on the location of the device generated in the context of providing the Services, and the date, time, duration and the type of communication.

"**Data Incident**" means a breach of ThingLink security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Account Data, Customer Usage Data, or End User Content on systems that are managed and controlled by ThingLink. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Customer Account Data, Customer Usage Data, or End User Content, including, without limitation, pings, port scans, denial of service attacks, network attacks on firewall or networked systems, or accidental loss or disclosure of Customer Account Data, Customer Usage Data, unsuccessful log-in attempts, or End User Content caused by Customer's use of the Services or Customer's loss of account authentication credentials.

"**EEA**" means the European Economic Area.

“**European Data Protection Legislation**” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

“End User Content” shall mean information uploaded by individuals authorized to use the Service by Customer (“**End Users**”), that ThingLink processes on behalf Customer pursuant to the Agreement. End User Content data types are optional and can be activated (or not) by the Customer, but may include profile information, videos, images, music, comments, questions, and other content or information on the Service. For clarity, ThingLink only collects the minimum amount of personal data necessary for it to perform its obligations under the Agreement.

“**GDPR**” means 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.

“**Model Contract Clauses**” or “**MCCs**” means the standard data protection clauses for the transfer of personal data to processors established in third countries that do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

“**Non-European Data Protection Legislation**” means data protection or privacy legislation other than the European Data Protection Legislation.

“**Services**” means the services received by Customer pursuant to the Agreement.

“**Subprocessor**” means a third party that we use to process End User Content in order to provide parts of the Service and/or related technical support.

The terms “**personal data**”, “**sensitive personal data**” “**data subject**”, “**processing**”, “**controller**”, “**processor**” and “**supervisory authority**” as used in this DPA have the meanings given in the GDPR, and the terms “**data importer**” and “**data exporter**” have the meanings given in the MCCs, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

2. DATA PROCESSING

2.1. Roles and Regulatory Compliance; Authorization

a. Processor and Controller Responsibilities. If European Data Protection Legislation applies to the processing of Customer’s Personal Data, the parties acknowledge and agree as follows: (i) with regard to the processing of End User Content, Customer is a controller or processor, as applicable, and ThingLink is a processor of End User Content; (ii) with regard to the processing of Customer Account Data and Customer Usage Data, Customer is a controller or processor, as applicable, and ThingLink is an independent controller, not a joint controller with Customer; and (iii) that each of us will comply with our obligations under applicable European Data Protection Legislation with respect to the processing of the Personal Data.

b. Authorization by Third Party Controller. If European Data Protection Legislation applies to the processing of End User Content and you are a processor of the End User Content, you warrant to us that your instructions and actions with respect to that End User Content, including your appointment of ThingLink as another processor, have been authorized by the relevant controller.

c. Responsibilities Under Non-European Legislation. If Non-European Data Protection Legislation applies to either party’s processing of Personal Data, the parties acknowledge and agree that each of us will comply with any applicable obligations under that legislation with respect to the processing of Personal Data.

2.2. Scope of Processing (End User Content)

a. Details of the Processing.

i. **Subject Matter:** ThingLink's provision of the Services to Customer.

ii. **Purpose of the Processing:** The purpose of the data processing under this DPA is the provision of the Services as initiated by Customer from time to time.

iii. **Categories of Data:** End User Content as defined above.

iv. **Categories of Data Subjects:** Data subjects may include End Users about whom data is provided to ThingLink via the Services by Customer or, or at the direction of Customer, directly by End Users.

v. **Duration of the Processing:** As between ThingLink and Customer, the duration of the data processing of End User Content under this DPA is necessarily determined by Customer.

b. Customer Authorization. By entering into this DPA, you hereby authorize and instruct us to process the Personal Data: (i) to provide the Service, and related technical support; (ii) as otherwise permitted or required by your use of the Service and/or your requests for technical support; (iii) as otherwise permitted or required by the Agreement, including this DPA; (iv) as instructed via Customer's configuration of the Services; ;and (v) as further documented in any other written instructions that you give us, provided we acknowledge those instructions in writing as constituting processing instructions for the purposes of this DPA. We will not process the Personal Data for any other purpose, unless required to do so by applicable law or regulation. Additional instructions outside the scope of that which is required to provide the Services pursuant to the Agreement and this DPA, may result in additional fees payable by Customer to ThingLink for carrying out those instructions. Customer shall ensure that its instructions comply with all laws, regulations and rules applicable to the End User Content, and that ThingLink's processing of the End User Content in accordance with Customer's instructions will not cause ThingLink to violate any applicable law, regulation or rule, including Applicable Data Protection Law. ThingLink agrees not to access or use End User Content, except as necessary to maintain or provide the ThingLink Services, or as necessary to comply with the law or other binding governmental order.

c. Prohibition on Sensitive Data. You will not submit, store, or send any sensitive personal data or special categories of Personal Data (together, "**Sensitive Data**") to us for processing, and you will not permit nor authorize any of your employees, agents, contractors, or data subjects to submit, store, or send any Sensitive Data to us for processing. You acknowledge that we do not request or require Sensitive Data as part of providing the Service to you, that we do not wish to receive or store Sensitive Data, and that our obligations in this DPA will not apply with respect to Sensitive Data.

d. Confidentiality of End User Content and Responding to Data Subject Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party is made directly to ThingLink in connection with ThingLink's processing of End User Content, ThingLink shall promptly inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, ThingLink shall not respond to any such request, inquiry or complaint without Customer's prior consent except to confirm that the request relates to Customer to which Customer hereby agrees.

e. Confidentiality Obligations of ThingLink Personnel. ThingLink will ensure that any person it authorizes to process the End User Content shall protect the End UserContent in accordance with ThingLink's confidentiality obligations under the Agreement.

f. Subprocessors.

i. Consent to Engagement. You specifically authorize us to engage third parties as Subprocessors. Whenever we engage a Subprocessor, we will enter into a contract with that Subprocessor to help ensure that the Subprocessor only accesses and uses End User Content to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement and this DPA.

ii. List of Subprocessors. A list of our current Subprocessors can be made available upon request to info@thinglink.com.

iii. Objections; Sole Remedy. You have the right, within ten (10) days of your receipt of notice of our intent to engage a Subprocessor, to object to the engagement of such Subprocessor by providing documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements set forth in this DPA (each, an “**Objection**”). If we do not remedy or provide a reasonable workaround for your Objection within a reasonable time, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party. We will not owe you a refund of any fees you have paid in the event you decide to terminate the Agreement pursuant to this Section.

g. Data Subject Rights. As part of the Services, ThingLink provides Customer with a number of self-service features, including the ability to retrieve, or restrict use of End User Content, which may be used by Customer to assist in its obligations under Applicable Data Protection Law with respect to responding to requests from data subjects. End User Content is never stored on the Services in a permanent manner. In addition, ThingLink will provide reasonable additional and timely assistance (at Customer’s expense) to the extent the self-service features of the Services do not sufficiently enable Customer to comply with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

h. Impact Assessments and Consultations. If ThingLink believes or becomes aware that its processing of End User Content is likely to result in a high risk to the data protection rights and freedoms of data subjects, ThingLink shall inform Customer and provide reasonable cooperation to Customer (at Customer’s expense) in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law.

i. Return or Deletion of End User Content. The Services provide Customer with the capability to obtain a copy of its End User Content by way of the API. End User Content is never stored beyond the short time frame necessary for ThingLink to provide the Services to Customer with respect to each End User. Your acceptance of this DPA shall constitute an instruction to us to delete End User Content as described herein. However, where we are required by law to retain some or all of the End User Content, ThingLink shall securely isolate such End User Content and protect it from any further processing except to the extent required by law. For avoidance of doubt, ThingLink may retain pseudonymous End User Content for so long as is necessary to meet its obligation to maintain records of its processing pursuant to Article 30 of the GDPR.

j. Audit Rights. If European Data Protection Legislation applies to the processing of End User Content, we will allow an internationally-recognized independent auditor that Customer selects to conduct audits to verify ThingLink's compliance with its obligations in this DPA. Customer must send any requests for audits under this Section to info@thinglink.com. Following ThingLink's receipt of Customer's request, the parties will discuss and agree in advance on the reasonable start date, scope, duration, and security and confidentiality controls applicable to the audit. Customer will be responsible for any costs associated with the audit. Customer agrees not to exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by a competent data protection authority; or (ii) an audit is necessary due to a Data Incident.

k. Violations of Applicable Data Protection Law. ThingLink will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

3. CONTROLLER OBLIGATIONS (CUSTOMER ACCOUNT AND USAGE DATA)

3.1. Purpose Limitation. ThingLink shall process Customer Account Data and Customer Usage Data in accordance with Applicable Data Protection Laws and consistent with the ThingLink Privacy Policy, available at https://www.thinglink.com/terms, and as amended from time to time.

3.2. Cooperation and Data Subject Rights. In the event that either party receives: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Customer Account Data and Customer Usage Data; (collectively, "**Correspondence**") then, where such Correspondence relates (or also relates) to processing conducted by the other party, it shall promptly inform the other party and the parties shall cooperate in good faith as necessary to respond to such Correspondence and fulfil their respective obligations under Applicable Data Protection Law.

3.3. Transparency. The parties acknowledge that where Customer permits its Authorized Users or End Users to access or use the Service, ThingLink may not have a direct relationship with Customer's Authorized Users or End Users whose personal data ThingLink may process in connection with Customer's use of the Services. In those instances where Thinglink does not maintain a direct relationship with Customer's Authorized Users or End Users, Customer shall be responsible for ensuring its Authorized Users and End Users are provided adequate notice of ThingLink's data processing activities, including with respect to Customer Account data for which ThingLink acts as a controller, and shall make available to Authorized Users and End Users a privacy notice that fulfills the requirements of Applicable Data Protection Law. ThingLink agrees to provide Customer with sufficient information regarding its processing activities to allow Customer to provide such notice.

4. DATA SECURITY

4.1. Security Measures.

a. Security Measures. We will implement and maintain appropriate technical and organizational measures to protect End User Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (collectively, the "**Security Measures**"). The Security Measures will have regard to the state of the art, the costs of implementation, and nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Security Measures will include, as appropriate: (i) the ability to ensure the ongoing security, confidentiality, integrity, availability, and resilience of data processing systems and services; (ii) the ability to restore the availability and access to End User Data in a timely manner, in the event of a Data Incident; and (iii) a process for regularly testing, accessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing. We may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

b. Security Compliance by our Staff. We will take appropriate steps to ensure that our employees, contractors, and Subprocessors comply with the Security Measures to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligations of confidentiality.

4.2. Data Incidents. If we become aware of a Data Incident, we will notify you promptly and without undue delay, and will take reasonable steps to minimize harm and secure Customer Account Data, Customer Usage Data, and/or End User Content . Any notifications that we send you pursuant to this Section 4.2 will be sent to the email address associated with Customer's account on the Service and will describe, to the extent possible, the details of the Data Incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for you to minimize the impact of the Data Incident. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third party notification obligations related to any Data Incident(s). Our notification of or response to a Data Incident under this Section will not constitute an acknowledgement of fault or liability with respect to the Data Incident.

4.3. Your Security Responsibilities. You agree that, without prejudice to our obligations under Sections 4.1 or 4.2:

a. you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Account Data, Customer Usage Data, or End User Content, securing any account authentication credentials, systems, and devices you use to use the Service, and backing up your End User Content.

b. You understand and agree that we have no obligation to protect End User Content that you elect to store or transfer outside of our or our Subprocessors' systems (e.g., offline or on-premise storage).

c. You are solely responsible for evaluating whether the Service and our commitments under this Section 4 meet your needs, including with respect to your compliance with any of your security obligations under European Data Protection Legislation and/or Non- European Data Protection Legislation, as applicable.

d. You acknowledge and agree that – taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of Personal Data, as well as the risks to individuals – the Security Measures that we implement in this DPA provide a level of security appropriate to the risk in respect to the Customer Account Data, Customer Usage Data, or End User Content.

5. DATA TRANSFERS

5.1. **Data Storage and Processing Facilities**. You agree that we may, subject to Section 5.2, store and process Personal Data in the United States and any other country in which we or our Subprocessors maintain facilities.

5.2. **Transfers of Data out of the EEA; Your Responsibilities.** Customer acknowledges that, as of the Effective Date of this DPA, ThingLink's primary processing facilities are in the Ireland. If the storage and/or processing of Personal Data as described in Section 5.1 involves transfers of Personal Data out of the EEA and European Data Protection Legislation applies to the transfers of such data (collectively, "**Transferred Personal Data**"), we will, at our sole discretion, either (i) ensure that we (as the data importer) have entered into MCCs set forth in Exhibit 1 to this DPA with you (as the data exporter), and that the transfers are made in accordance with the MCCs; or (ii) ensure that the transfers are made in accordance with an Alternative Transfer Solution. With respect to Transferred Personal Data, you agree that if we reasonably require you to enter into MCCs with respect to such transfers as required by European Data Protection Legislation, you will promptly do so; similarly, if we reasonably require you to use an Alternative Transfer Solution and we request that you take any action (including, without limitation, execution of documents) required to give full effect to that solution, you will promptly do so.

6. ADDITIONAL INFORMATION

You acknowledge that we are required under European Data Protection Legislation (i) to collect and maintain records of certain information, including, among other things, the name and contact detail of each processor and/or controller on whose behalf we are acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (ii) to make such information available to the supervisory authorities. Accordingly, if European Data Protection Legislation applies to the processing of Personal Data, you will, when requested, provide this additional information to us, and ensure that the information is kept accurate and up-to- date.

7. MISCELLANEOUS

There are no third party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to ThingLink's limitations of liability, which will remain in full force and effect. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA will control to the extent that the DPA is not in conflict with the MCCs, in which case the MCCs will control. This DPA consists of two parts: 1) the main body of this DPA, and 2) Exhibit a (including Appendices 1-3)

The parties authorized signatories have executed this Addendum as of _____________ ("Effective Date").

THINGLINK, INC.

____

Ulla Engestrom, CEO
470 Ramona Street, Palo Alto, CA 94301 - USA
Contact for data protection enquiries:
info@thinglink.com

CUSTOMER:

____

Name: ___________________________________

Title: ___________________________________

Address: ________________________________

____

DPO/Contact for data protection enquiries :

____

EXHIBIT I

Standard Contractual Clauses

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: The entity receiving services from the data importer pursuant to an agreement (Terms of Service, a Master Service Agreement, or other document) that references the Data Addendum to which these Standard Contractual Clauses are attached (the "data exporter").

And

ThingLink, Inc., 470 Ramona Street, Palo Alto, CA 94301; Tel.: ___________________; e-mail: info@thinglink.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 Controller;

(c) *'the data importer'* means Processor;

(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. 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 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, if applicable) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased access to the Service provided by ThingLink.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
ThingLink is a provider of an address book widget and an API that integrates with dozens of address book providers.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Data exporter may submit Personal Data to the Service provided by ThingLink, 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:

- Customers- Employees, agents, advisors, freelancers of data exporter
- Customer's End Users - customers or users of data exporter's products or services

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

- Customer Data - Identification information, namely full names, email addresses, and user ids; billing information, namely address and credit card or other financial information; device information, namely data about the data subject's device, such as an IP address, generated in the context of providing the Services, and usage information, namely the date, time, duration and the type of action(s) taken on the Services.
- Customer's End Users' Data - contact information, namely the contents of an end user's address books, contact lists, contact notes, and any images associated with an end user's address book. For clarity, ThingLink only collects the minimum amount of personal information that is necessary to fulfil its obligations under the Agreement. Accordingly, end user data containing personal data is only stored in the random access memory of ThingLink's servers and never written to a physical disc. Only pseudoanonymous end user data that remains with ThingLink, which is limited to a hash of each end user's email address, the source of the address book, and the number of contacts in the address book.

The data importer will receive any personal data that the data exporter instructs it to process through its software as a service products and services. The precise personal data that the data exporter will transfer to the data importer is necessarily determined and controlled solely by the data exporter, but likely include personal data, such as individual data subjects' full names, email addresses, user ids, and data about the data subject's device, such as an IP address, generated in the context of providing the Services, and the date, time, duration and the type of communication.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Special categories of data, such as data that reveals racial ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life are not required to be transferred in order for data exporter to use the Service provided by ThingLink and data exporter agrees not to transfer these special categories of data to data importer.

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 the performance of the Service pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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 Personal Data uploaded to the Service provided by ThingLink, as described in the Security and Compliance documentation, accessible via https://www.cloudsponge.com/security/or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Service during a subscription term.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

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

This Appendix does not vary or modify the Clauses. It sets out the parties' interpretation of their respective obligations under specific Clauses identified below. As permitted by Clause 10 of these Clauses, the purpose of the interpretations is to enable the parties to fulfil their obligations in practice.

Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the noncompliance (“**Cure Period**”).
4. If after the Cure Period the data importer has not or cannot cure the noncompliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(j): Disclosure of sub-processor agreements:

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub- processor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.
3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a

confidential basis) provide all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in data importer's Terms of Service in effect as of the date of execution of these Clauses or other written or electronic agreement for data exporter’s use and purchase of data importer’s products and services. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward sub-processing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer’s compliance with the requirements set out below, which collectively ensure that the onward sub-processor will provide adequate protection for the personal data that it processes:

   a) any onward sub-processor must agree in writing:
      i) to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Directive 95/46/EC; or
      ii) to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and
   b) data importer must restrict the onward sub-processor’s access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward sub-processor from processing the personal data for any other purpose.