

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) forms a part of the Ooyala Services Agreement (“**Agreement**”) between Ooyala and Company. By signing the DPA, Company enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Company Affiliates (defined below). The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

How to Execute this DPA:

1. This DPA consists of two parts: the main body of the DPA, and Annex 1 (including Appendices 1 and 2).
2. This DPA has been pre-signed on behalf of Ooyala. The Standard Contractual Clauses in Appendix 1 have been pre-signed by Ooyala as the data importer.
3. To complete this DPA, Company must:
 - a. Complete the information in the signature box and sign on Page 7; and
 - b. Complete the information in the signature box and sign on Pages 12, 13 and 15.
4. Send the completed and signed DPA to Ooyala by email with Company’s name in the Subject Line, to dpa@ooyala.com. Upon receipt of a valid, completed DPA by Ooyala at this email address, this DPA will become legally binding.

How this DPA Applies to Company and its Affiliates

If the Company entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Company entity who is a party to the Agreement executes this DPA.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

1. BACKGROUND

1.1 Company and Ooyala entered into the Agreement for the provision of the Services.

1.2 Both parties will comply with all applicable requirements of the Data Protection Laws. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Laws.

2. DEFINITIONS

2.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

2.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under

common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

2.3 "**Company Group Member**" means Company or any Company Affiliate;

2.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Agreement, including without limitation, End Users.

2.5 "**Contracted Processor**" means an Ooyala Group Member or a Subprocessor.

2.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

2.7 **"End Users Personal Data"** means the "personal data" (as defined in the GDPR).

2.8 **"European Economic Area"** or **"EEA"** means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

2.9 **"EU Data Protection Laws"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

2.10 **"GDPR"** means EU General Data Protection Regulation 2016/679.

2.11 **"Ooyala Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Ooyala, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

2.12 **"Ooyala Group Member"** means Ooyala or any Ooyala Affiliate;

2.13 **"Restricted Transfer"** means: (a) a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or (b) an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under this DPA.

2.14 **"Standard Contractual Clauses"** means the contractual clauses set out in Annex 1, amended as indicated (in square brackets and italics) in that Annex 1 and under section 13.4.

2.15 **"Subprocessor"** means any person (including any third party and any Ooyala Affiliate, but excluding an employee of Ooyala or any of its sub-contractors)

appointed by or on behalf of Ooyala or any Ooyala Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Agreement.

2.16 The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"End User Personal Data"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"**, **"Process"**, **"Processes"**, **"Processor"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2.17 **"Subprocessor"** means any Processor engaged by Ooyala who agrees to receive from Ooyala End Users Personal Data.

3. AUTHORITY

3.1 Ooyala warrants and represents that, before any Ooyala Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Ooyala's entry into this DPA as agent for and on behalf of that Ooyala Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Ooyala Affiliate.

4. PROCESSING OF COMPANY PERSONAL DATA

4.1 Ooyala Group Members shall:

(a) comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

(b) not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the relevant Ooyala Group Member shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

4.2 Each Company Group Member:

(a) Instruct Ooyala Group Members (and authorize Ooyala and each Ooyala Affiliate to instruct each Subprocessor) to: (i) Process Company Personal Data; and (ii) in particular, transfer Company Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement; and

(b) warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in clause 4.2(a) on behalf of each relevant Company Affiliate

5. OOYALA AND OOYALA AFFILIATE PERSONNEL

Ooyala Group Members shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. SECURITY

6.1 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, each Ooyala Group Member shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

6.2 In assessing the appropriate level of security, each Ooyala Group Member shall take account in particular of

the risks that are presented by Processing, in particular from a Personal Data Breach.

7. SUBPROCESSING

7.1 Each Company Group Member authorizes each Ooyala Group Member to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

7.2 Ooyala Group Members may continue to use those Subprocessors already engaged by an Ooyala Group Member as at the date of this DPA, subject to the Ooyala Group Member in each case meeting the obligations set out in section 7.4.

7.3 Ooyala shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment, then Ooyala shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and, where such a change cannot be made within ninety (90) days from Ooyala's receipt of Company's notice, notwithstanding anything in the Agreement, Company may by written notice to Ooyala with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

7.4 With respect to each Subprocessor, Ooyala or the relevant Ooyala Affiliate shall:

(a) before the Subprocessor first Processes Company Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Agreement;

(b) ensure that the arrangement between on the one hand (a) the Ooyala Group Member, or (b) the relevant intermediate Subprocessor; and on

the other hand, the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR;

(c) if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Ooyala Group Member, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

(d) provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Company may request from time to time.

7.5 Ooyala Group Members shall ensure that each Subprocessor performs the obligations under this DPA, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Ooyala.

8. DATA SUBJECT RIGHTS

8.1 Taking into account the nature of the Processing, Ooyala Group Members shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws

8.2 Ooyala shall:

(a) promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

(b) ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Ooyala shall: to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

9. PERSONAL DATA BREACH

9.1 Ooyala shall notify Company without undue delay upon Ooyala or any Subprocessor becoming aware of a Personal Data Breach affecting Company. Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2 Ooyala shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Ooyala Group Members shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

11. DELETION OR RETURN OF COMPANY PERSONAL DATA

11.1 Subject to sections 10.2 and 10.3 Ooyala Group Members shall promptly and in any event within thirty (30) of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

11.2 Subject to section 11.3, Company may in its absolute discretion by written notice to Ooyala within fourteen (14) days of the Cessation Date require each Ooyala Group Member to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Ooyala; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Ooyala Group Members shall comply with any such written request within thirty (30) days of the Cessation Date.

11.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that each Ooyala Group Member shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

12. AUDIT RIGHTS

12.1 Ooyala Group Members shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

12.2 Company or the relevant Company Affiliate requesting the information shall give Ooyala or the relevant Ooyala Affiliate reasonable notice of such request.

13. RESTRICTED TRANSFERS

13.1 Subject to section 13.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

13.2 The Standard Contractual Clauses shall come into effect under section 13.1 on the later of:

- (a) the data exporter becoming a party to them;
- (b) the data importer becoming a party to them;
- (c) and commencement of the relevant Restricted Transfer.

13.3 Section 13.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

14. GENERAL TERMS

Governing law and jurisdiction

14.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

- (a) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- (b) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or

territory stipulated for this purpose in the Agreement.

Order of precedence

14.2 Nothing in this DPA reduces any Ooyala Group Member's obligations under the Agreement in relation to the protection of Personal Data or permits Ooyala Group Members to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.3 Subject to section 14.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Severance

14.4 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

The parties' authorized signatories have duly executed this DPA:

On behalf of Company:

Company Name: _____

Signatory Name (written out in full): _____

Position: _____

Address: _____

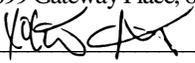
Signature: _____

On behalf of Ooyala Holdings, Inc.:

Name: Xochil Arkin

Position: General Counsel

Address: 2099 Gateway Place, 6th Floor, San Jose, California 95110

Signature:  _____

ANNEX 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of this 0, references to the "data exporter" and "data importer" shall be to Company and to Ooyala respectively (each a "party"; together "the parties").

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body

if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

- (ii) any accidental or unauthorised access, and
- (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor

of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract 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.

The parties' authorized signatories have duly executed this Annex 1:

On behalf of the Data Exporter:

Company Name: _____

Signatory Name (written out in full): _____

Position: _____

Address: _____

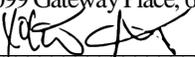
Signature: _____

On behalf of the Data Importer:

Name: Xochil Arkin

Position: General Counsel

Address: 2099 Gateway Place, 6th Floor, San Jose, California 95110

Signature:  _____

APPENDIX 1 TO THE STANDART CONTRACTUAL CLAUSES

DETAILS OF THE TRANSFER FORMING PART OF THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is Company.

Data importer

The data importer is Ooyala.

Data subjects

The personal data transferred concern the following categories of data subjects: employees and other personnel of Customer; end users of services of Customer; visitors to Customer's websites and mobile applications.

Categories of data

The personal data transferred concern the following categories of data: geographic data together with other segments of inferential data and IDs of Customer's registered members.

Processing operations

The personal data transferred will be subject to the following basic processing activities: transmitting, collecting, storing and analysing data in order to provide the Services to Customer, and any other activities related to the provision of the Services or specified in the Agreement.

Data Exporter:

Signatory Name (written out in full): _____

Signature: _____

Data Importer:

Name: Xochil Arkin

Signature:  _____

APPENDIX 2 TO STANDARD CONTRACTUAL CLAUSES
TECHNICAL AND ORGANISATIONAL SECURITY MEASURES FORMING PART OF THE STANDARD
CONTRACTUAL CLAUSES

Introduction

Ooyala maintains internal policies and procedures, or procures that its Subprocessors do so, which are designed to:

- (a) secure any personal data Processed by it against accidental or unlawful loss, access, or disclosure;
- (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the personal data Processed by it;
- (c) minimise security risks, including through risk assessment and regular testing.

Ooyala will (a) conduct periodic reviews of the security of its network and the adequacy of its information security program as measured against industry security standards; (b) conduct periodic reviews of its policies and procedures; and (c) use reasonable efforts to procure that its Subprocessors do so as well.

Ooyala will periodically evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews. Ooyala will use reasonable efforts to procure that its Subprocessors do so as well.

Access controls

Ooyala limits access to personal data by implementing appropriate access controls.

Disposal of IT equipment

Ooyala has in place processes to securely remove all personal data before disposing of IT systems (for example, by using appropriate technology to purge equipment of data and/or destroying hard disks).

Encryption

Ooyala uses encryption technology where appropriate to protect personal data held electronically.

Transmission or transport of personal data

Ooyala will implement appropriate controls to secure personal data during transmission or transit.

Device hardening

Ooyala will remove unused software and services from devices used to process personal data. Default passwords that are provided by hardware and software producers will not be used.

Physical security

Ooyala implements appropriate physical security measures to safeguard personal data.

Staff training and awareness

Ooyala carries out staff training on data security and privacy issues relevant to their job role and ensures that new staff receive appropriate training before they start their role. Staff are subject to disciplinary measures for breaches of Ooyala's policies and procedures relating to data privacy and security.

Data Exporter:

Signatory Name (written out in full): _____

Signature: _____

Data Importer:

Name: Xochil Arkin

Signature:  _____