Agora, Inc.

DocuSigned by:

By: ______________________________

24E99F50FCA642D...

Authorized Signature

Print Name: Reggie Yativ

Title: COO Agora Lab Inc

Date: 6/24/2020

Customer: ______________________________

DocuSigned by:

By: Leonard Witteler

2DCED8A222514D7...

Authorized Signature

Print Name: Leonard Witteler

Title: Mr

Date: 6/24/2020

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") amends and forms part of the written agreement between Agora, Inc. ("**Agora**") and [Yotribe GmbH] ("**Customer**") titled the [PaaS Customer Agreement] and dated [06/22/2020] (the "**Agreement**"). This DPA prevails over any conflicting term of the Agreement, but does not otherwise modify the Agreement.

This DPA regulates the Processing of Personal Data subject to EU Data Protection Law for the Purposes by the Parties. Annex 1 (including Appendices 1 and 2) forms an integral part of this DPA.

1. **Definitions.** The following terms have the meanings set out below for this DPA:

   1.1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

   1.2. "Data Subject" means a natural person whose Personal Data are processed in the context of this DPA.

   1.3. "EU Data Protection Law" means Directive 95/46/EC, Regulation (EU) 2016/679, Directive 2002/58/EC (as amended by Directive 2009/136/EC), and all other data protection laws of the European Union, the European Economic Area ("EEA"), and their respective member states, Switzerland and the United Kingdom, and any legal instrument for International Data Transfers, each as applicable, and as may be amended or replaced from time to time;

   1.4. "Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

   1.5. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

   1.6. "Processor" means the entity which processes Personal Data on behalf of a Controller.

   1.7. "Processing of Personal Data" (or "Processing/Process") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8. "Sub-Processor" means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

2. **Roles of the Parties.** For the purpose of this DPA, the Parties acknowledge and confirm that Customer is a Controller and Agora is a Processor for the Processing of Personal Data.

3. **Description of the Processing Activities**. Agora will Process Personal Data to provide services to Customer as set forth in the Agreement and only for the purpose of providing such service. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in Appendix 1 to the Standard Contractual Clauses, which is an integral part of this DPA, in the Agreement. Agora will Process Personal Data only for as long as necessary to provide services to Customer and as permitted under any other agreement between Customer and Agora governing Customer's use of Agora services.

4. **Obligations of Customer.** Customer confirms and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the Service, it acts as a Controller and that: (a) it complies with EU Data Protection Law when Processing Personal Data, and only gives lawful instructions to Agora; (b) Data Subjects have been informed of the uses of Personal Data as required by EU Data Protection Law; (c) it relies on a valid legal ground for the Processing of Personal Data under EU Data Protection Law (d) it complies with Data Subject requests to exercise their rights of access, rectification, erasure, data portability, restriction of Processing, and objection to the Processing; (e) it complies with data accuracy, proportionality and data retention principles; (f) it implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law; and (g) it will cooperate with Agora to fulfil their respective data protection compliance obligations in accordance with EU Data Protection Law.

5. **Obligations of Agora.** Agora confirms and warrants that it complies with EU Data Protection Law when Processing Personal Data for the Purposes in connection with providing services to Customer, and that it:

5.1. Only Processes Personal Data on behalf of Customer in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in Section 3 or as otherwise agreed by both Parties in writing. For the avoidance of doubt, Customer authorizes Agora to de-identify Personal Data for Agora's product development, product improvement, benchmarking and analytics purposes.

5.2. Will promptly inform Customer if, in its opinion, the Customer's instructions infringe EU Data Protection Law, or if Agora is unable to comply with the Customers' instructions.

5.3. Will notify Customer without undue delay after becoming aware of a Personal Data Breach. Agora will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach.

5.4. Will assist Customer in complying with data security, data breach notifications, data protection impact assessments, and prior consultations with supervisory authorities requirements under EU Data Protection Law, taking into account the nature of the Processing and the information available to Agora. To the extent authorized under applicable law, Customer shall be responsible for any costs arising from Agora's provision of such assistance.

5.5. Taking into account the nature of the processing, will assist Customer by appropriate technical and organizational measures, insofar as this is possible, to fulfil Customer's obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law and specified under 4(d) above. To the extent authorized by applicable law, Customer shall be responsible for any costs arising from Agora's provision of such assistance.

5.6. When this DPA expires or upon termination of this DPA or upon a request to delete or return Personal Data, Agora will, at the choice of Customer, delete, anonymize, or return all Personal Data to Customer, and delete or anonymize existing copies unless EU or EU member state law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Agora must keep them confidential).

6. **Data Transfers**. To provide services to Customer, Agora needs to import Personal Data to the [United States].

   6.1. Customer authorizes such cross-border Personal Data transfers and confirms and warrants that it will comply with any requirements under EU Data Protection Law with regard to such Personal Data transfers.

   6.2. By signing this DPA, the Parties execute the Standard Contractual Clauses attached in Annex 1, including Appendix 1 and Appendix 2 to the Standard Contractual Clauses. For the avoidance of doubt, the Standard Contractual Clauses will apply to Personal Data Processed by Agora in the context of providing services to Customer that are transferred to the United States or to any other country that does not provide an adequate level of protection under EU Data Protection Law.

7. **Sub-Processing.** Customer gives a general authorization to Agora to disclose Personal Data to Sub-Processors under the conditions set forth below and Agora represents and warrants that when sub-processing the Processing of Personal Data in the context of providing services to Customer:

   7.1. Agora binds its Sub-Processors by way of an agreement which imposes on the Sub-Processor the same data protection obligations as are imposed on Agora under this DPA, in particular providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the Processing will meet the requirements under EU Data Protection Law, to the extent applicable to the nature of the service provided by the Sub-Processors. Where the Sub-Processor fails to fulfil its data protection obligations under such agreement, Agora shall remain fully liable towards Customer for the performance of the Sub-Processor's obligations under such agreement.

   7.2. A list of Agora's current Sub-Processors is available at will be provided upon demand. Agora shall inform Customer of any intended addition or replacement of Sub-Processors and allow Customer to reasonably object to such changes by notifying Agora in writing within ten (10) business days after receipt of Agora's notice of the addition or replacement of a Sub-Processor. Customer's objection should be sent to privacy@agora.io and explain the reasonable grounds for the objection.

8. **Security of the Processing; Confidentiality.** Agora must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In assessing the appropriate level of security, Agora must take 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 Data Subjects and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Agora must take steps to ensure that any person acting under its authority who has access to Personal Data is bound by enforceable contractual or statutory confidentiality obligation.

9. **Data Protection Audit.** Upon prior written request by Customer, Agora agrees to cooperate and within reasonable time provide Customer with: (a) a summary of the audit reports demonstrating Agora's compliance with its obligations under this DPA, after redacting any confidential and commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability in Agora's systems, or to the extent that any such vulnerability was detected, that Agora has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection law or reveal some material issues, subject to the strictest confidentiality obligations, Agora allows Customer to request an audit of Agora's data protection compliance program by external independent auditors, which are jointly selected by the Parties. The external independent auditor cannot be a competitor of Agora, and the Parties will mutually agree upon the scope, timing, and duration of the audit. Agora will make available to Customer the result of the audit of its data protection compliance program. Customer must reimburse Agora for all expenses and costs for such audit.

10. **Liability Towards Data Subjects.** Each Party agrees that it will be liable to Data Subjects for the entire damage resulting from a violation of EU Data Protection Law. If one Party paid full compensation for the damage suffered, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's part of responsibility for the damage. For that purpose, both Parties

agree that Customer will be liable to Data Subjects for the entire damage resulting from a violation of EU Data Protection Law with regard to Processing of Personal Data for which it is a Controller, and that Agora will only be liable to Data Subjects for the entire damage resulting from a violation of the obligations of EU Data Protection Law directed to Processor or where it has acted outside of or contrary to Customer's lawful instructions. Agora will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

11. **Applicable Law**. The Processing of Personal Data under this DPA is governed by the law of the jurisdiction in which Customer is established.

12. **Modification of this DPA and Termination**. This DPA may only be modified by a written amendment signed by each of the Parties. Either Party may terminate this DPA upon written notice to the other Party.

13. **Invalidity and Severability.** If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

IN WITNESS WHEREOF, the Parties acknowledge their agreement to the foregoing by due execution of the DPA by their respective authorized representatives.

Agora

Name: Reggie Yativ

Title: COO Agora Lab Inc

Signature: DocuSigned by:
24E99F50FCA642D...

Address: 2804 Mission College Blvd

Santa Clara 95054

Contact Telephone: 9496328098

Customer

Name: Leonard Witteler

Title: Mr

Signature: DocuSigned by:
Leonard Witteler
2DCED8A222514D7...

Address: Yotribe GmbH, Kommandantenstrasse 77 10117 Be

Contact Telephone: ___

ANNEX 1

Standard Contractual Clauses (processors)

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

The entity identified as "**Customer**" in the DPA,

(the data **exporter**)

And

The entity identified as "**Agora**" in the DPA,

(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of

[1] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer.

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, namely California.

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. By signing the signature box on page 4 of the DPA, the parties will be deemed to have signed this Appendix 1.

Data exporter

The data exporter is the entity identified as “Customer” in the DPA.

Data importer

The data importer is the entity identified as “Agora” in the DPA.

Data subjects

The personal data transferred concern the following categories of data subjects:

- Customer’s administrative personnel responsible for maintenance of Customer’s account with Agora
- Customer’s end-users who communicate via Agora’s network and software

Categories of data

The personal data transferred concern the following categories of data:

- Customer’s end-users’ IP addresses, communications device type and communication data
- Customer’s administrative personnel’s phone number, email address, and telephone number

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: None.

Processing operations

The personal data transferred will be subject to the following processing operations.

- Agora provides a video and voice data communications platform that Customer incorporates into its customer applications to support voice and video communications capability.
- Agora processes name, phone number, and email address of Customer’s administrative personal responsible for maintaining Customer’s account with Agora or for resolution of technical issues with Agora and for billing purposes. Agora’s use of this data includes; communication of critical real-time information such as network outages, resolution of technical or administrative issues, validation of account during log-in credential recovery as well as biling.

- Agora processes the IP address of the Customer’s end-users. The IP address is used to route media and other communications data during a communications session between the Customer’s end-users.
- Agora processes communications device type information from Customer’s end-users. This information is used by Agora’s software to optimize the performance of real-time communications sessions as managed by Agora’s software and network.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature box on page 4 of the DPA, the parties will be deemed to have signed this Appendix 2.

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):

Agora will, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master record per user, user master data procedures, per data processing environment;

- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of Customer include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.