voximplant

DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "Addendum") amends the Terms of Service of the Voximplant Master Subscription Agreement available via https://voximplant.com/legal/tos (the "Agreement") by and between **ZINGAYA, INC., D/B/A VOXIMPLANT** (**"Voximplant"** or the **"PIP"**), a corporation duly organized and existing under and by virtue of the laws of the Delaware, United States, with principal office address at 594 Broadway, Suite 701, 10012, New York City, New York, United States of America and the undersigned Customer/Client of Voximplant.

This Addendum will be effective as of the date we receive a complete and executed Addendum from the Customer/Client indicated in the signature block below (the "Effective Date"). This Addendum shall apply to personal data processed by Voximplant on Customer/Client behalf in the course of providing the Service to Customer/Client ("Customer Personal Data"). The term of this Addendum corresponds to the duration of the Agreement.

Customer and **Voximplant** may hereinafter be referred to collectively as "**Parties**" or individually as "**Party**",

WHEREAS Customer and VOXIMPLANT enter into the Agreement pertaining to a defined and workable framework upon which the Parties wish to engage and enter into a partnership;

WHEREAS, the Parties acknowledge that the Data Subjects have express rights under the DPA that provide for protection and confidentiality of their Personal Data;

NOW, THEREFORE, for and in consideration of the foregoing premises and mutual covenants herein contained, the Parties hereby agree to bind themselves, as follows:

This DPA has been pre-signed on behalf of Voximplant as the data processor/importer.

To complete this DPA, Customer must:

1. Where applicable, complete the information as data exporter on Pages 4, 7, 12, 13 and sign Pages 6, 11 (if applicable), 12, 13.
2. Send the completed and signed DPA to Voximplant by email at privacy@voximplant.com.

Upon Voximplant's receipt of the validly completed DPA, this DPA will become legally binding.

1. Definitions

The following terms shall have the respective meaning whenever they are used in this Addendum:

A. **Consent –** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the Data Subject to do so;

B. **Data Processing** – refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

C. **Data Protection Officer** – refers to an individual designated by a Party to be accountable for compliance with the DPA and Applicable Law;

D. **Data Subject** – refers to an individual whose personal, sensitive personal, or privileged information is processed;

E. **Personal Data** – refers to either of the following:

   1. **Personal Information** – refers to any information, whether recorded in material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual; or

   2. **Sensitive Personal Information** – refers to personal information:

      i. About an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;
      ii. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

iii. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
iv. Specifically established by an executive order or an act of Congress to be kept classified.

F. **Personal Information Controller ("PIC")** – refers to the party who controls the processing of personal data, or instructs another to process Personal Data on its behalf. There is control if the party decides on what information is collected, or the purpose or extent of its processing;

G. **Personal Information Processor ("PIP")** – refers to any natural or juridical person or any other body to whom a Personal Information Controller may outsource or instruct the processing of Personal Data pertaining to a Data Subject;

H. **Personnel** – shall refer to the employees, officers, agents, or otherwise acting under the authority of the Personal Information Processor and the Personal Information Controller;

I. **Processing** – refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system;

J. **Security Breach** – refers to any unauthorized, unlawful or accidental access, processing, disclosure, alteration, loss, damage, or destruction of Personal Data whether by human or natural causes.

K. **Applicable Law** – means all international, national, provincial, federal, state, and/or local laws, codes, and/or regulations, including, without limitation, applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; EU Member State laws implementing GDPR, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications; EU Member State laws regulating security breach notification and imposing data security requirements; and the UK's national law implementing the GDPR; the Swiss Data Protection Law and any other law that applies to the Personal Data processed by the PIP.

2. Purpose

Client will share, provide, or disclose to Voximplant, Personal Data which is in the possession and control of Client pertaining to its clients for the purpose of communication related services.

3. Responsibilities

The PIC with regard to the Personal Data in their original possession, is responsible for ensuring that it collects Personal Data lawfully and in accordance with the requirements of the DPA, and the "Schedule A" and "Appendix 1", if applicable, each of which is incorporated into, and made a part of, this Addendum.

Prior to collection or sharing of Personal Data, a PIC shall be responsible for obtaining the necessary Consent of the Data Subject over the collection of Personal Data and of apprising the Data Subject with the nature, purpose, and extent of the processing of his or her Personal Data, including the risks and safeguards involved, the identity of the PIC, his or her rights as a data subject, and how these can be exercised.

The PIC shall be responsible for the accuracy, quality, and legality of Personal Data and the means by which they acquired them.

The PIC hereby represents and warrants that it is compliant with the DPA and Applicable Law in relation to its collection of Personal Data, and in obtaining the Data Subjects' Consent for the sharing of Personal Data with the PIP; and that it has in place appropriate administrative, physical, technical and organizational security measures that protect Personal Data from Security Breach.

The PIC shall be responsible for addressing any information request, or any complaint filed by a Data Subject and/or any investigation conducted by a governmental regulatory body. Provided, that the governmental regulatory body shall make a final determination as to which (PIC or PIP) is liable for any breach or violation of the DPA or Applicable Law

The PIC shall be responsible in providing a copy of this Addendum if requested by the Data Subject in writing.

The PIP shall process the Personal Data only in accordance with this DPA, the attached "Schedule A", which incorporated into, and made a part of this DPA, and the other lawful, documented instructions of the PIC, except where otherwise required by Applicable Law. The Addendum, Schedule A and this DPA sets out Clients complete instructions to Voximplant in relation to the processing of the Personal Data and any processing required outside of the scope of these instructions will require prior written agreement between the parties.

The PIP shall not share Personal Data obtained from the PIC with any other party without the prior written permission/instruction of the PIC or process Personal Data in any way or for any purpose other than those set out in this Addendum. The PIP shall segregate the Personal Data from its own and its other clients' data.

The PIC agrees that the PIP may engage PIP's affiliates and certain third party sub-processors (collectively, "Sub-processors") to process the Personal Data on the PIP's behalf. Sub-processors may provide hosting services and may provide plug-in tools and services that enhance the PIP product offering. A list of Sub-processors currently engaged by the PIP may be found at https://voximplant.com/legal/subprocessors-list. The PIC approves the use of the Sub-processors listed at the URL as of the date of this Addendum.

The PIP shall provide the PIC with two (2) weeks prior notice if there are any additions to the list of Sub-processors. The PIP shall obtain from all Sub processors the necessary assurances and guarantees that it has adequate administrative, physical, technical organizational and procedural security measures to protect the Personal Data in view of the relevant risks. The PIP may terminate the Agreement if it objects to the addition of a new Sub processor.

4. Categories of Personal Data and Purposes of Processing

The categories of Personal Data to be shared by PIC include the following:

- Name,
- Organization name,
- Email address,
- Phone number,
- Billing address
- Mailing address,
- Credit card and payment details
- SIP and a proprietary telecommunications applications information
- Number of calls to and from a provided number
- Call length to and from a provided number
- Numbers calling or called by a provided number
- Call content and usage information
- Contact information associated with a corporate Client account.
- Certain identification necessary to obtain telephone numbers, such as photo ID

The PIP shall only process Personal Data for the purpose of providing the services under the Agreement and/or as identified in Schedule A.

5. Security

The PIP shall implement appropriate security measures that ensure the availability, integrity, and confidentiality of Personal Data. The PIP shall implement reasonable and appropriate organizational, physical, technical, administrative, procedural and security measures to protect Personal Data against any Security Breach as prescribed in the DPA, its IRR, and circulars issued by a governmental regulatory body.

The PIP shall ensure that Personal Data is backed up on a regular basis and that any back up is subject to security measures as necessary to protect the availability, integrity and confidentiality of Personal Data.

The PIP undertakes that it will not, at any time, whether during the course of, or after the term of this Addendum, transfer, share, divulge, exploit, and modify any Personal Data to any person.

6. Audit.

Voximplant is diligently seeking to complete the process to obtain the applicable ISO 27001 certifications. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Voximplant shall make available to Customer a copy of Voximplant's then most recent third-party audits or certifications, as applicable.

7. Personnel

Each party shall take steps to ensure that any person acting under its authority and who has access to Personal Data, does not process them except for purposes of this Data Processing Addendum or as required by law.

Each Party shall ensure that access to Personal Data is limited only to its officer, employees, agents or representatives who need access only for purposes of this Data Processing Addendum.

Each Party shall ensure that its officers, employees, agents or representatives engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are subject to obligations of confidentiality and such obligations survive the termination of that officer's, employees', agents' or representatives' engagement or relationship with each Party.

Each Party shall take reasonable steps to ensure the reliability of any of its officers, employees, agents or representatives who have access to Personal Data, which shall include ensuring that they all understand the confidential nature of the Personal Data; and have received appropriate training in data protection prior to their access or Processing of Personal Data, and have agreed that they understand and will act in accordance with their responsibilities for confidentiality under this Data Processing Addendum.

8. Data Subject Access Rights

Data Subjects have a right to see what Personal Data is held about them, and to know why and how it is processed.

The PIC has an obligation to respond to these request or complaints. If a data subject contacts the PIP to exercise a right under Applicable law then the PIP will forward the request to the PIC. The PIC agrees to respond. Inquiry or request for Personal Data can be requested by submitting a written request with the following Data Protection Officers (or its equivalent):

_____:

Name of DPO: ……..……

Email: ……..……

Address : ……..……

Zingaya, Inc. d/b/a Voximplant:

Email: privacy@voximplant.com

Address: 594 Broadway, Suite 701, 10012, New York City, New York, USA.

The individuals listed in this section shall be the first port of call for questions about this Addendum, any complaint filed by the Data Subject and/or investigation by a governmental regulatory body. If there is a problem such as a potential Security Breach, the individuals listed in this section must be contacted.

Each Party shall rectify the complaint by any Data Subject within thirty (30) days from receipt of any such complaint. The Data Subject shall be given a response in writing describing how the complaint was rectified and how the situation complained of will be avoided moving forward.

9. Breach Management and Notification

Each Party shall implement policies and procedures for guidance of its personnel in the event of a Security Breach, including but not limited to:

A. A procedure for the timely discovery of Security Breach, including the identification of person or persons responsible for regular monitoring and evaluation of Security Breach;

B. A policy for documentation, regular review, evaluation and updating of the privacy and security policy and practices;

C. Clear reporting lines in the event of a possible Security Breach, including the identification of the person responsible for setting in motion the Security Breach response procedure, and who shall be immediately contacted in the event of a possible or confirmed Security Breach;

D. Conduct of a preliminary assessment for purpose of:
   1. Assessing the nature and scope of the Security Breach and the immediate damage;
   2. Determining the need for notification of law enforcement or external expertise; and
   3. Implementing immediate measures necessary to secure any evidence, contain the Security Breach and restore integrity to the Personal Data;

E. Evaluation of the Security Breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to Personal Data and affected Data Subjects;

F. Procedures for contacting law enforcement in case Security Breach involves possible commission of criminal acts;

G. Conduct of investigations that will evaluate fully the Security Breach;

H. Procedures for immediately notifying the PIC when the Security Breach is subject to notification requirement; and

I. Measures and procedures for mitigating the possible harm and negative consequences to the PIC and the affected Data Subjects in the event of a Security Breach. Each Party must be ready to provide assistance to the Data Subjects whose Personal Data may have been affected.

The Parties shall have the manpower, system, facilities and equipment in place to properly monitor access to Personal Data, and to monitor and identify a Security Breach.

If a party becomes aware of any Security Breach on its personnel, premises, facilities, system, or equipment, it shall: (a) notify the other Party of the Security Breach; (b) investigate the Security Breach and provide the other Party with information about the Security Breach; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

The Parties shall cooperate with each other on incident investigation requirements for any Security Breach of Personal Data.

Each Party shall send the written notification or notification to their DPO counterpart via e-mail of any Security Breach to the other within twenty-four (24) hours from knowledge or discovery thereof.

Upon receipt, confirmation and knowledge of the security breach, the DPO shall notify the required governmental regulatory body and the affected Data Subject within seventy-two (72) hours.

The Party who was notified of a Security Breach may require the other Party to provide further details and actions taken on the Security Breach.

10. Duration of this Addendum

Upon termination or expiry of Voximplant Master Subscription Agreement or upon the termination of the provision of data processing services and upon the written request of PIC, PIP shall immediately cease any Processing of Personal Data.

11. Retention of Personal Data

Personal Data should only be processed for as long as is necessary. Processing of Personal Data should be limited accordingly and for a period no longer than the term of this Addendum. Specific justification for processing of Personal Data beyond said period is required.

The PIC recognizes that the PIP may be required Personal Data to be retained for further use in the near future.

If a complaint is received about the accuracy of Personal Data which affects personal and/or sensitive personal information shared with the other Party, an updated replacement Personal Data will be communicated to the other Party. The other Party must replace the out of date data with the revised data.

12. Return or Destruction of Personal Data

Upon expiration or termination of the Agreement or this Addendum, whichever comes first, the PIP, unless otherwise required by applicable laws, shall perform the following within thirty (30) days from date of said expiration or termination:

a. Return all Personal Data of Data Subjects in any recorded form including any other property, information, and documents provided by the PIC;
b. Destroy all copies it made of Personal Data and any other property, information and documents if requested by the PIC. For print out or other tangible formats, the document will be shredded. For data in electronic form, the document must be deleted, wiped, overwritten or otherwise make it irretrievable; and
c. Deliver to the PIC a certificate confirming PIP's compliance with the return or destruction obligation under this section, if requested by the PIC.

13. Entire Agreement

This Addendum constitutes the entire agreement between the parties with respect to the subject matter hereof. It excludes and supersedes everything else which has occurred between the Parties whether written or oral, including all other communications with respect to the subject matter hereof.

14. Amendment

This Addendum may not be amended or modified except in writing and consented to by both Parties.

15. Separability Clause

If any provision of this Addendum is illegal or unenforceable, its invalidity shall not affect the other provisions of this Addendum that can be given effect without the invalid provision. If any provision of this Addendum does not comply with any law, ordinance or regulation, such provision to the extent possible shall be interpreted in such a manner to

comply with such law, ordinance or regulation, or if such interpretation is not possible, it shall be deemed to satisfy the minimum requirements thereof.

16. Counterparts

This Addendum may be executed in two or more counterpart copies, each of which shall be deemed to be an original, but all of which shall constitute the same agreement.

17. Assignment

Either Party shall not assign or delegate its rights or obligations under this Addendum, in whole or in part, to any third party by operation of law or otherwise, without the prior written consent of the other. Any attempted assignment or delegation that does not comply with this section shall be null and void and of no effect.

18. Non-Waiver of Rights

The failure of a Party to insist upon a strict performance of any of the terms, conditions and covenants hereof, shall not be deemed a relinquishment or waiver of any right/remedy that said Party may have, nor shall it be construed as a waiver of any subsequent breach of the same or other terms, conditions and covenants. Any waiver, extension or forbearance of any of the terms, conditions and covenants of this Addendum by any Party hereto shall be in writing and limited to the particular instance only and shall not in any manner be construed as a waiver, extension or forbearance of any of the terms, conditions and/or covenants of this Addendum.

19. Legal Capacity of Representatives

Each Party represents and warrants to the other Party that its representative executing this Addendum on its behalf is its duly appointed and acting representative and has the legal capacity required under the applicable law to enter into this Addendum and bind it.

20. Governing Law and Venue

This Addendum shall be governed by and construed in accordance with the laws of the State of New York in the United States, without regard to any conflicts of law rules. Exclusive jurisdiction over and venue of any suit arising out of or relating to this Addendum shall be in the courts of the State of New York, USA. The Parties hereby consent and submit to the exclusive jurisdiction and venue of those courts.

IN WITNESS WHEREOF, the Parties have hereunto affixed their signatures on the date and at the place first above-written.

_____

By:

_____

ZINGAYA, INC. D/B/A VOXIMPLANT

By: DocuSigned by: Alexey Aylarov 82FDAA670868423...

ALEXEY AYLAROV, CEO

voximplant

SCHEDULE A
EU STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Name of the data exporting organisation:

_____

(the data exporter)

and

Name of the data importing organisation:

ZINGAYA, INC. d/b/a VOXIMPLANT, A DELAWARE CORPORATION

(the data importer)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

DATA EXPORTER

Name, Title: _____

Authorised Signature _____

DATA IMPORTER

Name, Title: Alexey Aylarov, CEO

Authorised Signature _____

DocuSigned by:
Alexey Aylarov
82FDAA670868423...

voximplant

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

The data exporter is:

_____

The data importer is:

ZINGAYA, INC. d/b/a VOXIMPLANT, A Delaware Corporation

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

The data exporter and the individuals who are called or called by numbers provided by the importer to the data exporter.

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

- Name,
- Organization name,
- Email address,
- Phone number,
- Billing address
- Mailing address,
- Credit card and payment details
- SIP and Skype information
- Number of calls to and from a provided number
- Call length to and from a provided number
- Numbers calling or called by a provided number
- Call content and usage information
- Contact information associated with a corporate Client account.
- identification necessary to obtain telephone numbers, such as photo ID

Processing operations
The personal data transferred will be subject to the following basic processing activities:
These services will consist primarily of providing communication apps that facilitate communication between data subjects and the data exporter.

DATA EXPORTER

Name, Title: _____

Authorised Signature _____

DATA IMPORTER

Name, Title: Alexey Aylarov, CEO

DocuSigned by:
Alexey Aylarov
82FDAA670868423...

Authorised Signature _____

voximplant

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 organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the services provided by Zingaya pursuant to the Addendum, Zingaya will implement appropriate technical and organizational measures to ensure a level of security appropriate to the associated risk relative to Personal Data, including, inter alia, as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security Zingaya will take into account, in particular, the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Zingaya will take steps to ensure that any person acting under the authority of the Controller or Zingaya who has access to Personal Data does not process such Personal Data except on instructions from the Controller, unless he or she is required to do so by EU Data Protection Legislation.

DATA EXPORTER

Name, Title: _____

Authorised Signature _____

DATA IMPORTER

Name, Title: Alexey Aylarov, CEO

DocuSigned by:
Alexey Aylarov
82FDAA670868423...

Authorised Signature _____