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 / CPaaS (the "Agreement") by and between **Voximplant, Inc.** (**"Voximplant"** or the **"Processor"**), a corporation duly organized and existing under and by virtue of the laws of the Delaware, United States, with principal office address at 150 West 25th Street, RM 403 New York City, NY 10001, United States of America and the undersigned Client of Voximplant (**"Client"** or the **"Controller"**).

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

The Controller and **the Processor** may hereinafter be referred to collectively as "**Parties**" or individually as "**Party**",

WHEREAS, the Controller and the Processor 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 Addendum 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 Addendum has been pre-signed by the Processor.

To complete this Addendum, the Controller must:

1. *Fill in information on page 6 and sign page 10. If applicable, complete the information on pages 16-17 (clause 13 – Supervision) and fill in and sign page 21.*
2. *Send the completed and signed Addendum to the Processor by email at privacy@voximplant.com.*

Upon the Processor's receipt of the validly completed Addendum, this Addendum 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 Addendum 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. **Controller** – 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. **Processor** – refers to any natural or juridical person or any other body to whom a 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 Processor and the Controller;

I. **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.

J. **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 Processor.

2. Purpose

2.1. The Controller will share, provide, or disclose to the Processor Personal Data which is in the possession and control of the Controller pertaining to its clients for the purpose of communication related services (the "Services").

3. Responsibilities

3.1. Controller's Responsibilities

3.1.1. The Controller with regard to the Personal Data in its original possession is responsible for ensuring that it collects Personal Data lawfully and in accordance with the requirements of the Addendum and the "Schedule A", "Annex I" and "Annex II", if applicable, each of which is incorporated into, and made a part of, this Addendum.

3.1.2. Prior to collection or sharing of Personal Data, the Controller shall be responsible for securing appropriate legal grounds for the collection of Personal Data (such as obtaining the necessary Consent of the Data Subject) 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 Controller, his or her rights as a Data Subject, and how these can be exercised.

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

3.1.4. The Controller shall be responsible for ensuring that its instructions for the Processing of Personal Data comply with Applicable Law. The Controller shall provide the Processor only with instructions that are lawful under the Applicable Law and would not cause the Processor to breach Applicable Law.

3.1.5. The Controller hereby represents and warrants that it is compliant with the Addendum and Applicable Law in relation to its collection of Personal Data, and in obtaining the Data Subjects' Consent or other lawful grounds for the sharing of Personal Data with the Processor; and that it has in place appropriate administrative, physical, technical and organizational security measures that protect Personal Data from Security Breach.

3.1.6. The Controller 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, however, that the governmental regulatory body shall make a final determination as to which (the Controller or the Processor) is liable for any breach or violation of the Addendum or Applicable Law.

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

3.2. Processor's Responsibilities

3.2.1. The Processor shall process the Personal Data only in accordance with this Addendum, the attached "Schedule A", "Annex I" and "Annex II", if applicable, which incorporated into, and made a part of this Addendum, and the other lawful, documented instructions of the Controller, except where otherwise required by Applicable Law. The Agreement and this Addendum set out the Controller's complete instructions to the Processor 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.

3.2.2. The Processor shall assist the Controller in ensuring compliance with its obligations regarding security of Data Processing and notification of a Data Breach. The Processor shall also assist the Controller with Data Protection Impact Assessment and prior consultation with supervisory authority, taking into account the nature of processing and the information available to the Processor, provided, however, that if such assistance will entail excessive material costs or expenses to the Processor, the Parties shall first come to agreement on the Controller reimbursing the Processor for such costs and expenses.

3.2.3. The Processor makes available to the Controller all information necessary to demonstrate compliance with the Processor's obligations and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller according to section 6 of the Addendum and Applicable Law.

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

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

3.2.6. The Processor shall provide the Controller with two (2) weeks prior notice if there are any additions to the list of the Sub-processors thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the Sub-processor(s). The Processor 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. If, in Processor's reasonable opinion, such Controller's objections are legitimate, the Processor shall refrain from using such Sub-processor in the context of the Processing of Personal Data or shall notify the Controller of its intention to continue to use the Sub-processor. Where the Processor notifies the Controller of its intention to continue to use the Sub-processor in these circumstances, the Controller may, by providing written notice to the Processor, terminate the Agreement.

4. Categories of Personal Data and Purposes of Processing

4.1. The categories of Personal Data may be shared by the Controller 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 account of the Controller
- Certain identification necessary to obtain telephone numbers, such as photo ID

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

5. Security

5.1. The Processor shall implement appropriate security measures that ensure the availability, integrity, and confidentiality of Personal Data. The Processor 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 Addendum, its implementing rules and regulations, issued by a governmental regulatory body. Such security measures should be a subject of a regular review so as to ensure their appropriateness with regard to risks, which may evolve over time.

5.2. The Processor 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.

5.3. The Processor 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, except for approved Sub-processors.

6. Audit

6.1. Not more than once per annum, unless necessary due to security incident, the Processor shall allow for and contribute to audits during normal business hours and subject to a prior notice to the Processor of at least 30 (thirty) days as well as appropriate confidentiality undertakings by the Controller covering such inspections.

6.2. Before the commencement of any audit, the Controller and the Processor shall mutually agree upon the scope, timing, duration, and other significant terms of the audit. The Parties shall also agree on reimbursement rate for which the Controller shall be responsible unless such audit is the result of a security incident, and it reveals the Processor is at fault. All reimbursement rates shall be reasonable, taking into account the resources expended by the Processor. The Controller shall promptly notify the Processor with information regarding any non-compliance discovered during the course of an audit.

6.3. The Processor has created and is constantly improving the information security management system, which is confirmed by the ISO 27001 certificate. Upon Controller’s written request at

reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, the Processor shall make available to the Controller a copy of Voximplant's the most recent third-party audits or certifications, as applicable.

7. Personnel

7.1. 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 Addendum or as required by Applicable Law.

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

7.3. 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.

7.4. 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 Addendum.

8. Data Subject Rights

8.1. To the extent the Controller, in its use of the Services, does not have the ability to locate, correct, amend, restrict, copy, block, or delete Personal Data, as may be required by Applicable Law to ensure the rights of Data Subjects, the Processor shall comply with any commercially reasonable request by the Controller (including by appropriate technical and organizational measures) to assist such actions to the extent the Processor is legally permitted / required to do so by Applicable Law and the Controller of the Data Subject may be reasonably identified by the Processor.

8.2. Data Subjects have a right to see what Personal Data is held about them, and to know why and how it is processed. The Controller has an obligation to respond to these request or complaints. If a Data Subject contacts the Processor to exercise a right under Applicable Law, then the Processor will forward the request to the Controller. The Controller 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: ……

Voximplant, Inc.:

Voximplant Privacy Team

voximplant

Email: privacy@voximplant.com
Address: 150 West 25th Street, RM 403 New York City, NY 10001.

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.

8.3. Each Party shall rectify the complaint by any Data Subject within thirty (30) days from receipt of any such complaint. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 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.

8.4. The Parties shall cooperate with each other to promptly and effectively handle enquiries, subpoenas, complaints, audits, or claims from any court, government official, supervisory authority, third parties or individuals (including but not limited to the Data Subjects). The Processor shall promptly, and in any event within forty-eight (48) hours after having received any such enquiry, subpoena, complaint audit, claim or request, inform the Controller thereof.

9. Breach Management and Notification

9.1. 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 Controller when the Security Breach is subject to notification requirement; and
I. Measures and procedures for mitigating the possible harm and negative consequences to the Controller 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.

9.2. 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.

9.3. 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.

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

9.5. 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 Controller shall notify the required governmental regulatory body and the affected Data Subject within seventy-two (72) hours. If Applicable Law requires, both Parties or the Processor are responsible for reporting to the regulatory authorities.

9.6. 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. Cross-border Transfers

10.1. The Controller agrees that the Processor process Personal Data outside of the EEA or UK where the Processor, its Affiliates, or its Sub-processors maintain Data Processing operations, including in the United States. To ensure the security of cross-border transfers and to address the potential concern about governmental surveillance of mass communications, the Processor protects data in transit by end-to-end AES-128 encryption and high-level ciphers. The Processor also carefully monitors for emerging security threats and implement reasonable physical and technical security measures, which can be found at Annex II of the Addendum.

11. Duration of this Addendum

11.1. Upon termination or expiry of the Agreement or upon the termination of the provision of Data Processing services and upon the written request of the Controller, the Processor shall immediately cease any Processing of Personal Data.

12. Retention of Personal Data

12.1. 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.

12.2. If a complaint is received about the accuracy of Personal Data which affects Personal Data 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.

13. Return or Destruction of Personal Data

13.1. Upon expiration or termination of the Agreement or this Addendum, whichever comes first, the Processor, unless otherwise required by Applicable Law, 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 Controller;
b. Destroy all copies it made of Personal Data and any other property, information and documents if requested by the Controller. Request should be made via email specified in section 8 of the present Addendum. 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 Controller a certificate confirming Processor's compliance with the return or destruction obligation under this section, if requested by the Controller.

14. Liability

14.1. Each Party's and its Affiliates' liability arising out of or related to this Addendum (whether in contract, tort, or under any other theory of liability), is subject to the section 'Limitation of Liability' (or any similar section) of the Agreement.

15. Entire Agreement

15.1. Aside from the Standard Contractual Clauses governing Personal Data governed by GDPR, this Addendum constitutes the entire agreement between the parties with respect to the subject matter hereof. Aside from the Standard Contractual Clauses, this Addendum 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.

16. Amendment

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

17. Separability Clause

17.1. 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.

18. Counterparts

18.1. 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.

19. Assignment

19.1. 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 Party. Any attempted assignment or delegation that does not comply with this section shall be null and void and of no effect.

20. Non-Waiver of Rights

20.1. 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.

21. Legal Capacity of Representatives

21.1. 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.

22. Governing Law and Venue

22.1. 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. For clarity, any disputes regarding the Standard Contractual Clauses are governed as per Clause 18 of Schedule A. 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.

_____	**VOXIMPLANT, INC.**
By:	By:
_____	**ALEXEY AYLAROV, CEO**
	DocuSigned by: Alexey Aylarov 82FDAA670868423...

SCHEDULE A
EU STANDARD CONTRACTUAL CLAUSES (Controller to Processor Modules)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);
(viii) Clause 18(a) and (b).
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation
(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy
In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)
The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional
Docking clause
(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards
The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions
(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the

contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's

request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least two (2) weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

☐[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
☐[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
☐[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses
(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities
15.1 Notification
(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination
(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without

prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

voximplant

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____
_____

Activities relevant to the data transferred under these Clauses: the Services will consist primarily of providing communication tool that facilitate communication between Data Subjects and the Controller.

Signature and date: _____

Role: Controller

2. Data importer:

Name: Voximplant, Inc., a Delaware Corporation

Address: 150 West 25th Street, RM 403 New York City, NY 10001, USA

Contact: Voximplant Privacy Team; privacy@voximplant.com

Activities relevant to the data transferred under these Clauses: the Services will consist primarily of providing communication tool that facilitate communication between Data Subjects and the Controller.

Signature and date: DocuSigned by: Alexey Aylarov 7/7/2022
82FDAA670868423...

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
The personal data transferred concern the following categories of data subjects:
The data exporter and the individuals who are calling or called by numbers provided by the data importer to the data exporter.

Categories of personal data transferred
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.

Sensitive data transferred
The Processor does not knowingly process (and the Controller shall not provide) any sensitive data or any special categories of data.

The frequency of the transfer
Continuous through duration of the Agreement.

Nature of the processing
Processing of the Client's account data and, depending on configuration, limited end-user call information.

Purpose(s) of the data transfer and further processing
Provision of SaaS-based telecommunications platform for creation and utilization of voice and video calling via internet browser.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
For period no longer than the term of this Addendum, unless otherwise provided by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
See clause 3.2.5 of the Addendum.
Duration of the Processing: through duration of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY
Data Protection Commission, Republic of Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the services provided by the Processor pursuant to the Addendum, the Processor 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 Data Processing.

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

The Processor will take steps to ensure that any person acting under the authority of the Controller or the Processor 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

The Processor has created and is constantly improving the information security management system, which is confirmed by the ISO 27001 certificate.