EU DATA PROCESSING ADDENDUM

This EU Data Processing Addendum ("Addendum") supplements the SignalWire Cloud Agreement (the "Agreement") entered into by and between you and SignalWire. This Addendum is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order Form, or an executed amendment to the Agreement. Upon its incorporation into the Agreement, this Addendum will form a part of the Agreement. In accordance with Section 11 of the Agreement herein, you enter into this Addendum on behalf of yourself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of your Affiliates (defined below), if any. This Addendum incorporates the terms of the Agreement. Unless otherwise defined in this Addendum or in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them in Section 9 of this Addendum. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1. Details of Data Processing

1.1 Categories of data subjects: Your contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Customer.

1.2 Type of Personal Data. Contact Information, the extent of which is determined and controlled by you in your sole discretion, and other Personal Data such as communications data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the SignalWire Services.

1.3 Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by SignalWire is the provision of the services to Customer that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order Form.

1.4 Purpose. Personal Data will be Processed for purposes of providing the SignalWire Services set out and otherwise agreed to in the Agreement and any applicable Order Form.

1.5 Duration. As between SignalWire and you, the duration of the data processing under this Addendum is determined by you.

2. Processing of Data

2.1 Your rights and obligations with respect to this Processing are described herein. You shall, in your use of the SignalWire Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" and together, "Data Protection Laws")). You shall ensure that your instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with your instructions will not cause us to be in breach of the Data Protection Laws. You are solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to us by or on behalf of you, (ii) the means by which you acquired any such Personal Data, and (iii) the instructions it provides to us regarding the Processing of such Personal Data. you shall not provide or make available to us any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the SignalWire Services, and shall indemnify us from all claims and losses in connection therewith. This Addendum does not apply to Personal Data for which SignalWire is a controller.

2.2 We shall not Process Personal Data (i) for purposes other than those set forth in the Agreement (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by you, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which SignalWire is subject; in such a case, we shall inform you of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and (iii) in violation of the GDPR. You hereby instruct us to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by you in your use of the SignalWire Services.

2.3 Following completion of the SignalWire Services, at your choice, we shall return or delete the Personal Data, unless further storage of Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, We shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If you and SignalWire have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by us to you only upon your request.

3. Authorized Employees

3.1 We shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2 We shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with SignalWire, any Personal Data except in accordance with their obligations in connection with the SignalWire Services.

3.3 We shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees.

4. Authorized Sub-Processors

4.1 You acknowledge and agree that we may (1) engage our affiliates and the Authorized Sub-Processors to access and Process Personal Data in connection with the SignalWire Services and (2) from time to time engage additional third parties for the purpose of providing the SignalWire Services, including without limitation the Processing of Personal Data. By way of this Addendum, you provide general written authorization to us to engage Sub-Processors as necessary to perform the SignalWire Services.

4.2 A list of our current Authorized Sub-Processors (the "List") will be made available to you, either at a link provided to you, via email or through another means made available to you. Such List which may be updated by SignalWire from time to time. The List may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and you agree to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, we will add such third party to the List. You may reasonably object to such an engagement on legitimate grounds by informing us in writing within ten (10) days of receipt of the aforementioned notice by you. You acknowledge that certain Sub-Processors are essential to providing the SignalWire Services and that objecting to the use of a Sub-Processor may prevent us from offering the SignalWire Services to you.

4.3 If you reasonably object to an engagement in accordance with Section 4.2, and we cannot provide a commercially reasonable alternative within a reasonable period of time, we may terminate this Addendum. Termination shall not relieve you of any fees owed to us under the Agreement.

4.4 If you do not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by us, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5 We will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on us under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processors fails to fulfill its data protection obligations under such written agreement with us, we will remain liable to you for the performance of the Authorized Sub-Processor's obligations under such agreement

4.6 If you and SignalWire have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute your prior written consent to the subcontracting by us of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by us to you pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by us beforehand, and that such copies will be provided by us only upon request by you.

5. Security of Personal Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

6. Transfers of Personal Data

6.1 The parties agree that we may transfer Personal Data processed under this Addendum outside the European Economic Area ("EEA") or Switzerland as necessary to provide the SignalWire Services. If we transfer Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, we will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2 Where required, any transfer of Personal Data made subject to this Addendum to any countries which do not ensure an adequate level of data protection shall be undertaken by us through one of the following mechanisms: (a) in accordance with the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles"), or (b) the Standard Contractual Clauses set forth in Exhibit A to this Addendum.

6.3 If transfers are made pursuant to 6.2(a), we self-certify to, and comply with, the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and shall maintain such self-certification and compliance with respect to the Processing of Personal Data transferred from member states of the EEA or Switzerland to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of the foregoing countries for the duration of the Addendum.

7. Rights of Data Subjects

7.1 We shall, to the extent permitted by law, notify you upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If we receive a Data Subject Request in relation to your data, we will advise the Data Subject to submit their request to you and you will be responsible for responding to such request, including, where necessary, by using the functionality of the SignalWire Services. You are solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to us, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject

7.2 We shall, at your request, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist you in complying with your obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) you are unable to respond without our assistance and (ii) we are able to do so in accordance with all applicable laws, rules, and regulations. You shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by us.

8. Actions and Access Requests

8.1 We shall, taking into account the nature of the Processing and the information available to us, provide you with reasonable cooperation and assistance where necessary for you to comply with our obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that you do not otherwise have access to the relevant information. You shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by us.

8.2 We shall, taking into account the nature of the Processing and the information available to us, provide you with reasonable cooperation and assistance with respect to your cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. You shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by us.

8.3 We shall maintain records sufficient to demonstrate our compliance with our obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. You shall, with reasonable notice to us, have the right to review, audit and copy such records at our offices during regular business hours.

8.4 Upon your request, we shall, no more than once per calendar year, either (i) make available for your review copies of certifications or reports demonstrating our compliance with prevailing data security standards applicable to the Processing of your Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow you or your authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of our data security infrastructure and procedures that is sufficient to demonstrate our compliance with our obligations under this Addendum, provided that you shall provide reasonable prior notice of any such request for an audit and such inspection shall not be unreasonably disruptive to our business. You shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to us for any time expended for on-site audits. If you and SignalWire have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.4.

8.5 We shall immediately notify you if an instruction, in our opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6 In the event of a Personal Data Breach, we shall, without undue delay, inform you of the Personal Data Breach and take such steps as we in our sole discretion deem necessary and reasonable to remediate such violation (to the extent that remediation is within our reasonable control).

8.7 In the event of a Personal Data Breach, we shall, taking into account the nature of the Processing and the information available to us, provide you with reasonable cooperation and assistance necessary for you to comply with your obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8 The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from your actions or omissions. Our obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by us of any fault or liability with respect to the Personal Data Breach.

9. Definitions

"**Affiliate**" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

"**Anonymous Data**" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

"**Authorized Employee**" means an employee of SignalWire who has a need to know or otherwise access Personal Data to enable We to perform their obligations under this Addendum or the Agreement.

"**Authorized Sub-Processor**" means a third-party who has a need to know or otherwise access Personal Data to enable us to perform our obligations under this Addendum or the Agreement, and who is either (1) listed on the SignalWire Website at https://signalwire.com/legal/signalwire-cloud-sub-processors or (2) authorized by you to do so under Section 4.2 of this Addendum.

"**Data Subject**" means an identified or identifiable person to whom Personal Data relates.

"**Instruction**" means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by you to us and directing us to Process Personal Data.

"**Personal Data**" means any information relating to Data Subject which is subject to Data Protection Laws (defined below) and which we Process on your behalf other than Anonymous Data.

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

"**Privacy Shield Principles**" means the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"**Standard Contractual Clauses**" means the agreement executed by and between you and us and attached hereto as Exhibit A pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to us established in third countries which do not ensure an adequate level of protection (or any updated version thereof).

"**Supervisory Authority**" means an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, or Norway.

EXHIBIT A

Standard Contractual Clauses

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

The entity identified as "Customer" in the Agreement (the "data exporter") and SignalWire, Inc., 228 Hamilton Ave, Palo Alto, CA, USA (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', 'you', 'We', '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 you and any of your affiliates;

(c) 'the data importer' means SignalWire and any of our affiliates;

(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 you in the Member State in which the data exporter is established; and

(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 SignalWire 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 SignalWire 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 SignalWire 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.

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

4. 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 SignalWire Services

1. The parties agree that on the termination of the provision of data processing SignalWire Services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter: The data exporter is the entity identified as “Customer” in the Agreement

Data importer: The data importer is SignalWire, Inc., a provider of communications services.

Data subjects: Data subjects are defined in Section 1 of this Addendum.

Categories of data: the personal data is defined in Section 1 of this Addendum.

Processing operations: The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Section 1 of this Addendum.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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

1. General. SignalWire believes that information is an extremely valuable asset that must be protected. Therefore, we have created and implemented an Information Security Program (the "Program"), as further described in this Appendix 2. The objective of the Program is the effective protection of personally identifiable and other sensitive information relating to our company, customers, and business partners (collectively, "Sensitive Information").

2. Definitions. For the purposes of this Appendix 2, the terms below have the following meanings whenever capitalized:

"**Data Incident**" means any unauthorized access to or acquisition, disclosure, use, or loss of Sensitive Information resulting from breach or compromise of Company Systems.

"**Incident Response Team**" means the group of employees with the expertise, authority and resources to act quickly, efficiently and appropriately in the event of a Security Incident.

"**Company Systems**" means our information technology systems and devices that store, process, and/or transmit Sensitive Information, including without limitation our network, databases, computers, and mobile devices, to the extent applicable.

3. Sensitive Information. For clarity, Sensitive Information includes:

3.1 Any information that personally identifies an individual (including, but not limited to, name, postal address, email address, telephone number, date of birth, Social Security number, driver's license number, other government-issued identification number, financial account number, or credit or debit card number).

3.2 All financial, business, legal, and technical information which is developed, collected, learned, or obtained by us in the course of its business activities that would reasonably be understood to be confidential, including information belong to or pertaining to our customers.

4. Security Program. We shall create, implement, and maintain the Program to include reasonably appropriate administrative, technical, and physical safeguards to protect the confidentiality and security of Sensitive Information. We shall also periodically review and update the Program, paying attention to developments in technology and industry standard practices. Currently, protection for We Systems includes:

4.1 User authentication controls, including restricting access to authorized users.

4.2 Access controls and physical facility security measures, including controls that limit access to Sensitive Information to individuals that have a demonstrable genuine business need-to-know.

4.3 Regular monitoring of Company Systems to prevent loss or unauthorized access to, or acquisition, use, or disclosure of, Sensitive Information.

4.4 Technical security measures such as encryption, firewall protection and antivirus protection.

4.5 Ongoing training and awareness programs designed to ensure workforce members and others acting on our behalf are aware of and adhere to the Program's policies, procedures, and protocols.

4.6 Ongoing adjustments to the Program based on periodic risk assessments.

5. Access Control.

5.1 Rights to use and access Company Systems are based on each user's access privileges. Access privileges are granted on the basis of specific business need (i.e. a "need to know" basis) and are restricted to only those personnel who require such access to perform their job functions as determined by our management.

5.2 All Company resources, systems, and applications have access controls unless specifically designated as a public access resource.

5.3 Physical access to locations where Sensitive Information is stored is restricted to personnel and service providers who require access in order to perform their designated job functions or services.

5.4 Our employees, temps, contractors, consultants, and other workers including all personnel affiliated with third parties, are responsible for participating in maintaining secure access to Company Systems and for ensuring that we adhere to our posted Privacy Policy.

6. System Monitoring and Protection.

6.1 We reasonably monitor Company Systems for unauthorized use of or access to Sensitive Information.

6.2 Malware protection software is installed on all computers storing Sensitive Information.

6.3 We have a threat and vulnerability management program to monitor for vulnerabilities on an on-going basis that are acknowledged by vendors, reported by researchers, or discovered internally through vulnerability scans.

7. Evaluation and Adjustment of the Program.

7.1 We reserve the right to revise the conditions of this Program at any time. Adequate notification of updates will be provided to all personnel. Personnel are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this Program.

7.2 Company management will periodically evaluate and adjust the Program as appropriate to address: (a) the current risk assessment, management and control activities; (b) new risks or vulnerabilities identified by our top management using the standards set forth above; (c) technology changes that may affect the protection of Sensitive Information; (d) material changes to our business, including to the size, scope and type of our business; (v) the amount of resources available to us; (vi) the amount of Sensitive Information stored or held by us; (vii) any increased need for security and confidentiality of Sensitive Information; and (viii) any other circumstances that our management believes may have a material impact on the Program.

8. Personnel and Service Providers.

8.1 We shall exercise necessary and reasonably appropriate supervision over our employees and others acting on our behalf to maintain confidentiality and security of Sensitive Information.

8.2 Prior to engaging any third-party service provider who may receive Sensitive Information, we will take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect the Sensitive Information.

8.3 We shall terminate an individual’s access to Company Systems as soon as reasonably practicable after such individual is no longer employed or engaged by us. Terminated personnel are required to surrender all keys, IDs, access codes, badges, business cards and the like that permit access to our premises and/or systems.

9. Data Incidents.

9.1 In the event of a Data Incident, the Incident Response Team will conduct a post-incident review of events and decide the appropriate actions to take to minimize the Data Incident and mitigate the consequences.

9.2 If necessary, the Security Coordinator shall make changes in business practices relating to protection of Sensitive Information following a Data Incident, and promptly notifying affected parties.

9.3 The Security Coordinator shall document the foregoing and provide a report to management.

10. Secure Return or Dispositions. We shall return or dispose of Sensitive Information, whether in paper or electronic form, in a secure manner.