dialpad

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is between the entity listed on the signature block below, together with its subsidiaries and affiliates ("**Customer**") (each entity a "**data exporter**"), and Dialpad, Inc. ("**Dialpad**").

Customer and Dialpad are parties to the Master Service Agreement and any associated Amendments, ("**Agreement**"), under which Customer obtains services from Dialpad. Any terms not defined have the meaning as defined in the Agreement.

Dialpad periodically updates these terms. If you have an active account, Dialpad will let you know when we do via email or via in-app notification.

1. Definitions.

    a. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. Control means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

    b. **"Controller"** means the entity which (alone or jointly with others) determines the purposes and means of the Processing of Personal Data.

    c. "**Data Subject**" means a natural person or as otherwise defined in the GDPR.

    d. **"Data Protection Laws"** means, as applicable: (a) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"); (b) the Swiss Federal Data Protection Act of 19 June 1992; (c) European Union member state law; and any future amending acts.

    e. **"EEA"** means the European Economic Area.

    f. "**Standard Contractual Clauses**" means the language approved by European Commission decision 2010/87/EU, attached hereto as Exhibit A and available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010D0087-20161217.

    g. "**Personal Data**" shall mean all information relating to an identified or identifiable natural person or as otherwise defined in the GDPR.

    h. "**Processing**" or "**Processes**" shall have the meaning as defined in the GDPR.

    i. "**Processor"** means the entity which Processes Personal Data on behalf of, and under the instruction of the Controller.

2. Subject matter of the DPA and duration. Subject matter of the DPA, its nature and purpose is described in the Agreement. The duration of the DPA is the duration of the Agreement. The type of Personal Data and the categories of Data Subjects is described in Appendix 1 to Exhibit A to this DPA.

3. Compliance with Customer's instruction and Data Protection Laws. Dialpad will comply with the instructions of Customer and Data Protection Law relating to its privacy and data protection obligations under this DPA. In case Dialpad is required by law to Process Personal Data without Controllers' instruction, Dialpad will inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Dialpad will inform Customer if, in its opinion, an instruction infringes Data Protection Law. For the avoidance of doubt, all requirements and obligations herein related to Data Protection Law of union or member states shall only apply to EU-originating Personal Data that Dialpad Processes and shall not apply to the Personal Data of non-EU citizens.

4. Dialpad's Role:

   a. Dialpad is a Processor with respect to Dialpad's Processing of Personal Data provided by Customer or otherwise arising from Customer's use of the Services under the Agreement.

   b. Dialpad is a Controller with respect to Dialpad's Processing of Personal Data in connection with the Services to facilitate the following legitimate interests:
      i. contractual and pre-contractual business relationships;
      ii. regulatory and other legal obligations;
      iii. personalization of the Platform for you by understanding your needs;
      iv. research and development new features, tools and products;
      v. aggregate analysis, market research and planning;
      vi. protection of Dialpad, our Customers and the public;
      vii. customer support;
      viii. Services-related communications;
      ix. marketing communications;

5. Dialpad Obligations

   a. Dialpad will ensure that persons authorized to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Dialpad will ensure that access to Customer Personal Data is limited to only those individuals who need to know or access the Customer Personal Data for purposes of providing the Services in accordance with the Agreement.

   b. Dialpad will: (i) take appropriate and reasonable technical and organisational measures to guard against the unauthorised or unlawful processing of Customer Personal Data and against the accidental loss or destruction of, or damage to, such Personal Data to ensure a level of security appropriate to: (A) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (B) the nature of the data to be protected and (ii) take reasonable steps to ensure compliance with those measures. Notwithstanding any provision to the contrary, Dialpad may modify or update the security measures identified in Appendix 2 at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the security measures.

   c. All of Dialpad's employees authorised to Process Personal Data are required to commit themselves to confidentiality or need to be under an appropriate statutory obligation of confidentiality.

   d. Dialpad will make available to Customer all data necessary to demonstrate compliance with this DPA and applicable Data Protection Laws and will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

6. Notice of Data Subject Requests. Dialpad will notify Customer promptly, and where feasible within 15 days, if Dialpad receives a request from Data Subjects to exercise their rights with respect to their Personal Data being Processed by Dialpad. Dialpad will not respond to such individuals without Customer's prior written consent, except to confirm that such request relates to Customer.

7. Cooperation. Dialpad will meet its obligations under Data Protection Legislation to assist the Customer by implementing appropriate and reasonable technical and organizational measures to (i) fulfill the Customer's obligation to respond to requests from Data Subjects under Data Protection Law as they pertain to Dialpad data; and (ii) meet Customer's legal obligations with

respect to breach notification, data protection impact assessments, or the cooperation or prior consultation with a supervisory authority, taking into account the nature of the Processing and information available to Dialpad.

8. Data Breach. Dialpad shall promptly and, where feasible, within 72 hours, notify Customer upon Dialpad or any sub-Processor becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration Customer's Personal Data and shall take such commercially reasonable steps as are directed by Customer to assist in the investigation, mitigation, and remediation of such a breach.

9. Data Transfers. To permit Dialpad to transfer and Process Personal Data outside of the European Economic Area or the United Kingdom, Dialpad warrants that:
    a. it has and will maintain EU-U.S. and/or Swiss-U.S. Privacy Shield, as appropriate, and will make information available to Customer about such certification; and/or
    b. if Privacy Shield is unacceptable, it will enter into the Standard Contractual Clauses, which are incorporated by reference into this Agreement.

10. Sub-Processors. Customer specifically authorizes the engagement of Dialpad's Affiliates as sub-Processors. Customer also hereby provides general written authorization for Dialpad to use sub-Processors for the provision of the Services, provided that:
    a. Sub-Processors are engaged by written agreement under terms consistent with the material terms of this Agreement, as if the sub-Processor were Dialpad;
    b. Dialpad remains fully liable to Customer for the Sub-processor's performance of its data protection obligations;
    c. The sub-Processor complies with its obligations under the Data Protection Laws relating to any Personal Data and has sufficient organizational and technical measures in place to protect the Personal Data against unauthorized or unlawful processing;
    d. Dialpad will notify Customer of any intended addition or replacement of a sub-Processor, giving Customer at least fourteen (14) calendar days to object to the change. Should Customer reasonably object to the use of a new sub-Processor, Customer shall provide the reason(s) and work in good faith with Dialpad to resolve such concerns.

11. Audits. Dialpad will allow for and contribute to audits of itself or its sub-Processors, including inspections, conducted by Customer or another auditor mandated by Customer, upon reasonable notice, to demonstrate compliance with the obligations of this DPA providing that Dialpad reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance.

12. Data Deletion. Upon the expiration or termination of the Agreement, Dialpad will delete all Personal Data, unless further storage of the Personal Data is required or authorized by the applicable Data Protection Laws. Deleted data may continue to reside in Dialpad backups for up to 60 days.
    a. If Dialpad is unable to delete the Customer Personal Data for technical or other reasons, it will apply measures to ensure that Personal Data is restricted from any further Processing.
    b. Customer acknowledges and agrees that Customer will be responsible for exporting, before the expiration or termination of the Agreement of any Customer Personal Data it wishes to retain following the expiration or termination of the Agreement. Any additional cost arising in connection with the return or deletion of the Customer Personal Data after the termination or expiration of the Agreement shall be borne by the Customer.
    c. For clarity, Dialpad may continue to Process any Personal Data that has been aggregated in a manner that does not identify individuals or its customers to improve Dialpad's systems and Services or if Processing of the Customer Personal Data is needed to protect the legitimate interests of Dialpad and/or for any legal matters thereto.

13. General.

a. Except as expressly amended herein, the Agreement remains in full force and effect.

b. By executing this Addendum, the parties hereto ratify and confirm the terms of the Agreement, as modified by the terms of this Addendum.

c. If there shall be any conflict in the terms and conditions of the Agreement and the terms and conditions of this Addendum, the terms and conditions of this Addendum shall control and be binding. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

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

e. Without prejudice to Clause 7 (Mediation and Jurisdiction) and Clause 9 (Governing Law) of the Standard Contractual Clauses, Customer and Dialpad submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum and this Addendum and all non-contractual or other obligations arising out of or in connection with it shall be governed by the laws of the country or territory stipulated for such purpose in the Agreement.

f. All references in the Agreement in and/or to "this Agreement" and words of a like nature shall be deemed to refer to the Agreement, as amended and supplemented by this Addendum.

IN WITNESS WHEREOF, the parties have caused duly authorised representatives of their respective companies to execute this Addendum on the date or dates set forth below.

Customer: ______________________	**Dialpad, Inc.**
By: ______________________	By: ______________________
Name: ______________________	Name: ______________________
Title: ______________________	Title: ______________________
Date: ______________________	Date: ______________________

dialpad

EXHIBIT A
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Name of the data exporting organisation:

Customer accepting the Clauses on behalf of itself and its subsidiaries and Affiliates (each a "**data exporter**")

And

Dialpad, Inc.
100 California Street, Suite 500, San Francisco, CA 94111
Tel (415) 805-2100
e-mail legal@dialpad.com
(the **"data importer"**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

(d) the "**sub-Processor**" means an entity engaged by the Data Processor or any further sub-Processor to Process Personal Data on behalf and under the authority of Customer, i.e. Data Controller.;

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

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

Clause 2

Details of 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 sub-Processor 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 sub-Processor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the Data Exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

(g) to forward any notification received from the data importer or any sub-Processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-Processor 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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-Processor 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 sub-Processor 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 sub-Processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity

The data importer may not rely on a breach by a sub-Processor of its obligations in order to avoid its own liabilities

(3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-Processor 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 sub-Processor agrees that the data subject may issue a claim against the data sub-Processor 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 sub-Processor 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 sub-Processor, 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 sub-Processor preventing the conduct of an audit of the data importer, or any sub-Processor, 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

Sub-processing

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 sub-Processor which imposes the same obligations on the sub-Processor as are imposed on the data importer under the Clauses. Where the sub-Processor 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 sub-Processor's obligations under such agreement..

2. The prior written contract between the data importer and the sub-Processor 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 sub-Processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-Processor 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 sub-Processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Customer and its Affiliates established within the European Union

Data importer

The data importer is:

Dialpad, Inc., a provider of hosted telephony software applications, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data Subjects

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

The data transferred may involve all categories of Data Subjects of the Data Exporter including, without limitation:

- Current, past, potential employees, trainees, voluntary workers
- Current, past, potential employees of associated companies, organisations
- Current, past, potential employees of other organisations
- Current, past, potential recipients, customers, counter parties or clients for goods or services (direct or indirect)
- Current, past, potential suppliers of goods or services (direct or indirect)
- Current, past, potential directors, other senior officers
- Current, past, potential business or other contacts

Categories of data

The personal data transferred concern the following categories of data:

- Contact information including names, e-mails, phone numbers
- Device and browser information
- Profile photo
- Addresses where provided by users
- Call logs
- Voice recording and transcription
- Non-payment card billing information

Special categories of data (if appropriate)

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

Dialpad services do not require disclosure and Dialpad does not record the relation of special categories to any person. To the extent that data exporter provides information on special categories, Dialpad will keep such data secure, as with any other data provided by data exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

- Incidental access during the provision of information technology services by the data importer
- Storage or transport of data on equipment used by the data importer
- Provision of business services of an advisory, consulting or intermediary nature in relation to best practice and benchmarking services.

APPENDIX 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by Dialpad as the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. SECURITY

a. Security Policy. External policy and notice to the public, users, or customers that describes how the data importer protects the security and privacy of data.
b. Security Standards. Alignment with industry recognized security standards ("Security Standards"), specifically AICPA Trust Services Principles (SOC 2), and Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ), which may be amended, revised or updated in accordance with industry standards.
c. Incident Management. Processes and procedures to identify and address security and privacy incidents.
d. Process to ensure that service providers and subcontractors retained by data importer are capable of taking appropriate steps to protect sensitive data and systems.
e. Change management process to ensure that all changes to networks, systems, and processes are appropriately reviewed.

2. AUDITS

a. Internal audits of the security and privacy program.
b. Third party audits of the security and privacy program.

3. HUMAN RESOURCE SECURITY

a. Written internal policies, guidelines, and documented practices for the safe handling and protection of data.
b. Security and Privacy Awareness Training. Training program to ensure that relevant staff are familiar with data importer's information security and privacy program and processes.
c. Background Checks. To the extent lawfully permitted, conducting background screening of employees and staff who have access to customer data.
d. Disciplinary Policy and Process. A disciplinary process to enforce adherence to internal policy.

4. ACCESS MANAGEMENT

a. Processes and procedures to limit access to sensitive information and systems to staff that have a need to know.

5. SECURITY LOGS

a. Processes that log access to sensitive information and systems and procedures to audit those logs for unauthorized access.