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**") (a "**data importer"**).

Customer and Dialpad are parties to the Master Service Agreement and any associated Amendments, ("**Agreement**"), under which Customer obtains services from Dialpad.

1. Applicability

This DPA applies where Dialpad processes Personal Data as a Processor (or sub-Processor as applicable) on behalf of Customer and such Personal Data is subject to Applicable Data Protection Laws (as defined below). This DPA also applies where Dialpad processes Personal Data as a Controller and such Personal Data is subject to Applicable Data Protection Laws (as defined below). The parties have agreed to enter into this DPA in order to ensure that appropriate safeguards are in place to protect such Personal Data in accordance with Applicable Data Protection Laws.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement or Applicable Data Protection Laws. For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including the SCCs (where applicable), as defined herein).

2. Definitions

a. "**Applicable Data Protection Laws**" means all laws and regulations that are applicable to the processing of Personal Data under the Agreement, including European Data Protection Laws and the CCPA, as well as any future amending acts of the above-mentioned data protection laws any other applicable international, federal, national and state privacy and data protection laws, rules and regulations pertaining to privacy, data processing and use, data protection, data security, encryption or confidentiality.

b. **"CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199, 2018).

c. **"Customer Data**" means data and information (a) that is disclosed to Dialpad by Customer in connection with the provision of the Services; and (b) that is processed, prepared, accessed, used, aggregated or generated, or any combination thereof, in connection with the performance of the Services.

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

e. "**European Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii)).

f. "**Personal Data**" means all data which is defined as '*Personal Data*', '*personal information*', or '*personally identifiable information*' (or analogous term) under Applicable Data Protection Laws.

g. **"Restricted Transfer"** means: (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner; and (iv) where another applicable data protection law applies, an international transfer that is not automatically allowed pursuant to said applicable data protection law.

h. "**Standard Contractual Clauses**" and "**SCCs**" mean, depending on the circumstances unique to Customer, any of the following:

i. UK Standard Contractual Clauses, and

ii. EU Standard Contractual Clauses.

i. "**UK Standard Contractual Clauses**" and ("**UK SCCs**") means:

i. Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU ("*UK Controller to Processor SCCs*"), and

ii. Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC ("*UK Controller to Controller SCCs*").

j. **"EU Standard Contractual Clauses**" and ("**EU SCCs**") means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

k. "**Services**" shall refer to the Services described in the Agreement.

l. "**Controller**," "**Data Subject**," "**Joint Controller**," "**Processor**," and "**Supervisory Authority**" shall have the meanings as defined in the GDPR or other Applicable Data Protection Laws as applicable.

3. Subject Matter of the DPA; Duration

The subject matter of the DPA, its nature, and purpose are described in the Agreement. The duration of the DPA is the duration of the Agreement. The type of Personal Data processed pursuant to this DPA, the categories of Data Subjects, the subject matter, duration, nature and purpose of the processing, as well as a description of relevant data transfer are described in Annex 1.

4. Status of the Parties

a. In respect of the parties' rights and obligations under this DPA regarding the processing of Personal Data for the provision of the Services, as further described in Annex I, the parties acknowledge and agree that the Customer is the Controller (or a Processor processing Personal Data on behalf of a third-party Controller), and Dialpad is a Processor (or sub-Processor, as applicable). If Customer is a Processor, Customer warrants to Dialpad that Customer's instructions and actions with respect to the Personal Data, including its appointment of Dialpad as another Processor and, where applicable, concluding the SCCs, have been (and will, for the duration of this DPA, continue to be) authorised by the relevant third-party Controller.

b. In respect of the parties' rights and obligations under this DPA regarding the processing of Personal Data for the improvement of the Services, as further described in Annex I, the parties acknowledge and agree that Dialpad is a Controller for this limited processing purpose.

5. Dialpad Obligations

With respect to all Personal Data it processes in its role as a Processor (or sub-Processor, as applicable), Dialpad warrants all of items i-xi below. With respect to Personal Data it processes in its role as Controller, Dialpad warrants all of items iii-xi below.

i. Dialpad shall only process Personal Data in order to provide the Services and in accordance with: (i) the Customer's written instructions as set out in the Agreement and this DPA, unless required to do so by applicable European Union or Member State law to which Dialpad is subject, and (ii) the requirements of Applicable Data Protection Laws.

ii. Dialpad shall inform Customer if, in Dialpad's opinion, any processing instructions provided by the Customer infringe Applicable Data Protection Laws.

iii. Dialpad shall comply in all material respects with all laws, regulations, rules, orders and other requirements, now or hereafter in effect, of any governmental authority, applicable to its performance hereunder.

iv. Dialpad shall not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services, including for a commercial purpose other than providing the Services. Dialpad's performance of the Services may include disclosing Personal Data to sub-Processors where this is in accordance with Section 7 of this DPA.

v. Dialpad shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Dialpad may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

vi. 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 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.

vii. Dialpad shall without undue delay and, where feasible within 72 hours, notify Customer upon Dialpad becoming aware of any breach of security leading to the accidental or unlawful destruction, loss or alteration of Personal Data ("**Personal Data Breach**") and shall take such commercially reasonable steps as are directed by Customer to assist in the investigation, mitigation and remediation of such a breach.

viii. Dialpad shall not make any public announcement about a Personal Data Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law.

ix. To the extent that Dialpad is able to verify that a data subject is associated with the Customer, notify Customer promptly if Dialpad receives a request from data subjects to exercise their rights (including rights of access, rectification or erasure) with respect to their Personal Data being Processed by Dialpad (a "**Data Subject Request**"). Dialpad will not respond to a Data Subject Request without Customer's prior written consent, except to confirm that such request relates to Customer.

x. Other than to the extent required to comply with applicable law, following termination or expiry of the Agreement or completion of the Services, at the choice of Customer, Dialpad shall delete or return all Personal Data (including copies thereof) processed pursuant to this DPA.

xi. Taking into account the nature of processing and the information available to Dialpad, Dialpad shall provide such assistance to the Customer as the Customer reasonably requests in relation to Dialpad's obligations under Applicable Data Protection Laws with respect to:

1. data protection impact assessments;

2. notifications to the supervisory authority under Applicable Data Protection Laws and/or communications to data subjects by the Customer in response to any Personal Data Breach; and

3. the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to the security of processing;

provided that the Customer shall cover all costs incurred by Dialpad in connection with its provision of such assistance.

6. Customer Obligations

a. Customer shall comply in all material respects with all laws, regulations, rules, orders and other requirements, now or hereafter in effect, of any governmental authority, applicable to its performance hereunder, including all Applicable Data Protection Laws.

b. As between the parties, the Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which the Customer acquired Personal Data and by which Dialpad acquired Personal Data from Customer.

c. Customer agrees and warrants that:

i. it legally collected and is legally able to provide Customer Data to Dialpad in accordance with Applicable Data Protection Laws, including obtaining all appropriate consents or other valid legal bases for any processing by Dialpad, either as controller or processor, including all processing as described in the Agreement;

ii. it shall ensure that its privacy policy:

1. clearly identifies the controller(s) of Personal Data, including details of third parties such as Dialpad;

2. provides a conspicuous link to or description of how to access a relevant choice mechanism, including how to opt-out of data collection; and

3. includes any other information required to comply with the transparency requirements of Applicable Data Protection Law, including an indication of sharing and/or transfer of data to Dialpad.

iii. For clarity, where Customer is required to obtain consent on behalf of Dialpad to the collection and processing of Customer Data, Customer represents and warrants that it shall at all times maintain and make operational a mechanism for (i) obtaining and recording such consent; and (ii) that enables such consent to be withdrawn, in accordance with Applicable Data Protection Law. Customer agrees to provide such consent records to Dialpad promptly upon request.

7. Sub-Processors

a. Dialpad will only disclose Personal Data to Sub-Processors for the specific purposes described in Annex 1. Dialpad does not sell or disclose Personal Data to third parties for commercial purposes.

b. The Customer grants a general written authorization to Dialpad to appoint third parties as Sub-Processors to support the processing of data described in Annex 1.

c. Dialpad will maintain a list of Sub-Processors at https://www.dialpad.com/subprocessors/ and will add the names of new and replacement Sub-Processors to the list at least fourteen (14) calendar days prior to the date on which those Sub-Processors commence processing of Personal Data. If Customer objects to any new or replacement Sub-Processor on reasonable grounds related to data protection, it shall notify Dialpad of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Dialpad is reasonably able to provide the Services to the Customer in accordance with the Agreement without using the Sub-Processor and decides in its discretion to do so, then Customer will have no further rights under this clause 7.c in respect of the proposed use of the Sub-Processor. If Dialpad, in its discretion, requires use of the Sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement Sub-Processor, then Customer may terminate the applicable underlying agreement effective upon the date Dialpad begins use of such new or replacement Sub-Processor solely with respect to the Services that will use the proposed new Sub-Processor for the processing of Personal Data.

d. If Customer does not provide a timely objection to any new or replacement Sub-Processor in accordance with clause 7.c, Customer will be deemed to have consented to the Sub-Processor and waived its right to object.

e. Dialpad will ensure that any Sub-Processor it engages to provide an aspect of the Services on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such Sub-Processor terms that are no less protective of Personal Data than those imposed on Dialpad in this DPA. Dialpad remains fully liable to Customer for the Sub-Processor's performance of its data protection obligations.

8. International Provisions

a. Customer acknowledges that Dialpad's primary data processing facilities are in the United States of America.

b. To the extent Dialpad processes Personal Data originating from and protected by Applicable Data Protection Laws in one of the jurisdictions listed in Annex 4 (**Jurisdiction Specific Terms**) of this DPA, the terms specified in Annex 4 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

c. To the extent Customer's use of the Services requires an international data transfer mechanism to lawfully transfer Personal Data internationally, the terms set forth in Annex 3 (**Cross Border Transfer Mechanisms**) will apply in addition to the terms of this DPA.

9. Government Data Demands

If Dialpad becomes aware of any government data demands requesting Personal Data that Dialpad processes on behalf of Customer (such as a subpoena, court order, or search warrant) then Dialpad, in accordance with its Government Data Demands Policy, will:

a. immediately notify Customer of the government data demand unless such notification is legally prohibited;

b. take all reasonable steps to ensure the validity and enforceability of any governmental data demand;

c. disclose Personal Data only in response to a valid and enforceable government data demand; and

d. to the extent Dialpad provides access to or discloses Personal Data in response to valid and enforceable government data demand, then Dialpad will disclose the minimum amount of Personal Data to the extent it is legally required to do so and in accordance with the applicable legal process.

10. General

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

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

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

d. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA 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. Dialpad may update this DPA as necessary for compliance with the requirements of Applicable Data Protection Laws and/or changes in the Services, provided that Dialpad's practices and this DPA remain compliant with all Applicable Data Protection Laws, and updates do not reduce the privacy and/or security provided under this Agreement. Dialpad will provide notice of this update to Customer.

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 DPA.

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.

DIALPAD, INC.	**CUSTOMER:**
Signature: _____	Entity Name: _____
Printed Name: _____	Signature: _____
Title: _____	Printed Name: _____
Date: _____	Title: _____
	Date: _____

ANNEX I - DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name:	The Customer listed in the Agreement.
Address:	As provided in the Agreement.

Contact person's name, position and contact details: As provided in the Agreement.

Activities relevant to the data transferred under these Clauses: The Services as defined in the Agreement.

Signature:	See signature block of the DPA
Name:	See signature block of the DPA
Title:	See signature block of the DPA
Date Signed:	See signature block of the DPA
Role:	Controller or Processor (as applicable)

Data importer(s):

Name: Dialpad, Inc.

Address: 3001 Bishop Ranch, Suite 300, San Ramon, CA 94583.

Contact person's name, position and contact details: General Counsel, legal@dialpad.com.

Activities relevant to the data transferred under these Clauses: The Services as defined in the Agreement.

Signature:	See signature block of the DPA
Name:	See signature block of the DPA
Title:	See signature block of the DPA
Date Signed:	See signature block of the DPA
Role:	Processor and Controller (as defined in this DPA)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects are those personnel or customers of the data exporter who use the service or communicate Personal Data with those who use the service, which may include data exporter's employees, contractors and collaborators, as well as customers and potential customers.

Categories of personal data transferred

The Personal Data transferred includes information required to establish an account for the provisions of the Services, including names, email addresses, phone numbers, contact or location information, and billing information. Other than Personal Data required to establish an account, the data exporter solely determines the categories of Personal Data transferred, as determined through the data exporter's use of the Services to place calls, create contact lists, send messages, upload images, and record or transcribe calls.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data importer does not seek or require any transfer or processing of sensitive data. Data exporter solely determines whether sensitive data is processed by the data importer. In such case, the processing of sensitive data occurs exclusively with the consent and affirmative choice of the data exporter, as determined through the data exporter's use of the Services to discuss, capture, and retain sensitive data within the system, such as by placing calls, creating contact lists, sending messages, uploading images, and recording or transcribing calls.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data transfer is continuous up until the data exporter closes its Services account. At that point, the data transfer will cease and all stored data will be deleted in accordance with the contract between the data exporter and the data importer, the Standard Contractual Clauses and this DPA, and the privacy policy of the data importer.

Nature of the processing

The nature of the processing includes collection, recording, organisation, structuring, storage, retrieval, and erasure or destruction of data as governed by the contract between the data exporter and the data importer, in order to deliver and improve the Services, including VoIP phone service, and artificial intelligence transcription, analysis, and automation.

Purpose(s) of the data transfer and further processing

Data is transferred and processed for the purpose of providing, maintaining, improving, and billing for the Services pursuant to the contract between data exporter and data importer. The processing required under this purpose is justified by contract (for services delivery, including artificial intelligence training and customization), by legitimate interest (for development and improvement) and by consent (including for marketing).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data is retained for the duration of Services. Data exporter has the right to implement a retention policy that specifically governs the retention period.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data importer transfers Personal Data to sub-processors as governed by the Standard Contractual Clauses and this DPA. The subject matter and nature of the Personal Data transferred to sub-processors depends on the specific services used and sub-processor to whom the Personal Data is transferred, and is limited only to data required for sub-processor's role in providing the service. Personal Data that is transferred to sub-processors pursuant to the Standard Contractual Clauses and this DPA is retained by the sub-processor only for the minimum period required to perform their role. In line with the Standard Contractual Clauses and this DPA, the data importer maintains written contracts with all sub-processors governing the use and processing of Personal Data and that provide protections equal to those set out in the Standard Contractual Clauses and this DPA. Data importer remains responsible and liable for data processing by all sub-processors.

For more information on transfers to specific Sub-Processors, please refer to Annex III, below.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Dialpad incorporates the following technical and organizational measures:

1. **Access Management**
    a. Data processing systems are inaccessible without prior authorization.
        i. For Dialpad personnel, Single Sign On (SSO) and Multifactor Authentication (MFA) are required for all systems containing Personal Data.
        ii. Customers are able to access their account, including Personal Data, using either a Single-Sign On System, or a unique username and password combination.
        iii. All personnel access Dialpad's systems with a unique identifier (user ID), which is tied back to the user's Dialpad email address.
        iv. Customer data is separated from other customers to prevent unauthorized disclosure.
    b. Access to data is limited based on separation of duties, multiple authorization levels, and least privilege.
        i. Access is reviewed regularly and modified or revoked if not required.
        ii. Dialpad has procedures in place so that requested authorization changes are implemented only in accordance with the Information Security Policy. In case personnel leave the company, their access rights are revoked.
    c. Password Management
        i. Dialpad's Access Management Policy governs password policies
    d. Network Security
        i. Dialpad will maintain a network security program to meet best practices on physical and virtual networks.
    e. Logging
        i. Dialpad will maintain logs of critical infrastructure and systems that affect Dialpad's services and customer data. Logging shall be in place to monitor security, confidentiality and availability of Dialpad's products and services.
    f. Physical Access
        i. Unauthorized persons are prevented from gaining physical access to premises, buildings, or devices where data processing occurs or from where data may be accessed. Dialpad's physical access controls are detailed in its Information Security Policy.
        ii. Offices have entry protocols that are assigned to individuals. Key cards are assigned and used by one individual at a time.
        iii. Guests entering Dialpad offices are registered and checked in. All guests are required to sign confidentiality agreements prior to accessing sensitive areas.
        iv. Dialpad devices must be stored and used in secure environments to prevent loss, theft, and compromise.
    g. Infrastructure providers that are used to store customer data and provide capabilities to serve Dialpad products are SOC2 Type II or ISO 27001 certified environments.
        i. Hosting providers are reviewed by the Security and Compliance team prior to data and infrastructure being stored in such environments
        ii. Physical security is reviewed on an annual basis to ensure compliance is kept up to date.
2. **Data Processing Control**
    a. Data Categorization
        i. Data is classified into different components based on their sensitivity in order to determine the requirements associated with their processing.
        ii. Personal Data within any data classification is handled as sensitive and confidential.
    b. Processing Responsibilities
        i. Customer Data may only be used for what is necessary to deliver the Services. Consistent with Dialpad's Privacy Policy, all other uses should require pseudonymization of the Customer Data.
        ii. Prior to processing data within Dialpad, the basis for obtaining and using Personal Data must be determined based on an appropriate method as provided in Applicable Data Protection Laws. Appropriate methods to obtain and use data from a data subject include:
            1. Consent: an individual has given explicit consent to Dialpad to process their Personal Data for a specific purpose.
            2. Contract: data processing is necessary for a contract we have with the individual, or because

they have asked Dialpad to take specific steps before entering into a contract.

3. Legitimate Interest: the processing is necessary for Dialpad's legitimate interests or the legitimate interest of a third party unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests.
4. Legal Obligation: the processing is necessary for Dialpad to comply with the law (not including contractual obligations).
5. Vital Interest: the processing is necessary to protect someone's life.
6. Public Task: the processing is necessary for Dialpad to perform a task in the public interest or for Dialpad's official functions, and the task or function has a clear basis in law.

iii. A data privacy impact assessment is performed at a minimum on an annual basis or during a significant product change as determined by the DPO.

iv. Customer Data should be disposed of based on contractual requirements and terms of service agreements. Disposal can include permanent deletion of data, return of such data, or pseudonymization.

c. Data Distribution Requirements

i. Any disclosure of Dialpad non-public data requires a Non-Disclosure Agreement.

ii. Prior to any transfer or processing of non-general/public data outside of Dialpad's personnel or wholly-owned systems, a risk determination should be performed.

iii. Any breach of non-general/public information outside of authorized distribution should be reported to the Dialpad Security Team immediately upon discovery or suspicion of a data security breach.. Upon confirmation of a data security breach, remediation steps should be implemented based on Dialpad's Incident Response and Breach Notification Policy.

3. Data Availability

a. Dialpad maintains a current Disaster Recovery Plan and Incident Management Policy.

b. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) projections are tested and validated by Dialpad.

4. Data Integrity

a. Risk Assessment

i. Information risk assessments are performed against an industry-acceptable standard to determine areas of vulnerability within the organization. The control framework should be updated on a regular basis to include changes in the areas required to be covered.

ii. The information risk assessment must classify risk levels assigned to identified risks based on likelihood and impact and prioritize remediation according to the risk levels. Any Service Level Agreements committed by Dialpad for risks identified should be taken into account when planning remediation.

iii. Remediation should be coordinated with the Security and Compliance department, and the department responsible for the control areas, as well as systems, that are in scope of the identified risk.

b. Security Awareness

i. All personnel must complete security awareness training upon onboarding to Dialpad, as well as on an annual basis.

ii. The security awareness training is updated, at a minimum on an annual basis to ensure that any process and technology changes within the organization.

c. Data Protection and Encryption

i. Data is encrypted in transit and at rest based on the risk and classification of the data, using the algorithms that have received substantial public review and have been proven to work effectively.

ii. Cryptographic keys are generated and stored in a secure manner that prevents loss, theft, or compromise.

iii. Sensitive data is backed up to environments that are not the primary source of use. Backup frequency is determined based on data criticality.

iv. All customer data that is used to serve Dialpad products is backed up daily

v. Testing of customer data backups is done to meet an agreed upon Recovery Time Objective (RTO) s and Recovery Point Objective (RPO).

5. External Certification

a. Dialpad undergoes annual independent third party audit(s) to verify the operating effectiveness and design of its controls.

b. Third party audit reports should be available for review by customers with non-disclosure agreements.

Please also refer to Dialpad's Trust Page at www.dialpad.com/trust.

ANNEX III - CROSS BORDER TRANSFERS

Data transfers

1. To perform the contract and provide the requested Services, the parties anticipate that Dialpad (and its sub-Processors) may be required to conduct cross border data transfers, for example, outside of the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom.
2. The transfer of Personal Data will be subject to the applicable Standard Contractual Clauses as set forth in Section 3 (UK SCCs) or Section 4 (EU SCCs) of this Annex.
3. UK SCCs. The parties agree that the UK Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the UK Standard Contractual Clauses, the UK Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:
    a. The UK Controller to Processor SCCs will apply where Dialpad is processing Customer Data for the sole purpose of providing the Services pursuant to the Agreement. The optional indemnification clause will not apply. Annex I (Details of Processing) serves as Appendix I of the UK Controller to Processor SCCs. Annex 2 (Technical and Organizational Security Measures) of this DPA serves as Appendix II of the UK Controller to Processor SCCs.
    b. The UK Controller to Controller SCCs will apply where Dialpad is processing Customer Data for the purposes of Vi Training and improvement of the Services. In Clause II(h) of the UK Controller to Controller SCCs, Dialpad will process Personal Data in accordance with the data processing principles set forth in Annex A of the UK Controller to Controller SCCs. The optional commercial clause will not apply. Annex I (Details of Processing) serves as Annex B of the UK Controller to Controller SCCs. Personal Data transferred under these clauses may only be disclosed to the following categories of recipients: (i) Dialpad's employees, agents, affiliates, advisors, and independent contractors with a reasonable business purpose for processing such Personal Data; (ii) Dialpad vendors that, in their performance of their obligations to Dialpad, must process such Personal Data acting on behalf of and according to instructions from Dialpad; and (iii) any person (natural or legal) or organization to whom Dialpad may be required by applicable law or regulation to disclose Personal Data, including law enforcement authorities and central and local government authorities.
4. EU SCCs. The parties agree that the 2021 Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the EU SCCs, the applicable EU SCCs will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:
    a. Module One (Controller to Controller) of the EU SCCs will apply where Dialpad is processing Customer Data for the purposes of Vi Training and improvement of the Services.
    b. Module Two (Controller to Processor) of the EU SCCs will apply where Customer is a controller of Customer Content and Dialpad is processing Customer Data for the sole purpose of providing the Services pursuant to the Agreement.
5. The following terms shall apply to the SCCs:
    a. Dialpad may appoint sub-Processors as set out in, and subject to the requirements of, Section 7 of this DPA, and Customer may exercise its right to object to sub-Processors under the SCCs in the manner set out in Section 7.c of this DPA; and
    b. in the event that any provision of this DPA contradicts, directly or indirectly, the SCCs, the SCCs shall prevail.
6. In respect of Restricted Transfers made to Dialpad under Section 7, Dialpad shall not participate in (nor permit any sub-Processor to participate in) any further Restricted Transfers of Personal Data (whether as an "exporter" or an "importer" of the Personal Data) unless such further Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to SCCs implemented between the exporter and importer of the Personal Data.
7. In the event Customer seeks to conduct any assessment of the adequacy of the SCCs for transfers to any particular countries or regions, Dialpad shall, to the extent it is able, provide reasonable assistance to Customer for the purpose of any such assessment, provided Customer shall cover all costs incurred by Dialpad in connection with its provision of such assistance.
8. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this Addendum, including Annex 4 (Jurisdiction Specific Terms) of this Addendum, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

ANNEX IV - JURISDICTION SPECIFIC TERMS

1. Australia:
    a. The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).
    b. The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.
    c. The definition of “Sensitive Data” includes “Sensitive Information” as defined under Applicable Data Protection Law.
2. Brazil:
    a. The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (LGPD).
    b. The definition of “Security Incident” includes a security incident that may result in any relevant risk or damage to data subjects.
    c. The definition of “processor” includes “operator” as defined under Applicable Data Protection Law.
3. California:
    a. The definition of “Applicable Data Protection Law” includes the California Consumer Privacy Act (CCPA).
    b. The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law and, for clarity, includes any Personal Information contained within Customer Account Data, Customer Content, and Customer Usage Data.
    c. The definition of “data subject” includes “Consumer” as defined under Applicable Data Protection Law. Any data subject rights, as described in Section 8 (Data Subject Rights) of this Addendum, apply to Consumer rights. In regards to data subject requests, Dialpad can only verify a request from Customer and not from Customer’s end user or any third party.
    d. The definition of “controller” includes “Business” as defined under Applicable Data Protection Law.
    e. The definition of “processor” includes “Service Provider” as defined under Applicable Data Protection Law.
    f. Dialpad will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Dialpad agrees not to (a) sell (as defined by the CCPA) Customer’s Personal Data or Customer end users’ Personal Data; (b) retain, use, or disclose Customer’s Personal Data for any commercial purpose (as defined by the CCPA) other than providing the Services; or (c) retain, use, or disclose Customer’s Personal Data outside of the scope of the Agreement. Dialpad understands its obligations under the Applicable Data Protection Law and will comply with them.
    g. Dialpad certifies that its Sub-processors, as described in Section 7 (Sub-processors) of this Addendum, are Service Providers under Applicable Data Protection Law, with whom Dialpad has entered into a written contract that includes terms substantially similar to this Addendum. Dialpad conducts appropriate due diligence on its Sub-processors.
    h. Dialpad will implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Data it processes as set forth in Annex II to this DPA.
4. Canada:
    a. The definition of “Applicable Data Protection Law” includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
    b. Dialpad’s Sub-processors, as described in Section 7 (Sub-processors) of this Addendum, are third parties under Applicable Data Protection Law, with whom Dialpad has entered into a written contract that includes terms substantially similar to this Addendum. Dialpad has conducted appropriate due diligence on its Sub-processors.
    c. Dialpad will implement technical and organizational measures as set forth in Annex II to this Addendum.
5. European Economic Area (EEA):
    a. The definition of “Applicable Data Protection Law” includes the General Data Protection Regulation (EU 2016/679) (“*GDPR*”).
    b. When Dialpad engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:
        i. require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

ii. require any appointed sub-processor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

c. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

d. Customer acknowledges that Dialpad, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Dialpad to notify impacted data subjects with whom Dialpad does not have a direct relationship (e.g., Customer's end users), Dialpad will notify Customer of this requirement. Customer will provide reasonable assistance to Dialpad to notify the impacted data subjects.

e. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

i. Module Two will apply where Customer (or the relevant member of the Customer Group) is a Controller and Module Three will apply where Customer (or the relevant member of the Customer Group) is a Processor, and the provisions relating only to Modules 1 and 4 are deleted and shall not apply to such ex-EEA Transfer;

ii. All footnotes and explanatory notes in the EU SCCs are deleted.

iii. in Clause 7, the optional docking clause will apply;

iv. in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in Clause 4.3 of this DPA;

v. in Clause 11, the optional language will not apply;

vi. in Clause 17, Option 2 will apply, and the law of Belgium shall apply;

vii. in Clause 18(b), disputes shall be resolved before the courts of Belgium. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;

viii. Annexes I, II, and III of the EU SCCs shall be completed with the information set out in Annexes I and II of this Addendum, respectively.

6. Japan:

a. The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).

b. The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.

c. The definition of "controller" includes "Business Operator" as defined under Applicable Data Protection Law. As a Business Operator, Dialpad is responsible for the handling of Personal Data in its possession.

d. The definition of "processor" includes a business operator entrusted by the Business Operator with the handling of Personal Data in whole or in part (also a "trustee"), as described under Applicable Data Protection Law. As a trustee, Dialpad will ensure that the use of the entrusted Personal Data is securely controlled.

7. Singapore:

a. The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).

b. Dialpad will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Annex II to this Addendum and complying with the terms of the Agreement.

8. Switzerland

a. The definition of "Applicable Data Protection Law" includes the Swiss Federal Act on Data Protection.

b. When Dialpad engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

i. require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

ii. require any appointed sub-processor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

c. in relation to Personal Data that is protected by the Swiss Federal Act on Data Protection (as amended or replaced), the EU SCCs, completed as set out about in clause 6.2(a) of this DPA, shall apply to transfers of such Personal Data, except that:

i. the competent supervisory authority in respect of such Personal Data shall be the Swiss Federal Data Protection and Information Commissioner;

ii. in Clause 17, the governing law shall be the laws of Switzerland;

iii. references to "Member State(s)" in the EU SCCs shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland; and

iv. references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the SCCs shall be understood to be references to the Swiss Federal Act on Data Protection (as amended or replaced).

9. United Kingdom (UK)

a. References in this Addendum to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

b. When Dialpad engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

i. require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

ii. require any appointed sub-processor to (i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

c. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

d. Customer acknowledges that Dialpad, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Dialpad to notify impacted data subjects with whom Dialpad does not have a direct relationship (e.g., Customer's end users), Dialpad will notify Customer of this requirement. Customer will provide reasonable assistance to Dialpad to notify the impacted data subjects.

e. in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

i. The ex-UK Transfer shall be governed by the UK SCCs which are hereby incorporated into this Addendum with the following amendments (with references in this Clause 6(b) to Clauses being to Clauses of the UK SCCs):

1. all references to "Member State" or "State" means "Member State or territory";

2. for the purposes of clause II(h) of the Clauses, Service Provider hereby selects option (iii) and agrees to be governed by and comply with the data processing principles set out in Annex A to the UK SCCs;

3. Clause IV (Governing Law) shall read "The Clauses shall be governed by the law of England and Wales";

4. all references to "Annex B" is the Description of Transfer in Annex I;

5. Appendices 1 and 2 of the UK SCCs shall be completed with the information set out in Annexes I and II of this Addendum, respectively.

ii. If any of the UK SCCs are replaced or superseded by new standard data protection clauses pursuant to Article 46 of the UK GDPR and related provisions of the Data Protection Act 2018 (**"New UK SCCs"**), then Customer may give notice to Service Provider and, with effect from the date set out in such notice, amend the application of paragraph 1 to one or more ex-UK Transfers so that:

1. the UK SCCs cease to apply to those ex-UK Transfers as further specified in such notice;
2. those of the New UK SCCs as are specified in such notice shall apply in respect of such ex-UK Transfers in substitution for the UK SCCs; and
3. such consequential amendments as the parties reasonably consider necessary are made to this Addendum to ensure that it remains compliant with the provisions of UK Data Protection Law.